Criptografía en la administración pública: una perspectiva integral

Pino Caballero-Gil[1]
Catedrática de Ciencias de la Computación e Inteligencia Artificial
Universidad de La Laguna
pcaballe@ull.edu.es

RESUMEN: Este artículo aborda la importancia de la seguridad de la información en la administración pública, destacando el papel de la criptografía para garantizar propiedades como la integridad y confidencialidad de los datos. Se describen en detalle las infraestructuras de clave pública, y se analizan el DNIe y el sistema Cl@ve como ejemplos de identificación electrónica segura, con múltiples aplicaciones en la administración pública. Además, se presta atención a las estrategias desarrolladas por diversas administraciones públicas internacionales para implementar sistemas criptográficos resistentes a la amenaza emergente de la computación cuántica. Por otra parte, en un contexto actual, se enumeran algunas aplicaciones de tecnologías *blockchain*. En resumen, este trabajo proporciona una visión de algunos desafíos de ciberseguridad en la administración pública y varios avances basados en criptografía, subrayando la importancia de adaptarse constantemente a las ciberamenazas y oportunidades tecnológicas en evolución.

Palabras clave: Seguridad de la información, criptografía, identificación electrónica, computación cuántica, tecnologías ***blockchain***.

ABSTRACT: This paper addresses the importance of information security in public administration, highlighting the role of cryptography to guarantee properties such as data integrity and confidentiality. It describes in detail public key infrastructures and provides an analysis of the DNIe and the Cl@ve system as examples of secure electronic identification, with multiple applications in public administration. Furthermore, it pays attention to the strategies developed by various international public administrations to implement cryptographic systems resistant to the emerging threat of quantum computing. On the other hand, in the current context, some applications of blockchain technologies are listed. In summary, this work provides an overview of some cybersecurity challenges in public administration and various cryptography-

[1] ORCID: 0000-0002-0859-5876. El presente estudio ha sido realizado en el seno de la Cátedra Binter de Ciberseguridad de la ULL.

based advances, highlighting the importance of continuously adapting to evolving cyber threats and technological opportunities.

Keywords: Information security, cryptography, electronic identification, quantum computing, blockchain technologies.

1. INTRODUCCIÓN

El imparable y creciente uso de las Tecnologías de la Información y la Comunicación (TIC) ha estado revolucionando los servicios gubernamentales en los últimos años. El objetivo principal de dicho cambio ha sido aprovechar la era de la sociedad de la información para mejorar la calidad de vida de la ciudadanía, reforzando la cohesión social y garantizando que las administraciones públicas sean eficientes en el actual contexto electrónico, mediante la oferta de mayores oportunidades de participación. Así, el concepto conocido como gobierno electrónico o e-gobierno se utiliza para referirse al uso de las TIC en la administración pública con objeto de facilitar el acceso a la información y servicios gubernamentales a la ciudadanía (Silcock, 2001).

En un mundo donde el poder reside en la información, su protección se convierte en una necesidad crítica para los gobiernos de todo el mundo. Por ello, en el actual y cambiante panorama digital, subestimar la importancia de posibles ciberataques contra la administración pública no es recomendable (Szczepaniuk, Szczepaniuk, Rokicki y Klepacki, 2020). De hecho, cuestiones como el correcto funcionamiento de la administración electrónica y la protección de los datos sensibles dependen en gran medida de la implementación de sólidas prácticas de ciberseguridad (Moynihan, 2004).

Por otra parte, dado que una de las características más importantes de cualquier transacción organizacional es la confianza (Raab, 1998), especialmente en Internet, donde no hay contacto directo entre las partes que intercambian información, se hace imprescindible adoptar medidas proactivas de seguridad que permitan validar a la organización, usuarios, etc., antes de cualquier intercambio de datos y servicios. De hecho, un alto nivel de confianza entre todos los usuarios (ciudadanos, empresas y gobierno) es una condición necesaria como base para el lanzamiento exitoso de una iniciativa de gobierno electrónico.

Tomando como referencia experiencias no solo en España sino también a nivel internacional, y especialmente en Europa y Estados Unidos, se hace evidente que la protección de la información en las entidades gubernamentales es una preocupación global (Kovács, 2018). En España, al igual que en muchos

países europeos, la digitalización de los servicios gubernamentales ha ganado importancia a lo largo de los últimos años (Gennai, Martusciello y Buzzi, 2005). Esta transformación ha llevado a una mayor dependencia de los sistemas electrónicos para la comunicación, el almacenamiento de datos y la prestación de servicios. Con dicho cambio digital, la necesidad de medidas rigurosas de seguridad de la información se ha vuelto incrementada hasta convertirse en un requerimiento primordial.

En cuanto a legislación, a nivel europeo, la Unión Europea (UE) en 2013 aprobó la Estrategia de Ciberseguridad, con el objetivo de reducir la exposición y vulnerabilidad de la economía europea y aumentar la competitividad de la UE (EUR-Lex, 2013). Su primer pilar se centra en la Agenda Digital para Europa, cuyo objetivo clave es crear un mercado digital unificado para los estados miembros de la UE, basándose en beneficios económicos y sociales sostenibles para todos los ciudadanos europeos. Para lograr una mayor concienciación sobre ciberseguridad, en dicha Estrategia, la Comisión Europea solicitó a los países miembros que establecieran una formación básica en ciberseguridad para el personal de la administración pública. Esta Estrategia se complementa con la "Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión" conocida como Directiva NIS (EUR-Lex, 2016a). Según dicha directiva, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) debe prestar asistencia a los Estados miembros ofreciéndoles su experiencia, conocimientos y asesoramiento y facilitando el intercambio de buenas prácticas.

También a nivel nacional, en los últimos años, el gobierno español ha puesto en marcha diversas iniciativas relacionadas con la ciberseguridad y el e-gobierno:

- La Ley de Seguridad Nacional (Gobierno de España, 2015) considera el ciberespacio como un ámbito de especial interés de la seguridad nacional, que requiere una atención específica por resultar un elemento básico para preservar los derechos y libertades y el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales.
- Enmarcado dentro de la iniciativa internacional *Open Government Partnership* (Open Government Partnership, 2017) diseñada promover la transparencia, la participación ciudadana y la rendición de cuentas en los gobiernos de todo el mundo, el III Plan de Acción de España 2017-2019 (Gobierno de España, 2018) prevé el establecimiento de un gobierno abierto en España.
- Como parte del desarrollo de la Estrategia de Seguridad Nacional (Gobierno de España, 2017) fue aprobada la Estrategia Nacional de Ciberseguridad (Gobierno de España, 2019), con medidas para promover la ciberseguridad. Además, en 2022 fue aprobado el Plan Nacional de Ci-

berseguridad con el objetivo de concretar dicha Estrategia Nacional a través de actuaciones y proyectos específicos, siendo hasta el momento la iniciativa estatal más ambiciosa llevada a cabo en el ámbito de la ciberseguridad.

- El Esquema Nacional de Seguridad (ENS) (Gobierno de España, 2022) es un marco regulatorio que establece las pautas y requisitos para proteger la información y los sistemas utilizados por el gobierno y otras entidades que prestan servicios esenciales. En este sentido, el Centro Criptológico Nacional (CCN), del Centro Nacional de Inteligencia (CNI) adscrito al Ministerio de Defensa, es la entidad responsable de articular la respuesta a los incidentes de seguridad de entidades del sector público, mientras que con respecto a las entidades del sector privado, la respuesta ante incidentes de seguridad debe ser notificada al Instituto Nacional de Ciberseguridad de España (INCIBE).
- El INCIBE fue designado en 2022 como Centro de Coordinación Nacional del Centro Europeo de Competencia en Ciberseguridad con objeto de que dicha entidad actúe como punto de contacto en España y coopere con el resto de agentes competentes, la industria, el sector público, la comunidad académica de investigación y los ciudadanos.

A nivel práctico, dentro de la administración pública en España, merece la pena mencionar algunos ejemplos de soluciones habituales a problemas de ciberseguridad. Entre ellas destacan las omnipresentes infraestructuras de clave pública (PKI, *Public Key Infrastructure*), que desempeñan un papel esencial al proporcionar un marco sólido para la seguridad de la información y la autenticación en línea, permitiendo a las entidades gubernamentales garantizar la integridad y confidencialidad de los datos, así como verificar la identidad de las partes involucradas en las transacciones electrónicas (Vatra, 2010). Entre los retos subyacentes a las PKI está la gestión eficiente de certificados digitales, la interoperabilidad con sistemas existentes y la garantía de la seguridad en cada etapa del ciclo de vida de los certificados digitales (Prandini, 1999).

El Documento Nacional de Identidad Electrónico (DNIe) y el sistema Cl@ve son otros dos buenos ejemplos de soluciones prácticas de ciberseguridad implementados en España, en ambos casos como sistemas de identificación electrónica segura con múltiples aplicaciones en el sector público (León-Coca, Reina, Toral, Barrero y Bessis, 2013).

En Estados Unidos, como líder mundial en tecnología e innovación, su gobierno ha sido el primero que públicamente se está enfrentando al desafío que supone la amenaza del surgimiento de la computación cuántica, pues recientemente se ha publicado una legislación estatal que exige poner en marcha un enfoque proactivo en materia de ciberseguridad dentro de todas las agencias gubernamentales (Congress, 2022).

Con una fuerte componente criptográfica, la tecnología *blockchain* ofrece toda una variedad de aplicaciones que tienen una gran utilidad en la administración pública, para mejorar la transparencia y la trazabilidad de diversas transacciones y contratos gubernamentales (Rot, Sobińska, Hernes y Franczyk, 2020).

El presente artículo ofrece una perspectiva sobre esos y otros desafíos en el campo crítico de la seguridad de la información y de las soluciones basadas en criptografía que se están aplicando actualmente en el ámbito de la administración pública.

2. CRIPTOGRAFÍA EN LA ADMINISTRACIÓN PÚBLICA

El término criptografía se utiliza para referirse al estudio y la aplicación de diversas técnicas y algoritmos que permiten proteger la comunicación y la información mediante el uso de cifrados. Los cifrados son transformaciones de la información de manera que solo las partes autorizadas puedan recuperar la información original (Caballero, 2002). De hecho, las técnicas criptográficas son las herramientas más poderosas para salvaguardar los datos contra accesos y modificaciones no autorizadas, garantizando propiedades como la confidencialidad, integridad y autenticidad de la información que contienen. Entre las principales características de seguridad de la información destacan las siguientes:

- Confidencialidad: Consiste en que el carácter secreto de un mensaje quede protegido de forma que solo sea comprensible para los usuarios autorizados. Normalmente se logra mediante la aplicación de un cifrado tal que solo el receptor legítimo que tiene la clave de descifrado puede acceder a la información que contiene el mensaje.
- Integridad: Se basa en aportar alguna evidencia de que un mensaje no ha sido modificado. Habitualmente se obtiene con la ayuda de una función *hash* o una firma digital, pues las funciones *hash* condensan el contenido del mensaje en una secuencia, y la verificación de una firma digital permite confirmar que el mensaje no ha sido cambiado tras de la firma.
- Autenticidad: Consiste en la confirmación de la identidad de un usuario. Usualmente se protege esta característica o bien mediante una firma digital en el caso de un mensaje enviado por el usuario, o bien mediante un esquema de identificación en el caso de un control de acceso a un sistema.
- No repudio: Se basa en garantizar que un usuario no puede negar haber enviado o recibido un mensaje, o en general realizado una acción concreta.
- Privacidad: Consiste en garantizar la capacidad de un individuo o entidad para controlar el acceso, uso y divulgación de su información personal, así como la capacidad de mantener ciertas áreas de su vida o actividades fuera del alcance de otros.

Dado que en la administración pública normalmente hay que manejar grandes cantidades de datos personales e información confidencial, garantizar la ciberseguridad en general y la privacidad en particular es de suma importancia. De hecho, el artículo 32 del Reglamento General de Protección de Datos (RGPD) (EUR-Lex, 2016b) impone a los responsables de un tratamiento de datos personales la obligación de determinar y establecer las medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo.

El presente trabajo tiene como objetivo explorar el estado actual de la investigación y uso de criptografía para proteger la ciberseguridad de los datos en la administración pública. Durante su preparación se ha prestado especial atención tanto a numerosos artículos científicos publicados en los últimos años sobre el uso de técnicas criptográficas para la protección de los datos en entornos administrativos, como a diversas prácticas habituales e iniciativas nacionales e internacionales en la materia.

Los algoritmos y protocolos criptográficos se caracterizan por estar diseñados para abordar diferentes aspectos de la seguridad de la información y la comunicación. Así, en los cifrados de clave secreta se utiliza una única clave para cifrar y descifrar la información, y tanto el remitente como el destinatario deben conocer esta clave secreta. Por el contrario, en los cifrados de clave pública se utilizan dos claves: una clave pública y una clave privada, de manera que la clave pública se utiliza para cifrar la información, mientras que la clave privada se utiliza para descifrarla. Esto permite a cualquier persona cifrar un mensaje para el propietario de la clave privada, pero solo el propietario puede descifrarlo. Por otra parte, los protocolos de establecimiento de clave secreta compartida se utilizan para que dos partes puedan acordar de manera segura una clave secreta que luego utilizarán para cifrar y descifrar la comunicación. Otro algoritmo criptográfico de enorme utilidad es la firma digital, que permite proteger la autenticidad e integridad de un mensaje o documento digital. Esto se logra aplicando un cifrado de clave pública de manera que se utiliza la clave privada para crear la firma digital, que luego puede ser verificada por otros utilizando la correspondiente clave pública.

Los algoritmos y protocolos criptográficos más utilizados actualmente se basan en algunos problemas matemáticos difíciles de resolver. La factorización de enteros es uno de esos problemas, pues factorizar grandes números compuestos en sus factores primos es un problema difícil. Concretamente, si un número grande, de b bits es el producto de dos primos de aproximadamente el mismo tamaño, no existe algoritmo conocido capaz de factorizarlo en tiempo polinómico. Esto significa que ningún algoritmo conocido puede factorizarlo en tiempo $O(bk)$, para cualquier constante k. Otro problema matemático omnipresente en criptografía es el problema del logaritmo discreto, que es el análogo en grupos finitos del problema del logaritmo ordinario. Si bien calcular la operación inversa, conocida como exponenciación discreta, resulta una tarea computacional-

mente sencilla, calcular el logaritmo discreto en muchos grupos no es una tarea fácil. De hecho, este problema se considera irresoluble en un tiempo razonable cuando se utiliza aritmética modular. Una variante del problema del logaritmo discreto, definida sobre curvas elípticas, presenta numerosas ventajas para su uso en criptografía ya que permite implementar algoritmos criptográficos con claves más cortas, lo que reduce la cantidad de datos a procesar y acelera las operaciones criptográficas. Además, el problema del logaritmo discreto en una curva elíptica es considerado un problema intratable si la curva elíptica está bien seleccionada, lo que proporciona un alto nivel de seguridad y resistencia a los ataques para los algoritmos y protocolos criptográficos que se definan sobre él. En resumen, las matemáticas de las curvas elípticas ofrecen una combinación única de seguridad y eficiencia que ha conducido a que sean ampliamente utilizadas en criptografía moderna.

Entre los principales ejemplos actuales de algoritmos criptográficos usados en la administración pública destacan:

- el actual cifrado estándar, que es el cifrado de clave secreta AES (*Advanced Encryption Standard*) (Rijmen y Daemen, 2001);
- el cifrado de clave secreta ChaCha20 (Nir y Langley, 2018);
- el cifrado de clave pública RSA (Rivest, Shamir y Adleman, 1978), y
- la criptografía de curva elíptica (ECC, *Elliptic Curve Cryptography*) (Koblitz, Menezes y Vanstone, 2000), incluyendo las versiones elípticas
  - del algoritmo de establecimiento de clave secreta compartida de Diffie-Hellman (DH) (Diffie y Hellman, 1976), conocido como ECDH (*Elliptic Curve Diffie-Hellman*), y
  - del algoritmo de firma digital DSA (*Digital Signature Algorithm*), conocido como ECDSA (*Elliptic Curve Digital Signature Algorithm*).

Es habitual que los trabajos de investigación sobre estos algoritmos se centren en la evaluación de su fortaleza, eficiencia y resistencia frente a ataques conocidos, lo que permite identificar las técnicas criptográficas más adecuadas según el contexto administrativo en el que quieran aplicarse.

El presente artículo contiene una revisión de diversas técnicas criptográficas utilizadas en la práctica para mejorar la seguridad de los datos en la administración pública. Tecnologías como algoritmos criptográficos, mecanismos de gestión de claves, técnicas de protección de la privacidad de los datos, protocolos de autenticación de usuarios y aplicaciones de *blockchain* desempeñan un papel crucial en el fortalecimiento de la seguridad de los datos.

Una de las conclusiones claras es que la elección, implementación y despliegue de las herramientas criptográficas concretas más adecuadas debe tener en cuenta el entorno de la administración pública en el que se pretenden aplicar, con el objeto de abordar aspectos y retos específicos, y explorar las soluciones

criptográficas más adaptadas a los requisitos únicos de la administración pública.

Entre los aspectos más relevantes de la temática destaca sin duda el importante papel que juega la gestión de las claves criptográficas que se utilizan, incluyendo tanto la generación, como la distribución y el almacenamiento seguros. En ese sentido, la elección del primer tema a abordar en este trabajo fue clara, pues en la administración pública, las estructuras criptográficas más usadas son las infraestructuras de claves públicas o PKI, que hacen posible la implementación de cifrados y firmas digitales a través de la generación y el intercambio robusto de claves y certificados de claves. Además de su seguridad, dada la dimensión del conjunto de usuarios en entornos administrativos, son muy delicadas características como la eficiencia, escalabilidad y resiliencia de estos sistemas de gestión de claves cuando se usan en dichos entornos. Esto es así porque las operaciones criptográficas pueden introducir una sobrecarga de procesamiento adicional, con un potencial impacto en el rendimiento del sistema y el servicio a los usuarios. Por ello, las organizaciones necesitan evaluar cuidadosamente el impacto en el desempeño de técnicas criptográficas y optimizar su implementación para minimizar cualquier efecto negativo en la capacidad de respuesta y rendimiento del sistema.

Otras técnicas criptográficas que desempeñan un rol crucial en los sistemas administrativos son los mecanismos de autenticación de usuarios o identificación para el control de accesos. Diversos estudios se centran en el uso de algoritmos criptográficos, y esquemas biométricos para la identificación, con objeto de garantizar el acceso seguro a los recursos. Esas técnicas proporcionan mecanismos de autenticación fuerte, lo que garantiza que solo las personas autorizadas puedan acceder a datos confidenciales y realizar las tareas administrativas a las que tengan acceso legítimo.

En resumen, las personas que trabajan en el sector de la administración pública deberían tener la oportunidad de recibir capacitación formal sobre prácticas de ciberseguridad y conceptos básicos de criptografía para mejorar su nivel de conciencia y preparación para abordar posibles amenazas cibernéticas en su trabajo. Esta necesidad ha sido confirmada por la Comisión Europea en una de sus recientes iniciativas (EUR-Lex, 2013).

3. INFRAESTRUCTURA DE CLAVE PÚBLICA

Como se ha mencionado, al utilizar criptografía de clave pública, cada usuario debe poseer un par de claves, una clave privada y una clave pública. La clave privada, como su nombre indica, nunca se comparte y la utiliza únicamente su dueño. Por ejemplo, se puede utilizar para firmar documentos o para descifrar mensajes. Por otro lado, la clave pública está disponible de forma abierta y se utiliza, por ejemplo, para validar una firma digital o para cifrar mensajes. Uno

de los principales desafíos asociados al uso de criptografía de clave pública radica en asegurar que una clave pública pertenece realmente al usuario que afirma ser su propietario. La solución más común para abordar este problema se basa en el uso de certificados de clave pública, que son firmados digitalmente por una entidad de confianza para vincular la clave pública a su titular.

Se llama infraestructura de clave pública o PKI al conjunto de personas, procesos, políticas, protocolos, *hardware* y *software* que permite generar, gestionar, almacenar, implementar y revocar certificados de clave pública, que son necesarios para el uso de criptografía de clave pública. Así, las infraestructuras de clave pública constituyen el punto de partida necesario para la mayoría de los mecanismos de seguridad modernos usados en Internet, debido a que se basan en criptografía de clave pública.

Las PKI facilitan el almacenamiento e intercambio de datos electrónicos de forma segura, mediante el uso de criptografía de clave pública para la protección de diversas características de seguridad de la información, como confidencialidad, integridad, autenticidad o no repudio, por ejemplo.

Las características enumeradas forman parte de los requerimientos de las comunicaciones seguras en general, y en particular son requisitos de seguridad esenciales en muchos de los servicios ofertados por las administraciones públicas. De ahí que los servicios de seguridad ofrecidos por las PKI se pueden emplear para cumplir con la mayoría de los requisitos de seguridad identificados en las plataformas de gobierno electrónico (Lambrinoudakis, Gritzalis, Dridi y Pernul, 2003).

Concretamente, las infraestructuras de clave pública proporcionan la confianza necesaria para el uso de criptografía de clave pública mediante el uso de terceras partes de confianza (TTP, *Trusted Third Parties*), conocidas como autoridades de certificación (CA, *Certification Authorities*). Estas entidades firman digitalmente estructuras de datos llamadas certificados de clave pública, que garantizan que una clave pública específica pertenece a un determinado usuario. Por tanto, cada certificado digital conecta la clave certificada con el usuario que le corresponde.

El destinatario de un certificado de una clave pública siempre debe verificar la validez del certificado y la firma digital que contiene, antes de confiar en la clave pública que contiene. Si la misma CA emite los certificados de ambas partes comunicantes, es fácil verificar la firma del certificado de la otra parte comunicante, utilizando la clave pública de la CA de confianza. Sin embargo, para verificar la firma de un certificado emitido por otra CA se hace necesario que exista cierta relación de confianza entre las diferentes autoridades de certificación. Existen diferentes formas para establecer ese vínculo de confianza, denominados modelos de confianza. Estos modelos permiten a un usuario crear cadenas de certificados, llamadas cadenas de confianza, conectando los certificados firmados por su CA de confianza hasta los certificados firmados por las CA de otros usuarios.

El formato universalmente aceptado para definir un certificado digital de clave pública es X.509. Este formato surgió en 1988 y se encuentra descrito en el RFC 5280, actualizado por RFC 6818, RFC 8398 y RFC 8399. Este formato de certificado se utiliza en multitud de aplicaciones de seguridad, desde el protocolo usado en Internet para la navegación segura HTTPS llamado SSL/TLS, hasta otras aplicaciones como S/MIME, IPSec, etc. La estructura básica de un certificado digital estándar x.509 contiene los siguientes parámetros: versión, número de serie, algoritmo, nombre de la CA que lo firma, período de validez, nombre del dueño del certificado, clave pública, extensiones y firma digital generada por la CA.

Una PKI integra una o más autoridades de certificación, y varios elementos, como un depósito de certificados digitales, documentación que incluye la política de certificación y una o más declaraciones de prácticas de certificación, así como personal capacitado para desempeñar funciones confiables para operar y mantener el sistema. En general, una PKI de una organización típica abarca la emisión de certificados digitales a usuarios y servidores individuales, el *software* de inscripción de los usuarios finales, la integración con directorios de certificados, herramientas para gestionar, renovar y revocar certificados, y diversos servicios como el de soporte a usuarios (Menezes, van Oorschot y Vanstone, 2018).

Los principales componentes de una PKI son:

- Repositorio: donde se almacenan los certificados digitales en los que se confía.
- Autoridad de Registro (RA, *Registration Authority*): procesa las solicitudes de certificados digitales y valida dichas solicitudes y la identidad de los usuarios, antes de que se pueda proceder a la emisión de los certificados.
- Autoridad de Certificación CA: una vez notificada por la RA sobre el nivel de confianza que merece el solicitante de un certificado digital, la CA emite el certificado si dicho nivel es suficiente para la emisión. También se encarga de revocar aquellos certificados digitales que han perdido el nivel de confianza necesario.
- Autoridad de Sellado de Tiempo (TSA, *Time Stamp Authority*): da fe de la existencia de una determinada información en un momento concreto, lo que es fundamental cuando se usa firma electrónica.
- Autoridad de Validación (VA, *Validation Authority*): tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que hayan sido registrados por una RA y certificados por una CA.

En los últimos años se considera que la mejor tecnología para repositorios de certificados son los sistemas compatibles con el protocolo LDAP (*Lightweight Directory Access Protocol*), que es el estándar para acceder a sistemas de directorios.

La revocación de los certificados es uno de los problemas más difíciles relacionados con las PKI. En general, la validación de certificados puede basarse o bien

en CRL (*Certificate Revocation List*), que puede ser almacenada temporalmente para hacer consultas locales, o bien en OCSP (*Online Certificate Status Protocol*), que es un protocolo diseñado para la validación en tiempo real mediante el intercambio de mensajes por Internet. Por una parte, en el esquema basado en CRL, la CA periódicamente mediante la TSA registra la hora, firma y envía al repositorio una lista que contiene los números de serie de todos los certificados revocados, junto con la fecha y hora correspondientes. Esta solución es bastante simple y ofrece la ventaja de requerir un número mínimo de operaciones criptográficas para la verificación. Sin embargo, presenta dos inconvenientes significativos pues solo es posible verificar el estado de un certificado mediante el acceso a la lista completa y exhaustiva de todos los certificados revocados, y además, dado que la verificación se suele llevar a cabo fuera de línea, no hay garantía de actualización. Por otra parte, en un sistema basado en OCSP, la verificación del certificado se delega y no está garantizada directamente por la firma de la CA, así que su mayor inconveniente es que puede sufrir ataques a través de la red.

Así, para el despliegue de una PKI, como mínimo se hace necesario realizar las siguientes operaciones:

- Creación y configuración de una CA.
- Generación y firma de certificados digitales.
- Definición de la revocación de certificados basada en una CRL.
- Configuración y uso de un servidor OCSP.
- Aplicación de sellado de tiempo mediante una TSA.

Existen tres tipos básicos de arquitecturas de PKI según el número CA definidas:

- Una CA única es una CA que emite certificados para usuarios y sistemas, pero no para otras CA. Esta estructura es fácil de construir y mantener, pues todos los usuarios confían en ella, las cadenas de confianza contienen solo un certificado y existe solo una CRL.
- La PKI jerárquica es la arquitectura tradicional, en la que todos los usuarios confían en la misma CA raíz de primer nivel, y, salvo dicha CA raíz, el resto de CA son subordinadas pues tienen una CA superior que las valida.
- La PKI *mesh* es una alternativa a la PKI jerárquica, en la que múltiples CA autofirmadas proporcionan servicios de PKI de forma que se relacionan entre ellas mediante relaciones uno a uno no jerárquicas, y cada usuario confía en una única CA.

El funcionamiento de las CA y RA se rige por políticas como la política de certificación y la declaración de prácticas de certificación. La primera proporciona reglas para nombrar a los titulares de certificados, los algoritmos criptográficos que se utilizarán, la longitud mínima permitida de las claves de cifrado, etc. La segunda detalla cómo la CA implementará la política de certificación en sus procedimientos.

4. IDENTIFICACIÓN ELECTRÓNICA

La UE desde 2014 había establecido el Reglamento que define las normas para la identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado único europeo, conocido como sistema europeo de reconocimiento de identidades electrónicas (eIDAS, *electronic IDentification, Authentication and trust Services*) (Parlamento Europeo, 2014).

Existen tres formas principales de Identificación electrónica para realizar trámites electrónicos en la administración pública:

- los certificados electrónicos emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT),
- el DNI electrónico, y
- el sistema Cl@ve.

El certificado electrónico emitido por la FNMT puede obtenerse de tres formas: presencialmente, en una oficina de administración pública, o bien electrónicamente con vídeo identificación o con DNIe.

4.1. DNI electrónico

El DNI electrónico (DNIe) constituye desde 2015 el sistema de identificación obligatorio en España. Cumple el reglamento eIDAS, siendo España en el momento de su lanzamiento, uno de los seis únicos países que lo cumplían (Alemania, Italia, Estonia, Luxemburgo, Croacia y España).

El DNIe es un documento expedido por la Dirección General de la Policía (DGP) del Ministerio del Interior, que además de acreditar físicamente la identidad personal de su titular permite realizar gestiones telemáticas de manera segura con la administración pública, gracias a la posibilidad que da de:

- Acreditar electrónicamente y de manera inequívoca su identidad.
- Firmar digitalmente documentos electrónicos, dándoles una validez legal equivalente a la de la firma manuscrita.

El DNIe es una tarjeta inteligente (*smart card*) ya que incorpora un pequeño circuito integrado (*chip*). Dicho *chip* almacena los mismos datos que aparecen impresos en la tarjeta (datos personales, fotografía, firma digitalizada y huella dactilar digitalizada), junto con dos certificados digitales:

- Certificado de autenticación: Asegura electrónicamente la identidad del ciudadano al realizar una transacción en línea, mediante la clave privada usada en el proceso.
- Certificado de firma: Permite la firma de trámites o documentos, garantizando la identidad del firmante como poseedor de la clave privada que use para firmar.

La validez de los certificados contenidos en el *chip* del DNIe es de 24 meses. Su actualización exige la comparecencia personal del titular en una oficina de expedición para poder usar un punto de actualización del DNIe.

La DGP es el único organismo autorizado para actuar como CA de dichos certificados, firmándolos en su emisión. En la PKI asociada con el DNIe, con el propósito de separar la verificación de la validez de un certificado de los datos de identidad de su titular, las funciones de VA están asignadas a entidades distintas de la CA. Por tanto, la DGP, como CA, no tiene ningún acceso a los detalles de las transacciones realizadas con los certificados que emite, a la vez que las VA no tienen acceso a la identidad de los titulares de los certificados que validan. Existen dos proveedores de servicios de verificación que les permiten actuar como VA para el DNIe: la FNMT, para ciudadanos, empresas y Administraciones Públicas; y el Ministerio de Hacienda y Administraciones Públicas, para las Administraciones Públicas. En todo caso la validación del DNIe siempre se realiza en base al protocolo OCSP.

Para usar el DNIe, es necesario contar con algunos elementos de *hardware* y *software* que permitan acceder al *chip* de la tarjeta para poder utilizar los certificados que contiene, como un ordenador. Se puede acceder al DNIe con un lector de tarjetas inteligentes. Además, las dos últimas versiones del DNIe, 3.0 y 4.0, permiten la conexión inalámbrica a través de NFC. En este caso, para poder usarlo sin contacto, es necesario un dispositivo con NFC que cumpla con el estándar ISO 14443. En cuanto al *software*, el DNIe requiere la instalación de la última versión de un componente de *software* llamado módulo criptográfico: CSP (*Cryptographic Service Provider*) para el entorno Microsoft Windows, o PKCS#11 para entornos UNIX/Linux o MAC. Dichos módulos son descargables de la web https://www.dnielectronico.es. Por otra parte, la aplicación de firma electrónica diseñada para el DNIe, llamada AutoFirma, puede ser descargada desde la dirección https://firmaelectronica.gob.es.

La seguridad tanto del documento físico como de sus componentes electrónicos y del *software* asociado es mejorada en cada revisión. Antes de que se produzca la actualización del DNIe, los cambios se someten a un riguroso proceso de evaluación realizada por la FNMT, bajo solicitud de la DGP. Este proceso es llevado a cabo por un laboratorio acreditado y auditado. Dicha evaluación se realiza siguiendo la metodología *Common Criteria* (ISO/IEC 15408) (Real Casa de la Moneda, 2022). Concretamente, el *software* del DNIe ha sido certificado con el nivel de evaluación exigido, que es EAL4+ y EAL4 AVA_VAN.5, mientras que los *chips* utilizados han sido certificados como Dispositivos Seguros de Creación de Firma, en conformidad con los estándares europeos (Centro Criptológico Nacional, 2018). Sin embargo, a pesar de la tranquilidad que ofrecen estas certificaciones, a veces pueden pasar desapercibidos errores de diseño o de implementación en productos certificados que ya están en uso en dispositivos desplegados (Correa, 2022).

Entre los principales cambios criptográficos de la última versión del DNIe, 4.0, destacan los siguientes. Por una parte, el par de claves públicas vinculadas al certificado de autenticación incluido en el *chip* se utilizan para el protocolo de acuerdo de claves: DH según el RFC 2631, o ECDH según el ISO 11770-3. Por otra parte, la verificación de la firma digital se realiza de acuerdo con un algoritmo criptográfico específico: RSA o ECDSA, con tamaños de clave criptográfica de 3072-3840 bits (para RSA) o 256 bits, 384 bits, 512 bits y 521 bits (para ECDSA), en cumplimiento de los estándares actuales.

El protocolo PACE (*Password Authenticated Connection Establishment*), utilizado en el DNIe, fue diseñado para proteger los datos contenidos en los documentos de viaje electrónicos, con el fin de prevenir dos tipos de ataques:

- *Skimming*: ataque online que consiste en leer el *chip* sin acceso físico al documento y sin la aprobación del titular.
- *Eavesdropping*: ataque offline que comienza registrando los datos intercambiados entre el lector y el *chip*, para ser analizados posteriormente.

Los miembros de la UE deben implementar PACE en todos los pasaportes electrónicos. En el caso de España, también está implementado en el DNIe. En particular, en el DNIe 4.0 durante la ejecución del protocolo PACE se genera un valor secreto compartido con el terminal, que puede estar basado en ECDH. Luego, ese valor de secreto compartido se utiliza para derivar las claves de sesión AES para el cifrado y la autenticación de mensajes.

4.2. Sistema Cl@ve

Cl@ve es un sistema de identificación electrónica que complementa los sistemas de acceso mediante DNIe o certificado digital, para facilitar el acceso de los ciudadanos a los servicios ofrecidos por la administración pública en un entorno digital. Se basa en el uso de unas credenciales (usuario y contraseña) únicas, que evitan la necesidad de recordar claves diferentes para acceder a los diferentes servicios. El sistema Cl@ve ofrece también la posibilidad de realizar firmas electrónicas.

Para utilizar el sistema es necesario registrarse, ya sea de manera presencial en una de las oficinas de registro adheridas al sistema, o por Internet utilizando un certificado electrónico reconocido, como el del DNIe. Si no se dispone de certificado electrónico, es posible realizar el registro por videollamada o invitación por carta.

Tras el registro se pueden obtener dos tipos de credenciales de acceso:

- Cl@ve PIN: para accesos ocasionales, con una contraseña de corta validez.
- Cl@ve Permanente: para accesos o firmas digitales regulares, con una contraseña de larga validez. En este caso, el sistema se puede reforzar mediante claves de un solo uso enviadas por SMS.

Además, a través de la aplicación Cl@ve, se puede utilizar la opción Cl@ve Móvil, que permite identificarse sin necesidad de claves ni contraseñas, simplemente escaneando un código QR o confirmando una solicitud que llega al dispositivo móvil.

5. CRIPTOGRAFÍA RESISTENTE A LA COMPUTACIÓN CUÁNTICA

La administración pública lleva utilizando métodos de comunicación electrónica para la realización de numerosas gestiones diarias desde hace tiempo, de forma que los algoritmos criptográficos que utilizan para su protección tienen ya casi dos décadas. Dicha tecnología criptográfica ha sido considerada segura durante años, pero actualmente estamos siendo testigos de que la gestión de las transacciones sensibles que muchas veces conlleva la administración pública está cada vez más amenazada por el potencial despliegue de la computación cuántica. Por ese motivo, los principales gobiernos e instituciones admiten que en breve se requerirá un cambio total de tecnologías criptográficas para poder seguir protegiendo esas comunicaciones y datos frente a la amenaza cuántica.

Recientemente el presidente de los Estados Unidos decidió tomar medidas urgentes para fomentar la transición de la administración pública hacia criptografía resistente a la computación cuántica. Concretamente, Joe Biden firmó en diciembre de 2022 la Ley "*Quantum Computing Cybersecurity Preparedness Act*", que constituye una orden ejecutiva para establecer cuáles son las guías de transición para migrar a algoritmos de criptografía resistente a la computación cuántica para toda la administración pública, y presentar en un plazo máximo de 15 meses la estrategia nacional de ciberseguridad para la era postcuántica. La urgencia marcada en esa legislación conlleva la actualización de la infraestructura PKI actual utilizada en toda la administración pública estadounidense a una estructura resistente a la computación cuántica. Aunque la amenaza cuántica pueda parecer una amenaza del futuro, la amenaza ya puede considerarse actual porque existen evidencias de que se está llevando a cabo una recolección de comunicaciones cifradas y credenciales criptográficas con el claro objetivo de acceder a dicha información protegida una vez se disponga de un ordenador cuántico que permita romper los sistemas criptográficos usados. Si bien esa iniciativa legislativa solo afecta a Estados Unidos, parece evidente que eso mismo tendrá que hacerse en todas las naciones para evitar que la actual administración pública se pueda ver sometida a posibles ciberataques cuánticos futuros.

Como ya se explicó, las PKI constituyen la base criptográfica de los actuales esquemas de control de acceso y protección de la confidencialidad, integridad y autenticidad de la información que se gestiona dentro de la administración pública. El problema con los estándares criptográficos usados en las PKI actuales es que están seriamente amenazados por la previsible generación futura de ordenadores cuánticos.

Por una parte, el algoritmo cuántico de Grover, difundido en 1996, facilita llevar a cabo una búsqueda eficiente en una secuencia no ordenada de datos con *N* elementos en un tiempo *O(N1/2)*, mientras que el mismo problema con un ordenador clásico, la búsqueda se realizaría en un tiempo *O(N)*. En consecuencia, dicho algoritmo podría ser usado para acelerar los ataques por fuerza bruta contra esquemas criptográficos de clave secreta, como el actual cifrado estándar AES y las funciones *hash* usadas en firmas digitales. En este caso, para hacer dichos esquemas resistentes a la computación cuántica la solución pasa por aumentar el tamaño de las claves o la salida de las funciones *hash* al doble del tamaño actual.

Por otra parte, el algoritmo cuántico de Shor, publicado en 1994, permite factorizar un número *N* en tiempo *O((log N)3)* en un ordenador cuántico, lo que implica una sustancial mejora con respecto a la criba general del cuerpo de números (GNFS, *General Number Field Sieve*), que es el algoritmo clásico conocido más eficiente para factorizar enteros mayores de 100 dígitos con ordenadores clásicos. Así, dicho algoritmo supone la eventual desprotección de toda la criptografía de clave pública actualmente implementada en la administración pública, que está basada en RSA, DH o ECC.

Aunque la estimación del número de años necesarios para que dichos algoritmos cuánticos puedan ser ejecutados en la práctica contra los esquemas actuales sea pesimista, en cualquier caso dichos algoritmos suponen una importante reducción de tiempo en comparación con el tiempo que actualmente se requiere para romper los mencionados esquemas criptográficos, incluso con las supercomputadoras más potentes (Kaplan, Leurent, Leverrier y Naya-Plasencia, 2016).

Por tanto, para proteger el futuro de las PKI en la próxima era de la computación cuántica se hace necesario desarrollar e implementar ya métodos resistentes a ese tipo de computación pues se estima que la ruptura de los esquemas actuales presentes en las PKI usando el poder de la computación cuántica será factible en horas (Gidney y Ekerå, 2021).

En los últimos meses el Instituto Nacional de Estándares y Tecnología (NIST, *National Institute of Standards and Technology*) ha estado trabajando en el proceso de estandarización de criptografía postcuántica (*NIST Post-Quantum Cryptography Standarization)* para la elección de nuevos estándares algoritmos criptográficos basados en computación tradicional resistentes a la computación cuántica. Al final en 2022 han sido cuatro los algoritmos elegidos. Para el cifrado, se eligió a Crystals-Kyber como el algoritmo a utilizar como cifrado de clave pública, basado en una estructura matemática llamada retículo (*lattice*). Para firma digital, han sido tres los algoritmos elegidos: Crystals-Dilithium, Falcon y Sphincs+. De ellos, los dos primeros se basan también en retículos mientras que el último se basa en funciones *hash*. Afortunadamente, gracias al proceso público de selección de estándares que desde hace tiempo se lleva a cabo con los esquemas criptográficos, en cumplimiento del principio de Kerckhoffs todos

esos algoritmos son públicamente conocidos y están totalmente documentados, y disponibles en abierto para que todo el mundo los pueda implementar y analizar. De hecho, ya se sabe que una desventaja de estos algoritmos postcuánticos es que requieren claves más largas que los algoritmos actuales. Otra importante desventaja es que no tienen suficiente antigüedad como para poder considerarlos todavía seguros, pues los criptoanalistas apenas han tenido tiempo para intentar romperlos.

Idealmente, todos los gobiernos tendrían que iniciar ya la transición hacia implementaciones de los nuevos estándares postcuánticos en soluciones híbridas que integren criptografía pre-cuántica validada frente a ordenadores clásicos, con una capa adicional de criptografía resistente a la computación cuántica.

En la administración pública muchos servicios de gobierno electrónico se ofrecen por Internet, lo que implica una gran cantidad de requisitos relacionados con el nivel de seguridad exigido para dichos servicios. Por tanto, aparte de la mencionada propuesta de inminente transición a criptografía resistente a la computación cuántica llevada a cabo en la administración pública de Estados Unidos, merece la pena mencionar diversas iniciativas enfocadas a asegurar en general las comunicaciones por Internet en la era cuántica.

SSL/TLS es el protocolo criptográfico que se utiliza para la gran mayoría de transacciones seguras a través de Internet, tanto en general como en los sistemas de gobierno electrónico. Este protocolo usa criptografía de clave pública para autenticar a la contraparte con quien se esté comunicando, y para intercambiar la clave secreta que se usa para el cifrado de la comunicación. Concretamente en la última versión, TLS 1.3, se utilizan los algoritmos de clave secreta AES o ChaCha20 para el cifrado de la comunicación, y los algoritmos de clave pública DH, RSA, ECDH o ECDSA para el establecimiento de la clave secreta compartida. Esto quiere decir que, como ya se ha explicado, se hace necesario actualizar cuanto antes estos algoritmos para que la comunicación por Internet pueda considerarse segura en la era cuántica, lo que resulta fundamental en todos los servicios seguros que se ofrecen en el gobierno electrónico a través de Internet. De hecho, el algoritmo de cifrado Crystals-Kyber ya ha sido adoptado por Cloudflare, Amazon Web Services e IBM, y recientemente, en agosto de 2023 Google anunció que daría soporte para ese algoritmo de cifrado post-cuántico en su navegador Chrome. Concretamente implementará una solución híbrida que combina el algoritmo Crystals-Kyber con ECC para el establecimiento de claves secretas compartidas en TLS, brindando la flexibilidad para implementar y probar nuevos algoritmos resistentes a la cuántica al tiempo que garantizan que las conexiones sigan protegidas con un algoritmo seguro existente y bien conocido, como por ejemplo son los basados en ECC.

Dentro de la criptografía resistente a la computación cuántica, aparte de la mencionada postcuántica, que se basa en computación clásica; destaca la criptografía cuántica, que aplica principios de la mecánica cuántica. El objetivo principal de la criptografía cuántica es cifrar los mensajes de manera que

ningún destinatario externo pueda siquiera leerlos. De hecho, la comunicación cuántica debe considerarse más segura que cualquier sistema de transmisión de información existente. Se espera que para 2030 las comunicaciones cuánticas se extiendan a casi todos los países y se inicie lo que sería una era de Internet cuántica. En ese caso, todo tipo de comunicaciones (es decir, multimedia, texto, voz) se producirían mediante señales cuánticas en lugar de señales digitales tradicionales.

De especial interés para el objeto del presente artículo, sería lo que se ha dado en llamar la Internet cuántica. Esa Internet cuántica requeriría hacer uso de ordenadores cuánticos, pues de la misma manera en que tenemos *switches* en la Internet clásica como puntos intermedios para establecer las conexiones, en la Internet cuántica necesitaremos un tipo de conmutador que sea capaz de transmitir cúbits.

Aunque parezca lejana la disponibilidad de esos ordenadores cuánticos que faciliten la existencia de una Internet cuántica, merece mencionar que desde 2018, la Comisión Europea lanzó *Quantum Flagship*, una iniciativa de investigación a gran escala y a largo plazo para apoyar y fomentar la creación y el desarrollo de una industria europea competitiva de tecnologías cuánticas. así como la consolidación y ampliación del liderazgo y la excelencia en la investigación europea en tecnología cuántica.

6. APLICACIÓN DE TECNOLOGÍAS *BLOCKCHAIN*

La tecnología *blockchain* ha adquirido en los últimos años una importancia fundamental para los responsables de la toma de decisiones y el personal de ciertos sectores de la administración pública, ya que podría ayudarles a determinar si este enfoque puede ser de utilidad práctica en el cumplimiento de su misión. De hecho, las soluciones basadas en *blockchain* ya se han utilizado con éxito como base para diversas transacciones digitales en áreas como el mercado eléctrico, el comercio, las criptomonedas y la bolsa, entre otros. Además, su potencial de aplicación se ha explorado o se está explorando activamente en muchos otros sectores de la economía, como la banca o los seguros. En cualquier caso, existe cierto consenso general en que siempre es necesario llevar a cabo una evaluación de los posibles usos y condiciones para la aplicación efectiva de la tecnología *blockchain* antes de implementarla en cualquier ámbito. Esto es especialmente relevante en el sector de la administración pública, donde puede servir como plataforma para el seguimiento de impuestos y reembolsos, facturación electrónica, registros censales y registro de vehículos, entre otras aplicaciones.

Una *blockchain* o cadena de bloques consiste en un registro descentralizado conteniendo todas las operaciones o transacciones realizadas dentro de una red específica, de forma que los detalles quedan accesibles para todos los partici-

pantes. Cada operación se registra como un bloque separado y se agrega a la cadena. Por tanto, la cadena de bloques resultante contiene el historial de todas las transacciones, con sus correspondientes marcas de tiempo.

Gracias a su naturaleza descentralizada, los participantes pueden tanto acceder a los datos como agregar nuevos registros de operaciones, sujetos a verificación por otros participantes en la red. A diferencia de las soluciones tradicionales de bases de datos centralizadas, este sistema almacena datos en ubicaciones dispersas, lo que ofrece mejoras significativas en cuanto a la seguridad de los datos.

Por sus características intrínsecas, la tecnología *blockchain* representa una transformación radical de los métodos tradicionales de liquidación digital y registro de transacciones, con el beneficio adicional de reducir el riesgo de ataques maliciosos.

Es una solución digital que combina computación distribuida con criptografía de clave pública para crear un libro de contabilidad público descentralizado e inmutable en el que se pueden registrar una amplia variedad de datos, como títulos de propiedad, identidades y certificaciones, contratos, entre otros. Los servicios públicos desempeñan un papel especialmente importante y activo en la evolución y difusión de las soluciones *blockchain*, como se refleja en el número de implementaciones exitosas, proyectos en curso, pruebas y estudios analíticos relacionados con este aspecto particular del avance tecnológico. En el artículo (Ølnes, Ubacht y Janssen, 2017) se exponen los beneficios y las implicaciones del uso de *blockchain* en el gobierno electrónico. Además, existen otros artículos que abordan la aplicación de *blockchain* en el gobierno electrónico, aunque se centran principalmente en cuestiones del mercado local, como se puede ver en las referencias (Hou, 2017; Ojo y Adebayo, 2017; Weiss y Corsi, 2017). Asimismo, el artículo (Atzori, 2015) examina en qué medida la tecnología *blockchain* puede considerarse una herramienta política con capacidad para gestionar interacciones sociales a gran escala y desafiar a las autoridades centrales tradicionales.

Los organismos gubernamentales están liderando actualmente la adopción de la tecnología *blockchain* debido a su eficaz papel como solución para la gestión de bases de datos en la administración pública. Muchos países y regiones ya han implementado sistemas modernos que sustituyen los registros y libros de contabilidad tradicionales por aplicaciones *blockchain*, garantizando la seguridad en el almacenamiento de todo tipo de información, desde activos pecuniarios hasta registros de identidad personal. La información almacenada en sistemas basados en *blockchain* proviene de diversas fuentes y puede incluir datos altamente confidenciales a los que solo deben acceder o revelar individuos, instituciones u organizaciones gubernamentales independientes.

Una de las funciones clave de los organismos gubernamentales es registrar y almacenar datos confiables, como nacimientos, defunciones, cambios de estado civil, licencias comerciales, transferencias de derechos de propiedad y antece-

dentes penales. La gestión de estos registros puede ser complicada, ya que algunos de ellos aún se almacenan en papel, y cada modificación requiere una visita física a la oficina correspondiente. Además, muchas agencias gubernamentales tienden a mantener sus propios protocolos de datos y procedimientos de gestión de información, lo que dificulta la comparación de registros en un contexto más amplio.

Actualmente, existen numerosas herramientas y aplicaciones *blockchain* diseñadas para satisfacer las necesidades de los organismos gubernamentales, ofreciendo protección y simplificación en el manejo de registros críticos relacionados con la propiedad y la identidad. La tecnología blockchain puede mejorar la gestión y el acceso a datos altamente confidenciales para los organismos gubernamentales pues brinda la capacidad de acceder y operar fácilmente con información crítica, al tiempo que garantiza la seguridad e integridad de los datos almacenados.

A largo plazo, con avances continuos en la tecnología *blockchain*, los gobiernos podrán utilizar esta solución para ofrecer servicios públicos digitales de manera más efectiva. Los resultados de los estudios piloto pueden ayudar al sector público a abordar desafíos clave relacionados con la normalización, la seguridad y la regulación. Varios organismos gubernamentales pueden considerarse pioneros en la implementación de soluciones *blockchain* por el desarrollo de soluciones prácticas o la realización de estudios piloto en áreas de la administración pública como:

- Gestión de identidad digital: Algunos gobiernos han implementado sistemas de identificación basados en *blockchain* para que los ciudadanos tengan un control más seguro y privado de su información personal. Por ejemplo, Estonia en su programa "e-Residency" utiliza *blockchain* para garantizar la autenticidad de las identidades digitales.
- Votación electrónica: Varios países han explorado la posibilidad de utilizar *blockchain* para garantizar la seguridad e integridad de los procesos de votación electrónica y reducir el riesgo de fraude electoral y aumentar la confianza en los resultados. Estonia también ha realizado pruebas exitosas en este ámbito.
- Gestión de registros de propiedad: Se pueden almacenar registros de propiedad de bienes raíces y terrenos de forma segura en una *blockchain*, lo que ayuda a prevenir la falsificación y simplifica la transferencia de propiedad. Por ejemplo, Suecia ha realizado pruebas de registro de propiedades en *blockchain*.
- Transparencia en gastos gubernamentales: Algunos gobiernos utilizan *blockchain* para hacer que los gastos públicos sean más transparentes y audibles, lo que permite a los ciudadanos rastrear cómo se utiliza el dinero del gobierno en tiempo real. La ciudad de Austin, Texas, ha implementado un proyecto de este tipo.

- Gestión de contratos inteligentes: Los contratos inteligentes basados en *blockchain* se utilizan para automatizar y hacer cumplir acuerdos legales sin necesidad de intermediarios, lo que puede aplicarse en la administración pública para la gestión de contratos gubernamentales y acuerdos con proveedores.
- Seguimiento de productos y suministros: Algunos gobiernos utilizan *blockchain* para rastrear el suministro y la distribución de productos como alimentos o medicamentos. Esto garantiza la seguridad y autenticidad de los productos, y ayuda a prevenir falsificaciones.
- Gestión de registros de salud: En el ámbito de la atención médica se ha utilizado *blockchain* para gestionar de manera segura los registros de salud de los ciudadanos, lo que permite un acceso controlado a la información médica y una mayor privacidad.
- Gestión de subvenciones y ayudas: Algunos gobiernos utilizan *blockchain* para administrar y distribuir subvenciones y ayudas de manera eficiente y transparente. Esto reduce el riesgo de fraude y garantiza que los fondos lleguen a quienes los necesitan.

La suma de esos y otros logros muestra como resultado el potencial de los instrumentos basados en blockchain, lo que permite comprender la viabilidad de su implementación en el sector de la administración pública.

La estructura de la *blockchain* se asienta sobre el concepto de confianza distribuida y descentralizada, presentando una serie de propiedades muy interesantes, entre las que destacan las siguientes:

- Eliminación de intermediarios: Es un sistema integrado, completamente seguro y confiable que proporciona a los clientes acceso directo a los servicios, reduciendo al mínimo el uso de instituciones intermediarias.
- Automatización: Las tediosas operaciones manuales pueden ser reemplazadas por interacciones automatizadas entre los usuarios del sistema.
- Estandarización: El procesamiento automatizado de transacciones está diseñado para cumplir con reglas y procedimientos específicos, lo que puede llevar a la formulación de nuevos estándares en este ámbito.
- Racionalización de procesos: La tecnología *blockchain* ofrece mejoras sustanciales en los procesos comerciales a través de la racionalización y la transparencia.
- Eficiencia de procesamiento: La estructura *blockchain* ofrece un aumento en la velocidad de procesamiento de forma que los datos de las transacciones se pueden procesar casi en tiempo real.
- Reducción de costos: Con beneficios como la automatización, la racionalización de procesos y el procesamiento de datos casi en tiempo real, las soluciones *blockchain* ayudan a minimizar los costos de los servicios y, a largo plazo, estimulan cambios y ajustes en muchas áreas de la economía.

- Mayor confianza: En lugar de depender de las relaciones tradicionales de confianza entre personas e instituciones contratantes, las soluciones *blockchain* se basan en la confianza en la lógica infalible de las TIC.

Estas propiedades son posibles gracias a que la estructura utilizada es una cadena de bloques, en los que las transacciones se almacenan encadenadas usando una función *hash*, en forma de árbol. Concretamente, para agregar un nuevo bloque a la cadena, se genera un valor *nonce* pseudoaleatorio para obtener un *hash*. Cada bloque almacena la marca de tiempo de la transacción y el valor *hash* del bloque anterior, además del *nonce*, entre otros valores. De esa forma, cualquier intento de cambiar un valor almacenado en cualquier bloque anterior propagará el cambio por toda la cadena y en consecuencia será rápidamente detectado.

En el árbol que se forma con las cadenas, llamado árbol de Merkle, la raíz es el *hash* de todos los *hashes* contenidos en el árbol, lo que permite resumir el contenido de todas las transacciones para que, por una parte, ocupen la menor cantidad de espacio posible, y por otra parte, sea posible que esas transacciones puedan ser verificadas. Las nuevas transacciones son verificadas por los llamados mineros, que ganan criptomonedas por su cooperación. Sin embargo, antes de ganar tienen que competir entre ellos resolviendo un problema matemático complejo normalmente basado en una función *hash*. Uno de esos problemas se conoce tradicionalmente como prueba de trabajo (PoW, *Proof of Work*), consistente en que los mineros encuentren un valor aleatorio que añadido al *hash* del bloque que se está minando produciendo una salida de la función *hash* que comienza por un número determinado de ceros. La única forma de encontrar ese valor aleatorio es mediante búsqueda exhaustiva, hasta dar con el valor de salida *hash* deseado.

Los contratos inteligentes (*smart contracts*) son programas implementados para ser ejecutados en la máquina virtual de Ethereum, que es una plataforma de código abierto basada en tecnología *blockchain* que permite a los desarrolladores implementar en una red P2P aplicaciones descentralizadas de muy diferentes tipos (votaciones, registros de activos o propiedades, subastas, apuestas, etc.). Las cuentas de usuario de Ethereum requieren un par de claves asimétricas de usuario ya que se basan en ECC. En Ethereum, como en todas las *blockchain*, las transacciones son paquetes de datos firmados por el usuario mediante el algoritmo de firma digital de curva elíptica ECDSA. Ethereum fue muy criticado por la huella de carbono que generaba así desde 2022 migró del modelo de PoW, que requiere grandes cantidades de energía, hacia un modelo de prueba de participación en el que la probabilidad de minar un bloque de transacciones y recibir el premio correspondiente es directamente proporcional a la cantidad de monedas que se tiene.

7. CONCLUSIONES

El creciente uso de las TIC está transformando la prestación de servicios gubernamentales. Este artículo ha abordado la relevancia de la ciberseguridad en

el ámbito de la administración pública, prestando especial atención al papel fundamental de la criptografía como piedra angular para salvaguardar la integridad y confidencialidad de los datos en ese entorno. Además, proporciona una visión detallada de las infraestructuras de clave pública y un análisis sobre el DNIe y el sistema Cl@ve, ilustrando su utilidad como ejemplos de identificación electrónica segura con múltiples aplicaciones dentro de la administración pública. Asimismo, se ha dedicado atención a las estrategias implementadas por las administraciones públicas a nivel internacional para hacer frente a la amenaza emergente que representa la computación cuántica, destacando la importancia de desarrollar sistemas criptográficos resistentes a esta nueva realidad tecnológica. En un contexto actual en constante evolución, se han enumerado algunas de las aplicaciones de vanguardia de las tecnologías *blockchain* que están comenzando a transformar la forma en que se gestionan los procesos administrativos.

En resumen, este trabajo ha proporcionado una visión completa de los desafíos y avances en seguridad de la información en la administración pública, subrayando la necesidad de adaptarse de manera continua a las ciberamenazas en constante evolución, así como de aprovechar las oportunidades que ofrecen las tecnologías emergentes para garantizar la seguridad y eficiencia en la gestión de datos en este sector crucial.

Muchos temas de interés han quedado en el tintero. Por ejemplo, entre las aplicaciones del gobierno electrónico, una de las áreas pendientes en España es la adopción del voto electrónico. En este caso, los requisitos de seguridad subyacentes que se aplican a otros servicios de la administración pública se vuelven aún más críticos al implementar el voto electrónico debido a la gravedad de las consecuencias en caso de un fallo. Por ese motivo, las herramientas criptográficas necesarias para desplegar elecciones electrónicas son de las más complejas que se pueden implementar en la administración pública.

8. REFERENCIAS

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary? Available at SSRN 2709713.

Caballero Gil, P. (2002) Introducción a la Criptografía. 2a edición actualizada. Editorial Ra-Ma.

Centro Criptológico Nacional (2018). Resolución 1A0/38016/2018, de 15 de junio, del Centro Criptológico Nacional, por la que se certifica la seguridad del producto DNIe-DSCF (dispositivo seguro de creación de firma), versión 3.0.

Congress.gov (2022) H.R.7535 – Quantum Computing Cybersecurity Preparedness Act. 117th Congress. https://www.congress.gov/bill/117th-congress/house-bill/7535/

Correa Marichal, J. (2022). Seguridad de las tarjetas NFC. Trabajo de Fin de Grado. Universidad de La Laguna. https://riull.ull.es/xmlui/handle/915/28735

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory 22 pp. 644-654.

EUR-Lex (2013). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

EUR-Lex (2016a). Reglamento general de protección de datos (RGPD). https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html

EUR-Lex (2016b). DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SPA

Gennai, F., Martusciello, L., & Buzzi, M. (2005). A certified email system for the public administration in Italy. In IADIS International Conference WWW/Internet (Vol. 2, pp. 143-147).

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433.

Gobierno de España (2015). Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389

Gobierno de España (2017). Estrategia de Seguridad Nacional. Disposición 15181 del BOE núm. 309 de 2017. https://www.boe.es/boe/dias/2017/12/21/pdfs/BOE-A-2017-15181.pdf

Gobierno de España (2018). III Plan de Acción de España 2017-2019. https://transparencia.gob.es/transparencia/dam/jcr:540931bc-376c-43a7-8bd7-1569006e97cd/Spain_III_Plan_GA_v2018_vf.pdf

Gobierno de España (2019). Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. https://www.boe.es/eli/es/o/2019/04/26/pci487

Gobierno de España (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. https://www.boe.es/diario_boe/txt.php?id=-BOE-A-2022-7191

Hou, H. (2017). The application of blockchain technology in e-government in China. In 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1–4). New York: IEEE.

Kaplan, M., Leurent, G., Leverrier, A., & Naya-Plasencia, M. (2016). Breaking symmetric cryptosystems using quantum period finding. In Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36 (pp. 207-237). Springer Berlin Heidelberg.

Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. Designs, codes and cryptography, 19, 173-193.

Kovács, L. (2018). Cyber security policy and strategy in the European Union and NATO. Land Forces Academy Review, 23(1), 16-24.

Lambrinoudakis, C., Gritzalis, S., Dridi, F., & Pernul, G. (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. Computer communications, 26(16), 1873-1883.

León-Coca, J. M., Reina, D. G., Toral, S. L., Barrero, F., & Bessis, N. (2013). Authentication systems using ID Cards over NFC links: the Spanish experience using DNIe. Procedia Computer Science, 21, 91-98.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.

Moynihan, D. P. (2004). Building secure elections: e-voting, security, and systems theory. Public administration review, 64(5), 515-528.

Nir, Y., & Langley, A. (2018). ChaCha20 and Poly1305 for IETF Protocols (No. rfc8439).

Ojo, A., & Adebayo, S. (2017). Blockchain as a next generation government information infrastructure: A review of initiatives in D5 countries. In Government 3.0–Next Generation Government Technology Infrastructure and Services (pp. 283–298). Cham: Springer.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing.

Open Government Partnership (2017). https://www.opengovpartnership.org/

Parlamento Europeo y Consejo de la Unión (2018). Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0910

Prandini, M. (1999). Efficient certificate status handling within PKIs: an application to public administration services. In Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99) (pp. 276-281). IEEE.

Raab, C. D. (1998). Electronic confidence: Trust, information and public administration. Public Administrations in an Information Age: A Handbook" eds. Snellen, I. Th. M & Van De Donk, WBHJ, 113-133.

teriaportal.org/files/epfiles/2019-06%20ST_LITE.pdf

Rijmen, V., & Daemen, J. (2001). Advanced encryption standard. Proceedings of federal information processing standards publications, national institute of standards and technology, 19, 22.

Rivest, R., Shamir, A., & Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). Communications of the ACM. 21 (2): 120–126.

Rot, A., Sobińska, M., Hernes, M., & Franczyk, B. (2020). Digital transformation of public administration through blockchain technology. Towards Industry 4.0—current challenges in information systems, 111-126.

Silcock, R. (2001). What is e-government. Parliamentary affairs, 54(1), 88-101.

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. Computers & Security, 90, 101709.

Vatra, N. (2010). Public key infrastructure for public administration in Romania. In 2010 8th International Conference on Communications (pp. 481-484). IEEE.

Weiss, M., & Corsi, E. (2017). Bitfury: Blockchain for government. In Harvard Business School Case (pp. 818–031).