Blockchain y otras tecnologías para la seguridad. Aplicación sobre el registro documental de información clasificada.

Autor: Méndez García, Ángel

Directores: Rodríguez Martínez, Francisco Javier. Álvarez Sabucedo, Luis.

Contacto: pitrinos@fn.mde.es; franjrm@uvigo.es; lsabucedo@det.uvigo.es

---

Resumen: En el estado español, distintos organismos manejan a diario gran cantidad de información tanto de origen nacional como de otros estados y organizaciones, que puede comprometer o afectar al propio Estado, a la seguridad nacional o a la de otros estados, organismos u organizaciones internacionales. Por ello debe ser protegida. Esa información se conoce como información clasificada y se rige por una normativa específica.

Las tecnologías de la información y las comunicaciones (TIC) permiten en la actualidad la gestión eficaz y segura de cualquier información en soporte digital, utilizando distintas técnicas y procedimientos y, como no, personas. La normativa nacional para la protección de la información clasificada, recogida en las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, exige un tratamiento específico para ese tipo de información, conforme a una serie de procedimientos y requisitos, depurados y establecidos tras muchos años de experiencia y mejora continua.

Dado que la información clasificada exige un especial cuidado en lo relativo a su seguridad, a que cada vez más la información se maneja en soporte digital, y a que, como se ha mencionado, las TIC ofrecen garantías suficientes de seguridad a la información clasificada, los órganos responsables de su manejo y custodia deberían disponer de herramientas basadas en las TIC que garanticen la gestión segura y la protección de este tipo de información. Pero la realidad es muy distinta. Los servicios de protección de información clasificada no disponen de herramientas TIC apropiadas.

La normativa exige que esas herramientas informáticas estén aprobadas por la Oficina Nacional de Seguridad (responsable principal en la estructura nacional de protección de la información clasificada) para el manejo de este tipo de información.

Este trabajo plantea una posible solución, analizando distintas TIC disruptivas, emergentes o maduras como puedan ser blockchain, la criptografía visual, o el Data Loss Prevention entre otras.

Palabras clave: Información clasificada, Blockchain, criptografía visual, *Smart Contracts*, gestión documental.

---

1. Introducción

1.1. Antecedentes

Todas las naciones del mundo han manejado históricamente y con mayor o menor acierto, información que por su valor debía estar al alcance de muy pocos y que por ello se protegía de una u otra forma. Era información clasificada (en adelante, se utilizará indistintamente la denominación o la abreviatura IC).

Los organismos y estructuras del estado español, incluidas las Fuerzas Armadas (en adelante FAS) manejan a diario gran cantidad de esa IC: contiene datos que pueden comprometer la seguridad nacional o la de organizaciones internacionales. Por ello debe ser protegida.

La normativa nacional para la protección de la IC exige que este tipo de información se gestione y trate de una manera específica, conforme a unos procedimientos y requisitos, depurados y mejorados tras muchos años de experiencia y mejora continua.

En España existe una estructura nacional, consistente en una serie de oficinas, responsables de custodiar y proteger ese tipo de información. Estas Oficinas se conocen como *servicios de protección de información clasificada* (SPIC).

1.2. Objetivo

La motivación de este trabajo arranca de la percepción de un potencial problema por falta de soluciones TIC en lo relativo a la trazabilidad, registro y manejo de la IC en los SPIC. Esta potencial debilidad fue identificada en el curso de la relación laboral normal del autor con estas Oficinas.

Este trabajo pretende estudiar el problema en profundidad y proponer posibles soluciones a las necesidades que tiene la estructura nacional de protección de la IC de manejar, registrar y controlar la citada información, aprovechando los avances en distintos campos de las TIC y otras tecnologías que podrían ser disruptivas en este campo.

2. Desarrollo

2.1 Definiciones previas

Información Clasificada es cualquier información o material respecto de la cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad entendiéndose como información todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.

La información puede estar clasificada en distintos grados en función del perjuicio que puede ocasionar su difusión no autorizada. En España los grados reconocidos son SECRETO, RESERVADO, CONFIDENCIAL y DIFUSIÓN LIMITADA.

A su vez, se debe distinguir entre información clasificada española o extranjera (propiedad de otros países u organizaciones internacionales, como OTAN o Unión Europea).

Documentación clasificada es cualquier soporte que contenga información clasificada registrada, en cualquier formato físico (escrito, impreso, cinta, fotografía, mapa, dibujo, esquema, nota, soporte informático, óptico o vídeo, etc.). La más tradicional es en formato papel, aunque cada día se hace un uso más extensivo de los soportes informáticos.”

Es decir, que la IC no se considera documentación clasificada hasta que no sufre el proceso de registro. Es un acto que le infiere una serie de características que obligan a su debido tratamiento. Esto significa que hay que garantizar la Confidencialidad, Integridad y Disponibilidad de la citada información. A su vez, la trazabilidad y el no repudio son relevantes

2.2 Normativa y estándares.

La normativa relativa a las TIC es numerosa y profusa. Partiendo de la normativa ISO (ISO/IEC 27000:2018), pasando por el estándar *Common Criteria* para productos software, el estándar TIA 942 para la instalación de Centros de datos o Data Center.

A su vez, para la información clasificada existe también numerosa normativa a nivel nacional e internacional. Comenzando por la Ley de secretos Oficiales, siguiendo con las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, las guías CCN-STIC, y llegando a las normas internas del Ministerio de Defensa como las Normas de seguridad de la información para elaboración, clasificación, cesión, distribución y destrucción de información en el Ministerio de Defensa.

Toda esta normativa en su conjunto impone una serie de requisitos y restricciones al manejo y registro de la información clasificada. Cualquier red, sistema informático o dispositivo de almacenamiento de información clasificada en soporte digital que maneje ese tipo de información debe cumplir unos estrictos protocolos de seguridad tanto a nivel de seguridad física, de emanaciones electromagnéticas, seguridad del personal que los utiliza y seguridad documental, lo que acaba perfilando el estudio realizado en este trabajo sobre las tecnologías TIC que podrán o no implementarse para mejorar la situación actual de los SPIC.

2.3 Tecnologías disruptivas y emergentes aplicables a la protección de la información clasificada.

En este trabajo se analizan las siguientes tecnologías:

- Blockchain
- Criptografía Visual
- Software y hardware de cifrado offline
- Tecnología de impresión con tinta ultravioleta
- Borrado seguro de datos
- Prevención de pérdida de datos (*Data Loss Prevention*)
- Cifradores hardware

2.4 Trabajos relacionados. Iniciativas relevantes existentes

Existen numerosos artículos y trabajos relacionados con la gestión documental, las arquitecturas de seguridad en redes de comunicaciones, y tecnologías como *blockchain*, Data Loss Prevention, o criptografía visual.

El estado del arte en estas tecnologías y arquitecturas es muy diverso y se encuentra en continua evolución. Se ha procedido en este trabajo a una revisión de distintos artículos académicos e informativos en fuentes como IEEE.org, ResearchGate.net, y fuentes abiertas de Internet.

No obstante, **no se han encontrado trabajos relacionados con el manejo de la información clasificada**, quizás por su carácter sensible y por ello los trabajos que puedan existir al respecto no sean de acceso público.

En lo referente a iniciativas relevantes existentes, se exponen en el trabajo varios proyectos interesantes, como el proyecto *Cert Chain* de la Armada para la implementación de una red blockchain que permita supervisar y controlar documentación de mantenimiento que implique desmontaje de los elementos de los nuevos submarinos S-80, para posteriormente comprobar que los elementos mantienen la certificación previa.

Otro proyecto de alto interés es la herramienta Libro de Registro, proyecto liderado por la Oficina Nacional de Seguridad (ONS) del CNI, que pretende subsanar el problema existente en los SPIC nacionales respecto de la gestión y registro de documentación clasificada. Si bien el proyecto es interesante, la herramienta se ha diseñado para su uso en terminales aislados, y no en una red de Oficinas, lo que inicialmente le resta atractivo.

Otras herramientas o soluciones tecnológicas relevantes basadas en iniciativas del Centro Criptológico Nacional son, por ejemplo, la herramienta CARLA, que supone un avance en la protección del dato, permitiendo una mejora notable de la trazabilidad de documentos. Entre sus actuales limitaciones está que sólo se autoriza su uso para redes que manejen información clasificada nacional y de grado difusión limitada. Un desarrollo de la herramienta para su uso en redes que manejen información clasificada hasta secreto supone un interesante desafío y mejorará la seguridad en una futura red informática entre los distintos SPIC.

3. Resultados y discusión

Resultado de un análisis de las diversas tecnologías, sus posibilidades y su aplicabilidad, se presenta a continuación una tabla con los resultados, para cada tecnología y tipo de implementación resultante del trabajo.

Se quiere destacar en este punto que, si bien se trata de una interpretación del autor basada en su conocimiento y el estado actual de desarrollo de muchas de esas tecnologías, la tabla no se debe considerar estática, ya que en el futuro muchas de las soluciones que se descartan aquí podrían perfectamente ser de aplicación.

Como posible discusión, se considera que los fabricantes de varios de los productos y herramientas expuestas en este trabajo, deberían llevar a cabo el I+D+I necesario para aportar mejoras a sus soluciones de forma que permitan su uso en redes de información clasificada de grado hasta secreto y ámbitos nacional, OTAN y UE.

ANÁLISIS DE APLICABILIDAD DE LAS DISTINTAS TECNOLOGÍAS ANALIZADAS

Herramienta	Tecnología	Aplicable	Observaciones
Blockchain	Trazabilidad permanente	**SI**	Red federada. Uso de oráculos y *Smart Contracts* viable. En continuo desarrollo de nuevas funcionalidades y amplio soporte.
Criptografía visual	Autenticación/Confidencialidad	**SI**	Uso para autenticación y no repudio.
CARLA (Sealpath)	Protección del dato	**NO**	Limitado a IC difusión limitada nacional. Sólo S.O. Windows y limitado soporte de protección a ficheros. Requiere mayor desarrollo.
McAfee DLP	Data Loss Prevention	**SI**	Garantiza la seguridad de los datos dentro de la red e impide la exfiltración no autorizada de información clasificada. Tecnología madura y con soporte.
Aplicación Libro de Registro (ONS)	Libro de registro documental	**NO**	Instalación *on premise*. No permite su uso en red. No compatible con otras tecnologías como *blockchain*. Requiere mayor desarrollo (uso en red, compatibilidad con BC, DLP, etc.)
BLANCCO File eraser/Drive eraser	Software de borrado seguro	**SI**	Software aprobado por CCN. Deberá ser acreditado para uso con IC SECRETO o equivalente.
Solpheo Suite	Herramienta de gestión documental	**NO**	Desarrollo enfocado al ámbito empresarial, centrado en posibilitar teletrabajo
Herramienta Shaadow	Herramienta de no repudio	**SI**	Se desconoce la tecnología subyacente. Sólo aplicable a ficheros pdf. Contratado actualmente por el EMAD.
Software EP-880	Cifra offline de ficheros	**SI**	Garantiza la confidencialidad, autenticidad y el no repudio de la IC. Actualmente sólo se autoriza su uso para cifrar IC nacional de grado difusión limitada
Cifradores HARDWARE	Cifra online de datos	**SI**	Exigido por normativa para redes que manejan IC. Pendiente de disponer de cifradores para todos los ámbitos
GPG4Win/GnuPG	Criptografía de clave pública (cifra offline)	**SI**	Alternativa a EP880. Garantiza la confidencialidad, autenticidad y el no repudio de la IC. Pendiente de certificación por parte del CCN para su uso con IC SECRETO o equivalente.
PKI	Criptografía de clave pública (cifra offline)	**SI**	Requiere de infraestructura de AC, y certificados validados (FNMT)
Dispositivo USB cifrador EP852	Cifra offline de ficheros	**SI**	Exigido por normativa para transferencia o almacenamiento cifrado de ficheros.
Tinta UV	Autenticación/no repudio	**SI**	Utilización en tarjetas de credenciales ocultas para acceso a las sesiones de los terminales, o para el marcado invisible de documentos clasificados.

Tabla 1 Comparativa de tecnologías aplicables.

4. Conclusiones

La investigación inicial demuestra la necesidad que tiene la ONS y los OOC del ámbito de las FAS de disponer de una red segura para el intercambio de IC.

Existen diversas tecnologías, algunas de ellas disruptivas y otras innovadoras, que pueden aumentar la seguridad de la citada red, garantizando en gran medida la Disponibilidad, Integridad y Confidencialidad de esa IC. Es innegable que ciertas soluciones empleadas en el momento actual son susceptibles de mejora en ciertos aspectos que pueden considerarse críticos.

A su vez, otras tecnologías garantizan la trazabilidad como blockchain. No obstante, para la implementación de todas las tecnologías aplicables contempladas en este trabajo y que mejoraran aspectos claves, será preciso un proyecto que permita integrarlas en el ecosistema actual del Ministerio de Defensa para garantizar la sostenibilidad e interoperabilidad con otras herramientas en uso actualmente.

Dados los requisitos de seguridad que debe cumplir una aplicación software para poder manejar IC y servir de herramienta de registro documental, es muy recomendable diseñar y crear una aplicación desde cero. Del mismo modo, parece razonable sugerir una arquitectura de red basada en la seguridad, liderada por el CNI o la ONS por su parte, y el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones, por parte del Ministerio de Defensa. Como complemento, otras autoridades de la AGE pueden participar del proyecto. El punto de partida es el software Libro de Registro de la ONS.

Blockchain se ha mostrado como la tecnología más disruptiva y que más valor aporta en lo tocante a trazabilidad, inalterabilidad y seguridad. Se ha demostrado que existen iniciativas en el ámbito militar de gran interés basadas en ella y que mejorarán en un futuro cercano las operaciones militares, la gestión logística, y la seguridad de las redes militares ya sean para propósito general (sin clasificar) como de Mando y Control (clasificadas). La evolución y maduración que ha experimentado en otros ámbitos como la logística empresarial o la DeFI (decentralized finance) puede aprovecharse en este ámbito.

Este trabajo demuestra que *blockchain* tiene aplicación práctica en la gestión y manejo de IC. No se han encontrado estudios previos específicamente sobre este ámbito. Por eso este TFM abre una nueva línea de investigación en el ámbito militar que no se había abordado previamente.

Por último, hay que tener en cuenta que la normativa, al igual que las tecnologías, está sujeta a cambios. Durante el desarrollo de este trabajo se ha producido un cambio sustancial en la normativa de aplicación a nivel nacional. En 2022 se va a modificar la NS/05 contenida en las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, y se sustituirán varias guías CCN-STIC por unas nuevas *Instrucciones Generales* y otras guías denominadas ahora *Recomendaciones*, adaptando todo el conjunto al Esquema Nacional de Seguridad (ENS).

Independientemente de lo anterior, la metodología del análisis realizado hace que este trabajo mantenga su valor. Surgen nuevos estándares, pero se mantiene el enfoque tecnológico del trabajo.