INNOVACIÓN EN CIBERSEGURIDAD. ESTRATEGIA Y TENDENCIAS

JUAN GONZÁLEZ MARTÍNEZ
Centro Tecnológico Gradiant

La adopción masiva de tecnologías de la información y telecomunicaciones está transformando nuestra sociedad y todos los sectores de nuestra economía. Está cambiando como nos relacionamos como sociedad, como interactuamos con las Administraciones Públicas y como las empresas desarrollan y entregan sus productos.

INTRODUCCIÓN

Digitalización del sector público

Las Administraciones Públicas, locales, autonómicas y estatales, se encuentran en pleno proceso de transformación, proporcionando cada vez más procedimientos e información a los ciudadanos de forma digital, para la conveniencia de estos últimos y con el objetivo de conseguir una administración más eficiente, interconectada e interoperable.

Desde la escueta mención al impulso de los medios técnicos presente en el artículo 45 de la ya derogada Ley de Procedimiento Administrativo del año 1992 (Ley 30, 1992), pasando por la ley de Administración Electrónica de 2007 (Ley 11, 2007), se ha llegado a las actuales leyes de Régimen Jurídico (Ley 39, 2015) y Procedimiento Administrativo (Ley 40, 2015) de 2015 donde ya no se habla de la posibilidad de la Administración Electrónica sino que se considera que la Administración es (o debe ser) electrónica, siguiendo así lo que se conoce como la estrategia digital por defecto (*digital by default).*

Según datos de Eurostat, el porcentaje de ciudadanos que se relaciona con la Administración mediante medios electrónicos supera el 50% (Eurostat, 2017). Otro indicador de la evolución es el número de ciudadanos registrado en el servicio de identidad Cl@ve, que unifica y simplifica el acceso electrónico a los servicios públicos. Según datos del Observatorio de Administración Electrónica OBSAE, el crecimiento de los usuarios registrados entre 2015 y 2017 ha sido superior al 200%, situándose en más de 5 millones (OBSAE, 2018).

Digitalización del sector privado

La transformación digital también está teniendo un gran impacto en las empresas, en cómo entregan los productos a sus clientes, en su organización interna y en la relación con sus proveedores.

Uno de los sectores que mejor refleja la adopción de nuevas tecnologías TIC es el comercio electrónico. No solo ha supuesto la aparición de grandes gigantes nativos digitales, sino que ha sido asumido por pequeñas empresas y negocios tradicionales. El 28% de las em-

presas medianas (entre 50 y 250 empleados), venden sus productos online (Eurostat, 2017). Por parte de los usuarios la compra por Internet ha aumentado drásticamente. En España el 40% de los ciudadanos ha realizado al menos una compra online en los últimos 3 meses en 2017, cuando este indicador era tan solo del 22% en 2012 (Eurostat, 2017).

En la gestión de sus procesos internos, la digitalización está cada día más presente en las empresas, el 46% ha integrado sus procesos en productos software, valor que apenas superaba el 20% en el año 2012 (Eurostat, 2017).

Aumento de los riesgos asociados a la digitalización

Si bien son indudables los beneficios derivados de esta transformación digital también han aumentado los riesgos asociados a la adopción de nuevas tecnologías, principalmente los generados por amenazas a la seguridad de la información o ciberamenazas. Estas amenazas ponen en riesgo no solo el crecimiento y la sostenibilidad de nuestra economía, sino también nuestro modo de vida.

Así, la Ciberdelincuencia, como fenómeno que va parejo al uso de las nuevas tecnologías, ha experimentado un crecimiento durante los últimos años, como consecuencia de un mayor uso por parte de la sociedad de todas las nuevas formas de conectividad tecnológica (Ministerio del Interior, 2017).

En los datos del Sistema Estadístico de Criminalidad (SEC) se aprecia un crecimiento de los delitos para cuya comisión se han empleado Tecnologías de la Información y Comunicaciones (TIC). Según el Estudio de Cibercriminalidad de 2017, «en el periodo comprendido entre 2014 a 2017, como hecho irrefutable extraído de los resultados registrados por las Fuerzas y Cuerpos de Seguridad se constata el aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2017, se ha conocido un total de 81.307 hechos, lo que supone un 22,1% más con respecto al año anterior. De esta cantidad, el 74,4 % corresponde a fraudes informáticos y el 13,9% a amenazas y coacciones.» (Ministerio del Interior, 2017)

El crecimiento de los ciberataques tiene diversas causas. La Estrategia de Ciberseguridad Nacional identifica las siguientes (Presidencia del Gobierno, 2013):

- Bajo coste: muchas de las herramientas utilizadas por los atacantes pueden obtenerse de forma gratuita o a un coste muy reducido.
- Ubicuidad y fácil ejecución: la ejecución de los ataques es independiente de la localización de los agresores, no siendo imprescindible, en muchos casos, grandes conocimientos técnicos.
- Efectividad e impacto: si el ataque está bien diseñado, es posible que alcance los objetivos perseguidos. La ausencia de políticas de ciberseguridad, la insuficiencia de recursos y la falta de sensibilización y formación pueden facilitar este adverso resultado.
- Reducido riesgo para el atacante: la facilidad de ocultación hace que no sea fácil atribuir la comisión de un ciberataque a su verdadero autor o autores, lo que, unido a un marco legal dispar o inexistente, dificulta la persecución de la acción.

Innovación en ciberseguridad

Las amenazas a la seguridad de la información han existido siempre, pero ha sido en los últimos años cuando los riesgos asociados a las mismas han sufrido un crecimiento exponencial. Esto se debe principalmente a los siguientes factores:

- El impacto de ataques a la seguridad es mucho mayor debido a la mayor adopción de tecnologías como elementos fundamentales en los procesos de negocio.
- La probabilidad de que se produzcan los ataques ha aumentado. La complejidad de las tecnologías empleadas aumenta la superficie de ataque y la innovación por parte de los atacantes incrementa la capacidad de los mismos para amenazar la seguridad de la información.

Estos factores explican la necesidad de investigar e innovar en ciberseguridad. Por un lado, la rápida evolución de las tecnologías y la necesidad por parte de las organizaciones por adoptarlas para mantener su competitividad y mejorar su eficiencia lleva asociada un incremento en el número de vulnerabilidades a las que están expuestas las empresas. Es imprescindible mantener el mismo ritmo de innovación en ciberseguridad para poder adoptar nuevas tecnologías sin superar un nivel de riesgo aceptable.

Por otro lado, los actores que buscan explotar las vulnerabilidades son activos, innovadores y usan igualmente los avances tecnológicos para lleva a cabo sus ataques. Esto provoca que el riesgo al que se ven expuestas las organizaciones sea especialmente dinámico y difícil de gestionar. En seguridad de la información, las amenazas a la disponibilidad, confidencialidad e integridad de la misma no tienen por qué venir causadas por un atacante. Por ejemplo, el fuego es una amenaza clásica en seguridad de la información y deben establecerse los controles necesarios para mitigar su riesgo, pero, afortunadamente, no es necesario protegerse de cambios en el comportamiento del fuego o que se apoye en nuevas tecnologías.

La innovación y el uso de nuevas tecnologías en los ataques (por ejemplo: el uso de Inteligencia Artificial para mejorar las campañas de *phising* (Palmer, 2017) o el uso de dispositivos IoT para ataques de denegación de servicio (Krebs, 2016)) obliga a innovar en ciberseguridad para hacer frente al desarrollo de nuevas amenazas.

Por ello, la ciberseguridad debe verse como un elemento habilitador, imprescindible para la adopción de

nuevos tecnologías y alcanzar los beneficios asociadas a las mismas. La innovación en tecnologías de ciberseguridad es un elemento fundamental que debe jugar un papel habilitador en la digitalización de la sociedad y de la economía.

El mercado de la ciberseguridad

Desde el punto de vista de mercado, la ciberseguridad es un sector en crecimiento, de hecho, debería tener un crecimiento como mínimo igual al del de desarrollo de nuevas tecnologías para poder adoptar éstas de manera segura. Al invertir en tecnologías, las organizaciones deben realizar una inversión proporcional en ciberseguridad para que los riesgos asociados a su implantación no destruyan los beneficios esperados.

Desafortunadamente para España y para Europa en general, el mercado de los productos de ciberseguridad está dominado principalmente por empresas estadounidenses al igual que la innovación (EOS, 2015). Esto es negativo principalmente por dos aspectos:

– La balanza comercial en productos de ciberseguridad es deficitaria para Europa. Somos principalmente importadores en un mercado con grandes expectativas de crecimiento.

– La ciberseguridad es un mercado estratégico. Los productos de ciberseguridad son necesarios para la protección de nuestras empresas y la industria, de nuestro sector público, de las infraestructuras críticas y de los ciudadanos en general. Es evidente que sería preferible disponer de tecnología propia europea y no depender exclusivamente de tecnología extracomunitaria.

Estos aspectos están claramente reconocidos en Europa y en España y a ambos niveles se están desarrollando estrategias para mejorar la balanza comercial y reducir la dependencia de tecnología externa. En estas estrategias juega un papel relevante la innovación en ciberseguridad.

ESTRATEGIA EUROPEA PARA LA INNOVACIÓN EN CIBERSEGURIDAD

Los primeros pasos en la Unión Europea para abordar los problemas de ciberseguridad, tanto las relativas a las amenazas al mercado único digital (*Digital Single Market*) como a la dependencia y exportación de productos extracomunitarios, se dieron en la Estrategia de Ciberseguridad Europea en el año 2013.

La estrategia establece los siguientes principios para guiar la política de la Unión Europea en materia de ciberseguridad (European Comission, 2013):

– Los valores fundamentales de la UE se aplican tanto en el mundo digital como en el físico.

– Protección de los derechos fundamentales, la libertad de expresión, los datos personales y la privacidad.

– Acceso para todos.

– Gobernabilidad democrática y eficiente de múltiples partes interesadas.

– Una responsabilidad compartida para garantizar la seguridad.

En la definición de las prioridades estratégicas junto con las relacionadas con reducir el ciber-crimen, alcanzar ciber-resiliencia, mejorar la ciber-defensa y establecer una política para el ciber-espacio, se encuentra desarrollar los recursos industriales y tecnológicos para la ciberseguridad.

Es en esta prioridad estratégica donde se aborda el riesgo de que Europa no solo sea excesivamente dependiente de soluciones TIC producidas fuera de sus fronteras, sino también de productos de seguridad extracomunitarios.

Entre las medidas a tomar para desarrollar los recursos industriales y tecnológicos para la ciberseguridad destaca el fomentar las inversiones en investigación, desarrollo e innovación. En la estrategia se considera que la inversión en innovación servirá para promover la industria TIC en Europa y reducir la dependencia europea de las tecnologías extranjeras. La innovación también ayudaría a reducir las carencias tecnológicas en la seguridad informática y a prepararnos para las próximas generaciones de ciberamenazas.

Otro punto fundamental abordado en esta medida es complementar la inversión en I+D+i con esfuerzos para traducir esta inversión en soluciones comerciales. Se debe conseguir que las innovaciones alcanzadas se integren en el mercado de la ciberseguridad.

Para ello, en la estrategia, la Comisión Europea se compromete a utilizar el programa marco de investigación e innovación *Horizon 2020*, para cubrir aspectos de ciberseguridad y privacidad desde el I+D hasta la innovación y despliegue. También invita a los Estados Miembro a utilizar la fuerza de compra de las Administraciones Públicas para estimular el desarrollo de características de seguridad en productos TIC, es decir, utilizar herramientas de Compra Pública Innovadora que sirvan de instrumento para el fomento de la innovación en ciberseguridad.

Como consecuencia de la definición de la estrategia europea en ciberseguridad surge el interés de la industria en firmar una asociación público-privada contractual (cPPP por sus siglas en inglés) con la Comisión Europea. La propuesta de cPPP (ECSO, 2016) se hace oficial en junio de 2016 coincidiendo con la creación de la European Cybersecurity Organization (ECSO) que engloba todas las organizaciones con intereses en seguridad de la información. Los miembros de la ECSO incluyen a grandes compañías TIC, Universidades, PYMEs y otras entidades como pueden ser distintos organismos del sector público, grandes empresas no TIC (finanzas, seguros, energía,...). El cPPP (ECSO - European Comission, 2016) se firma finalmente en julio de ese mismo año.

Dentro del contrato se determinan los principales objetivos del mismo agrupados en: mejoras de competitividad, operacionales, sociales e innovación. Tanto los relativos a la mejora de la competitividad como, obviamente, los referidos a la innovación, destacan ésta como uno de los principales aspectos a tener en cuenta para posicionar Europa en el mercado de la ciberseguridad, habilitar el mercado digital europeo y mejorar la seguridad y la confianza en el mismo.

A nivel económico la Comisión estima financiar proyectos en innovación en materia de ciberseguridad, dentro del programa marco H2020, por un importe de 450M de euros. Por su lado se espera que el mercado de ciberseguridad invierta tres veces dicha cantidad.

ECSO está estructurado en grupos de trabajo. Desde el punto de vista de innovación el más destacado es el grupo de trabajo 6 (WG6). Este grupo fue el encargado de definir la agenda para la estrategia en innovación (SRIA, *Strategic Research and Innovation Agenda)*. Los objetivos principales del grupo de trabajo son los siguientes:

– Coordinación de resultados y expectativas de la Comisión Europea y proyectos de I + D

– Coordinación de actividades de ciberseguridad en la cPPP e iniciativas de la UE

– Apoyo a la implementación de cPPP y los proyectos de ciberseguridad en el programa marco H2020

– Sugerencias detalladas para el Programa de Trabajo 2017-2020 usando una SRIA actualizada y enfocada

En resumen, su principal función es aconsejar e influir en la Comisión Europea sobre los aspectos a financiar en ciberseguridad en el programa H2020.

En la primera versión de la SRIA, publicada en junio de 2017, se identifican cuatro tipos de proyectos para H2020 (ECSO, 2016):

– Ecosistema: Proyectos dedicados al desarrollo de un ecosistema favorable a la implementación de soluciones innovadoras en ciberseguridad.

– Proyectos de demostración: Demostración de soluciones de ciberseguridad en dominios verticales (telecomunicaciones, energía, salud,...) en colaboración con la industria que permita acelerar la implantación de soluciones innovadoras.

– Infraestructuras transversales: Proyectos que permitan integrar tecnologías transversales, independientes del sector, que afronten desafíos comunes en ciberseguridad.

– Componentes tecnológicos: Proyectos para el desarrollo de tecnologías transversales en ciberseguridad.

Como se puede ver, la estrategia para la innovación en ciberseguridad es apoyarse en las necesidades de distintos sectores dentro de Europa que faciliten el desarrollo de una industria europea en ciberseguridad. Para ello, el grupo de trabajo 6 colabora estrechamente con el grupo de trabajo 3, formado principalmente por representantes de las principales empresas y organizaciones en distintos sectores en Europa: Industria, Energía, Edificios y Ciudades Inteligentes, Transporte, Salud y Servicios Electrónicos.

Esta estrategia, la colaboración con los usuarios finales de las tecnologías de ciberseguridad en Europa, es clave. No solo permite conocer de primera mano sus necesidades, y en particular las necesidades no cubiertas con los productos existentes, sino que servirán de plataforma para la maduración de las tecnologías desarrolladas en Europa. Para ello es fundamental convencer a estas organizaciones de las ventajas de afrontar conjuntamente estos retos y la financiación mediante el programa marco de innovación es una gran medida para ello.

ESTRATEGIA ESPAÑOLA PARA LA INNOVACIÓN EN CIBERSEGURIDAD

La importancia de la transformación digital de la sociedad ha puesto como objetivo prioritario en la agenda de la mayoría de los Gobiernos garantizar la seguridad del ciberespacio. En el caso de España, este objetivo se plasmó, en 2013, en la Estrategia de Seguridad Nacional.

La Estrategia de Seguridad Nacional establece como uno de sus principales objetivos (Presidencia del Gobierno, 2013) «garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques» y se reconoce al ciberespacio como un «... nuevo ámbito de relación que ha proporcionado el desarrollo de las nuevas tecnologías de la información y las comunicaciones, ha diluido las fronteras, permitiendo una globalización sin precedentes, que propicia nuevas oportunidades, pero conlleva serios riesgos y amenazas.»

Para ello, en diciembre de 2013, se publicó la Estrategia de Ciberseguridad Nacional. Entre los objetivos de la misma destaca el Objetivo V (Presidencia del Gobierno, 2013): «Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad«.

Como justificación del objetivo en el documento se incluye que «Es importante, además, fomentar y potenciar las capacidades tecnológicas precisas para disponer de soluciones nacionales confiables que permitan proteger adecuadamente los sistemas frente a las diferentes amenazas». Para alcanzar este objetivo la Estrategia concluye que «se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva».

Al igual que en la estrategia europea, se identifica la actividad innovadora en ciberseguridad como un punto fundamental para garantizar la confianza en la sociedad digital, aunque en el caso de la española no se hacer referencia a la necesidad de contar con mayor presencia en el mercado global de productos de ciberseguridad.

Para alcanzar los objetivos, la Estrategia de Ciberseguridad Nacional se articula a través de una serie de líneas de acción. El objetivo de innovación en ciberseguridad se cubre en la línea de acción 6: «Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad». En el desarrollo de la línea de acción el Gobierno se compromete a «Extender y ampliar los programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con Universidades y centros especializados» y «Fomentar el desarrollo industrial de productos y servicios en materia de ciberseguridad por medio de instrumentos, entre otros, como el Plan Estatal de Investigación Científica y Técnica y de Innovación».

En paralelo, el Plan de confianza en el ámbito digital, en respuesta al objetivo cuatro de la Agenda Digital para España, «Reforzar la confianza en el ámbito digital», identifica como objetivo específico «Contribuir a que la industria, el sector académico y los profesionales aprovechen la oportunidad de la confianza digital para la innovación, la generación de talento y la investigación avanzada, especialmente en materia de ciberseguridad, construyendo un mercado de productos y servicios competitivo y de referencia internacional».

En resumen, tanto a nivel europeo, en la Estrategia de Ciberseguridad Europea, como a nivel estatal, en la Estrategia de Ciberseguridad Nacional y en el Plan de confianza en el ámbito digital, se identifican como clave la innovación en ciberseguridad. La innovación en ciberseguridad es estratégica no solo por ser clave para habilitar el crecimiento de la industria y sociedad digital sino también por las oportunidades de mercado para el desarrollo de nuevas tecnologías en este campo.

En este contexto de innovación, uno de los agentes que está ejecutando la estrategia es el Instituto Nacional de Ciberseguridad (INCIBE). INCIBE es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación española y empresas, especialmente para sectores estratégicos.

Entre las actividades llevadas a cabo por INCIBE para el fomento de la innovación en ciberseguridad destaca el impulso del «Estudio de la viabilidad, oportunidad y diseño de una Red de Centros de Excelencia en I+D+i en ciberseguridad». Este estudio fue el germen de la creación de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), asociación sectorial que engloba centros de investigación, universidades y otros agentes del ecosistema investigador de ciberseguridad en España. Entre los principales objetivos de RENIC están:

- Aglutinar la experiencia necesaria para fomentar el posicionamiento, competitividad y liderazgo del sector de ciberseguridad a nivel internacional.
- Lograr la cooperación de los agentes expertos en ciberseguridad, sirviendo de nexo de unión de cara a posibles colaboraciones.
- Difundir los resultados de investigación promoviendo la trasferencia de conocimiento y de soluciones a la industria.

INCIBE también participa en iniciativas de Compra Pública Innovadora en ciberseguridad que pueden suponer un gran impulso para el desarrollo de soluciones nacionales en este sector. De manera similar, en el contexto de las Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), promueve que las empresas planteen a la comunidad investigadora los desafíos de seguridad a los que están expuestas y que no están adecuadamente cubiertos por productos existentes.

TENDENCIAS EN CIBERSEGURIDAD

Una vez establecida la necesidad de invertir en innovación en ciberseguridad, el objetivo del apartado actual es centrarnos en qué aspectos de la ciberseguridad innovar. Si bien existen multitud de tecnologías y campos donde la innovación en ciberseguridad es beneficiosa, se incluyen a continuación aquellos que consideramos más relevantes.

Inteligencia Artificial

Paseando por cualquiera de las ferias de seguridad informática es fácil ver que los principales fabricantes de productos de ciberseguridad, principalmente los emergentes, están apostando por la Inteligencia Artificial para mejorar las capacidades de sus productos, ya sean antivirus, sistemas de detección de intrusión, sistemas de gestión de eventos de seguridad, cortafuegos, detectores de spam, etc., pero por ahora son pequeñas funcionalidades construidas sobre el núcleo de sus productos. Los algoritmos de Inteligencia Artificial, por su capacidad de aprendizaje, son una tecnología apropiada para un problema, los ciberataques, que evolucionan constantemente para evitar las herramientas de detección. Se busca, por tanto, invertir el paradigma clásico en ciberseguridad, según el cual las medidas defensivas siempre van detrás de las técnicas que desarrollan los atacantes. La aplicación de IA a la ciberseguridad es un campo emergente, influido también, por supuesto, por el efecto en marketing de palabras como *Machine Learning, Deep Learning,* etc. Así y todo, con la aplicación de IA se espera una nueva generación de productos que mejoren la seguridad al mismo tiempo que disminuyen los costes asociados a su gestión.

El concepto de aplicar la Inteligencia Artificial al campo de la ciberseguridad no es nuevo. Cuando Willian Gibson escribió la novela Neuromante en 1984, años antes del nacimiento de la *World Wide Web*, no solo se anticipó a la realidad de un mundo hiperconectado,

sino que predijo también los problemas de ciberseguridad que vendrían asociados. En la novela, Case, el antihéroe y hacker (*cybercowboy* en el texto de Gibson), es contratado para vulnerar la seguridad de un sistema crítico de una gran corporación. Este tipo de ataques, técnicamente avanzados, empleando el ciberespacio y bien financiados, no nos son desconocidos a día de hoy, de hecho nos referimos a ellos como Amenazas Persistentes Avanzadas (APT, *Advanced Persistent Threats).*

En la novela de Gibson, las corporaciones protegen sus sistemas de información más críticos empleando herramientas de detección y neutralización de ataques, conocidas por el acrónimo ICE (*Intrusion Countermeasures Electronics).* El equivalente en nuestra realidad son los sistemas de detección o prevención de intrusión (IDS, *Intrusion Detection System* – IPS, *Intrusion Prevention System).* En Neuromante, las versiones más avanzadas de ICE, denominadas *Black ICE*, son controladas mediante una Inteligencia Artificial.

Uno de los principales problemas en la detección y prevención de intrusiones es la cantidad ingente de información a analizar, en la que hay que buscar patrones que indiquen ataques, intentos de modificaciones no autorizadas en los sistemas de información o exfiltración de datos de la organización. Los sistemas de detección de intrusión tradicionales se basan en la comparación de los datos de tráfico de red o de acceso y uso de los sistemas con patrones de ataques conocidos, pero son ineficaces en la detección de nuevas técnicas de ataque o en modificaciones de las ya existentes. Son estas vulnerabilidades las que utilizan los atacantes para pasar inadvertidos.

El uso de técnicas de Inteligencia Artificial en sistemas de detección de intrusión u otros sistemas como antivirus, permitiría la detección de los ataques, no mediante el uso de patrones conocidos como de ataque, sino mediante el aprendizaje de lo que es normal en una organización: su tráfico de red, el patrón de acceso a los sistemas y aplicaciones, el comportamiento de sus usuarios,… Los sistemas de ciberseguridad basados en Inteligencia Artificial podrían detectar si una determinada actividad en los sistemas de información de una organización es anómala e informar de ello a los analistas de seguridad.

Si bien ya se está aplicando la Inteligencia Artificial en productos de ciberseguridad, todavía existe mucho campo de mejora. El principal sería la reducción de los falsos positivos, es decir, cuando se alerta al analista de seguridad de una potencial amenaza que resulta ser falsa. Los sistemas actuales tienen un índice alto de falsos positivos, lo que aumenta el trabajo de los analistas y reduce la eficiencia de la gestión de la seguridad. El uso del conocimiento en el proceso de toma de decisiones en ciberdefensa requiere un soporte de decisión inteligente que se puede lograr con éxito usando métodos de inteligencia artificial (Dilek, Çakır, & Aydın, 2015).

Criptografía – Protección de la información

La seguridad de la información girar alrededor de tres dimensiones a proteger: confidencialidad, integridad y disponibilidad. Las dos primeras se han protegido tradicionalmente utilizando criptografía. Dentro del campo de la criptografía destacan dos tendencias innovadoras: procesado seguro de la información y criptografía post-cuántica.

Procesado seguro de la información

La información se debe proteger de accesos no autorizados en todo el ciclo de vida de la misma, desde su creación hasta su destrucción. En ese ciclo de vida la información se presenta en tres estados: Transmisión, almacenamiento y procesamiento. Con la tecnología existente a día de hoy es relativamente sencillo proteger la información en transmisión y almacenada. Sin embargo, asegurar que la información no es accedida por terceros no autorizados mientras se procesa es un problema más complejo de resolver. Este problema tiene especial protagonismo por la adopción de servicios de *Cloud Computing*, donde la información de las organizaciones se procesa en infraestructura de terceros.

Existen dos aproximaciones para la protección del procesado de la información. La primera se basa en el uso de elementos hardware, que pueden ir desde los tradicionales HSMs (*Hardware Security Modules)* a otras plataformas conocidas como enclaves seguros basadas en hardware embebido en microprocesadores. En ambos casos se protege el procesado de la información proporcionando un entorno confiable, externo en el caso de los HSM e interno en caso de los enclaves. Los HSMs son grandes soluciones para problemas específicos de dominio, por ejemplo la verificación de PIN o de transacción EMV en el dominio financiero, pero requieren de innovaciones que faciliten su uso y su extensión a otros dominios, por ejemplo el voto electrónico. Respecto a los enclaves seguros es necesario buscar soluciones que permitan su escalabilidad en entornos Cloud (Beekman & Porter, 2017).

La segunda aproximación, la más innovadora, no utiliza hardware específico sino que se basa en una propiedad de la que habría que dotar a los criptosistemas denominada homomorfismo. Un criptosistema homomórfico tiene la propiedad de permitir operar con los datos cifrados de una manera análoga a la que se operaría con los datos en claro. La existencia de este tipo de criptosistemas era teórica hasta que Craig Gentry en su tesis doctoral diseño el primer sistema totalmente homomórfico (Gentry, 2009).

Los criptosistemas homomórficos suponen un gran avance para la protección del procesado de la información en entornos no confiables sin necesidad de utilizar hardware especializado. Un posible campo de aplicación es el procesado de algoritmos de identificación biométrica en el Cloud, especialmente ahora que el Reglamento General de Protección de Datos (REGLAMENTO (UE) 679, 2016) ha clasificado los datos biométri-

cos para identificación como particularmente sensibles. Aun así existen grandes desafíos en este campo, como pueden ser disminuir la capacidad de cómputo necesaria para el procesamiento de los datos cifrados o simplificar el uso de los algoritmos existentes para facilitar su implantación.

Criptografía post-cuántica

Se han producido grandes inversiones en los últimos años para lograr un computador cuántico universal. El impacto en criptografía sería dramático ya que este tipo de computadores podrían resolver los problemas de factorización de enteros y el logaritmo discreto en tiempo polinómico, lo que comprometería la seguridad de los criptosistemas de clave pública RSA y curva elíptica, utilizados en la actualidad para proteger la mayor parte de las comunicaciones por Internet (Nguyen, 2017).

Este problema no solo comprometería la confidencialidad e integridad de la información una vez se desarrolle el computador cuántico universal sino que comunicaciones cifradas actuales podrían ser almacenadas y desveladas en el futuro. Por ello es fundamental el desarrollo de nuevos criptosistemas de clave pública cuya seguridad no esté amenazadas por la capacidad de procesamiento de computadores cuánticos. En la actualidad existen varias propuestas de criptosistemas post-cuánticos, pero es un campo en el que se espera gran actividad en los próximos años.

Biometría para verificación de identidad

La identidad, y su verificación, es una de las dimensiones básicas de la seguridad de la información. La seguridad de la información debe proteger que solo aquellos individuos con permisos puedan acceder o modificar determinada información. Para ello es imprescindible contar con mecanismos que permitan, con un nivel adecuado de certeza, garantizar que un individuo es quien dice ser.

Las soluciones clásicas, basadas en usuario y contraseña, fueron diseñadas para otras necesidades, sistemas de información centralizados para uso interno dentro de organizaciones. Su uso en un mundo hiperconectado ha dado lugar a numerosas incidencias de seguridad, principalmente debido a bases de datos de usuarios y contraseñas comprometidos y hecho públicos en Internet o ataques de *phising*. Es un grave problema que hoy en día existan servicios en Internet que basen la verificación de identidad exclusivamente en esquemas de usuario y contraseña.

Se podría pensar que los retos asociados a la verificación de identidad ya están resueltos. La tecnología de certificados electrónicos e infraestructuras de clave pública está ampliamente extendida y regulada por el reglamento EIDAS (Reglamento (UE) n ° 910, 2014) que establece los requisitos para certificados electrónicos, firma electrónica y proveedores de servicios de confianza. El uso de certificados electrónicos para la firma de contratos es el preferido en la Ley de Comercio Electrónico (LSSI) (Ley 34, 2002) y también la legislación que regula el funcionamiento de la Administración Pública (Ley 39, 2015) (Ley 40, 2015) los contempla. Pero, siendo así, ¿por qué la adopción de este sistema no está siendo la esperada?

El principal problema para la adopción es la usabilidad. Por ejemplo: el DNI electrónico; incorpora certificados electrónicos que permiten la autenticación y la firma de documentos, cada ciudadano tiene el suyo y está aceptado en las sedes electrónicas de las Administraciones Públicas y en la mayor parte de los servicios de banca electrónica. Además, aunque sufrió un grave problema de seguridad causado por el fabricante del chip que incorpora (CVE, 2017) (Nemec, Sys, & Svenda, 2017), es una tecnología segura, que obliga a disponer del DNI físico y conocer una clave secreta. Aun así, su uso por parte de la ciudadanía es mínimo. En la campaña de la renta de 2012, al finalizar la campaña en julio de 2013 tan solo un 0,7% de los certificados utilizados se correspondía al DNI Electrónico (Fundación Orange, 2014). La causa es que el uso del DNI Electrónico, aunque seguro, es complejo para el ciudadano medio. Las tecnologías no solo deben ser seguros sino que deben tener en cuenta la usabilidad para garantizar su adopción.

Otro problema de la adopción de certificados es electrónicos es su seguridad. En el caso de certificados software, que no están protegidos ningún hardware como una *smartcard*, no dan garantías suficientes de seguridad a las corporaciones para usarlos en sus procesos. Por ejemplo, los certificados de la FNMT, aunque ampliamente aceptadas en Administración Electrónico no son admitidos en banca electrónica.

La biometría es una tecnología de verificación de identidad que está ganando fuerza principalmente por su gran usabilidad, especialmente en dispositivos móviles. Los usuarios utilizan cada vez más distintas modalidades de biometría: cara, huella dactilar, voz,... para acceder a través de sus móviles a servicios bancarios y pasarelas de pago. Su uso es rápido y sencillo, aunque existen diversos retos que se deben abordar para garantizar su seguridad.

El mecanismo más habitual para intentar vulnerar sistemas de verificación de identidad basados en biometría es el ataque de presentación. El atacante presenta al sensor que va a capturar los rasgos biométricos una representación de los mismos. Por ejemplo en biometría de cara se podría presentar una fotografía del individuo o suplantar, en biometría de voz una grabación o en biometría de huella dactilar una huella falsa de silicona.

Es necesario el desarrollo de tecnologías innovadoras que posibiliten la adopción segura de tecnologías biométricas que los usuarios demandan por su usabilidad y conveniencia. Entre las tecnologías en las que se trabaja para mejorar la seguridad ante ataques de presentación están las siguientes:

– Detección de vida (*Liveness detection):* Tecnologías que permitan garantizar que no estamos ante una

reproducción. Estas tecnologías pueden ser colaborativas, donde se le solicita al usuario que realice una determinadas acción, por ejemplo un gesto en el caso de biometría de cara a repetir unas palabras aleatorias en caso de biometría de voz. También pueden ser no colaborativas, donde se utilizan avances en la visión por computador para detectar anomalías que indiquen un ataque de presentación.

– Fusión de biometrías: Combinación simultánea de varias biometrías para disminuir la eficacia de un ataque de presentación. Por ejemplo, capturar cara y voz al mismo tiempo.

Otro de los retos en el campo de la biometría es la protección de la privacidad. El nuevo reglamente europeo de protección de datos (REGLAMENTO (UE) 679, 2016) ha incluido los datos biométricos para identificación entre los datos especialmente sensibles a proteger. Es evidente que un mal uso de estas tecnologías, como la identificación masiva de personas mediante cámaras en lugares públicos o mediante fotos en redes sociales, es una amenaza a la privacidad. Para ello se deben desarrollar tecnologías que protejan adecuadamente la información biométrica. Las tecnologías comentadas en el punto anterior, principalmente las relativas al procesado seguro de la información en el dominio cifrado son un ejemplo de ellas.

La biometría también abre nuevas oportunidades, como su uso para el alta de nuevos clientes mediante la comparación automática de la fotografía en documentos de identidad con un vídeo (*digital onboarding*). Esta tecnología tiene especial aplicación en sectores donde la verificación de identidad en el momento de contratar productos tiene especial relevancia y por ello están especialmente regulados, como puede ser el sector bancario o los proveedores de servicios de confianza.

Otra oportunidad es su uso en aplicaciones donde es necesario que la verificación se realice de forma continuada y no como un proceso independiente al inicio. Por ejemplo, posibilitaría la realización de exámenes online u el acceso remoto a información especialmente sensible.

Privacidad

El derecho a la privacidad, regulado por el Reglamento General de Protección de Datos (REGLAMENTO (UE) 679, 2016), está profundamente ligado con la seguridad de la información, la obligación de proteger adecuadamente los datos personales. Adecuadamente no es un adverbio vacío de significado en la oración anterior; la protección de los datos personales debe ser la que se adecue a las necesidades de cada organización tras un análisis de los riesgos de privacidad a los que están expuestos los datos que maneja, que no son suyos sino de las personas asociadas.

Sobre tecnologías innovadoras en protección de la información hemos hablado en el apartado anterior, pero en este punto nos gustaría resaltar dos aspectos tecnológicos adicionales relacionados con la privacidad:

Identidades digitales seguras

La gestión de la identidad es clave para un correcto funcionamiento de los servicios proporcionados a través de Internet. Es necesario lograr un equilibrio entre la necesidad de asegurar la identidad, por parte de los proveedores de servicios, para evitar fraudes y la protección de la privacidad de las personas. Mientras que las empresas deben poder contar con los medios necesarios de identificación de identidad para poder tomar medidas legales contra comportamientos fraudulentos los ciudadanos deben tener derecho a disfrutar de cierto nivel de anonimato al contratar servicios o adquirir productos.

La innovación en tecnologías de identidad seguras debe proporcionar mecanismos para proveer de anonimato cualificado. La identidad digital no debería ser un elemento absoluto, que identifique completamente a un individuo, sino un conjunto de atributos cualificados y verificables, de manera que las empresas tengan seguridad sobre los datos que necesitan, por ejemplo: una dirección, la mayoría de edad, etc., pero no el conocimiento completo de la identidad. Para la creación de estas identidades digitales sería necesario contar con un ecosistema de verificadores de atributos de identidad. Por ejemplo: una operadora de telecomunicaciones podría certificar la posesión de un número de teléfono por parte de un individuo, un ayuntamiento su residencia, una universidad la posesión de un título, un banco la titularidad de un número de cuenta,... Estos atributos verificables de identidad permitirían a los ciudadanos la contratación de servicios que los requieran, proporcionando garantías a las empresas, pero sin revelar su identidad completa a las mismas.

Tecnologías como blockchain pueden servir de base para la construcción de plataformas de identidades seguras, donde de una manera descentralizada, empresas, administraciones públicas y ciudadanos puedan solicitar, almacenar y verificar los atributos de identidad. Blockchain actuaría como registro inmutable y transparente de las identidades, permitiendo a los ciudadanos demostrar ante terceros determinados datos personales sin dar a conocer su identidad.

Anonimización

Hoy en día los datos tienen un gran valor. Gracias a tecnologías de análisis de información a las que denominamos *Big Data*, podemos procesar, analizar y compartir cantidades masivas de datos, con enormes beneficios en distintos dominios. Por ejemplo, datos de estudios clínicos realizados en los servicios de salud son de gran valor para investigadores para el desarrollo de nuevos fármacos. Para ceder esos datos, el servicio de salud debería recabar el consentimiento expreso, inequívoco y verificable de cada uno de los pacientes informando

claramente del organismo destino y de la finalidad de la cesión; este proceso es complejo y conlleva riesgos evidentes de incumplimiento normativo.

Una alternativa a los consentimientos es eliminar los datos personales de manera que el conjunto de datos resultante quede fuera del ámbito de aplicación de la RGPD. Para ello es imprescindible que este procesos, conocido como anonimización, sea irreversible, es decir, que con los datos resultantes y otras fuentes de información no sea posible re-identificar a un individuo en el conjunto de datos anonimizados.

Por ello, las tecnologías de anonimización son una herramienta fundamental para poder extraer, compartir y transferir el valor oculto en grandes conjuntos de datos, al mismo tiempo que se garantiza la privacidad de las personas y el cumplimiento normativo de las organizaciones. Las tecnologías de anonimización deben estar orientadas a riesgos, proporcionando a los responsables de los datos del nivel de anonimización resultante, de manera que puedan tomar decisiones informadas y diligentes al compartir los datos. Estas tecnologías también deben ser capaces de medir la utilidad de los datos anonimizados y ayudar a buscar puntos óptimos de equilibrio entre utilidad y anonimización.

Internet of Things (IoT)

IoT se ha definido como una arquitectura emergente de información basada en Internet que facilita el intercambio de bienes y servicios en una cadena global de suministro. Por ejemplo, la carencia de algún bien puede ser automáticamente reportada a un proveedor que responderá inmediatamente con la entrega, electrónica o física, del bien (Weber, 2010).

La seguridad en IoT es aspecto que ha alcanzado especial relevancia, tanto por ataques provenientes de dispositivos IoT (Krebs, 2016) como por su importancia para el desarrollo de la Industria 4.0 (*European Factories of the Future Research Association*, 2016).

Las especificidades de los dispositivos IoT en relación a la ciberseguridad son las siguientes:

- Su gran número y dispersión: Los analistas de la industria prevén que el número de dispositivos conectados a redes móviles alcance los 50.000 millones en el año 2020 (National Instruments, 2015).
- Su escasa capacidad de almacenamiento y procesamiento que dificulta o imposibilita incorporar funciones de seguridad como cifrado.
- Su capacidad, en algunos casos, de actuar sobre el mundo físico, en particular en el entorno industrial o en infraestructuras críticas.
- Su uso para obtener y transmitir datos privados, por ejemplo los destinados a teleasistencia.

Es necesario, por tanto, desarrollar tecnologías de ciberseguridad que permitan el uso seguro de arquitecturas distribuidas basadas en dispositivos IoT. En particular, se deberían explorar nuevos aspectos tales como: criptografía ligera para dispositivos de baja capacidad, arquitecturas de gestión de identidad ligeras, escalables y descentralizadas, monitorización eficiente de políticas de seguridad en sistemas altamente distribuidos y tecnologías de protección del derecho a la intimidad.

Blockchain

El *blockchain* nace en el año 2009 como solución para crear una moneda electrónica, Bitcoin, que pueda ser transmitida entre dos entidades sin necesidad de una institución financiera. La solución se basa en una estructura de bloques enlazados, que contienen las transacciones, cuyo consenso sobre el contenido de cada uno de ellos se alcanza mediante la combinación de una prueba de trabajo (*proof-of-work)* y una recompensa (Nakamoto, 2009). La seguridad de la solución se basa en parte en conceptos económicos, donde los nodos distribuidos en la red, conocidos como mineros, se comportan de modo honesto por el coste de oportunidad asociado a la prueba de trabajo. Aunque su uso original era exclusivamente permitir el funcionamiento de una moneda electrónica descentralizada fue el nacimiento de la tecnología de libro de cuentas distribuido (DLT, *Distributed Ledger Technology)*, una tecnología descentralizada que permite crear un registro inalterable consensuado entre varios participantes.

En los últimos años han surgido varias iniciativas basadas en DLT. Desde iniciativas abiertas, similares a Bitcoin, pero con otras metas, como la creación de aplicaciones descentralizadas utilizando programas que se conocen como *smart contracts*, a iniciativas cerradas, donde solo un conjunto de organizaciones están autorizadas a realizar escrituras y/o lecturas sobre el *blockchain.*

Si bien es cierto que existen numerosos detractores que opinan que *blockchain* tan solo es eficaz para monedas electrónicas y que, por su carácter descentralizado, no es una solución adecuada para empresas (Sztorc, 2016), también es cierto que los conceptos y tecnologías detrás de *blockchain* se están viendo con gran interés tanto por parte de la comunidad investigadora como por parte de la industria por lo que es más que probable que en los próximos años continúe la tendencia de aplicar DLT a diversos ámbitos: gestión de la identidad, logística, transacciones financieras, certificados de autenticidad, cadena de suministro, etc.

CONCLUSIÓN

La innovación en ciberseguridad es estratégica no solo por ser clave para habilitar el crecimiento de la industria y sociedad digital sino también por las oportunidades de mercado para el desarrollo de nuevas tecnologías en este campo. En este sentido, es fundamental que en Europa en general y en España en particular se fomente y cultive la investigación y desarrollo en ciberseguridad, creando un ecosistema que facilite la innovación y la adopción por parte de la industria de las tecnologías desarrolladas. Estas ideas están presentes tanto en la

estrategia europea como en la española en materia de ciberseguridad, concretándose en el caso de la europea en el programa marco H2020. A nivel nacional están empezando a surgir en el sector público iniciativas de compra pública innovadora en materia de ciberseguridad que pueden suponer un gran impulso para el desarrollo de soluciones nacionales en este sector. El sector privado podría jugar igualmente un papel habilitador planteando a la comunidad de I+D+i de ciberseguridad los desafíos a los que se enfrentan que no están suficientemente resueltos en los productos en mercado.

BIBLIOGRÁFIA

Beekman, J. G., & Porter, D. E. (2017). *Challenges For Scaling Applications Across Enclaves.*

CVE. (2017). *CVE-2017-15361.*

Dilek, S., Çakır, H., & Aydın, M. (2015). *Application of Artificial Intelligence techniques to combating cyber crimes: A review.*

ECSO - European Comission. (2016). *Contractual arrangement setting up a Public-Private Partnership in the area of cybersecurity industrial reserarch and innovation.* Estrasburgo.

ECSO. (2016). *European Cybersecurity Proposal for a contractual Public-Private-Partnership.*

ECSO. (2016). *European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a cPPP.*

EOS. (2015). *Cybersecurity for a trusted EU Digital Single Market - EOS Market Study for a Cybersecurity Flagship Programme.*

European Comission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Brussels.

European Factories of the Future Research Association. (2016). *Factories 4.0 and beyond.*

Eurostat. (2017). *E-commerce sales.* Obtenido de https://ec.europa.eu/eurostat

Eurostat. (2017). *E-government activities of individuals via websites.* Obtenido de https://ec.europa.eu/eurostat

Eurostat. (2017). *Integration of internal processes*. Obtenido de https://ec.europa.eu/eurostat

Eurostat. (2017). *Internet purchases by individuals.* Obtenido de https://ec.europa.eu/eurostat

Fundación Orange. (2014). *Informe eEspaña.*

Gentry, C. (2009). *A fully homomorphic encryption scheme.*

Krebs, B. (2016). *Source Code for IoT Botnet 'Mirai' Released.* Obtenido de https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

Ley 11. (2007). *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.*

Ley 30. (1992). *Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.*

Ley 34. (2002). *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*

Ley 39. (2015). *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

Ley 40. (2015). *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.*

Ministerio del Interior. (2017). *Estudio sobre la criminalidad en España.*

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

National Instruments. (2015). *5G: The Internet for Everyone and Everything.* Obtenido de ww.ni.com/pdf/company/en/Trend_Watch_5G.pdf

Nemec, M., Sys, M., & Svenda, P. (2017). *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli.*

Nguyen, P. Q. (2017). *Quantum-Safe Cryptography.*

OBSAE. (2018). *DATAOBSAE - Área Atencion Ciudadano y Empresa.* Obtenido de https://dataobsae.administracionelectronica.gob.es

Palmer, D. (2017). *AI will supercharge spear-phishing.* Obtenido de https://www.darktrace.com/blog/ai-will-supercharge-spear-phishing/

Presidencia del Gobierno. (2013). *Estrategia de Ciberseguridad Nacional.*

Presidencia del Gobierno. (2013). *Estrategia de Seguridad Nacional.*

REGLAMENTO (UE) 679. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.*

Reglamento (UE) n ° 910. (2014). *Reglamento (UE) n ° 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.*

Sztorc, P. (2016). *Private Blockchains, Demystified.* Obtenido de http://www.truthcoin.info/blog/private-blockchains/

Weber, R. H. (2010). *Internet of Things – New security and privacy challenges.*