La calificación de la seguridad de los sistemas de información en Europa

Manuel Carpio | Responsable académico del área de ciberseguridad, IMF Smart Education

Tema

La UE debería adoptar e impulsar los modelos basados en calificación (rating) de seguridad como complemento e integración de los múltiples esquemas de certificación de productos y servicios basados en tecnologías de la información y comunicaciones.

Resumen

La UE y sus Estados miembros exigen a las cadenas de suministro de tecnologías de la información y comunicaciones (TIC) la certificación del cumplimiento de variadas normas y estándares para poder comercializar sus productos o servicios con seguridad. Certificar la seguridad de los sistemas no es fácil, porque el nivel de exigencia varía dentro de las cadenas de suministro, ni sencillo, porque se multiplican las normas a cumplir sin disponer de un modelo unificado de calificación de ciberseguridad. Este análisis expone los antecedentes del proceso de certificación de la UE, las dificultades para su gestión eficaz y el modelo de calificación en seguridad como solución a los problemas mencionados.

Análisis

El Convenio de París de 1919 estableció la primera reglamentación para la navegación aérea internacional. Entre otras normas para poder volar, se exigía a las aeronaves disponer de un certificado de navegabilidad expedido por la autoridad competente. A lo largo de los últimos 100 años, todas las compañías, desde la industria del transporte hasta la manufacturera del juguete, han necesitado exhibir diversos certificados de conformidad respecto de reglamentaciones oficiales o estándares de la industria para poder comercializar sus productos o servicios.[1]

Sin embargo, hasta hace poco no ha existido un convenio para la certificación de la seguridad de productos relacionados con las tecnologías de la información y comunicaciones (TIC) como pudiera ser, por ejemplo, una tarjeta *chip* o un sistema operativo. Incluso hoy se carece de unos estándares que certifiquen la seguridad intrínseca y global de sistemas complejos, con base en diversos productos *hardware* y *software*, como, por ejemplo, un sistema de control de tráfico aéreo o un sistema de información electoral. Sin embargo, y paradójicamente, sí que existen estándares que permiten emitir certificados de conformidad para el sistema de gestión de la seguridad

[1] Por ejemplo, la etiqueta de conformidad europea, según la Directiva 93/68/CEE, visible en muchos productos que se utilizan a diario. Véase https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31993L0068&from=ES.

de dichos sistemas, es decir, para las tareas llevadas a cabo por la organización que los opera y mantiene.

Europa se ha convertido en una colonia tecnológica norteamericana y china. La llegada masiva de sistemas basados en comunicaciones 5G ha encendido las alarmas. La falta de control sobre la multiplicidad de proveedores que han intervenido en la fabricación de cada producto intenta paliarse con recomendaciones específicas (EU 5G Toolbox)[2] y actualización del marco regulatorio (NIS),[3] dirigida a los operadores de infraestructuras críticas que los incorporan y servicios esenciales que se prestan a los ciudadanos europeos.

Asegurar la red y los sistemas de información en la UE se considera un objetivo clave como parte del esfuerzo por mantener la economía en línea funcional y segura. Si esto no se hace, podría afectar a la confianza de los ciudadanos, a la industria y a la Administración pública, lo que implicaría consecuencias de gran alcance. Así, por ejemplo, cuando subamos a un automóvil sin conductor, además de ver los diversos sellos o etiquetas correspondientes a los variados controles de calidad que se han pasado a cinturones, *airbags*, antiderrape y otros sistemas de seguridad, deberíamos poder ver también una única etiqueta que comunique de forma sencilla, el nivel de ciberseguridad global del vehículo.

La Ley de Ciberseguridad Europea[4] de 2019 encomendó a la Agencia Europea de la Seguridad de la Información y de las Redes (ENISA) la coordinación de los esfuerzos en normalización y certificación en todos los ámbitos de la seguridad de la información: productos, sistemas, servicios y procesos mediante esquemas de certificación válidos en toda la UE.

Su elaboración tiene como objetivo proporcionar los criterios para que organismos independientes y debidamente acreditados puedan llevar a cabo evaluaciones de conformidad que establezcan el grado de adherencia de los productos, servicios y procesos. Todo esto siguiendo una lista de requisitos específicos para que finalicen con la emisión de un certificado que indique conformidad. Además, cada esquema de certificación especificará uno o más niveles de garantía (básico, sustancial o alto), con base en el nivel de riesgo asociado al uso previsto del producto, servicio o proceso. De igual manera, las certificaciones emitidas bajo un determinado esquema serán, de momento, voluntarias, aunque se deja abierta la posibilidad de que algún día la Comisión las convierta en obligatorias.

[2] NIS Cooperation Group (2020), "Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures", 29/I/2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[3] 'Propuesta de Directiva del Parlamento y del Consejo COM (2020) 823 final relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148', Bruselas, 16/XII/2020, https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)823&lang=en.

[4] Reglamento (UE) 2019/881 de 17 de abril de 2019 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

Se observan ya dos candidatos a esquemas de certificación: uno para servicios prestados desde la nube (*European Cybersecurity Certification Scheme for Cloud Services*, EUCS)[5] y otro para productos varios (*Common Criteria Based European Candidate Cybersecurity Certification Scheme*, EUCC)[6] que verán la luz en breve, previsiblemente. Pero, ¿qué ocurre con la certificación de los sistemas complejos? Probablemente se optará por esquemas que resulten de la composición o "ensamblaje" de las certificaciones de sus componentes, como si se tratase de un *puzzle*, aunque todo el mundo es consciente de que la mera combinación de productos seguros no garantiza que el resultado sea un sistema seguro.

La dificultad de certificar

Yendo más arriba en la escala, se encontraría la certificación de la seguridad de los procesos y de su gestión. Como se mencionaba anteriormente, en este nivel sí que es posible encontrar multitud de regulaciones, estándares, guías de buenas prácticas, etc., publicadas tanto por organismos públicos como privados, sectoriales (banca, telecomunicaciones, industria, etcétera) o genéricos. Tantos que, como dice con fina ironía el profesor Andrew S. Tanenbaum: "lo bueno de los estándares es que hay muchos donde elegir".

De entre todos estos, sólo unos pocos son certificables. Por citar algunos, en España y para la Administración pública existe el Esquema Nacional de Seguridad (ENS),[7] el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS,[8] que se enfoca en la utilización de medios de pago por tarjeta), el Reglamento General de Protección de Datos (RGPD,[9] que atiende a las cuestiones relacionadas con la privacidad) y la norma ISO 27001[10] (que se orienta a la gestión de la seguridad de la información en las empresas TIC en general). Por supuesto, se obvia una larga lista de siglas que sería interminable.

Como resultado, y con el modelo actual (al que podríamos denominar "modelo *collage*") de regulaciones oficiales y estándares de la industria, por ejemplo, una entidad financiera o un prestador de servicios de telecomunicaciones, para poder ofrecer sus servicios en España, se ve obligado a demostrar que está en posesión de no menos de media docena de certificados relacionados con la gestión de la seguridad de la información y las infraestructuras sobre las que se prestan. Si se examinan en detalle, se comprobará que el 80% de los controles de seguridad que exigen estas normativas son esencialmente los mismos. Este hecho parecería divertido si no fuera porque los

[5] EUCS, https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

[6] EUCC, https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme.

[7] Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, https://www.boe.es/eli/es/rd/2010/01/08/3.

[8] PCI Security Standards Council, LLC. Requisitos y procedimientos de evaluación de seguridad. v3.2.1. mayo 2018.

[9] Reglamento (UE) 2016/679 de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32016R0679.

[10] ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements, https://www.iso.org/standard/54534.html.

procesos de auditoría para la certificación son largos, costosos y sobrecargan a las organizaciones.
Habitualmente, un certificado se emite por un período de validez de varios años (tres en el caso de la ISO 27001), y la entidad certificadora establece una pauta de al menos una revisión anual para cerciorarse de que no se están produciendo desviaciones respecto de la norma. Es un juego de "todo o nada", es decir, a pesar de revisar varias facetas de la seguridad y de que se "suspenda" en algunas de ellas, sería posible seguir teniendo el certificado "por el todo". De igual modo, por contra, se podría perder el certificado por culpa de alguna "no-conformidad" no resuelta, a pesar de ser excelentes en todo lo demás.

Para completar el panorama, las regulaciones oficiales en materia de ciberseguridad que han visto la luz recientemente, tanto sectoriales (DORA)[11] como generales (ISO 27036),[12] bien sean nacionales o europeas, exigen a las empresas que supervisen la ciberseguridad de sus proveedores, entre otras razones para evitar el temido "efecto dominó" en operadores de servicios esenciales.[13] En ocasiones, los *hackers* utilizan como caballo de Troya una pequeña empresa contratista, cuyas medidas de seguridad resultan más fáciles de sortear que aquellas de las que habitualmente disponen estos gigantes clientes suyos, y que tienen fácil acceso al corazón de sus infraestructuras.

El modelo de calificación en seguridad

En los últimos meses se ha desatado una suerte de "frenesí auditor" en el ecosistema empresarial, en un ambiente de desconfianza mutua en el que "nadie conoce a nadie". Infórmese el lector, y comprobará que las empresas que prestan servicios de auditoría informática tienen comprometido su calendario durante muchos meses. Llegamos así al problema de N^2 ("ene al cuadrado"), es decir, en un ecosistema en el que hay N empresas que se prestan servicios entre sí, pero en el que todas desconfían de todas, llevado al extremo, eso implica N*(N-1) auditorías. Si, además, estas empresas mantienen un número "M" de certificaciones, habría que añadir otras tantas auditorías. Una cantidad próxima a N^2.

Lo anterior propicia un grave problema de eficiencia en el ecosistema. En palabras de un consultor caro podría decirse que "el sistema no es escalable" y, tarde o temprano, colapsará porque los costes de transacción no lo harán eficiente frente a otros modelos más ágiles, pero no por ello menos garantistas, en otras regiones económicas.

Es necesario un modelo que evalúe la madurez alcanzada en materia de seguridad de la información, pero que sea más ligero, dinámico y, al mismo tiempo, más preciso que el "modelo *collage*" actual. Una alternativa integradora podría ser el modelo de "calificación en seguridad".

[11] Propuesta de Reglamento COM (2020) 595 de 24 de septiembre sobre la resiliencia operativa digital del sector financiero, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595.

[12] ISO/IEC 27036:2014 Information technology. Security techniques. Information security for supplier relationships, https://www.iso.org/standard/59689.html.

[13] La película *La jungla IV*, estrenada en 2007, plantea la posibilidad de que un grupo terrorista bloquee el sistema de ordenadores que controla las comunicaciones, el transporte y el suministro de energía de un país entero.

En los últimos años se han popularizado los modelos de calificación. Quizá el más conocido es el de calificación crediticia (también denominada *rating*), avalado por agencias como Moody's, Standard & Poor's o Fitch IBCA. Según este modelo, una tercera parte confiable e independiente, la agencia calificadora, valora la calidad de la deuda tomada por un prestatario, en base a la capacidad para generar flujos financieros, beneficios, volumen de deuda y crecimiento a medio o largo plazo en el caso de un país, y la califica utilizando una escala de hasta 20 niveles etiquetados (desde la AAA hasta la D).

Pero también existen otros modelos de calificación que resumen, dicho *grosso modo*, las complejidades técnicas inherentes al cálculo de la inercia térmica de un edificio o las emisiones contaminantes de vehículos a motor. Hoy en día, todo el mundo está habituado a ver estas etiquetas de eficiencia energética o contaminante, e incluso a exigirlas a la parte vendedora antes de adquirir una casa o un coche.

Conclusiones

Quién sabe. Quizá a no mucho tardar se vea alguna propuesta de integración de certificación de conformidad con regulaciones y estándares de seguridad TIC basados en modelos de calificación. Tal propuesta podría dar lugar a un etiquetado del tipo ABCD para empresas, servicios o sistemas complejos, donde cada una de estas letras representaría, por ejemplo, el nivel de madurez alcanzado en diferentes dominios o facetas de la seguridad. Esto ayudaría, sin duda, a despejar las desconfianzas actuales y a mejorar las eficiencias del ecosistema empresarial, pues satisfaría de forma rápida y sencilla, y de una sola vez, la necesidad existente de conocer si la calidad de la seguridad del servicio que se presta se corresponde con el precio que por él se paga.