CCCAB, la apuesta europea por la automatización en los Organismos de Certificación

El número de fabricantes que desean certificar la ciberseguridad de sus productos crece continuamente. Entre los estándares más utilizados internacionalmente se encuentra Common Criteria, cuyo proceso de certificación puede llegar a ser complejo y costoso. Ante tal problemática, una de las posibles mejoras que hay que implementar, a medio plazo, en las certificaciones de ciberseguridad consiste en la automatización de procesos mediante el desarrollo de herramientas como CCCAB, un proyecto financiado por la Comisión Europea en el marco del programa Connecting Europe Facility (CEF), que permite ahorrar tiempo y esfuerzo a los CABs (Certification Assessments Bodies), aligerando su carga de trabajo para optimizar la fase de certificación.

José Ruiz Gualda

Europa es una de las mayores potencias en cuanto a certificación de ciberseguridad se refiere, acumulando algo más de la mitad de las certificaciones que se han llevado a cabo hasta la fecha siguiendo el estándar *Common Criteria*, el más utilizado internacionalmente. El número de fabricantes/desarrolladores IT, ya sea de software, hardware o *firmware*, que requieren una certificación de ciberseguridad para sus productos es cada vez mayor. Esto incrementa notablemente el volumen de trabajo de los Organismos de Certificación que, como encargados de verificar el trabajo de los laboratorios evaluadores y de emitir los certificados de aquellos productos que han superado una evaluación de ciberseguridad, constituyen el último eslabón del proceso de certificación.

Además, Europa está decidida a liderar el sector de la ciberseguridad siendo la punta de lanza en estandarización y en certificación. Buena muestra de ello es la aprobación del Reglamento (UE) 2019/881, más conocido como 'Cyber Security Act', así como la preparación del futuro 'Cyber Resilience Act'. La Unión Europea, a través de su agencia de ciberseguridad, ENISA, está apostando por crear esquemas de certificación que sean comunes a toda Europa para facilitar una mayor cohesión del mercado interior y la mejora de la ciberseguridad a nivel europeo. Un ejemplo de ello es el denominado EUCC (*Common Criteria based European Cybersecurity Certification scheme*).

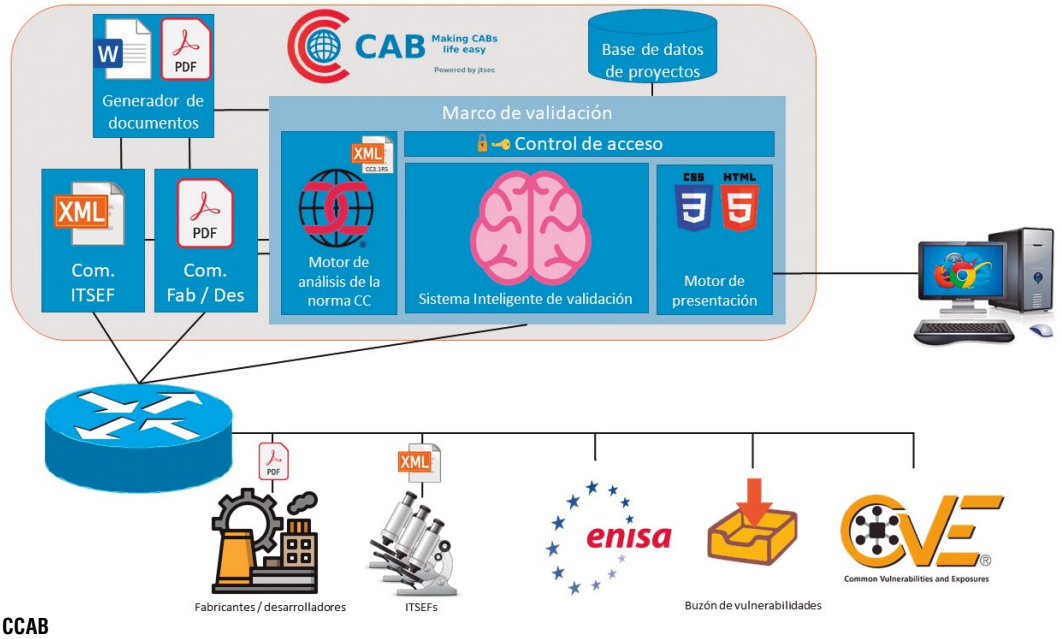
¿Qué es Common Criteria y quiénes son sus actores principales?

ISO/IEC 15408, más comúnmente conocido con el nombre de *Common Criteria*, es un estándar internacional para la evaluación de la seguridad de productos IT reconocido en más de 30 países. De hecho, es el estándar más utilizado con más de 400 productos certificados sólo en 2021.

Esta metodología de evaluación es muy completa, incluyendo análisis de vulnerabilidades, pruebas funcionales, revisión de la documentación de desarrollo y del ciclo de vida del producto. También es multinivel, permitiendo elegir el alcance y profundidad de la evaluación. Esta completitud implica que, cuando se eligen un alcance y profundidad elevados, la evaluación sea compleja, requiriendo un elevado coste en tiempo, recursos humanos y económicos, y que el proceso dure un mínimo de seis meses, pudiendo prolongarse varios meses más.

Son varios los actores involucrados en el proceso, tal y como vemos en el siguiente gráfico, siendo el desarrollador / fabricante, el laboratorio de evaluación y el organismo de certificación los principales.

En el caso de España, la función de organismo de certificación corresponde al **CCN** (**Centro Criptológico Nacional**) que, en los últimos cinco años, ha emitido 94 certificados *Common Criteria*, aunque el número total de expedientes que ha ges-



Arquitectura CCAB

tionado supera los 300 en este periodo de tiempo.

La carga de trabajo y la especialización que requiere este tipo de proyectos implica que los organismos de certificación manejen una elevada carga de trabajo por especialistas certificados, siendo la falta de personal un gran riesgo para el sector.

Automatización de procesos, el futuro de la certificación de ciberseguridad

Una mayor agilidad en la obtención de la certificación, para cumplir con el tiempo de comercialización de los productos, es uno de los grandes retos de mejora a los que nos enfrentamos todos los que formamos parte del mundo de la certificación de ciberseguridad.

Teniendo en cuenta el gran esfuerzo que supone crear una metodología de evaluación reconocida en el ámbito internacional, conllevando años de trabajo y de implicación por parte de numerosas entidades -tanto públicas como privadas- en diferentes países, no parece, al menos a corto-medio plazo, que la solución pase únicamente por la modificación sustancial de las normas de evaluación (se publicará próximamente una nueva versión de *Common Criteria*), sino que la propuesta más viable pasa por automatizar procesos, permitiendo así ahorrar tiempo y esfuerzo a la hora de realizar una evaluación de ciberseguridad.

Tanto en el ámbito privado, como en el público, han surgido a lo largo del tiempo diferentes iniciativas para automatizar ciertos procesos en las evaluaciones con *Common Criteria*. Entre ellas cabe destacar STGen, que actualmente se encuentra desarrollando NIAP (el organismo de certificación estadounidense) y que pretende automatizar la creación y validación de la declaración de seguridad (ST, por sus siglas en inglés) principalmente para los perfiles de protección *Common Criteria* utilizados en el mercado norteamericano. En cuanto a iniciativas privadas, cabe destacar CCToolBox, una herramienta desarrollada por **jtsec** y que permite automatizar sustancialmente los procesos de consultoría y evaluación bajo la metodología *Common Criteria*. También hay que poner de relieve Greenlight Conformance Automation Platform, una herramienta desarrollada por el laboratorio de ciberseguridad canadiense Lightship Security Inc, y que se basa en automatizar pruebas de evaluación de *Common Criteria*, creando reportes de las mismas.

Sin embargo, quedaba pendiente crear una herramienta que permitiese la automatización de procesos del último paso, la validación de las actividades de evaluación por parte de los organismos de certificación (CAB), motivo por el que surgió la iniciativa de desarrollar CCCAB.

CCCAB (Common Criteria Conformity Assessment Body)

Esta herramienta permitirá a los CABs (*Conformity Assessments Bodies*) de *Common Criteria* facilitar el proceso de validación y certificación de los productos TIC, asistiendo al certificador y reduciendo el esfuerzo y el tiempo necesarios en cada proceso.

El desarrollo de esta herramienta está financiado por la Comisión Europea en el marco del programa Connecting Europe Facility (CEF) y cuenta con tres participantes dentro del consorcio:

1. jtsec Beyond IT Security: Es la empresa encargada de todo el desarrollo de CCCAB.

2. CCN (**Centro Criptológico Nacional**): El Organismo de Certificación público español, designado por el Real Decreto 421/2004 de 12 de marzo, que validará la adecuación de las funcionalidades de la herramienta a las tareas de validación y certificación requeridas por los nuevos esquemas de certificación europeos.

3. Direzione Generale per le Tecnologie delle Comunicazioni e la Sicurezza Informatica - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (**ISCOM**). El Organismo de Certificación italiano tendrá un papel similar al del CCN, favoreciendo una doble verificación de la herramienta.

El proyecto CCCAB se inició en abril de 2021 y se desarrollará durante un período de dos años, por lo que se espera que esta herramienta esté disponible para abril de 2023. Durante estos 24 meses se irán cumpliendo los hitos marcados en la hoja de ruta del proyecto, que periódicamente se reportan a la Comisión Europea.

En este proyecto, financiado por la Comisión Europea, participan jtsec Beyond IT Security, el CCN-Centro Criptológico Nacional y la Direzione Generale per le Tecnologie delle Comunicazioni e la Sicurezza Informatica - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM) .

La herramienta se distribuirá como código abierto de manera gratuita a todos los CABs públicos o privados que estén interesados en la iniciativa.

Especificaciones técnicas y uso de CCCAB

CCCAB funcionará como un asistente que guiará al usuario paso a paso en la validación del trabajo del laboratorio, solicitando la introducción de la información necesaria para validar una evaluación. El asistente informará a los validadores del siguiente paso en el proceso de validación y detectará las partes de la validación que deben completarse o que presentan algún tipo de problema.

CCCAB también permitirá la gestión del conocimiento dentro del CAB, ya que será fácil añadir y comprobar los comentarios de los expertos y los consejos y sugerencias sobre cómo validar fácilmente los trabajos de evaluación siguiendo la norma *Common Criteria*, permitiendo escribir y generar informes de validación.

Las características y ventajas técnicas más destacadas que aportará el CCCAB podríamos resumirlas en los siguientes puntos:

- Gestión de proyectos y control de accesos para múltiples validadores con diferentes tipos de roles disponibles.
- Interfaz de usuario intuitiva y atractiva, permitiendo la configuración de colores y logotipos corporativos.
- Instalación sencilla.
- Edición web e impresión de reportes en formatos docx/pdf.
- Panel de control centralizado.
- Requisitos *Common Criteria* integrados *online*.
- Basado en tecnologías web de última generación, como HTML5, CSS3 y AngularJS.
- Especificación de lenguaje máquina a máquina para intercambiar información con los laboratorios.
- Especificación de humano a máquina para obtener información de los fabricantes.
- Especificación para la comunicación entre todas las partes involucradas.
- Generación automática de informes de validación y emisión de certificados.
- Sistema de almacenamiento en la base de datos.
- Adaptación a los requisitos del EUCC.

Conclusiones

CCCAB pretende mejorar y agilizar el proceso de validación, con la intención de llegar a ser una herramienta común para los más de 30 países que reconocen *Common Criteria* y para el resto de CABs dentro del Marco Europeo de Certificación de la Ciberseguridad. CCCAB estará adaptado al EUCC (más conocido como el *Common Criteria* europeo) y, al ser una herramienta de código abierto, la comunidad podrá contribuir a desarrollar la herramienta, por lo que el potencial de uso y mejora es exponencial, pudiendo en el futuro ampliarse a otros Esquemas de Certificación de la Ciberseguridad Europeos que empleen otras metodologías de evaluación como LINCE, esquema 5G o el esquema *cloud* europeo, entre otros.

El impacto de CCCAB en los años venideros cuenta con excelentes perspectivas, siendo la primera versión que se desarrolle en este primer proyecto sólo el germen de una herramienta mucho más avanzada. ■

José Ruiz Gualda
CTO
jtsec Beyond IT Security