

# Despliegue de auditoría continua en sistemas de información en el Ministerio de Defensa

**Autor:** Carrasco Santiago, Rafael

**Director/es:** Rodríguez Rodríguez, Francisco Javier

Contacto: Mando Conjunto del Ciberespacio. Base Retamares. Carretera de Boadilla del Monte, km 3,4. 28223 Pozuelo de Alarcón (Madrid) / rcarsan@ea.mde.es

## Resumen:

Los informes del estado de la ciberseguridad en España elaborados por organismos como el Instituto Nacional de Ciberseguridad (INCIBE) o el Centro Criptológico Nacional (CCN) demuestran que estamos expuestos de manera continua a ciberataques que, sin entrar en el detalle del propósito de los mismos, -económicos, desinformación, exfiltración de información, etc.-, supone perder el control de nuestros activos que, en el caso del Ministerio de Defensa, podrían llegar a comprometer incluso la Seguridad Nacional.

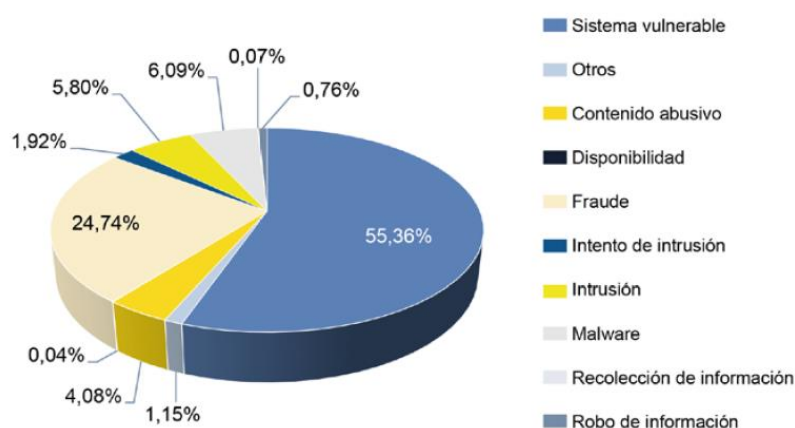


**Figura 1.** Porcentaje y tipología de incidentes gestionados por INCIBE-CERT en 2022

Los resultados de esos informes revelan que, un porcentaje elevado de los ataques que se reciben –más del 55% en el año 2022, tal y como se refleja en la figura 1 del informe del INCIBE-CERT<sup>1</sup>-, son debidos a vulnerabilidades existentes en los sistemas que soportan el

<sup>1</sup> CERT- Computer Emergency Response Team (equipo de personas dedicado a prevenir, detectar y responder de manera eficaz ante incidentes de ciberseguridad)

manejo de la información, así como a fallos en el cumplimiento de las guías de bastionado y securización de los mismos.

Además, debe tenerse en cuenta que el nivel de peligrosidad de cada una de las vulnerabilidades que se detecte no es siempre el mismo, como puede verse en la figura 2, extraída del informe de ciberseguridad del CERT de Defensa –ESPDEF-, lo que puede permitir priorizar las acciones de corrección atendiendo a este criterio de criticidad.

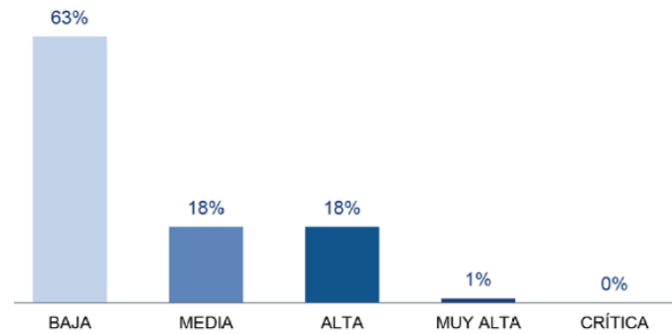


**Figura 2.** Peligrosidad de los incidentes gestionados por el ESPDEF-CERT en 2022

Ante esta situación, se hace evidente y se considera necesaria la implementación de herramientas que provean de la información suficiente sobre el estado de seguridad en el que se encuentra los diferentes elementos que conforman cada uno de los sistemas que utiliza el Ministerio de Defensa, siendo este el motivo de la realización de este Trabajo Fin de Máster (TFM).

En este sentido, en el TFM se presentan una serie de herramientas que están enfocadas en el análisis de las vulnerabilidades que tienen los sistemas y redes que escaneen, centrándose en una de ellas, el software Tenable Nessus, dado que proporciona un análisis más completo y exhaustivo. Además, esta herramienta permite la generación de diferentes tipos de informe en los que se muestran tanto las vulnerabilidades detectadas con los escaneos, como la criticidad que tienen cada una de ellas. En el trabajo se incluye igualmente un detalle de la instalación, así como de la configuración elegida para la realización de las pruebas, teniendo en cuenta que los anchos de banda en los que van a tener que ejecutarse los escaneos, pueden no tener la suficiente capacidad como para coexistir con otros servicios que estén en ejecución. Este caso podría ser el de un Destacamento de las Fuerzas Armadas que opera fuera de territorio nacional y cuya capa de transporte y conectividad le viene proporcionada por un terminal satélite desplegable que, generalmente, va a proporcionar un ancho de banda reducido y que deberá ser usado por todos los sistemas que tenga desplegados, lo que va a obligar a dimensionar y establecer calidad de servicios para aquellas tareas que, o bien se consideren críticas, o bien se consideren prioritarias.



**Figura 3.** Logotipo del fabricante Tenable y la herramienta Nessus

Por otro lado, se analizará la solución ANA-CLARA proporcionada por el CCN, que permite comprobar el grado de cumplimiento con el que están configurados los sistemas. A la hora de instalar y configurar un sistema operativo del tipo que sea, tanto en servidores como en clientes, es necesario securizarlo y bastionarlo de la manera oportuna, siendo requisito imprescindible si va a estar incluido en algún sistema que va a manejar información clasificada. Para tal fin, el CCN ofrece diferentes guías de configuración segura –CCN-STIC- que, mediante scripts y otras directrices, permiten al administrador del sistema el establecimiento de parámetros que ajusten y afinen la instalación tanto del software en las máquinas como de cada uno de los elementos de hardware que se utilicen.



**Figura 4.** Logotipo de las soluciones del CCN ANA y CLARA

La utilización conjunta del software indicado en los dos párrafos anteriores, Tenable Nessus y ANA-CLARA, proporciona una visión general del estado de ciberseguridad en el que se encuentran las TIC de la organización objeto de análisis. La generación de informes de las soluciones citadas, ofrecerá al personal responsable de la seguridad y al de la administración de los sistemas, la posibilidad de tomar las acciones conducentes a depurar los fallos mediante la actualización del software y firmware de los equipos, así como a aplicar correctamente las guías de seguridad que correspondan. Por otra parte, la Dirección de la organización, a tenor de la información proporcionada por las herramientas comentadas, estará en condiciones de dimensionar y adecuar la toma de decisiones que corresponda, asignando o detrayendo recursos para mantener o aumentar la seguridad de sus sistemas.

La elección de utilización de la herramienta Tenable Nessus para el análisis de vulnerabilidades, aunque existen otras muchas opciones en el mercado, algunas de ellas incluidas en el TFM, se justifica por dos motivos principales: la enorme cantidad de plugings que ofrece –más de 130 mil-, así como por el soporte que proporciona el fabricante de la herramienta, tanto para las actualizaciones del propio software, como para el desarrollo de soluciones *ad hoc* si fuera el caso. Además, en el caso del Ministerio de Defensa, en el que la instalación *on premise* se puede llegar a considerar como determinante o la única opción para la adopción de uno u otro software por el motivo antes citado de la existencia y manejo

de información clasificada, la solución Tenable Nessus es la más válida. En este sentido debe señalarse que para que un sistema pueda manejar información clasificada requiere de una acreditación por la Autoridad correspondiente exigiéndose, como uno de los requisitos, que el software instalado esté soportado por un fabricante.

En el caso del análisis de cumplimiento, la herramienta que se ha empleado es la que ofrece el CCN a través de la solución ANA-CLARA. La implementación de esta herramienta permite, al igual que en el caso de Tenable Nessus, de una instalación *on premise* que, como se ha comentado anteriormente, se considera relevante a la hora de decidir su instalación en redes y sistemas que van a manejar información clasificada. El proceso de instalación y configuración, con las particularidades mencionadas en cuanto a anchos de banda se refiere, así como la realización de diversas pruebas de escaneo, también han sido realizadas y comentadas en la memoria del trabajo.

Una vez decididas las herramientas a implementar, se hace preciso elaborar un documento para la contratación del software. En el apartado de valoración económica de ambas herramientas, Tenable Nessus y ANA-CLARA, hay que diferenciar entre el software comercial de Tenable, que requiere de una licitación a través de Acuerdos Marco y/o publicación en el Portal de Contratos de la Administración Pública, del que se muestra una captura de la barra de navegación en la figura 3, debiendo elaborar los correspondientes pliegos de prescripciones técnicas (PPT) y pliegos de condiciones administrativas particulares (PCAP), y la de la solución ANA-CLARA, cuyo utilización es gratuita para los diferentes organismos de la Administración General del Estado.



**Figura 5.** Captura de pantalla de la barra de navegación de la Plataforma de Contratación del Sector Público

Con los resultados que arrojan las herramientas seleccionadas, que además vienen priorizados en función de la criticidad de las vulnerabilidades halladas, se podrán tomar las acciones oportunas conducentes a corregir las desviaciones que mitiguen los riesgos que pueda provocar el tener sistemas vulnerables o indebidamente securizados, todo ello de acuerdo a las directrices del responsable de seguridad correspondiente de cada uno de los sistemas.

Como finalización al trabajo, se establecen una serie de consideraciones sobre líneas futuras de evolución de un sistema de auditoría continua, en el que, a través de cuadros de mando o *dashboards*, integren los resultados de otras herramientas y soluciones de ciberseguridad como EDR (*Endpoint Detection Response*), IDS (*Intrusion Detection System*), SIEM

(*Security Information and Event Management*), antivirus y otras. Este aglomerado de información en una sola herramienta de gestión de información o cuadro de mando, ofrecerá una visión más amplia y completa del estado de ciberseguridad de los sistemas, permitiendo controlar la evolución de los mismos a lo largo del tiempo, como puede verse en la figura.4, en la que se incluye, a modo de ejemplo, la evolución de los incidentes, su estado y el tiempo medio de resolución mensual de los mismos. Obviamente, este cuadro de mando podrá configurarse con las informaciones que ofrezcan las diferentes soluciones que implementemos en cada uno de nuestros sistemas.

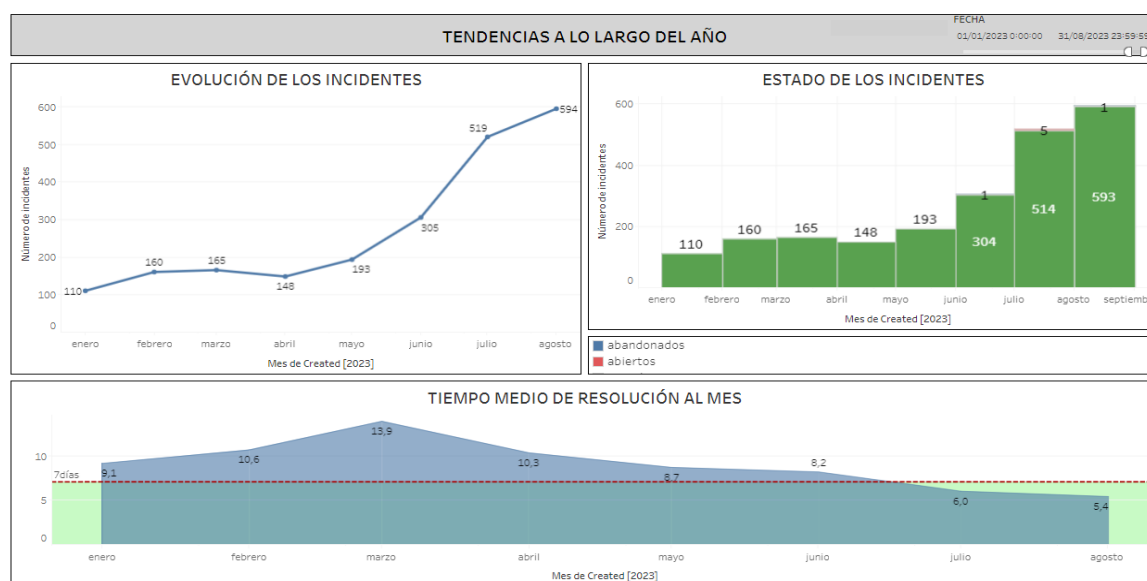


**Figura 6.** Tendencias de incidentes

**Palabras clave:** auditorías de seguridad CIS, sistemas de información, ciberseguridad, vulnerabilidades, Ministerio de Defensa

## Agradecimientos

A mis compañeros del Grupo de Auditorías del Mando Conjunto del Ciberespacio por los apoyos prestados para la realización de las pruebas llevadas a cabo durante el desarrollo del TFM.

## Referencias

1. Balance de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE) 2022.
2. Guías CCN-STIC del Centro Criptológico Nacional [diciembre de 2023] <https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es>
3. Informe Anual de Seguridad Nacional 2022. Catálogo de publicaciones de la Administración General del Estado [diciembre de 2023] <https://cpage.mpr.gob.es>
4. Ley 9/2017 de 8 de noviembre de Contratos del Sector Público
5. National Institute of Standards and Technology (NIST) [diciembre de 2023] <https://www.nist.gov/>
6. Real Decreto 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad

7. Solución ANA-CLARA del CCN <https://www.ccn-cert.cni.es/es/comunicacion-eventos/comunicados-ccn-cert/7540-ana-el-nuevo-sistema-de-auditoria-continua-del-ccn-cert> [noviembre de 2023]
8. Tenable Nessus <https://es-la.tenable.com/products/nessus> [noviembre de 2023]