Del riesgo al control: así avanzan las Universidades Públicas Andaluzas hacia el ENS a través de la Guía CCN-STIC 881.

María Ángeles de la Torre Parra
Auditora de la Cámara de Cuentas de Andalucía.

María Soledad Martín Castellano
Técnico de la Cámara de Cuentas de Andalucía.

Revista Auditoría Pública nº 87. Junio 2026. Páginas: 89-97

Resumen: Las TIC se han convertido en un elemento táctico para la labor de las universidades públicas lo que ha derivado en que la seguridad de la información se convierta en una prioridad para estas instituciones. En esta tarea, es clave que exista una gobernanza de las TI que se integre en los objetivos estratégicos de la universidad.
El ENS surge en 2010 en un contexto en el que las TIC estaban calando cada vez más en la operativa del sector público. Con el nuevo desarrollo del Esquema en 2022, unido a la elaboración de Guías por el Centro Criptológico Nacional, como la Guía CCN-STIC 881[1], han servido para dotar de herramientas a las universidades. La Guía elabora un Perfil de Cumplimiento Específico para Universidades (PCEU) para facilitar la obtención de la certificación al ENS.
La reciente fiscalización llevada a cabo por la Cámara de Cuentas de Andalucía pone de manifiesto que, aunque se han logrado avances significativos, aún queda camino por recorrer en el proceso de obtención de la preciada certificación bajo el ENS. Además, la presión de los ciberataques en este sector acentúa la importancia de incluir la ciberseguridad entre las prioridades estratégicas de las universidades para dotarlas de los recursos y la formación necesaria.

Palabras Clave: Seguridad de la información; Gobernanza de las TI; ENS; PCEU; ciberataques.

Abstract: The increasing role of Information and Communication Technologies (ICT) as a strategic component in the operations of public universities has made information security a priority for these institutions. In this context, effective IT governance is essential to ensure its integration with the universities' strategic objectives.
The National Security Framework (NSF), introduced in 2010, emerged in a context where ICTs were becoming increasingly embedded in public sector operations. Its subsequent development in 2022, together with the publication of guidelines by the National Cryptologic Centre (NCC) –such as CCN-STIC Guide 881– has provided universities with practical tools. In particular, this Guide establishes a Specific Compliance Profile for Universities (SCPU), aimed at facilitating the process of obtaining NSF certification.
A recent audit conducted by the Chamber of Accounts of Andalusia reveals that, although significant progress has been made, there is still a long way to go in achieving NSF certification. Furthermore, the growing pressure of cyberattacks in this sector underscores the importance of including cybersecurity among universities' strategic priorities, ensuring the provision of adequate resources and training.

Keywords: Information Security; IT Governance; NSF (National Security Framework); SCPU (Specific Compliance Profile for Universities); Cyberattacks.

1 Guía del Centro Criptológico Nacional de Seguridad de las TIC de adecuación al ENS para Universidades, de mayo de 2022.

1. Las universidades en la era digital: cómo las TI redefinen la actividad diaria de estas instituciones.

Las Tecnologías de la Información (en adelante, TI) han ido adquiriendo un papel fundamental en la operativa cotidiana a todos los niveles y en todo tipo de instituciones. Centrándonos en el ámbito universitario, las TI han permeado en sus diferentes ámbitos: docencia, investigación y administración.

Con el objetivo de realizar un análisis temporal, si nos remontamos a 2004, la Conferencia de Rectores de las Universidades Españolas (CRUE[2]) publicó por primera vez un informe[3] acerca de las Tecnologías de la Información y las Comunicaciones (TIC) en el Sistema Universitario Español (SUE). En este informe se daba traslado de cómo las universidades españolas habían asumido el compromiso de implementación de las TIC en las 3 áreas mencionadas. Además, se ponía de manifiesto la necesidad de una planificación formal para llevar a cabo esa implementación.

Para abordar esta falta de planificación, en 2005, la CRUE propuso dotar a las universidades de una herramienta para elaborar la estrategia de las TIC. De esta manera, a través de la Comisión Sectorial TIC se diseñó un Modelo de Análisis y Planificación TIC que tenía como punto de partida un Catálogo de Objetivos e Indicadores consensuados y comunes para todo el SUE.

En 2006, surge UNIVERSITIC, una encuesta con la que se pretendía establecer cuál era la situación de las TIC en las universidades españolas en torno a 6 ejes: enseñanza/aprendizaje, investigación, gestión universitaria, gestión de la información, formación y cultura TIC y organización de las TIC.

A partir de los resultados de esta encuesta, se proponía un conjunto de acciones que las universidades podían emprender, tanto individualmente como de forma conjunta, con el objetivo de mejorar los servicios y aspectos de planificación relacionados con las TIC.

En 2009, en otro de los informes de la CRUE-TIC, se indicaba que las TI eran un elemento táctico para las universidades que les aportaba soporte en los principales servicios universitarios, convirtiéndose en un componente crítico en todos sus ámbitos. Aparecía entonces un concepto que daba nombre a dicho informe, *"el gobierno de las TI"* que se definía en el mismo como: *"una responsabilidad al más alto nivel directivo y se encuentra en lo más alto de una pirámide que estaría basada en las operaciones TI y la gestión TI".*

Con objeto de coordinar las TI, debían establecerse los objetivos estratégicos para lograr una mejora de la competitividad y eficacia de la universidad. De esta manera, el proceso de toma de decisiones sobre dónde, cuándo y cómo invertir los recursos en tecnología estaría alineado con el cumplimiento de los objetivos de la universidad.

En la edición de 2010 de UNIVERSITIC, se incluía una evolución de las TIC en el SUE 2006-2010. A continuación, se recogen algunos indicadores por ejes estratégicos donde se observan cuestiones que si bien hoy en día pueden darse más que por sentado, en aquellos años, reflejaban que se estaban dando los primeros pasos en el uso de las TIC:

1. **Docencia:** el objetivo principal era facilitar la docencia virtual a través de la implantación de plataformas informáticas. Paralelamente, se consiguió que el cuerpo docente y el alumnado se implicara e hiciera uso de estas plataformas.

2. **Investigación:** se dotó a los investigadores de un ordenador y cuenta de correo y, a nivel universidad, de aplicaciones de gestión de la investigación y un portal web para la divulgación de la oferta tecnológica e investigadora.

3. **Procesos de gestión universitaria:** el Personal de Administración y Servicios del SUE disponía ya en 2008 de un ordenador, de un correo electrónico y en 2010 un 72% contaba con una herramienta de trabajo colaborativo.

4. **Gestión de la información de la institución:** en 2010, el 51% de las Universidades disponían de una aplicación de archivo documental.

5. **Formación y cultura TIC:** un 38% de los cursos impartidos eran de formación TIC y lo recibieron en

2 Web CRUE: *"es una asociación sin ánimo de lucro que fue creada en 1994, y que, en la actualidad, está formada por un total de 77 universidades españolas de las cuales, 50 son públicas y 27 son privadas. CRUE representa al conjunto de las Universidades Españolas que forman parte de ella, fomentando la cooperación entre éstas y las Administraciones públicas, y las relaciones con las universidades extranjeras y con los agentes sociales".*

3 *"Las TIC en el Sistema Universitario Español"* (Barro y otros, 2004).

2010 el 16% del Personal Docente e Investigador (PDI) y el 27% del Personal Administrativo y Servicios (PAS). Sin embargo, el presupuesto destinado a formación del personal especializado en TIC para formación por técnico disminuyó en un 37% en 2010, con respecto a 2006.

6. **Organización de las TIC:** en 2010, el 80% de las universidades disponían o estaban desarrollando un plan estratégico que incluyera las TIC. Además, más del 90% de las universidades había diseñado un plan de renovación continua y periódica de todas sus infraestructuras TIC; en cambio, apenas el 50% de las universidades disponían de un plan de dotación y distribución de recursos humanos TIC.

De este estudio, se desprende que las universidades españolas estaban apostando de forma decidida por el uso de las TIC, como pilar fundamental de sus procesos universitarios y para situarlas como principal motor de cambio e innovación.

En este contexto de implantación de las TIC, se aprueba el primer desarrollo del Esquema Nacional de Seguridad (ENS) mediante el Real Decreto 3/2010, de 8 de enero[4], en el ámbito de la Administración Electrónica en respuesta al artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Posteriormente, en la edición de UNIVERSITIC 2017, se puso de manifiesto la conciencia y preocupación por la seguridad de la información por parte de las universidades. Por ello, se recogieron diferentes aspectos que abordan dicha preocupación: ENS, los datos relacionados con la seguridad, los distintos roles y sus responsabilidades y los criterios de valoración. Esto arrojó como conclusión que debía hacerse una aproximación integral a la seguridad de la información y entender que debía ser una función diferenciada del responsable de los sistemas de información[5].

En 2020, se destacó el interés que tenían las universidades de nuevo por los aspectos de seguridad e indicadores del ENS de 2010 el cual les resulta de aplicación[6], presentando un índice de madurez[7] medio de 57 de los 100 puntos posibles del ENS en su cumplimiento. Desde entonces, el ENS está en constante evolución con modificaciones notables en 2015 y su última actualización en 2022 mediante Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad que es el texto actualmente en vigor.

Por último, en el informe de 2022, se esbozó como una nueva oportunidad el uso de la inteligencia artificial y como nueva amenaza, los ciberataques y la vulnerabilidad de las estructuras digitales de las universidades ante este tipo de situaciones, lo que hace necesario dar respuesta a estos nuevos retos que se plantean.

Se sigue una senda de mejora en el proceso de transformación digital de este sector y en lo que a ciberseguridad[8] se refiere, aumenta la preocupación por este tema. Ello se refleja en que 3 de cada 4 universidades contaban en 2022 con una política de seguridad (un 20% más que en 2020) y una normativa que la desarrollaba. Sin embargo, el índice de madurez medio se mantenía desde 2020 en 57 puntos y, aunque 3 de cada 4 universidades habían llevado a cabo una auditoría de seguridad, solo el 10% contaba con la certificación exigida.

En la actualidad, se evidencia que los ciberataques han ido evolucionando en complejidad, lo que dificulta la respuesta y la disposición de medidas de prevención por parte de estas instituciones. A su vez, la seguridad de la información se ha convertido en prioritaria para garantizar estos activos, al manejarse datos e información muy sensibles y relevantes.

4 Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS, Preámbulo: *"cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información."*

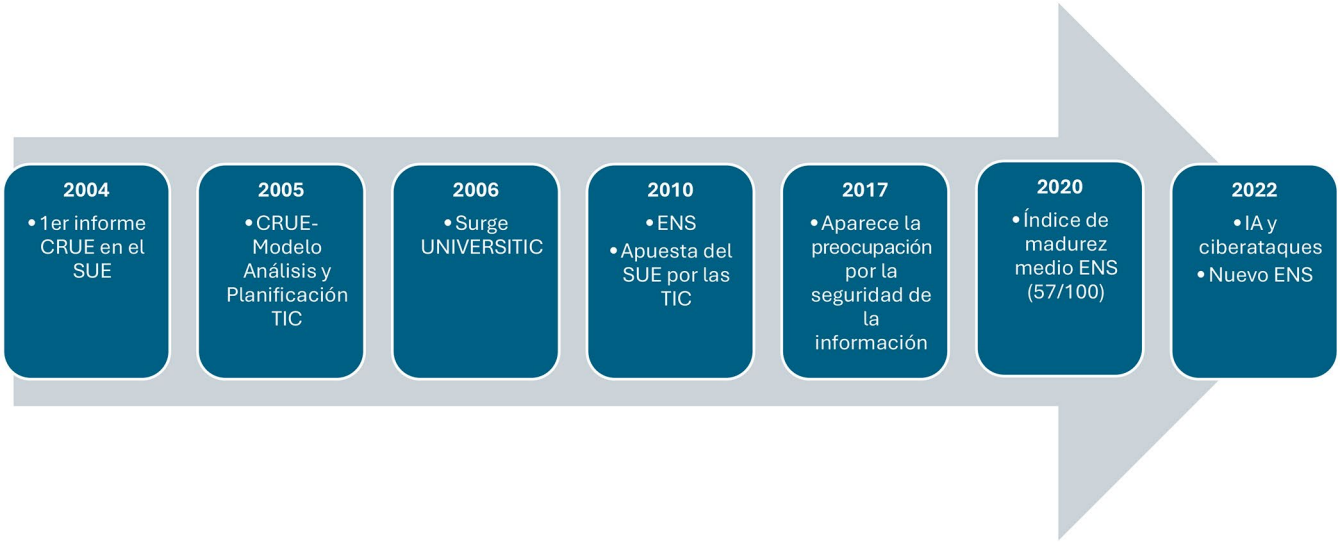
5 Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS, artículo 10: *"en los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad."*

6 Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS, artículo 1.2: *"El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias."*

7 Se refiere al grado de cumplimiento y eficacia en la implementación de los controles y medidas de seguridad requeridos.

8 Si bien la seguridad de la información y la ciberseguridad no son lo mismo, porque la primera se refiere a la protección de los datos valiosos de una institución y la segunda, es una rama de la primera centrada en la protección de los sistemas digitales, en el contexto del artículo, le damos un tratamiento indistinto, en la medida en la que no entramos en un análisis de los sistemas.

Figura 1. La evolución de las TIC en el SUE (2004-2022).



Fuente: elaboración propia.

2. Del marco normativo a la acción: aplicación de la Guía CCN-STIC 881 en el sistema universitario público andaluz.

2.1. El papel del CCN en el cumplimiento del ENS.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda a este Centro las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, así como la dirección el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, dicho Centro realiza diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Debido al carácter sectorial del mundo universitario, y bajo el amparo del Real Decreto 311/2022 (que regula el ENS) así como de la LOSU[9], el CCN a través de la Guía CCN-STIC 881[10] ha adaptado la adecuación al Esquema Nacional de Seguridad a la propia naturaleza y funciones de las universidades públicas, mediante la elaboración de un Perfil de Cumplimiento Específico para Universidades (PCEU), para la implementación de las medidas del Anexo II[11] de la citada Guía de la forma más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida exigible.

Con esta serie de documentos el CCN, en cumplimiento de sus cometidos y de lo regulado por el ENS en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

9 Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario.

10 Aunque esta Guía no es de obligado cumplimiento, constituye un marco de referencia para apoyar al personal de la Administración en la tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

11 Referido al Plan de Adecuación al ENS de las Universidades.

2.2. El objetivo y el alcance de la Guía CCN-STIC 881.

El objetivo de la Guía es proporcionar un modelo que facilite la Adecuación al ENS de los sistemas de las universidades públicas de forma ordenada y efectiva, que permita obtener la Certificación de Conformidad para sus sistemas según el Perfil de Cumplimiento Específico para Universidades antes mencionado.

La Guía abarca la gestión de la ciberseguridad en las universidades públicas de manera integral y consta de tres partes claramente diferenciadas:

- *Modelo de Gobernanza de las TI.*
- *Política de Seguridad.*
- *Plan de Adecuación al ENS.*

El Modelo de Gobernanza se ocupa desde la designación de roles de seguridad hasta la constitución de los órganos específicos que la gestionen, teniendo en cuenta las particularidades propias que se derivan de la naturaleza jurídica de las universidades públicas. Esta organización, junto con los compromisos de seguridad, se debe reflejar en la Política de Seguridad. A continuación, habrá que elaborar un Plan de Adecuación de los sistemas de la universidad, mediante la identificación de los activos esenciales, su valoración, categorización, obtención de la declaración de aplicabilidad, análisis de riesgos, etc., del que resultará un Perfil de Cumplimiento Específico con las medidas que resulten de aplicación a sus sistemas para garantizar la seguridad de los mismos.

Y como objetivo último, las universidades deberán superar el proceso de Certificación al ENS conforme al Perfil de Cumplimiento recomendado en la citada guía, iniciando así el ciclo de gobernanza de la ciberseguridad, mediante la revisión y mejora continua de los procesos de seguridad desplegados en el sistema.

Además, la Guía se completa con 2 anexos que incluyen un modelo de Política de Seguridad y un Plan de Adecuación al ENS para universidades.

2.3. Aplicación práctica de la Guía CCN-STIC 881 por parte de los Órganos de Control Externo.

En el marco del Plan de Actuaciones para el ejercicio 2024 de la Cámara de Cuentas de Andalucía (CCA), se ha llevado a cabo la realización del informe anual de las Universidades Públicas de Andalucía (ejercicios 2022-2023) que incluye una referencia especial a la ciberseguridad.

Dicho informe tiene como objetivo verificar de manera transversal el cumplimiento Guía CCN-STIC 881. Para ello, tomando como base el contenido de la citada Guía de mayo de 2022[12], la CCA confeccionó un cuestionario para evaluar el nivel de implantación en las UPAS al PCEU.

El sector universitario público andaluz se compone de 10 universidades situándose el presupuesto agregado de las mismas para el año 2023 en 1.149M€, lo que muestra la significatividad de este sector.

La respuesta por parte de las UPAS a dicho cuestionario ha constituido la base de las conclusiones del informe referenciado, reflejando las mismas el grado de implantación declarado por las universidades públicas andaluzas. Asimismo, para la evaluación del nivel de cumplimiento de las UPAS, de acuerdo con sus respuestas, se ha considerado que el nivel de cumplimiento es bajo cuando las

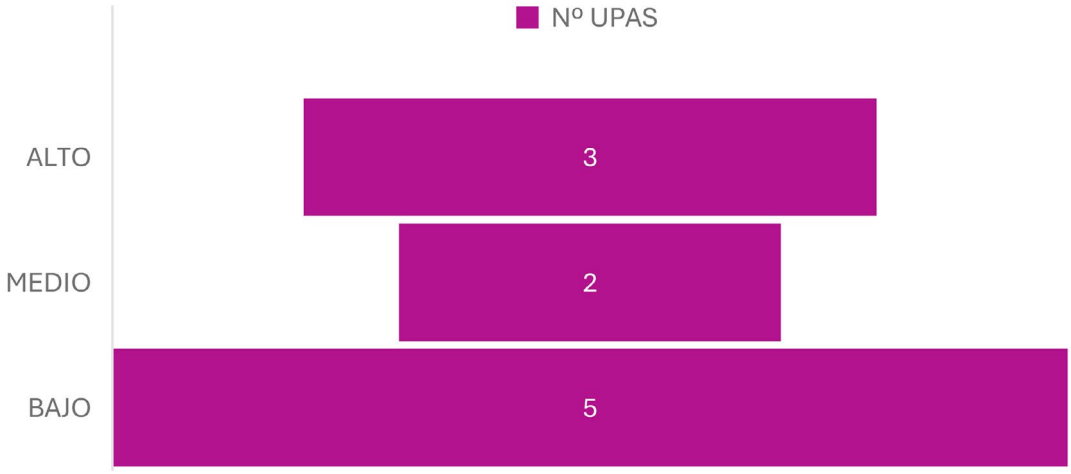
12 Se aprueba con posterioridad al ENS de 2022 (R.D. 311/2022).

respuestas afirmativas han sido inferiores al 50%, medio si han obtenido menos del 70% y alto cuando han superado el 70%.

En el informe de referencia se concluye que las UPAS responden de forma afirmativa al 57%[13] de las cuestiones formuladas en base al Perfil de Cumplimiento Específico recogido en la Guía CCN-STIC 881 siendo negativa su respuesta en un 28%[14] de los casos.

El gráfico nº1 refleja los niveles de cumplimiento del PCEU, encontrándose en un nivel de cumplimiento alto 3 UPAS, 2 en un nivel medio y en un nivel bajo el resto de UPAS. Esta catalogación responde normalmente al tamaño de la Universidad que facilita lógicamente la implantación al ENS, aunque se evidencia que existen excepciones.

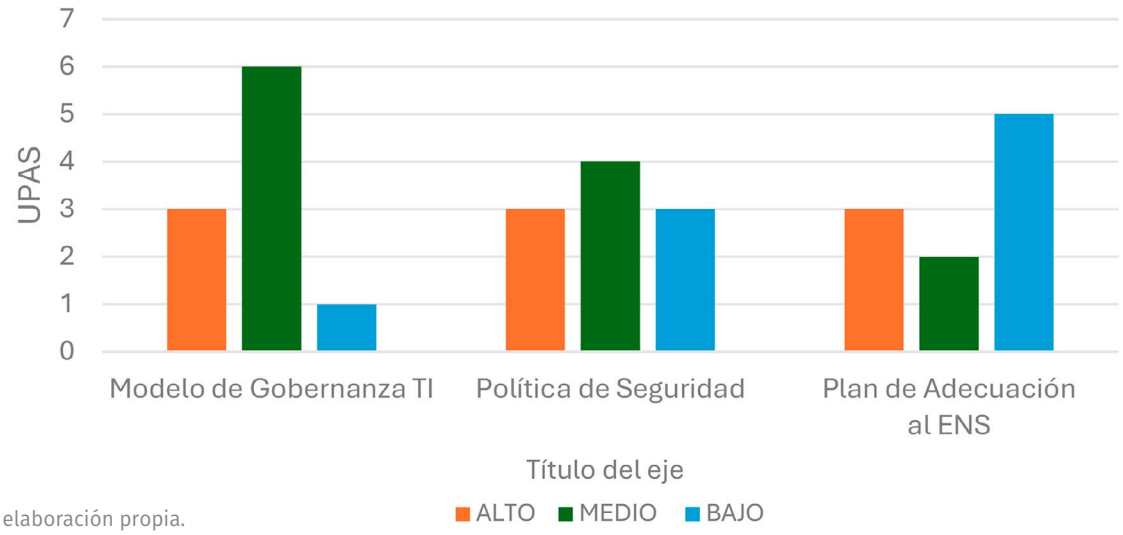
Gráfico 1. Grado de implantación PCEU.



Fuente: elaboración propia.

Por áreas de análisis, el gráfico nº2 siguiente muestra la situación según el nivel de implantación de cada UPA:

Gráfico 2. Grado de implantación por áreas de análisis.



Fuente: elaboración propia.

13 El 57% se obtiene de dividir el número de respuestas afirmativas totales (233) entre el número total de respuestas posibles (410=41*10 UPAS).

14 El resto de las respuestas posibles ascienden al 1% (N/A) y al 11% (para respuestas parcialmente afirmativas).

Respecto a las áreas de análisis, el grado de implantación del Modelo de Gobernanza es del 63% en el sector universitario público andaluz siendo el nivel de cumplimiento del PCEU alto en 3 UPAS, medio en 6 y bajo en una de ellas. En relación a la Política de Seguridad, el nivel de cumplimiento de las UPAS en base a las respuestas del mencionado cuestionario alcanza el 64% (siendo alto en 3 UPAS, medio en 4 y bajo en el resto) así como el 44% en el Plan de Adecuación (siendo alto igualmente en 3 UPAS, medio en 2 y bajo en el resto). Se concluye, por tanto, que aunque la Gobernanza y la Política de Seguridad son mejorables al menos obtienen el aprobado, resultado que no se alcanza en el plan de implantación del ENS que se sitúa en el 44%. Lo anterior justifica que sólo 1 de 10 UPAS esté certificada bajo el ENS desde 2018 (siendo preceptiva su obtención desde el 5 de mayo de 2024 en base a la normativa de aplicación).

Modelo de gobernanza TI.

Según se establece en la Guía CCN-STIC 881, la gestión de la seguridad de los sistemas de información de las universidades (definición, implantación y mantenimiento) exige establecer una Organización Interna de la Seguridad. Tal organización debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.

El Modelo de Gobernanza propuesto por la Guía facilita la toma de decisiones interna y articula la colaboración entre ellas, estando destinado a la gestión de los procesos relacionados con el ENS y basado en bloques de responsabilidad. Así, la mayor parte de las universidades (9 de las 10 UPAS) cuentan con Comités de Seguridad TIC, Áreas TIC y reconocen utilizar las Herramientas[15] de Gobernanza, no contando ninguna con Oficina de Seguridad TIC debido principalmente al proceso y costes necesarios para dotarla de personal, así como la formación correspondiente en materia de ciberseguridad.

Por otro lado, sólo 2 de 10 UPAS disponen de Centro de Operaciones de Ciberseguridad (COCS[16]). En relación al Foro de seguridad TIC, todas las UPAS asisten a la Sectorial CRUE-TIC[17] que dispone de un Grupo de Trabajo específico de Seguridad y Auditoría TI. En cuanto a la estructura y flujo de autorizaciones TIC, se han establecido los roles y las funciones de los miembros en el 60% de los casos.

Los cuestionarios arrojan que el 50% de las UPAS reconocen tener un modelo extendido de gobernanza[18].

Política de seguridad.

Aunque todas las UPAS cuentan con Políticas de Seguridad aprobadas y en vigor, sólo el 40% de ellas, las tienen adaptadas al nuevo ENS y únicamente 2 UPAS cumplen con el PCEU, en cuanto a su estructura y contenido conforme a la Guía CCN-STIC 881.

En relación a la "gestión de riesgos", 6 de 10 UPAS realizan este análisis anualmente, tal y como aconseja la Guía, poniéndose de manifiesto además que sólo en 2 UPAS el Responsable de la Seguridad se encarga de verificar la realización de dicho análisis, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información. Se concluye que, aunque el proceso de gestión de riesgos es conforme a la normativa de aplicación en un 70% de los casos, únicamente el 30% de ellos comprende las fases de categorización de sistemas, análisis de riesgos y selección de medidas por parte del Comité de Seguridad de la Información.

Respecto al apartado de "Mejora continua y modificaciones", hay que tener presente que la gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Sin embargo, se incluyen estos apartados en el 50% y 60% de las políticas de las UPAS, respectivamente.

Plan de adecuación.

En lo que concierne al alcance de los sistemas a certificar, aunque el 70% de las UPAS indican en su Plan de Adecuación el catálogo de servicios prestados y sistemas en el que están alojados, sólo en el 50% de las

15 Para la gobernanza de la ciberseguridad, en consonancia con lo establecido en el artículo 10 Vigilancia continua y reevaluación periódica del RD ENS, *"las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario"* desde el Centro Criptológico Nacional, se proporcionan las herramientas de gobernanza INES y AMPARO que garantizan la gestión de la ciberseguridad.

16 Según la Guía, este Centro desarrolla la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

17 Constituye una de las Comisiones Sectoriales de la CRUE Digitalización, la cual crea estos Grupos de Trabajo para alcanzar los objetivos planteados y cumplir con su misión.

18 Según el CCN, representa un marco avanzado y estructurado para gestionar la seguridad de la información, adaptado a organizaciones complejas o con mayores necesidades de cumplimiento.

UPAS se refleja el resultado de la valoración de las dimensiones de seguridad de los servicios e información alojados en el mismo.

En relación al Plan de Implantación, el 40% de las UPAS dispone del mismo, no constando con este documento en el 40% restante y siendo incompleto en el resto de los casos (20%), teniendo en cuenta que dicho documento debe incluir el marco organizativo, operacional y de protección.

3. Cuando la ciberseguridad falla: riesgos y aprendizajes a partir de casos reales.

Cerca del 70% de las universidades españolas han sufrido ciberataques o incidentes de seguridad en el año 2025, siendo el sector educativo uno de los principales objetivos. Los ataques más comunes incluyen ransomware[19] y robo de datos, afectando a la operatividad y a la información de estudiantes y docentes. Como ejemplos de ataques recientes y comunes, un informe del sector asegurador[20] indica que el 68% de las universidades españolas sufrieron incidentes en los últimos meses de 2025.

Algunos casos destacados en el sector universitario español:

- Consejo Superior de Investigaciones Científicas (2022)[i]: fue blanco de un ciberataque de *ransomware* que obligó a un corte de acceso a la red en diversos centros, siguiendo el estricto protocolo internacional necesario para atajar el incidente y garantizar que no se extendiera el ataque a los centros que no se vieron directamente afectados.

- Universitat Pompeu Fabra (2023)[ii]: consiguió evitar un ataque que le obligó a estar sin acceso a sus servicios informáticos ni a internet, con el agravante de que tuvo lugar justo en el cierre del tercer trimestre y el inicio del respectivo periodo de exámenes.

- Universidad Complutense de Madrid (2024)[iii]: sufrió un ciberataque a través de una aplicación desarrollada por la propia institución para gestionar la información de los estudiantes en prácticas. Consiguieron extraer datos personales de los estudiantes.

Los ciberataques buscan paralizar los servicios y extorsionar a las instituciones, a menudo con ataques dirigidos al final del curso. Esta situación ha generado una mayor necesidad de reforzar la ciberseguridad en el ámbito académico.

A nivel andaluz, en los últimos años varias instituciones educativas y plataformas universitarias han sido objeto de ciberataques, destacando incidentes de *ransomware* y acceso ilícito a datos. Los casos más relevantes incluyen:

- Universidad de Cádiz (2020)[iv]: la Universidad denunció ante la policía un ciberataque que afectó a cientos de sus cuentas de correo corporativas, según indicaba la propia universidad en un comunicado[v], parecía que en dichos correos se incluía un archivo PDF que podía no ser legítimo y llevar a ejecutar un programa ejecutable de Windows con un virus del tipo ransomware.

- Universidad de Córdoba (2021)[vi]: ciberataque que resultó en el secuestro de datos por parte del grupo de ransomware 'Conti'.

- Plataforma Séneca (2025)[vii]: en agosto, un ciberdelincuente fue detenido como resultado de la Operación Drawer que se inició tras la denuncia de un profesor de un instituto de Jaén. Se produjo el hackeo y suplantación de identidad de cuentas de correo electrónico pertenecientes a docentes, algunos de ellos encargados de confeccionar los exámenes de Selectividad (PAU) de ese año.

4. Conclusiones.

A través del presente artículo, hemos pretendido poner de manifiesto la importancia de la seguridad de la información en general, y en el sector universitario en particular, y cómo la gestión que se hace de la misma puede afectar a la obtención de la preceptiva certificación del ENS exigible desde el año 2010. Según el propio ENS, la gestión de la ciberseguridad es una tarea clave para la

19 El *ransomware* es un tipo de software malicioso (*malware*) que secuestra datos o dispositivos cifrándolos, exigiendo un rescate económico a cambio de liberarlos. Se propaga principalmente por correos electrónicos de phishing, descargas maliciosas o vulnerabilidades del sistema.

20 La ciberseguridad en el sector de la educación. Análisis completo de los principales retos y cómo mejorar la resiliencia cibernética.

prevención proactiva y requiere el establecimiento de un marco de gobernanza que designe roles y responsabilidades en la organización.

Los datos que manejan las universidades (por su especial sensibilidad) dada la actividad que las mismas realizan, hacen que la vulnerabilidad ante un ciberataque sea mayor en este sector, aumentando la frecuencia de estos incidentes debido al valor de estos activos.

Pese a los esfuerzos realizados hasta la fecha en todos los ámbitos (legislativo, organizativo y tecnológico), se evidencia que, aunque se han realizado avances significativos, aún queda camino por recorrer, ya que a nivel andaluz sólo el 10% de las UPAS se encuentran certificadas bajo el ENS. Este dato es además extensible a nivel nacional en el que los niveles de certificación actualmente alcanzan cotas similares.

Bibliografía.

- Barro, S y Burillo, P (ed.) (2007). UNIVERSITIC 2006. Las TIC en el sistema universitario español (2006): un análisis estratégico. Ciudad: Madrid, Editorial: Crue Universidades Españolas.

- Uceda, J y Barro, S. (ed.) (2011). UNIVERSITIC 2010. Evolución de las TIC en el Sistema Universitario Español 2006-2010. Ciudad: Madrid, Editorial: Crue Universidades Españolas.

- Fernández, A. y Llorens (ed.) (2011). Gobierno de las TI de las Universidades. Ciudad: Madrid, Editorial: Crue Universidades Españolas.

- Gómez, J. (ed.) (2017). UNIVERSITIC 2017. Análisis de las TIC en las Universidades Españolas. Ciudad: Madrid, Editorial: Crue Universidades Españolas.

- Gómez, J. (ed.) (2021). UNIVERSITIC 2020. Análisis de la madurez digital de las Universidades Españolas. Crue Universidades Españolas, Madrid.

- Crespo, D. (ed.) (2023). UNIVERSITIC 2022. Evolución de la madurez digital de las Universidades Españolas. Crue Universidades Españolas, Madrid.

- Centro Criptológico Nacional (2022). Guía CCN-STIC 881-Guía de Adecuación al ENS para Universidades.

- Esquema Nacional de Seguridad. https://ens.ccn.cni.es/es/inicio

- Cámara de Cuentas de Andalucía (2026). Informe anual de las Universidades Públicas de Andalucía especial referencia a la ciberseguridad. 2022-2023.

i El Consejo Superior de Investigaciones Científicas (CSIC) recibe un ciberataque

ii La Universitat Pompeu Fabra bloquea su sistema informático ante un posible ciberataque

iii Filtración de datos en la Universidad Complutense de Madrid | INCIBE-CERT | INCIBE

iv La Universidad de Cádiz sufre ciberataque de ransomware | INCIBE-CERT | INCIBE

v Cientos de mails de la UCA reciben ataques informáticos en las últimas 24 horas desde una cuenta de "alumnos indignados" – Portal UCA

vi La Policía Nacional investiga un ciberataque a la UCO con secuestro de datos

vii Un ciberdelincuente 'hackea' las cuentas de profesores en Séneca para alterar las notas de estudiantes en Andalucía