Adecuación en las Universidades del marco legislativo español en materia de Ciberseguridad (Guía CCN-STIC 881)

1. Resumen del proyecto:

En enero de 2010 se aprobó en España el marco legislativo para garantizar la seguridad de los sistemas de información en las Administraciones Públicas, que se denominó "Esquema Nacional de Seguridad" (ENS en adelante).

El ENS ha sufrido recientemente una renovación, publicada en mayo de 2022. Esta nueva versión en su artículo 30, establece la posibilidad de elaborar *perfiles de cumplimiento específico* por sectores, que incluirán las medidas de seguridad y los refuerzos que les sean de aplicación a los organismos que se acojan a dicho perfil.

> *En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.*

Siendo las universidades públicas un sector muy concreto dentro del ámbito de aplicación del ENS, teniendo todas ellas estructuras, circunstancias y regulaciones comunes, son susceptibles de poder adoptar un perfil de cumplimiento propio para alcanzar una mejor y más eficiente adaptación al ENS.

Por todo ello, el grupo de seguridad de la Sectorial CRUE-TIC (Universidades españolas), que engloba tanto a las públicas como a las privadas, planteó al CCN-CERT[1] la posibilidad de trabajar conjuntamente para la elaboración de la guía.

En colaboración con el organismo CCN-CERT, se ha desarrollado la guía CCN-STIC 881 de "Adecuación al ENS para las universidades", como modelo de referencia y marco de certificación del cumplimiento legal y, fundamentalmente, como herramienta de ayuda a la implantación de un sistema de gobernanza y gestión de la ciberseguridad en las universidades.

2. Desarrollo del proyecto:

La Guía CCN-STIC 881 de "Adecuación al ENS para las universidades", contiene la propuesta de un modelo que facilite la adecuación al ENS por parte de las universidades.

[1] CCN-CERT: acrónimo del Centro Criptológico Nacional-Computer Emergency Reaction Team; es el organismo encargado de coordinar la ciberseguridad y la respuesta a incidentes en las Administraciones Públicas españolas.

Objetivos:

- ✓ Detallar un Plan de Adecuación basado en un perfil de cumplimiento específico.
- ✓ Establecer un marco de certificación para universidades, pues el ENS exige dicha certificación a través de una auditoría externa periódica.

Recursos utilizados para el proyecto:

Para el desarrollo de esta iniciativa se constituyó un grupo de trabajo mixto entre expertas del CCN-CERT y responsables de seguridad de 7 universidades españolas que representaban a la Sectorial CRUE-TIC. Los trabajos se desarrollaron en 2021, a lo largo de 6 meses en los que se establecieron reuniones quincenales de debate, puesta en común y acuerdos adoptados.

Actividades llevadas a cabo:

Se comenzó por la identificación de los denominados “activos esenciales”, o sea, los servicios (a alto nivel) prestados por las universidades y la información tratada por ellos; para ello se consideraron las competencias básicas, misiones y cometidos de las Universidades recogidas en marco legislativo español en materia de universidades.

Esto permitió la definición de un catálogo de los activos esenciales (servicios e información) y una propuesta de valoración de estos activos y de categorización del sistema.

Se valoraron conjuntamente las 5 dimensiones de seguridad consideradas en el ENS:

- Confidencialidad, Integridad, Trazabilidad y Autenticidad de la información.
- Disponibilidad del servicio que da acceso a la información.

En el caso de las universidades, nuestra propuesta, reflejada en la guía, es que el sistema de información debe categorizarse como de nivel MEDIO, dentro de la escala propuesta por el ENS. Así mismo, se propuso la consideración de un sistema de información único para cada universidad. Esto aporta uniformidad a las medidas de seguridad a aplicar, independientemente del tipo de infraestructura que sustente los servicios y la información.

Según establece el ENS, la categoría de un sistema condiciona el conjunto de medidas, así como su grado, que son de aplicación sobre una propuesta global que son exigibles a los sistemas catalogados como de nivel “alto”. Al considerar el sistema de información en las universidades como de nivel medio, hay medidas que no son de aplicación en nuestro entorno o cuyos requisitos serán en un grado menor. Pero entendemos que esto aún no es suficiente, pues hay que tener en cuenta determinadas características propias del entorno universitario en relación con otros sectores de la Administración Pública, que pueden desembocar en matizaciones sobre las medidas propuestas, tal y como se refleja en la introducción de la propia guía:

> *El sistema universitario se ha convertido en un marco de innovación tecnológica abierto y flexible que promociona y difunde el conocimiento a toda la sociedad*

con diferentes modalidades incluida la colaboración y cooperación con diferentes sujetos.

Es necesario cuadrar una visión holística y transversal de la seguridad con el carácter abierto y colaborativo de la vida universitaria. Por ello se han modificado ciertas medidas exigidas por el ENS para el nivel medio, reflejando ciertas "características especiales" del entorno universitario que en el ENS son difíciles de encajar. Con esto, se conforma el **perfil de cumplimiento específico** para Universidades. Además, el perfil establece el marco de certificación de las universidades en el ENS y, por lo tanto, de acreditación fehaciente del cumplimiento legal por parte de la mismas.

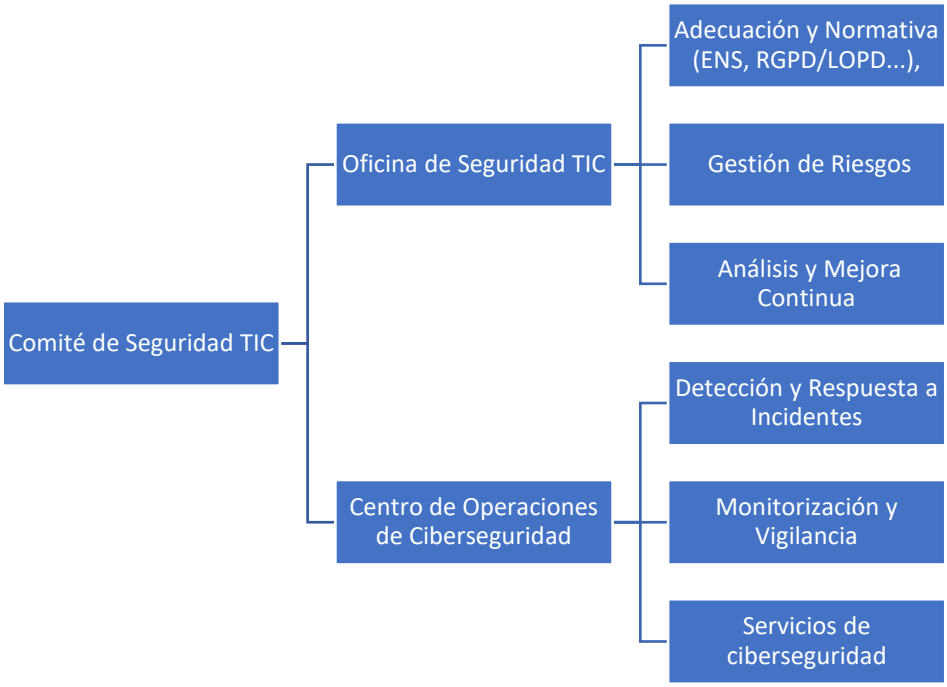
Con este trabajo habríamos cubierto los objetivos planteados inicialmente en el proyecto, pero se quiso dar a la guía una utilidad práctica aún mayor. El ENS propone un sistema de gestión de la seguridad (SGSI), con sus medidas o controles y la elaboración de planes de mejora de la seguridad; pero es de especial trascendencia tener en cuenta que este SGSI debe funcionar sobre una "organización de la seguridad" en la institución. Esta organización debe determinar los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de las estructuras de gobierno y operativas que la soporte.

Por eso, vimos fundamental proponer a las universidades un **marco de gobernanza** (a máximos) en el que se indican las distintas estructuras que deben intervenir en la gestión y gobierno de la seguridad (Comité de Seguridad, Oficina de seguridad, Centro de operaciones, Foro de universidades) y las relaciones entre ellas. También se proponen los diferentes roles y responsabilidades y todo esto se detalla en un modelo de "Política de Seguridad" que puede servir de plantilla para la elaboración de la Política de seguridad de cada universidad.

El modelo es una propuesta, que cada universidad podrá adaptar a sus circunstancias particulares. A modo de resumen muy breve, se propone la creación de las siguientes estructuras:

1. Comité de Seguridad TIC: órgano de carácter más político, encargado de la gobernanza de la seguridad de la información en la universidad.
2. Oficina de Seguridad TIC: encargada de la gestión y seguimiento de los planes y normativa de seguridad.
3. Centro de Operaciones de Ciberseguridad (COCs): encargado de 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.

En la siguiente figura se muestran de forma gráfica las dependencias y responsabilidades de estas estructuras:



3. Conclusiones:

Ha resultado una experiencia muy positiva de colaboración entre el organismo de referencia para la ciberseguridad en la Administración Pública española (CCN-CERT) y las universidades, con dos visiones inicialmente muy distintas sobre el tratamiento de la ciberseguridad, pero en el que finalmente ellos (el CCN-CERT) han podido adquirir una visión más clara de las limitaciones y características propias del entorno universitario; y las universidades nos hemos concienciado de la importancia de determinadas medidas y de hacer una gestión adecuada de la ciberseguridad. La comunicación ha sido muy fluida y el debate nos ha llevado a un aprendizaje mutuo y, sobre todo, a obtener un resultado de aplicación práctica que esperamos que mejore el posicionamiento de las universidades españolas en materia de ciberseguridad.

La visión de la seguridad de la información como un preocupación integral (de toda la organización); la implicación de los equipos de gobierno (en políticas y estrategias); la visión de la gestión basada en los riesgos; la seguridad basada en distintas líneas de defensa (organizativas, operativas y técnicas); y, muy especialmente, la diferenciación de responsabilidades en materia de ciberseguridad, son los principios que han guiado el desarrollo de este trabajo y que se pretenden reforzar con el mismo.

4. Resultados alcanzados:

En definitiva, el resultado de los trabajos realizados ha sido una Guía, publicada por el CCN-CERT en febrero de 2022, como documento de referencia, aunque no de obligado cumplimiento, que contiene los siguientes documentos:

1. El documento principal (Guía CCN-STIC 881): contiene la propuesta de un modelo para facilitar la adecuación al ENS por parte de las universidades:
    - Se propone un **modelo de gobernanza** de la ciberseguridad.

- Se indica el proceso a seguir en la adecuación al ENS (plan de adecuación).
- Se detalla cómo debe ser la aplicación de las medidas que nos afectan.

2. El **Perfil de cumplimiento** (CCN-STIC 881A): contiene la declaración de aplicabilidad (DoA) específica para las universidades y la particularización para nuestro entorno de algunas medidas. Constituye además el marco para la certificación en el ENS de las universidades.
3. Una propuesta (modelo) de **Política de Seguridad** (Anexo I).
4. Plan de adecuación (Anexo II): que contiene:
    - Una **propuesta de los activos esenciales** (servicios e información).
    - Se hace una **propuesta de valoración** de estos activos y de categorización del sistema.
    - Se obtiene una **declaración de aplicabilidad**.

Esta guía se está difundiendo y dando a conocer a las universidades y otros entornos de la Administración Pública española a través de distintos eventos.

Referencias:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
  URL: https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf

- Guía CCN-STIC 881 de Adecuación al ENS para Universidades:

  URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/6446-ccn-stic-881-adecuacion-al-ens-para-universidades.html