# EL ENS COMO MARCO DE SEGURIDAD DE LA INFORMACIÓN PARA LAS UNIVERSIDADES ESPAÑOLAS

# "NATIONAL SECURITY SCHEME" AS A FRAMEWORK FOR INFORMATION SECURITY IN SPANISH UNIVERSITIES

**Autores[1]:**

Antonio Muñoz Ropa. Universidad de Granada. aropa@ugr.es

Francisco José Sampalo Lainz. Universidad Politécnica de Cartagena. paco.sampalo@upct.es

**Resumen:**

El Esquema Nacional de Seguridad (ENS) constituye el marco normativo de obligado cumplimiento al que las Administraciones Públicas españolas deben adecuar sus políticas y actuaciones para que se garantice adecuadamente la seguridad de la información tratada. El artículo hace una revisión a muy alto nivel de los principios básicos del ENS, cómo propone afrontar el proceso de mejora en la gestión de la seguridad de la información y, finalmente, veremos algunos aspectos concretos de su aplicación a la seguridad de la información en el entorno universitario.

**Abstract:**

The National Security Scheme (ENS) constitutes the obligatory regulatory framework to which the Spanish Public Administrations must adapt their policies and actions so that the security of the information processed is adequately guaranteed. The article reviews at a very high level the basic principles of the ENS, how it proposes to deal with the improvement process in information security management and, finally, we will see some specific aspects of its application to information security in the university environment.

[1] Los autores son miembros del Grupo de Trabajo de Seguridad y Auditorías de la Sectorial CRUE-TIC.

**Palabras clave:**

Seguridad de la información; Gestión de la seguridad; Medidas de seguridad

**Keywords**

Information Security; Security Management; Security Measures

## 1. VISIÓN GENERAL DEL ESQUEMA NACIONAL DE SEGURIDAD (ENS)

El origen del Esquema Nacional de Seguridad (en adelante ENS) hay que buscarlo en la Ley 11/2007 de Acceso Electrónico de los ciudadanos a los Servicios Públicos, en la cual se establece y regula el derecho de los ciudadanos a comunicarse con las Administraciones Públicas a través de medios temáticos.

La propia ley 11/2007, en su artículo 42, apartado 2, indica la necesidad de crear un Esquema Nacional de Seguridad que establezca los principios y requisitos de una Política de Seguridad en la utilización de medios electrónicos que permitan garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de modo que los sistemas de información prestarán sus servicios y custodiarán la información sin interrupciones, modificaciones, fuera de control y sin que la información sea accedida por personas no autorizadas, asegurando la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos. De esta necesidad nace la publicación, el 29 de enero de 2010, del 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.

Esto ha sido refrendado posteriormente por las Leyes 40/2015 (Régimen Jurídico del Sector Público) y 39/2015 (Procedimiento Administrativo Común de las Administraciones Públicas) para las relaciones entre las Administraciones Públicas y de estas con los ciudadanos.

El Real Decreto por el que se regula el ENS comienza enumerando una serie de principios básicos que deben regir la gestión de la seguridad de la información en las Instituciones; estos principios sirven de base para el desarrollo de las medidas concretas. Los principios básicos establecidos son los siguientes:

- **Seguridad Integral:** La seguridad se entenderá como un proceso integral a toda la organización.
- **Gestión de riesgos:** permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.
- **Prevención, reacción y recuperación:** para conseguir que las amenazas no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.
- **Líneas de defensa:** disponer de una estrategia de protección constituida por múltiples capas de seguridad.
- **Reevaluación periódica:** basada en la mejora continua.
- **Función diferenciada:** especifica que debe existir una función diferenciada en materia de seguridad de la información, con su correspondiente responsabilidad.

Y de igual forma, en el artículo 11, se establecen unos requisitos mínimos de seguridad, entre los cuales destacamos en este artículo aquellos que afectan más directamente a la seguridad de la información:

- Análisis y gestión de los riesgos.
- Autorización y control de los accesos.
- Seguridad por defecto.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.

Todos estos apartados aparecen desarrollados en los artículos siguientes del ENS. Pero todo ello nos da una idea para que todo el sistema de información este completamente cubierto.

## 2. EL PROCESO DE CATEGORIZACIÓN EN EL ENS

El espíritu de este Real Decreto es el de garantizar el acceso del administrado, el ciudadano, a la administración electrónica los siete de días de la semana y los 365 días del año, para lo cual se establecen, en su Anexo II, las medidas de seguridad que se deben cumplir. La obligatoriedad para el cumplimiento de estas medidas viene

determinada por cómo sea nuestro sistema de información; o sea, por cómo lo tengamos categorizado y por las dimensiones de la seguridad debemos cubrir.

El ENS establece que un sistema de información puede ser de *categoría baja, media o alta*. Esto se deduce según la valoración de impacto que tendría sobre nuestra organización un incidente que pueda afectar a la seguridad de la información y de los sistemas. Este procedimiento se define en el Anexo I del Real Decreto. Así hay que decir que el entorno universitario la mayoría de los sistemas se han declarado como de *categoría media*.

Pero para hablar de la categorización se debe hablar también de las dimensiones de la seguridad, para poder valorar correctamente la categoría de nuestro sistema.

Así tenemos como dimensiones más elementales:

- ***Confidencialidad [C]*:** la información o un activo sólo es accesible por las personas interesadas.
- ***Integridad [I]*:** debemos saber cómo de importante es que la información sea veraz, no se haya modificado de forma indebida y que está actualizada.
- ***Disponibilidad [D]*:** cómo de importante es que el activo está disponible. Hay situaciones que es necesario un 24x7.

Estas tres dimensiones son sobre las que se habla en la seguridad de la información, pero hay otras dimensiones de la seguridad que se tienen en cuenta en el ENS, no menos importantes.

- ***Trazabilidad [T]*,** tener control sobre quién ha modificado o accedido a un activo/información y qué se ha modificado.
- ***Autenticidad [A]:*** como de veraz es la información; se debe valorar la importancia de que sea correcta la información.

Una vez que sabemos qué son las dimensiones se evalúa cada una de ellas para cada activo (un “activo” es cualquier componente del sistema de información que una empresa considera como valiosa: los recursos físicos, el software, todo tipo de documento, servicios, instalaciones, recursos humanos). Por lo que para llegar a la categorización del nuestro sistema debemos saber qué valoración tiene cada

dimensión (bajo, medio o alto, según el impacto) y acorde a esto, finalmente, podremos obtener la categoría del sistema, que se corresponderá con la valoración más alta que se haya obtenido para todos los activos/dimensiones.

Una vez realizada la valoración, hay que continuar con el proceso de adecuación al ENS; en el siguiente gráfico podemos ver los pasos que se deben realizar para adecuar nuestra universidad al ENS. Hay una serie de guías que suministra el CCN-CERT (Centro Criptológico Nacional) y que son de gran ayuda en cada uno de los pasos que debemos dar, todo ello mediante la elaboración previa de un plan de adecuación; el gráfico nos da una visión general del proceso.

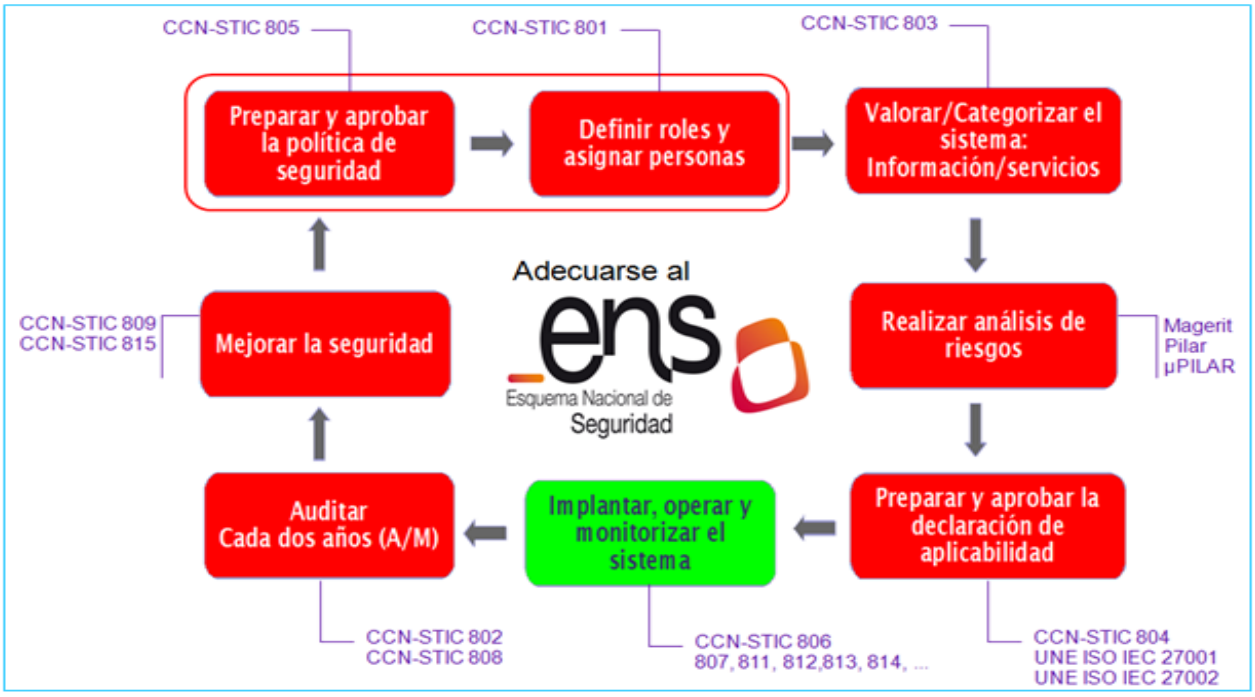


*Figura: Adecuación al Esquema Nacional de Seguridad.*

**Figura 1**
**Esquema Nacional de Seguridad**
Fuente: https://administracionelectronica.gob.es

## 3. EL ENS Y PRIVACIDAD

La nueva Ley de Protección de Datos (Ley 3/2018, de 6 diciembre, de Protección de Datos y Garantía de Derechos Digitales, en adelante LOPDGDD) tiene su origen como consecuencia de la adecuación por parte del Estado Español al RGPD (Reglamento General de Protección de Datos) de la Unión Europea. De esta forma se persigue que

todos los países miembros de la Unión tengamos un marco común en esta materia. En esta normativa se trata constantemente del principio de confidencialidad de la información, lo que nos da una idea de la importancia de esta dimensión de la seguridad.

¿Y cómo se relaciona todo esto con el ENS? Para responder a esta pregunta tenemos que acudir a la Disposición Adicional Primera de la LOPDGDD se establece que las medidas de seguridad que se deben aplicar en el ámbito del sector público son las que se indican el ENS.

EL ENS está en constante proceso de revisión y mejora y se prevé la aprobación de un nuevo Real Decreto, cuyo borrador definitivo ya está elaborado, a principios de 2022. Además, se ha complementado con un conjunto de guías de ayuda para su implantación (Guías CCN-STIC, serie 800). Algunas de estas guías han sido particularizadas para el entorno universitario y son las que hemos tomado de base para la elaboración de este artículo.

## 4. LA VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN EN LAS UNIVERSIDADES

Una vez expuesto el contexto y el proceso general que propone el ENS para la gestión de la seguridad de la información es hora de que nos centremos en su aplicación específica dentro del entorno universitario. Como se explicó anteriormente, una vez aprobada la Política de Seguridad de la Información y definidas las distintas responsabilidades en materia de seguridad, el siguiente paso es la “categorización” del sistema de información, mediante la valoración de los denominados “activos esenciales”, que son los que determinan el “alcance del sistema” o, dicho de otra forma, el ámbito en el que se van a aplicar las medidas de seguridad que se determinen.

Los “activos esenciales” son aquellos que constituyen la esencia y razón de ser del sistema y pueden ser de tipo “servicio” o de tipo “información”.

El primer paso es, por lo tanto, elaborar un catálogo identificando los activos esenciales, servicios e información, y el sistema en el que se alojan. En el caso de las

universidades, nuestra propuesta es elaborar un catálogo de servicios estándar, válido para cualquier universidad, basado en las competencias de las Universidades recogidas en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (LOU). Habría que realizar un trabajo exhaustivo de identificación de la información manejada por cada servicio, de forma que la universidad pueda encontrar todas las funciones que realiza en la columna de información.

No es el propósito de este artículo proponer un catálogo de activos esenciales, pero sí exponer el proceso por su interés para la gestión de la seguridad, así que, a modo de ejemplo y posible guía, y sin ánimo de ser exhaustivos, proponemos un par de activos relevantes y cómo se tratarían:

a. **"Docencia y Estudios":** se considera que constituye un "servicio esencial" prestado por la universidad, pues así está indicado en el artículo 1 de la LOU (funciones de la universidad) y desarrollado en los títulos VI (De las enseñanzas y títulos) y VIII (De los estudiantes).
   Este servicio se fundamenta en el tratamiento de la siguiente información (que constituyen los "activos esenciales de información" asociados a este servicio) relacionadas con las enseñanzas impartidas en la universidad:
   - Gestión académica
   - Becas y ayudas
   - Docencia (presencial y virtual)
   - Guías docentes
   - Matrícula
   - Títulos
   - Enseñanzas propias
   - Secretaría virtual.

b. **Régimen económico:** se considera que constituye un "servicio esencial", pues en el artículo 79 de la LOU se establece la autonomía económica y financiera de la universidad, cuyos términos se desarrollan en el título XI (Del régimen económico y financiero de las Universidades públicas). Este servicio se fundamenta en el tratamiento de la siguiente información:

- Gestión económica:
    - Contabilidad
    - Tesorería
    - Presupuestos
- Colaboraciones con empresas
- Fundaciones
- Patrimonio
- Personas físicas
- Personas jurídicas

Otros activos o servicios esenciales a desarrollar con su información asociada podrían ser: investigación, extensión universitaria, comunicación institucional, profesorado y PAS (Recursos Humanos), colaboración universitaria, sede electrónica, movilidad, etc.

El paso siguiente, una vez establecido este catálogo de activos esenciales, sería su valoración. Para los activos de tipo "información" se valoran las siguientes dimensiones de seguridad: confidencialidad, integridad, autenticidad, trazabilidad y, si fuera relevante, disponibilidad. Es frecuente que la disponibilidad no sea un atributo relevante de la información y quede sin adscribir a ningún nivel.

Para los activos de tipo "servicio" se valora la disponibilidad pues los requisitos en materia de confidencialidad, integridad, autenticidad y trazabilidad suelen venir impuestos por los tipos de información que maneja el servicio.

Continuando con los ejemplos expuestos (repetimos que sin ánimo de ser exhaustivos ni establecer una valoración definitiva) y siguiendo los criterios establecidos[2], podemos proponer los siguientes valores:

[2] Los criterios de valoración de las dimensiones de seguridad, y la asignación de sus niveles, están descritos en la Guía CCN-STIC 803 de Valoración de Sistemas.

| INFORMACIÓN | SERVICIOS | [C] | [I] | [T] | [A] | [D] |
|---|---|---|---|---|---|---|
| Gestión académica<br>Becas y ayudas<br>Docencia (presencial y virtual)<br>Guías docentes<br>Matrícula<br>Títulos<br>Enseñanzas propias<br>Secretaría virtual | DOCENCIA-ESTUDIOS | Medio | Medio | Medio | Medio | Medio |
| Gestión económica:<br>− Contabilidad<br>− Tesorería<br>− Presupuestos<br>Colaboraciones con empresas<br>Fundaciones<br>Patrimonio<br>Personas físicas<br>Personas jurídicas | RÉGIMEN ECONÓMICO | Bajo | Bajo | Bajo | Bajo | Medio |

Finalmente, siguiendo el procedimiento descrito en el Anexo I del ENS, procederemos a la determinación de la categoría del sistema, que en el caso de nuestro ejemplo será MEDIA.

| CATEGORÍA DEL SISTEMA | [C] | [I] | [T] | [A] | [D] |
|---|---|---|---|---|---|
| NIVEL MÁXIMO SERVICIOS+INFORMACIÓN | [M] | [M] | [M] | [M] | [M] |
| **CATEGORÍA MEDIA [ C=M, I =M, T=M, A=M, D=M ]** | | | | | |

## 5. MEDIDAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Dentro del conjunto de las 75 medidas que se enumeran en el Anexo II del Real Decreto, a continuación proponemos aquellas que se pueden considerar más relevantes para la seguridad de la información y que afectan principalmente a las dimensiones de confidencialidad, integridad y disponibilidad:

— **Política de seguridad**: el primer paso para trabajar en materia de seguridad es definir la Política de Seguridad de la Información de la Institución, que debe

definir un modelo organizativo y de gobernanza, así como los compromisos de seguridad de la institución.

— **Análisis de riesgos**: es un proceso básico también para saber cómo nos encontramos en materia de seguridad de la información y saber que salvaguardadas debemos aplicar para tener nuestro sistema de la información lo más seguro posible, aunque siempre debemos aceptar un riesgo ya que el 100% de la seguridad no lo vamos a conseguir. Debe ser un análisis de riesgos semiformal que se debe actualizar al menos, anualmente o bien cuando haya cambios relevantes en el sistema.

— **Control de acceso**: son medidas fundamentales para preservar la confidencialidad y privacidad de la información. La identificación de usuarios en el sistema se implementará asegurando un identificador singular (cuentas individualizadas) de tal forma que se pueda conocer a quién pertenece, y con qué privilegios se accede y qué acciones realiza. Debemos exigir que las credenciales estén bajo el control exclusivo del usuario, reconociendo que las ha recibido y que acepta las condiciones que implica su tenencia. Estas credenciales se cambiarán con la periodicidad marcada por la política de la universidad y se retirarán e inhabilitarán cuando se termine la relación con el sistema o cuando se detecte que su pérdida o control por parte del usuario; se establecerá una limitación de intento de accesos.

  Los **mecanismos de autenticación** se adecuarán al nivel de seguridad del sistema, pudiendo usarse, de manera aislada o combinada, los siguientes factores de autenticación: "algo que se sabe" (contraseñas o claves concertadas), "algo que se tiene" (certificados, aplicaciones móviles, tokens, etc.) y algo que se es" (elementos biométricos: huella digital, patrón del iris, etc.)

  El proceso de **gestión de derechos de acceso** se realizará en base al cumplimiento principios tales como, “todo acceso está prohibido, salvo autorización expresa”, “mínimo privilegio”, “necesidad de conocer y responsabilidad de compartir” y “capacidad de autorizar”. Una vez otorgado el acceso se informará al usuario de sus obligaciones. Se habilitará el registro de

los accesos con éxito y fallidos, y se informará al usuario del último acceso realizado con su identidad.

— **Gestión del personal**: Se deben realizar acciones de concienciación sobre las responsabilidades de todo el personal de la universidad respecto a la seguridad del sistema, especialmente aquellas relacionadas con la normativa de seguridad, las técnicas de ingeniería social más habituales, la identificación de incidentes de seguridad y la forma de comunicarlos. También se realizarán acciones de formación en materia de seguridad de la información, necesarias para el desempeño de las funciones del personal, orientadas al personal técnico. En ambos casos se recomienda realizar una planificación por ciclo anual.

— **Protección de equipos y puesto de trabajo**: debemos tener siempre la mesa de trabajo despejada de forma que una vez terminado la actividad laboral la información se quede bajo llave, ya que es la única forma de preservar la confidencialidad (o privacidad) de la información, teniendo en cuenta que pueda ser accesible a personas que no deban tener acceso a esa información. De igual forma tenemos que tener cuidado en los desplazamientos con nuestros dispositivos portátiles, cifrar los contenidos en la medida de lo posible y establecer canales para avisar de los posibles robos o accesos no autorizados.

— **Protección de las comunicaciones**: se dispondrá un sistema de protección perimetral que establezca un perímetro seguro que separe la red interna del exterior. Para la protección de la confidencialidad cuando la comunicación discurra por redes fuera del propio dominio de seguridad, se emplearán redes privadas virtuales (VPN) cifradas y algoritmos y parámetros autorizados por el CCN.

  Para la protección de la integridad y de la autenticidad en las comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información y se prevendrán ataques activos (alteraciones de información, inyección de información espuria o secuestros de sesión).

Para el control de acceso a la información y la mitigación de los efectos de propagación de los incidentes de seguridad será necesario llevar a cabo una segmentación en la red de tal forma que cada equipo solamente tenga acceso a los servicios e información que necesita; y en caso de utilizar comunicaciones inalámbricas, estas se dispondrán en un segmento de red separado.

— **Protección de los soportes de información**: Debemos proteger la información en dispositivos removibles (CD, DVD, discos extraíbles, pendrives, memorias USB, u otros de naturaleza análoga), cuando salgan de las áreas controladas; en estos casos se aplicará criptografía, garantizando de este modo la confidencialidad e integridad de la información contenida en los mismos. Siendo necesario el uso de algoritmos y parámetros autorizados por el CCN. Las copias de seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

  Se deben implementar y documentar los **métodos de borrado y destrucción** seguros a aplicar en función del dispositivo, garantizando que los soportes que vayan a ser reutilizados o liberados a otra organización sean objeto de un borrado seguro, empleando productos certificados, y cuando este no sea posible, no sea utilizado en ningún otro sistema.

— **Protección de la información:** cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y en la Ley Orgánica 3/2018, de 5 de diciembre. Será recomendable aplicar medidas técnicas y organizativas para la **anonimización y seudonimización** de datos personales y que, en los tratamientos con fines estadísticos, los datos son destruidos lo antes posible y que solo se conservan los necesarios, respetando el principio de minimización.

  Se implementará y documentará un proceso de **calificación de la información**, que tenga en cuenta que esta se realizará según lo establecido legalmente sobre la naturaleza de la misma; se utilizará la etiqueta “USO OFICIAL” para información con algún tipo de restricción ya sea en su manejo, sensibilidad y confidencialidad.

En cuanto a la **firma electrónica**, se emplearán los tipos previstos en el ordenamiento jurídico. Se emplearán sistemas de firma electrónica avanzada basados en certificados cualificados, empleando algoritmos y parámetros autorizados. Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte.

Cuando los documentos vayan a ser difundidos ampliamente ya sea directamente o a través de su publicación en sitios web o sedes electrónicas, se definirá y documentará un proceso de **limpieza de documentos**, de tal forma que se garantice que con carácter previo a su difusión se ha eliminado toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores.

Se implementarán políticas de **copias de seguridad** que garanticen la recuperación de la información ante un incidente de seguridad, definiéndose su periodicidad y plazos de retención. Se realizarán y planificarán pruebas periódicas de recuperación.

Las medidas descritas deben ser valoradas, adaptadas y aplicadas a cada universidad. Este proceso de análisis y toma de decisiones debe ser colegiado y en él deben intervenir no sólo personas del ámbito técnico, sino también (y fundamentalmente) personas con responsabilidades de gobierno o del tratamiento de la información. Este modelo de gobernanza y toma de decisiones debe estar reflejado en la Política de Seguridad de la Información y deberá tener como estructura central a un Comité de Seguridad de la Información.