# LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS UNIVERSIDADES ESPAÑOLAS

Vicente Andreu, Francisco J. Sampalo y Víctor Huerta

## Resumen

Históricamente, el tratamiento de la Seguridad de la Información en las universidades españolas se ha planteado desde la perspectiva puramente técnica: se ha considerado, más bien, como seguridad de los sistemas de información y se ha venido atribuyendo la responsabilidad exclusiva a las áreas de TI o incluso se ha asumido como una función propia de los administradores de las infraestructuras o de los desarrolladores de los servicios. Esta aproximación ha dado lugar a la aplicación de medidas técnicas u organizativas concretas, más o menos efectivas, pero que adolecen de una visión de conjunto y en muchos casos no están alineadas con las políticas y estrategias de los equipos de dirección.

El Esquema Nacional de Seguridad (ENS[5]) ha supuesto un hito fundamental para el impulso de la *Gestión global de la Seguridad de la Información* en las Administraciones Públicas Españolas (entre ellas las Universidades) y se ha constituido como el marco común de referencia para la gestión de la Seguridad en estos entornos. El ENS es un instrumento detallado y de carácter práctico que se basa en una serie de principios básicos. El primero de ellos es el de *Seguridad Integral* (Art. 5):

> 1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

En UNIVERSITIC hemos sido conscientes de la creciente importancia de la seguridad en la prestación de los servicios TI y por ello se ha incluido en los últimos años como un objetivo dentro del eje correspondiente del apartado de Gestión.

La Gestión de la Seguridad TI debe comenzar por la definición de una Política de Seguridad en la que se determina la estructura de gobernanza de la misma, lo cual se plasma desde un punto de vista organizativo en la definición y asignación de los distintos roles o responsabilidades previstos en el ENS. El siguiente paso es el proceso de valoración de los sistemas, lo cual nos pondrá en contexto sobre los requisitos y medidas de seguridad que serán de aplicación a nuestro sistema o sistemas. Es importante resaltar que la valoración no es responsabilidad exclusiva de un rol concreto, sino que en este proceso de valoración deben intervenir, en sus respectivos ámbitos de competencia, los distintos responsables establecidos en la Política de Seguridad.

---

[5] 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. https://boe.es/buscar/pdf/2010/BOE-A-2010-1330-consolidado.pdf

Tal y como se expresa en este capítulo del Informe UNIVERSITIC, en este artículo queremos ir más allá de los datos, analizando los mismos y proponiendo unos criterios concretos que ayuden a las universidades a la designación de los roles y a la valoración de sus Sistemas, teniendo en cuenta las peculiaridades de las estructuras universitarias.

## Análisis de datos de UNIVERSITIC

Para conocer el estado de la seguridad en las universidades la referencia fundamental es el Informe Nacional sobre el Estado de la Seguridad (INES[6]). Este informe anual, de cumplimentación obligatoria para todas las administraciones públicas, es la base para otro elaborado por el CCN-CERT[7] (Informe IT 09/17), que compila los datos proporcionados por las Universidades públicas y contiene un análisis detallado de toda la información aportada por las mismas en cuanto a su organización, sus procedimientos de seguridad, los incidentes reportados y las medidas de seguridad aplicadas. El informe incluye, además, datos globales, conclusiones y recomendaciones y permite el análisis comparativo del grado de implantación del ENS en el sistema universitario público español. Dado el elevado grado de análisis y detalle de este informe no entraremos en este artículo a analizar el grado de cumplimiento del ENS en las universidades españolas, pero sí recomendamos su lectura detallada.

Una segunda referencia de gran valor es nuestro informe UNIVERSITIC. Dado su carácter global, la información solicitada en UNIVERSITIC sobre gestión de la seguridad es menos detallada, pero también nos ofrece información de interés que puede ser complementaria a la del Informe INES. Y esto es lo que queremos analizar en este apartado. En primer lugar, como ya se ha indicado, se ha dedicado el objetivo 3.3 de la capa de Gestión de las TI de UNIVERSITIC ("Proveer a los servicios de las condiciones de seguridad adecuadas") a una serie de indicadores básicos que reflejan la organización en materia de seguridad (tabla 3.5). Para este artículo nos interesa centrarnos en la asignación y roles y responsabilidades, así que ahondaremos un poco más en la información aportada por las universidades. Dentro del eje 3 Servicios TI del catálogo de Gestión de las TI, en concreto en el Objetivo 3.3 se pide a las universidades que indiquen quién tiene asignado cada uno de los tres roles (Responsable de la Información, Responsable de los Servicios y Responsable de Seguridad) dentro de su organización. En los siguientes gráficos 4.5, 4.6 y 4.7 vemos cómo se han ido asignando estas responsabilidades dentro de las Universidades.

[6] Informe Nacional de Estado de la Seguridad. https://www.ccn-cert.cni.es/ens/ines.html

[7] Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional. https://www.ccn-cert.cni.es/

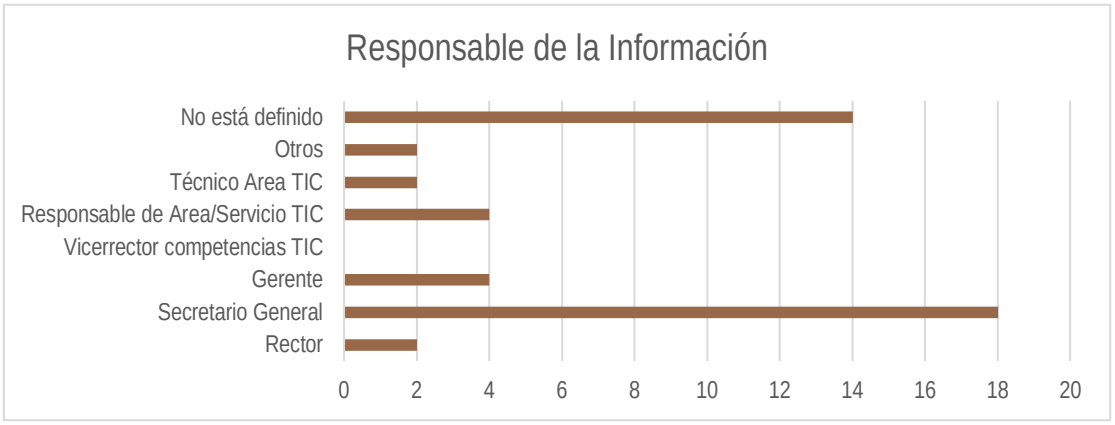


Gráfico 4.5. Asignación del responsable de la información en las universidades

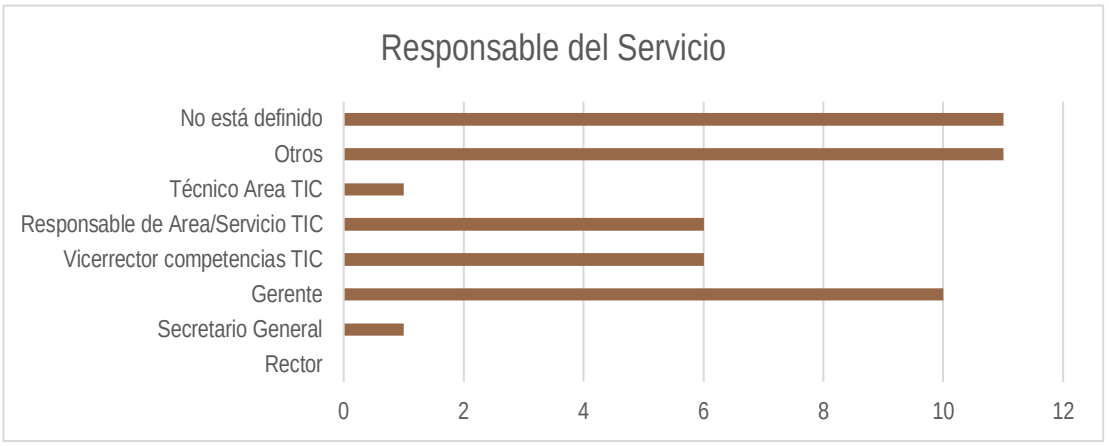


Gráfico 4.6. Asignación del responsable del servicio en las universidades

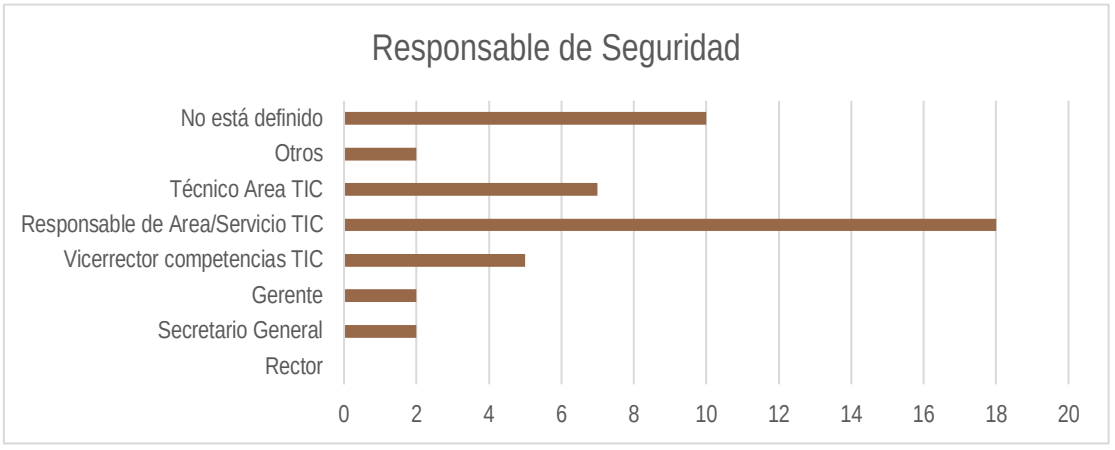


Gráfico 4.7. Asignación del responsable de seguridad en las universidades

Es relevante constatar y resaltar, por su trascendencia, algunos hechos que se deducen del estudio UNIVERSITIC y que evidencian una falta de homogeneidad en la toma de decisiones que resulta, cuanto menos, curiosa en entornos tan semejantes como los sometidos a análisis. Así, pues, podemos observar lo siguiente:

- Hay 10 universidades que no tienen definido ninguno de los roles.
- Hay 2 universidades en la que los tres roles recaen sobre la misma persona (Responsable del Área TIC) y hay 6 en la que una misma persona asume dos roles.
- Hay 4 universidades en las que el Responsable de la Información y/o el Responsable del Servicio están bajo de la dependencia jerárquica del Responsable de Seguridad.

Todos estos datos evidencian dos conclusiones:

1. No existe la uniformidad que cabría esperar a la hora de asignar los roles y responsabilidades básicos en materia de gobierno y gestión de la seguridad de los sistemas de información en las Universidades.
2. No existen unos criterios claros y homogéneos sobre las funciones a desempeñar que permitan la integración de los roles del ENS en las estructuras TI de las Universidades de una manera sencilla y sobre la que exista cierto consenso.

Por otro lado, dentro de la relación de los *10 Temas clave para el Equipo de Gobierno* se incluyó la Seguridad de la Información (definido como "Desarrollar un enfoque holístico y ágil para reducir la exposición institucional a las amenazas a la seguridad de la información"). Los resultados de este apartado se han analizado más en profundidad en el primer apartado de este tercer capítulo del informe (*Líneas estratégicas TI de presente y de futuro* de F. Llorens y R. Molina). Pero centrándonos en la Seguridad de la Información, podemos observar que en la valoración global resultó el segundo tema clave más valorado, justamente detrás de la Transformación Digital del Aprendizaje. El detalle de las respuestas obtenidas es:

- 23 universidades lo consideran un tema clave que están abordando ya.
- 12 universidades lo consideran un tema clave a abordar en el futuro.
- 1 universidad no lo considera un tema clave.

Finalmente, para cubrir todos los aspectos de la Seguridad, aparte de su gobierno y gestión, si bajamos a un ámbito más operativo, otro dato que podemos analizar es el número de técnicos que se están dedicando a la seguridad (gestión y/o operación) en las plantillas de los Servicios TI. Analizando las respuestas a la pregunta "¿A qué se dedican los técnicos TI?" obtenemos los siguientes resultados:

- Sobre un total de 4.853 técnicos en las plantillas TI de las universidades, se dedican exclusivamente a seguridad unos 117 técnicos, lo que supone un 2,14% del total de las plantillas.
- 16 universidades afirman no tener ningún técnico asignado a tiempo completo a tareas de gestión u operación de la seguridad TI.
- 26 universidades tienen un único técnico dedicado a seguridad.
- 8 universidades tienen 3 o más de 3.

Estos datos ponen de manifiesto que la dotación de recursos humanos para la seguridad TI en las universidades es claramente escasa e insuficiente para los retos que se plantean. Esto coincide con una de las recomendaciones de actuación que aparecen en las conclusiones del Informe INES:

Emplear recursos en:

- Elaboración de normativa y procedimientos de seguridad.
- Mecanismos asociados a la gestión y mantenimiento del proceso de seguridad y a la monitorización del mismo.
- Desplegar soluciones que faciliten el uso de mecanismos de autenticación fuerte y mejora en la continuidad de los servicios

Una vez expuestos y analizados estos datos básicos que nos reflejan la situación actual, y volviendo a lo expuesto en el resumen, en los siguientes apartados vamos a proponer unos criterios básicos para abordar tanto la asignación de roles como la valoración de los Sistemas de Información en las universidades.

## Los roles de seguridad de la información en las universidades

En el ENS y sus Guías de desarrollo se establece que "todas las decisiones deben estar debida y formalmente aprobadas". Para ello se definen los diferentes cuatro roles con sus correspondientes responsabilidades, que son los siguientes:

- El *Responsable de la Información* debe establecer el valor que los activos de información tienen para cada organización.
- El *Responsable del Servicio* hace lo propio con el servicio o servicios TI que se presten a la comunidad.
- El *Responsable de la Seguridad* debe determinar y aprobar las medidas de seguridad que son de aplicación (Declaración de Aplicabilidad) y las medidas técnicas que se toman para sustanciar dichas medidas de seguridad.
- Si se toman decisiones de suspensión parcial o total de un sistema, estás vendrán aprobadas por el *Responsable del Sistema* y los responsables de los servicios afectados por la suspensión.

En el ámbito universitario las distintas responsabilidades introducidas por el ENS, justo en medio de un entorno especialmente restrictivo para la incorporación de recursos humanos y para la modificación de las plantillas, se han asociado desde la aprobación del Real Decreto 3/2010 con diferentes cargos o perfiles profesionales preexistentes. No ha habido una postura homogénea sobre los roles a desempeñar en todo el sistema universitario público, tal y como se deduce del análisis de datos del apartado anterior.

Atendiendo a lo anteriormente expuesto, creemos conveniente formular una serie de recomendaciones relacionadas con la atribución de funciones del ENS a cargos o perfiles profesionales de las universidades atendiendo a la capacidad de decisión o a los conocimientos técnicos exigibles para desempeñarlas. Obviamente, nuestra propuesta debe entenderse como una recomendación o una posible solución ante el problema que ha planteado la aplicación del ENS. Queda a la libre decisión de cada universidad, en el ejercicio de su autonomía, determinar el órgano, cargo o puesto de trabajo que debe asumir cada rol, de acuerdo con su propia organización interna y los perfiles profesionales con los que cuente. En todo caso, resulta especialmente importante, imprescindible desde nuestro punto de vista, respetar lo previsto por el ENS en materia de compatibilidad de funciones e independencia en la toma de decisiones.

Una solución común, como se ha visto en los datos expuestos, y contemplada en el propio esquema y en las guías de aplicación del mismo es que determinados roles sean asumidos por un comité. No es, en absoluto, cuestionable esta decisión, pero sí que consideramos que en aquellos casos en los que alguna de las funciones sea asumida por un Comité y no por un órgano unipersonal o por un funcionario, deberá garantizarse que la operativa del mismo (frecuencia de las reuniones, capacidad de decisión…) sea adecuada al cumplimiento de las funciones previstas en la guía CCN-STIC 801[8], en la que nos hemos basado para definir los perfiles que recomendamos a continuación.

### Responsable de la Información

Corresponde a un miembro del equipo de dirección determinar los fines y ostentar la responsabilidad última de la información de la Universidad. Esta función puede ser asumida por:

- El Secretario o la Secretaria General
- El o la Gerente
- Un Comité de Seguridad

En todo caso, este rol no debe o no es aconsejable que sea compatibilizado, conforme a la guía CCN-STIC-801, con el que se atribuya al:

- Responsable del Servicio, en aquellos casos en que la prestación del servicio no dependa de la unidad que es Responsable de la Información
- Responsable del Sistema

### Responsable del Servicio

Corresponde a un miembro del equipo de dirección, o al nivel de responsabilidad inmediatamente inferior a éste, establecer los requisitos del servicio en materia de seguridad en la universidad. Esta función puede ser asumida por:

- El Vicerrector o la Vicerrectora con responsabilidad TIC
- El o la Gerente
- El o la Vicegerente TIC
- Un Comité de Seguridad

En todo caso, este rol no debe o no es aconsejable que sea compatibilizado, conforme a la guía CCN-STIC-801, con el que se atribuya al:

- Responsable de la Información, en aquellos casos en que la prestación del servicio no dependa de la unidad que es Responsable de Información,
- Responsable del Sistema.

[8] Guías CCN-STIC de Seguridad. https://www.ccn-cert.cni.es/guias.html

### Responsable de la Seguridad

Corresponde a un cargo o funcionario, a nivel ejecutivo, designado formalmente por el Rector o el Equipo de Dirección, mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información de la Universidad. El Responsable de la Seguridad no puede pertenecer a los órganos de gobierno de la Universidad y no deberá tener ninguna responsabilidad sobre la prestación de los servicios TIC, ni deberá estar bajo la dependencia jerárquica del Responsable del Sistema. El Responsable de Seguridad debe ser designado atendiendo a sus cualidades profesionales y a los conocimientos especializados que garanticen su capacidad para desempeñar las tareas previstas en el ENS, en particular:

- Determinar la categoría de los sistemas.
- Analizar los riesgos.
- Establecer la aplicabilidad de las medidas de seguridad.
- Elaborar planes de formación y concienciación.

Esta función puede ser asumida por:

- Un técnico con nivel de responsabilidad y de cualificación adecuados para supervisar y, en su caso, aprobar las decisiones que en materia de seguridad adopte el Responsable del Sistema.
- Un Delegado del Rector (PAS o PDI).

En todo caso, este rol no debe o no es aconsejable que sea compatibilizado, conforme a la guía CCN-STIC-801, con el que se atribuya al:

- Responsable de la Información
- Responsable del Servicio
- Responsable del Sistema

### Responsable del Sistema

Corresponde a una persona designada por los órganos de dirección desarrollar, operar y mantener el sistema o los sistemas de información de la universidad durante todo su ciclo de vida. Esta función puede ser asumida por:

- Un Jefe o una Jefa de Área TIC
- Un Jefe o una Jefa de Servicio TIC

El Responsable del Sistema es un puesto operativo, no un cargo directivo o de gobierno. En todo caso, este rol no debe o no es aconsejable que sea compatibilizado, conforme a la guía CCN-STIC-801, con el que se atribuya al:

- Responsable de Seguridad
- Responsable del Servicio
- Responsable de la Información

## Criterios de valoración

Otro de los aspectos sobre los que se fundamenta la Gestión de la Seguridad es el proceso de valoración de los activos esenciales, definido en la Guía CCN-STIC 803 como:

> "la determinación de los tipos de información que se van a manejar y una clasificación de los servicios que se van a prestar. Definidos los tipos de información y de servicios, considerando los activos esenciales, una tarea del Comité STIC puede ser el establecimiento de los niveles de seguridad en cada dimensión, recomendados para cada uno de estos activos esenciales, y dentro de ellos cada uno de los tipos de información y servicios que los componen."

Los criterios de valoración que se proporcionan en la Guía CCN-STIC son generales, pues se refieren al ámbito global de las Administraciones Públicas españolas. Al igual que sucedía con la designación de los roles, cabría esperar cierta homogeneidad en la valoración de sistemas o de información que, en mayor o menor medida, se utilizan para prestar servicios similares en cada universidad. No parece, en consecuencia, muy congruente la disparidad en las categorizaciones que es, sin lugar a dudas, producto de la subjetividad con la que pueden aplicarse los criterios de valoración.

La tabla 4.8, obtenida a partir del informe INES sobre el estado de la Seguridad en las Universidades públicas muestra que hay ciertas diferencias de criterio a la hora de valorar los sistemas de información en las universidades.

Tabla 4.8. Categorías de los sistemas TIC de las universidades

| Organismos | Básica | Media | Alta | Global |
|---|---|---|---|---|
| Universidades | 5 | 32 | 5 | 42 |

Debido a ello, nos hemos planteado la conveniencia de establecer criterios específicos de valoración para el ámbito universitario que sean de aplicación a todas las dimensiones de seguridad, tanto de tipos de información como de servicios considerando las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios. Estos criterios deben servir para, al aplicarlos conjuntamente con los criterios de carácter general contemplados en la guía CCN-STIC 803, matizar o equilibrar la aplicación de los mismos tomando en consideración la naturaleza de los datos tratados por las universidades, la finalidad de los sistemas y el hecho de que los mismos se produzcan en ámbitos acotados y restringidos. Los criterios de impacto hemos considerado son los siguientes:

- Investigación científica: determinados tratamientos de información llevados a cabo con fines científicos, al aplicarles los criterios generales, pueden exigir una categorización excesiva para el nivel de riesgo que suponen si se toma en consideración que el tratamiento se produce en un ámbito acotado y de acceso muy restringido (grupos de investigación, laboratorios… ).

- Docencia: a la hora de categorizar los sistemas debe tomarse en consideración que los usuarios de los mismos (profesores y alumnos) interactúan sobre ellos en un ámbito cerrado y con una finalidad muy concreta.
- Gestión: aunque mayoritariamente sean de aplicación los criterios generales contemplados en la guía CCN-STIC 803, algunas peculiaridades de las universidades, deben ser tomadas en consideración como, por ejemplo, el hecho de que los afectados por múltiples procedimientos son alumnos vinculados a la universidad y sometidos a un régimen particular y no ciudadanos cualesquiera. Este hecho puede moderar el criterio general dado que el impacto en la imagen o en un número elevado de ciudadanos puede verse disminuido.
- Actividades culturales, deportivas o de ayuda al estudiantado: aunque sean actividades desarrolladas por un organismo público, carecen de relevancia administrativa.

En las siguientes tablas (4.9, 4.10 y 4.11) proponemos una serie de criterios de valoración específicos para el ámbito universitario, tanto en las dimensiones aplicables a la información (confidencialidad, integridad, autenticidad y trazabilidad), como a los servicios (disponibilidad). Esto se completa con un apartado específico para los datos personales alineado con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Si bien será la Agencia Española de Protección de Datos la que establezca reglamentariamente los criterios a emplear, en este apartado se incluyen algunos criterios específicos del sector universitario a título orientativo para facilitar la labor del Responsable de la Seguridad, de forma que permitan establecer los sistemas que intervienen en las actividades de tratamiento de datos de carácter personal, en función de dos criterios:

- El tipo de datos personales incluidos en los tipos de información identificados.
- Determinadas características de las operaciones de tratamiento, como son:
  a) Cantidad considerable de datos personales.
  b) Importante riesgo para los derechos y libertades de los interesados.
  c) Evaluación sistemática de aspectos personales de los estudiantes.
  d) Videovigilancia, control de acceso a campus y otras zonas de acceso público.
  e) Personas con acceso a la información: cuando la información es tratada por un número reducido de personas el riesgo es menor.
  f) Ámbito: el tratamiento en determinados ámbitos como el de la salud o el de la investigación científica, llevado a cabo por profesionales sanitarios o investigadores, puede ser un factor de impacto a considerar.

Tabla 4.9. Criterios de valoración ámbito universitario (información general)

| CRITERIOS PARA TIPOS DE INFORMACIÓN GENERAL | | | | |
|---|---|---|---|---|
| | No adscrito (N/A) | BÁSICO | MEDIO | ALTO |
| Datos de investigación | UNI.INF.INV.N<br>Datos públicos o que pueden ser publicados sin causar perjuicio a la investigación. | UNI.INF.INV.B<br>Datos cuya publicación podría causar un perjuicio a la investigación. | UNI.INF.INV.M<br>Datos vinculados a investigación o resultados de investigación susceptibles de generación de patentes o pueda suponer un riesgo para:<br>a) Los intereses económicos y comerciales.<br>b) La propiedad intelectual e industrial. | UNI.INF.INV.A<br>Datos vinculados a investigación o resultados de investigación cuya revelación pueda suponer un riesgo para:<br>a) La seguridad nacional.<br>b) La defensa.<br>c) Las relaciones exteriores.<br>d) La seguridad pública.<br>e) La protección del medio ambiente. |
| Datos de infraestructuras | UNI.INF.INR.N<br>Datos públicos de infraestructuras universitarias. | UNI. INF.INR.B<br>Datos de infraestructuras básicas y ubicaciones físicas relacionadas con las funciones básicas de gestión, docencia e investigación. | UNI. INF.INR.M<br>Datos de infraestructuras relacionadas con las funciones de investigación cuya revelación y/o modificación pueda suponer un grave riesgo para los intereses de la Universidad o de entidades vinculadas o colaboradoras. | UNI. INF.INR.A<br>Datos de infraestructuras relacionadas con las funciones de investigación cuya revelación pueda suponer un grave riesgo para:<br>a) La seguridad nacional.<br>b) La defensa.<br>c) Las relaciones exteriores.<br>d) La seguridad pública.<br>e) La protección del medio ambiente. |
| Datos de docencia | UNI.INF.DOC.N<br>Datos públicos de docencia. | UNI. INF.DOC.B<br>Datos de docencia, guías docentes, materiales protegidos por la normativa de propiedad intelectual | UNI. INF.DOC.M<br>N/A | UNI. INF.DOC.A<br>N/A |
| Gestión | UNI.INF.GES.N<br>Datos abiertos de gestión y *datawarehouse*. | UNI. INF.GES.B<br>Datos de gestión relacionados con las funciones básicas de gestión, docencia e investigación. | UNI. INF.GES.M<br>Datos de gestión cuya revelación y/o modificación pueda suponer un grave riesgo para los intereses de la Universidad o de entidades vinculadas o colaboradoras. | UNI. INF.GES.A<br>N/A |
| Control de zonas de acceso público a gran escala | UNI.PRI.VID.N<br>Operaciones de control de aforos mediante dispositivos optoelectrónicos que no permitan identificar a las personas. | UNI.PRI.VID.B<br>Operaciones de control de zonas de acceso público a gran escala mediante dispositivos optoelectrónicos con grabación o sin grabación. | UNI.PRI.VID.M<br>Operaciones de control de zonas de acceso público a gran escala mediante dispositivos optoelectrónicos con grabación o sin grabación y vinculados a sistemas de identificación automatizados | UNI.PRI.VID.A<br>Operaciones de control de zonas de acceso público a gran escala mediante dispositivos optoelectrónicos con sistema de registro o grabación utilizados conjuntamente con otros que , en su conjunto, puedan afectar a los derechos y libertades fundamentales de los individuos |

Tabla 4.10. Criterios de valoración ámbito universitario (disponibilidad servicios)

| CRITERIOS PARA LA DISPONIBILIDAD DE LOS SERVICIOS PRESTADOS POR LOS SISTEMAS | | | | |
|---|---|---|---|---|
| | No adscrito (N/A) | BÁSICO | MEDIO | ALTO |
| Servicios de soporte a la docencia | UNI.DIS.DOC.N<br>El sistema está relacionado con la docencia pero tiene carácter auxiliar o complementario de otros | UNI. DIS.DOC.B<br>El sistema es necesario para dar soporte a la docencia, pero una interrupción de 24h en el servicio no afecta gravemente a la misma. | UNI. DIS.DOC.M<br>El sistema es necesario para dar soporte a la docencia, y cualquier interrupción superior a 2h afecta significativamente al servicio. | UNI. DIS.DOC.A<br>El sistema es imprescindible para dar soporte a la docencia y cualquier interrupción afecta gravemente al servicio. |
| Servicios de soporte a la gestión | UNI.DIS.GES.N<br>El sistema está relacionado con la gestión pero tiene carácter auxiliar o complementario de otros | UNI.DIS.GES.B<br>El sistema es necesario para la gestión, pero una interrupción de 24h no afecta al servicio. | UNI.DIS.GES.M<br>El sistema es necesario para dar soporte a la gestión, y cualquier interrupción superior a 2h afecta significativamente al servicio. | UNI.DIS.GES.A<br>El sistema es imprescindible para dar soporte a la gestión y cualquier interrupción puede afectar gravemente al servicio. |
| Servicios de soporte a la investigación | UNI.DIS.INV.N<br>El sistema está relacionado con la investigación pero tiene carácter auxiliar o complementario de otros | UNI.DIS.INV.B<br>El sistema es necesario para la investigación, pero una interrupción de una semana no afecta a la misma. | UNI.DIS.INV.M<br>El sistema es necesario para dar soporte a la investigación, y cualquier interrupción superior a 24h afecta significativamente al servicio. | UNI.DIS.INV.A<br>El sistema es imprescindible para dar soporte a la investigación y cualquier interrupción puede afectar gravemente al servicio. |

Tabla 4.11. Criterios de valoración ámbito universitario (datos personales)

| CRITERIOS PARA TIPOS DE INFORMACIÓN CON DATOS PERSONALES | | | | |
|---|---|---|---|---|
| | No adscrito (N/A) | BÁSICO | MEDIO | ALTO |
| Tipo de Datos | UNI.PRI.TIP.N<br>No incluye datos de carácter personal. | UNI.PRI.TIP.B<br>Datos de carácter personal no incluidos en categorías especiales de datos | UNI.PRI.TIP.M<br>Datos pertenecientes a categorías especiales de datos u otros datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y libertades fundamentales y cuyo tratamiento responde a fines de atención a la salud, investigación científica o es exigido por la normativa vigente, y siempre que el tratamiento lo lleven a cabo, respectivamente, personal sanitario, personal investigador o personal al servicio de las administraciones públicas en el ejercicio de sus funciones | UNI.PRI.TIP.A<br>Datos pertenecientes a categorías especiales de datos u otros datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y libertades fundamentales y cuyo tratamiento no responde a fines de atención a la salud investigación científica o su tratamiento no es exigido por la normativa vigente. |
| Cantidad de Información de un afectado | UNI.PRI.PER.N<br>No incluye datos de carácter personal. | UNI.PRI.PER.B<br>Datos de carácter personal que, en su conjunto, no permitan evaluar aspectos de la personalidad de un individuo | UNI.PRI.PER.M<br>Datos de carácter personal que por la cantidad de información relativa a un interesado pueden tener un impacto importante en su esfera privada o permiten evaluar aspectos íntimos de su personalidad. | UNI.PRI.PER.A<br>Datos de carácter personal que, por la cantidad información relativa a un interesado, pueden tener un impacto grave en su esfera privada con independencia de los fines del tratamiento. |
| Volumen de datos | UNI.PRI.PER.N<br>No incluye datos de carácter personal. | UNI.PRI.PER.B<br>Operaciones de tratamiento a pequeña escala que persiguen tratar datos personales a nivel regional o nacional y que podrían afectar a un número reducido de interesados. | UNI.PRI.PER.M<br>Operaciones de tratamiento que persigan tratar una cantidad considerable de datos personales a nivel regional o nacional y que podrían afectar a un número elevado de interesados. | UNI.PRI.PER.A<br>Operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala |

## Conclusiones

De los datos analizados en este apartado podemos concluir sin ningún género de dudas que la Seguridad de los Sistemas de información es una de las preocupaciones mayores en materia de TI para los equipos de gobierno de las universidades, lo que está en clara consonancia con el principio de *Seguridad Integral* del ENS. Por otro lado, se han detectado carencias y diferencias de criterio a la hora de abordar la gestión de la seguridad en las universidades. A nuestro criterio, una de las causas fundamentales de esto debe ser el hecho de no haber aplicado correctamente en la organización universitaria otro de los principios básicos del ENS: la Seguridad como función diferenciada. Citando textualmente parte del artículo 10 del ENS:

> En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.
> /…/
> La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

Este principio de segregación de funciones resulta básico para entender la aproximación integral a la seguridad de la información. Por lo tanto, entendemos necesario que las universidades empiecen a incorporar y encajar en sus estructuras (organización, RPT) este principio de *seguridad como función diferenciada*, definiendo las estructuras necesarias, las dependencias de las mismas en relación con los órganos de gobierno y de dirección y también las plantillas de personal asignadas de manera dedicada a la seguridad.

Queda claro, por todo lo anteriormente expuesto, que existen diferentes aproximaciones a la hora de abordar, por parte de las Universidades públicas, la aproximación integral a la Seguridad de la Información que establece el RD 3/2010 del Esquema Nacional de Seguridad. En este artículo hacemos una propuesta sobre la aplicación de los diferentes roles, adaptable a las especificidades de la estructura orgánica de cada Universidad, pero que contempla los condicionantes relacionados con la capacidad de tomar decisiones, los conocimientos técnicos y la segregación de determinadas funciones prevista en el Esquema.

Posiblemente, lo deseable fuera que la homogeneidad de criterios en estos temas condujera a asumir que determinados órganos o puestos directivos concretos deben asumir un rol específico de los previstos en el ENS. De este modo se garantizaría que la gestión de la seguridad fuera objeto de debate en los foros correspondientes y la misma se beneficiaría de la colaboración y las sinergias que, a distinto nivel, se dan en la actualidad en los foros de tecnologías de la información. Así, si mayoritariamente se optara porque el rol de Responsable de Información del ENS fuera asumido por las Secretarías Generales de las Universidades, la valoración de los activos de información sería a la larga un aspecto más a incluir en los debates y foros en los que estas participan.

No obstante, es comprensible que cada Universidad adapte a sus estructuras internas y a su propia personalidad lo previsto en el ENS. No es tan comprensible, desde nuestro modesto punto de vista, que existan clasificaciones dispares de los sistemas que prestan servicios similares y tratan información equivalente en diferentes instituciones. Esto es especialmente cierto en los ámbitos académico y de gestión y, únicamente en el ámbito de la investigación y exclusivamente en aquellos casos en que el resultado de las investigaciones o los datos tratados para llevarlas a acabo así lo justificaran, sería aconsejable clasificar de modo particular esos sistemas. En el resto de casos, aun entendiendo que las universidades deben elegir libremente la categoría de sus sistemas en función del valor que asignen a la información que tratan y a los servicios que prestan, debería ser posible hallar cierta homogeneidad en los futuros informes sobre estado de la seguridad de la información.