VºBº

LA SECRETARIA GENERAL


Fdo.: Eva María Cordero González

**Dictamen:** R1/2019

**Consultante**: Vicerrectorado de Recursos Materiales y Tecnológicos.

**Asunto:** Informe sobre la propuesta de Acuerdo del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la Norma de Seguridad sobre Roles y Responsabilidades en relación con el Esquema Nacional de Seguridad.

**Normativa aplicable**: El marco jurídico aplicable viene configurado por las siguientes normas:

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

- Ley 59/2003, de 19 de diciembre, de firma electrónica.

- Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- 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.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

- Acuerdo de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la Política de Seguridad de la Universidad de Oviedo.

## INFORME

### *Antecedentes de Hecho*

Con fecha de 8 de enero de 2019, tiene entrada en el Registro del Servicio Jurídico solicitud de informe a la Propuesta de Acuerdo del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la Norma de Seguridad sobre roles y responsabilidades en relación con el Esquema Nacional de Seguridad.

### *Fundamentos Jurídicos*

**PRIMERO.** El 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 da cumplimiento a lo previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Por tanto, la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

**SEGUNDO**. El art. 3 del ENS señala:

*"El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.*

*Están excluidos del ámbito de aplicación indicado en el párrafo anterior los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo."*

Por la parte que ahora interesa, el citado art. 2.1 de la Ley 11/2007, señala:

*"La presente Ley, en los términos expresados en su disposición final primera, será de aplicación: a) A las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas."*

Para determinar el alcance de la expresión *"entidades de derecho público vinculadas o dependientes de las mismas*", que aparece en el artículo 2 anterior, habrá que relacionarla con lo establecido en el artículo Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas en la que parece inspirada.

En concreto, el artículo 2.2.b de la citada Ley 39/2015 señala:

*"Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas, que quedarán sujetas a lo dispuesto en las normas de esta Ley que específicamente se refieran a las mismas, y en todo caso, cuando ejerzan potestades administrativas".*

Y el número c del citado artículo establece que:

*"Las Universidades públicas, que se regirán por su normativa específica y supletoriamente por las previsiones de esta Ley".*

Finalmente, señalar que el art. 2.2 de la Ley 11/2007, prescribe:

*"La presente Ley no será de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado."*

Así pues, la Universidad posee la consideración de entidad de derecho público (vinculada o dependiente, de la Administración General del Estado, de las Comunidades Autónomas o de las Entidades Locales), le será de plena aplicación lo dispuesto en el ENS en aquellas actividades que no desarrolle en régimen de derecho privado

**TERCERO**. En cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad, el 22 de diciembre de 2015, se aprueba el Acuerdo del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la Política de Seguridad de la Universidad de Oviedo.

El artículo 3 del citado Acuerdo establece que: *"La estructura organizativa de la gestión de la seguridad de la información en la Universidad de Oviedo estará compuesta por un Comité de seguridad TiC y por los responsables de la información, del servicio y de la seguridad."*

Recogiendo el número 3 del citado artículo 3 que: "*La Universidad de Oviedo (...), diferenciará, dentro de su estructura organizativa, al responsable de la información, que determinará los requisitos de la información tratada, al responsable del servicio, que establecerá las exigencias de los servicios prestados, y al responsable de la seguridad, que adoptará las decisiones para satisfacer los requisitos de seguridad, de la información y de los servicios.*

***Las funciones, ámbito de actuación y procedimientos de designación de cada una de estas tres figuras se especificarán en una norma de seguridad elaborada a tal efecto por la Universidad de Oviedo."***

**CUARTO**. En cumplimiento de lo establecido en el citado artículo 3 del Acuerdo de 22 de diciembre de 2015, se regulan en el presente documento sometido a informe la figuras del Responsable de Información y Servicio y del Responsable de Seguridad Informática y de Comunicaciones.

**QUINTO**. A la hora de regular el equipo humano de la seguridad de la información dos cuestiones son importantes:

• El principio de la seguridad como **función diferenciada**, que se trata en el artículo 10 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.

*"Artículo 10. La seguridad como función diferenciada.*

***En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad****. El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la*

*responsabilidad sobre la prestación de los servicios. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos."*

• El requisito de **profesionalidad** que se trata en el artículo 15.

*"Artículo 15. Profesionalidad.*

*1. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.*

*2. El personal de las Administraciones públicas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.*

*3. Las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados."*

**SEXTO**.-Y la primera nota a resaltar en la regulación del presente acuerdo sometido a informe es la de que, en contra de lo establecido en el anterior Acuerdo de 22 de diciembre de 2015 y el propio Real Decreto 3/2010, de 8 de enero, que establecen una regulación diferenciada de las tres figuras (Responsable de información, Responsable de servicio y Responsable de seguridad), se ha optado por aunar en una sola figura al Responsable de Información y al Responsable de servicio, y así el Capítulo II del documento regula el denominado Responsable de Información y Servicio, dedicando el Capítulo III a la figura del Responsable de seguridad que aquí se denomina Responsable de Seguridad Informática y de Comunicaciones.

**SEPTIMO**. Dada esta específica regulación, la primera pregunta que debe hacerse es la de si, efectivamente, puede una misma persona ser Responsable de Información y Responsable de Servicio. el ENS prohíbe, explícitamente, que el Responsable del Sistema sea la misma persona que el Responsable de Seguridad. Obviamente, quien está legitimado para pronunciarse sobre la idoneidad de las medidas de seguridad adoptadas para securizar un Sistema, no puede ser la misma persona encargada de su explotación. Y fuera de esta expresa prohibición, desde un punto de vista formal nada impide que el resto de las responsabilidades enunciadas por el ENS sean asumidas de manera unificada. Sin embargo, esta parte entiende que dicha coincidencia puede originar algunas disfunciones operativas que deberían ser tenidas en cuenta a la hora de

proceder a su regulación. Como sabemos el Responsable de la Información es la persona (u órgano colegiado con responsabilidad unitaria identificable) que tiene la potestad de establecer los requisitos de la información en materia de seguridad, o, en terminología del ENS, la persona que determina los niveles de seguridad de la información; mientras que el Responsable del Servicio determina los requisitos de los servicios prestados. Y debe de tenerse en cuenta que la Información puede ser generada por la propia institución universitaria, o provenir de un organismo externo. Si la formación se *importa* desde un organismo externo, será el Responsable de la Información de aquel organismo el que señalará su nivel de seguridad y, en su consecuencia, marcará las medidas de seguridad que habrá de adoptar el organismo receptor de la información.

Por otro lado, obsérvese que una misma información puede alimentar varios servicios, que podrán tener, cada uno su propio Responsable del Servicio.

**OCTAVO**. Como resumen diremos que, dejando a salvo lo preceptuado por el ENS, en relación con la exigencia de diferenciación personal entre el Responsable del Sistema y el Responsable de Seguridad, la posibilidad de hacer coincidir en una única persona las responsabilidades de la información, los servicios y la seguridad, se hará tanto más inconveniente cuanto mayor sea la multiplicidad de las informaciones manejadas y los servicios prestados, o cuanto mayor relación o interdependencia tengan los sistemas de información de la Universidad con otros sistemas de información exteriores.

En Oviedo, a 16 de enero de 2019.

EL ASESOR JURÍDICO

Fdo.: Jorge García Monsalve