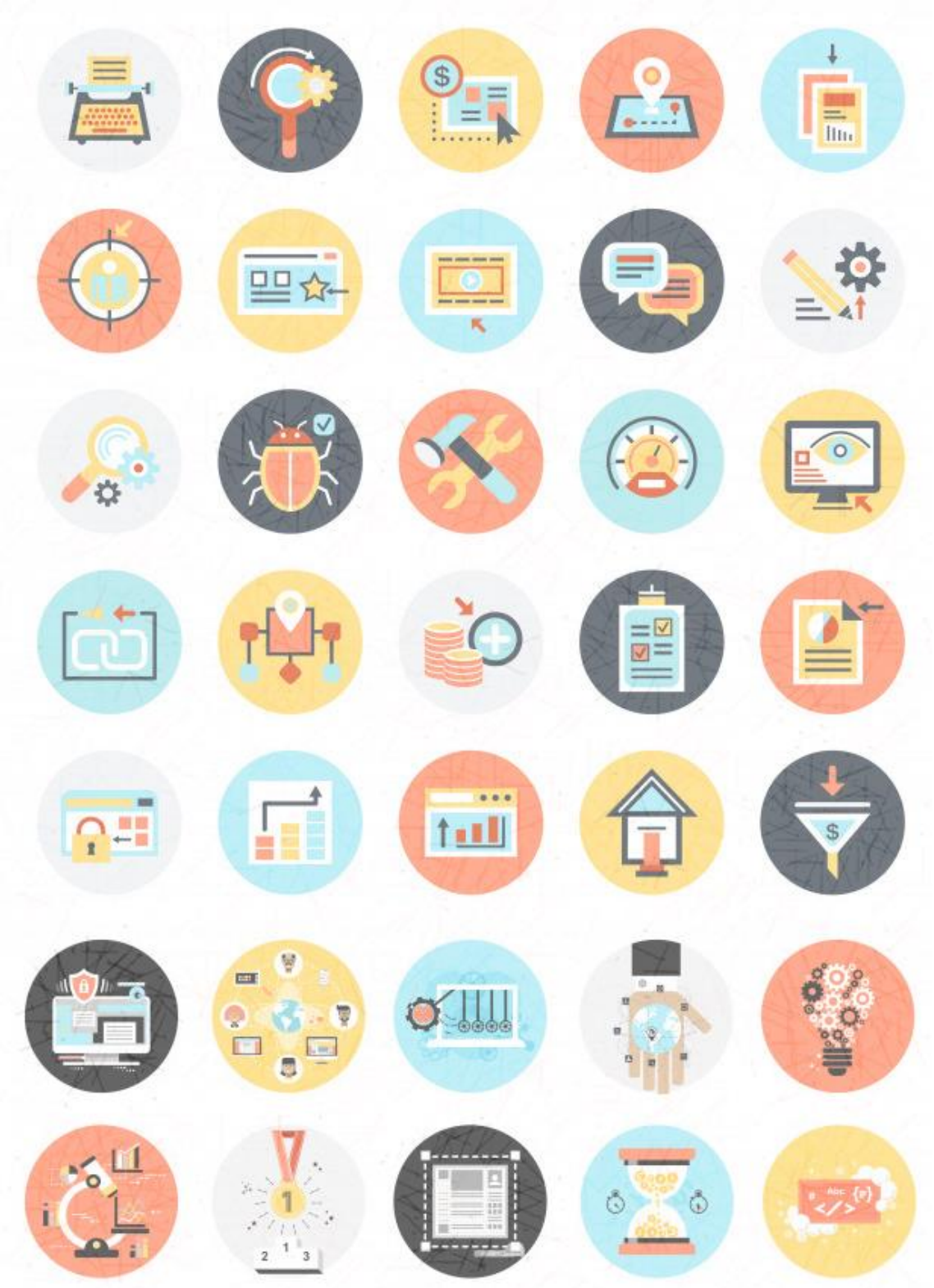
Marco de recomendaciones de Seguridad y Auditoría en Universidades

crue Universidades Españolas TIC



Marco de recomendaciones de Seguridad y Auditoría en Universidades

Elaborado por el Grupo de trabajo de Administración electrónica, Seguridad y Auditorías de la Sectorial Crue-TIC.

Cortés Delgado, Julia (Universidad de Sevilla)

Gumbau Mezquita, José Pascual (Universidad Jaume I)

Mendívil Caldentey, Josu (Universidad de Deusto)

Sampalo Lainz, Francisco José (Universidad de Alcalá)

Índice

1. ¿Por qué un documento sobre Auditoría de Seguridad?

La elevada sofisticación e intensidad de las ciberamenazas, las crecientes exigencias normativas, la naturaleza crítica de muchos de los datos que gestionamos y del tratamiento que se hace de los mismos, así como el impacto de una inadecuada custodia nos obligan a abordar la seguridad TI con rigor y un claro convencimiento de su importancia. A este respecto, es conveniente exponer y compartir algunos conceptos que están reconfigurando el actual paradigma de seguridad, y que nos permitirán entender y valorar los cambios en los que estamos trabajando desde hace tiempo.

Dos de los cambios fundamentales en el tratamiento de la seguridad son la necesidad de disponer de un Sistema integrado de gestión de la seguridad (SGSI) y la función de Auditoría de seguridad TI, que controla el buen funcionamiento del mismo, lo que es fundamental para generar la confianza necesaria en nuestro Sistema de información.

Centrándonos en el marco normativo, vemos reflejada la importancia y necesidad de las auditorías en el Esquema Nacional de Seguridad (ENS). Su Capítulo V está íntegramente dedicado a la auditoría de seguridad, señalando en su artículo 34 que «Los sistemas de información… serán objeto de una auditoría regular ordinaria, al menos cada dos años. Con carácter extraordinario… siempre que se produzcan modificaciones sustanciales».

Además, la Disposición Adicional Cuarta de Desarrollo del ENS abunda en la necesidad de realizar auditorías sobre el sistema de gestión, al indicar la necesidad de establecer Instrucciones Técnicas de Seguridad, ITS, de obligado cumplimiento, siendo una de ellas la de Auditoría de Seguridad.

Finalmente, por si fueran necesarios más argumentos, el propio Reglamento General de Protección de Datos hace referencia expresa a la necesidad de llevar a cabo auditorías de seguridad, al señalar en su artículo 47.2.j la utilización de auditorías de protección de datos como una de las normas corporativas vinculantes. Puesto que este nuevo enfoque implica nuevos roles, nuevas responsabilidades y cambios en las estructuras e incluso en la "cultura" de las organizaciones, hemos querido en este documento aportar información que pueda servir de ayuda a los responsables políticos y organizativos de las universidades en el proceso de adaptación a este cambio.

Aclarar finalmente que en este documento no hemos querido hacer distinción entre universidades públicas y privadas, pues va dirigido a ambas. Aunque en algunos aspectos el ámbito normativo es distinto (el Esquema Nacional de Seguridad no es un marco normativo que obligue necesariamente a las universidades privadas) sí va siendo una práctica cada vez más necesaria en el ámbito privado el disponer de un sistema integrado de la gestión de la seguridad (SGSI), basado en estándares (por ejemplo la ISO 27001 o el propio ENS que, aun no siendo de obligado cumplimiento para las universidades privadas, es un marco al que pueden acogerse y acreditarse voluntariamente) en los que la mejora continua y, por tanto, la auditoría, es un elemento clave para su funcionamiento.

2. Auditoría y seguridad

Seguridad gestionada e integrada

Una seguridad efectiva no puede ser meramente reactiva. Ya no sirve una seguridad basada únicamente en intentar responder de la mejor manera posible a las amenazas y ataques recibidos, o parchear y corregir vulnerabilidades sufridas o detectadas.

No sirve por ineficaz y en consecuencia por cara. Es necesaria una seguridad organizada sobre un sistema de gestión en el que se establezcan las oportunas normas y controles, y que esté enfocada al cumplimiento de objetivos específicos, tangibles y medibles. **Para que la seguridad TI sea mínimamente efectiva a un coste razonable y conocido debe estar gestionada.**

Pero siendo la gestión una condición necesaria, no es suficiente. No sólo debemos articular un Sistema de Gestión de la Seguridad de la Información (SGSI); también será de especial relevancia que este SGSI forme parte indisoluble de los procesos de gestión general de la organización.
Este concepto de seguridad gestionada e integrada podemos encontrarlo en el Esquema Nacional de Seguridad en su Artículo 5, donde señala que "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 ENS estará presidida por este principio, que **excluye cualquier actuación puntual o tratamiento coyuntural.**"

La misma idea también la encontramos en la Introducción de la norma ISO 27001, cuando señala que "La adopción de un SGSI es una decisión estratégica para la organización. Es importante que el **SGSI forme parte y esté integrado con los procesos de la organización** y con la estructura de gestión global."

Es muy importante tener en cuenta la ruptura que esto supone sobre el tratamiento de la seguridad TI que se ha venido realizando tradicionalmente en las organizaciones: la seguridad TI era considerada un asunto técnico y su tratamiento y solución era competencia de los administradores de sistemas y personal técnico en general. Así, la función de seguridad permanecía como una competencia exclusiva del Servicio TI, realizando cada área sus tareas concretas (seguridad en las redes, seguridad en los sistemas, seguridad en el puesto de usuario, seguridad en el desarrollo de aplicaciones) sin visión de conjunto y sin un control externo de la eficacia y adecuación de las medidas.

Para ver esto de una forma más gráfica, demos un vistazo rápido a las medidas que se recomiendan y a los posibles impactos que puede tener un problema de seguridad en las organizaciones.

El informe «Principios y recomendaciones básicas en ciberseguridad – 2017» publicado por el CCN-CERT (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html) incluye un decálogo de medidas básicas de seguridad, entre las que encontramos medidas como:

- La cultura de la ciberseguridad, la concienciación del empleado, debe ser uno de los pilares en lo que se asiente la ciberseguridad de cualquier Organización.

- Limitar la superficie de exposición a las amenazas, no solo hay que implementar medidas de seguridad que protejan el acceso a la información, sino que hay que determinar los servicios que son estrictamente necesarios.
- Clasificar la información y cifrar aquella que sea sensible.

Estas medidas (por citar algunas), aunque finalmente puedan apoyarse en alguna herramienta informática, requieren la implicación de la alta dirección de la Universidad tanto en la toma de decisiones como en los criterios organizativos que requiere su implantación y, por lo tanto, trascienden del entorno técnico en el que hasta ahora se tomaban decisiones y se ejecutaban las actuaciones en materia de seguridad.

También las consecuencias de un fallo de seguridad en los sistemas de información pueden tener un impacto sobre la organización en general:

- Incumplimiento normativo/legal.
- Pérdidas económicas.
- Interrupciones en la continuidad del servicio que se presta a los ciudadanos.
- Filtración de información confidencial y de datos personales.
- Daños reputacionales.
- Riesgos a la hora de implantar nuevas tecnologías para mejoras en la prestación de los servicios.

Está claro, por tanto, que la seguridad informática es una responsabilidad de toda la organización, y esta realidad debe percibirse en todos los procesos de la misma. El Sistema de Gestión de la Seguridad de la Información (SGSI) es la herramienta que nos facilita este tratamiento global de la seguridad, pues en él se definirán los distintos roles, responsabilidades y funciones en materia de seguridad, alineados con los objetivos y la estructura organizativa de la Universidad.

Control del sistema de gestión de la Seguridad

Un SGSI nos ayudará a preservar la confidencialidad, integridad y disponibilidad de la información que manejan nuestras universidades. Pero **es necesario asegurar que éste funciona adecuadamente y que en efecto cumple los objetivos para los que fue creado**. El modo de resolver este aseguramiento nos lo señala el propio ENS en el apartado III del Prólogo, cuando afirma que, para permitir una protección adecuada de la información y sus servicios, «se determinan las dimensiones de seguridad y sus niveles… y la **auditoría periódica de seguridad**».

También lo hace la cláusula 9.2.a de la ISO 27001, donde se nos dice que «La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el SGSI cumple con los requisitos propios de la organización y está implementado y mantenido de manera eficaz».

Por lo tanto, la función de control sobre el correcto funcionamiento del SGSI recae sobre la auditoría. Es fundamental resaltar que la auditoría debe ser «independiente»: los auditores no deben haber participado el desarrollo ni en la prestación de los servicios de los sistemas auditados, ni tampoco deben tener dependencia jerárquica del responsable de esos servicios. Sobre esto se darán más detalles más adelante.

De cara a la realización de auditorías se plantean dos escenarios complementarios:

- Dado que el SGSI es dinámico y está en continua ejecución, se debe estar auditando continuamente y controlando el grado del cumplimiento de objetivos, posibles desviaciones, cambios debidos a nuevos riesgos o amenazas, etc. Este trabajo, dado su carácter permanente y la valiosa información que puede proporcionar a la dirección (de cara al cumplimiento de objetivos) debe ser desarrollado por personal propio, que son los **auditores internos**.

- Por otro lado, serán necesarias **auditorías para certificación** del cumplimiento legal (ENS, RGPD) o de un estándar internacional (ISO 27000). Estas auditorías deben realizarse por parte de personal o empresas **externas** debidamente acreditadas.

El disponer de la función de auditoría interna facilita enormemente los procesos de certificación mediante auditorías externas.

Entre las funciones encomendadas al Responsable de Seguridad, según las guías de desarrollo del ENS, está la de supervisar los controles necesarios para proteger los datos y los servicios y controlar su eficacia. Esto se corresponde claramente con la función de Auditoría interna, por lo que consideramos que el **Responsable de seguridad puede ejercer también como «Auditor interno».**

Necesidad de informar

Es conveniente señalar que los resultados de una auditoría de seguridad no son únicamente técnicos. Existen también aspectos organizativos o formativos que deben ser atendidos y que sin el conocimiento y participación de la dirección no es posible llevar a cabo. Es por ello crítico informar de los resultados a la dirección y contar con su apoyo a la hora de adoptar medidas correctivas. Mantener un SGSI auditado no tiene sentido si no es considerado en última instancia como un elemento de gobernanza que permite conocer con claridad el nivel de seguridad de la organización, establecer sus niveles de riesgo, mitigar riesgos inasumibles o establecer planes de mejora en seguridad. En relación con este aspecto profundizaremos en el punto siguiente.

El ENS nos señala esta necesidad en su artículo 34.8 al afirmar que «Los informes de auditoría podrán ser requeridos por los responsables de cada organización».

También aparece reflejada en la Cláusula 9.2.f de la ISO 27001, cuando afirma que la organización debe "asegurarse de que **se informa a la dirección** pertinente de los resultados de las auditorías" o en la 9.3.c.3 donde se señala que «**La alta dirección debe revisar el SGSI a intervalos planificados**, para asegurarse de su conveniencia, adecuación y eficacia continuas, incluyendo consideraciones sobre... los resultados de auditoría».

3. Auditoría y la prestación de los servicios

¿Qué servicios prestamos? Vs. ¿Qué auditamos?

En este apartado veremos la relación holística que hay detrás de los conceptos de «Prestación de servicios» y de «Auditoría» y como se realimentan.

La entrada en vigor del Reglamento General de Protección de Datos (RGPD), ha puesto de manifiesto que los datos que gestionamos son de los interesados y nosotros (las universidades en nuestro caso) simplemente los custodiamos, por lo que cada organización deberá evaluar los riesgos a los que pueden estar sujetos e implantar los mecanismos necesarios para protegerlos. Todo ello independientemente del soporte: papel, electrónico y digital (imagen, video, audio…). Para ello es fundamental que informemos en el momento de adquirir los datos de las finalidades por las que los recogemos, qué base legal nos ampara y cómo ejercer sus derechos. Es lo que se llama **tratamiento**.

- **Finalidad:** en este punto informamos de "para qué" recogemos los datos, que, dicho de otra forma, significa qué "servicios" vamos a prestar con esos datos.
- **Protección:** es necesario garantizar que los datos se tratan y se custodian adecuadamente conforme a lo pactado.

Según el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de las Administraciones Públicas, la consagración del derecho de los ciudadanos a comunicarse con ellas a través de medios electrónicos comporta asimismo tanto garantizar el acceso por medios electrónicos como proteger adecuadamente la información. El objetivo del ENS es fundamentar la confianza en que los *sistemas de información* prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Como podemos observar, se ha popularizado nombrar a los sistemas electrónicos como sistemas informáticos o sistemas de información. Quedando claro que hablamos siempre del «servicio que prestan los sistemas automatizados». Pero cuando hablamos de protección de la información tenemos que distinguir entre tres ideas que pueden confundirse: Seguridad de la información, Seguridad Informática y Garantía de la información.

La *Seguridad Informática* se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios no sólo en formatos informáticos. Los activos a proteger por la seguridad informática son: datos y equipos, o sea, la infraestructura. Sin embargo, la *Seguridad de la Información*, según la ISO 27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información, independientemente del formato que tengan: papel, estructurado en ficheros electrónicos, o digitales (Imagen, video y audio). Siendo pues un concepto más amplio y que incluye al anterior.

El significado de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización.

¿Es esto suficiente y aclaratorio? En nuestra opinión, para defender los derechos de los interesados, no es suficiente. Se necesita, además, «garantizar» que esto es así, y «garantizar» que podrán ejercer en condiciones sus derechos, que sus datos están protegidos, que los tratamientos de los que son objeto son los informados y adecuados para los trámites para los que han sido cedidos. **O sea, además de disponer de servicios seguros, necesitamos garantizar y asegurar la prestación de servicios**.

La información y la tecnología que la soporta, representan unos activos muy valiosos y críticos de una universidad. Es por tanto necesario realizar un *control de todo ello en su conjunto*, desde la planificación de la continuidad de negocio hasta la comprobación del correcto funcionamiento de los servicios. Hace falta, pues, adquirir la función de auditoría de los sistemas de información en nuestras organizaciones.

En resumen, **es necesario separar las funciones de prestación y administración de servicios, de la función de planificación y control de los mismos**, y con ello cumpliremos con el artículo 10 del ENS sobre separación de funciones. Lo que se desprende de esta propuesta es:

- El rol de «Responsable del Servicio» será asimilado por el prestador del servicio y administrador de la seguridad informática
- La asimilación de responsable de seguridad del sistema de información con la figura del auditor, como garante del cumplimiento y la protección.

Y la asimilación de *servicio informático o sistema de información al de activo* a proteger.
Para más detalle de las diferentes adopciones de este modelo ver el informe del Universitic 2017, *La Gestión de la Seguridad de la Información en las Universidades Españolas*, así como la guía 801- Responsabilidades y funciones en el ENS.

¿Qué protegemos?

Protegemos datos y prestamos servicios. Necesitamos tener claro el conjunto de servicios, aplicaciones y tratamientos que gestionan nuestros datos, teniendo en cuenta que los tratamientos incluyen aquellos datos que residan en papel. Todo ello formará lo que llamaremos el catálogo de activos de la organización.

Es sobre este catálogo sobre el que podremos realizar las valoraciones de impacto y los análisis de riesgo necesarios para garantizar su protección. Del catálogo, se diseñará la prestación del servicio deseada e informada, asumiendo las medidas de seguridad (declaración de aplicabilidad) y los riesgos que se determinen.

Corresponde al prestador del servicio, como responsable del servicio, aplicarlas; y al auditor o al responsable de la seguridad, comprobarlas. Siendo por tanto el catálogo de activos la herramienta fundamental para la prestación de los servicios informáticos.

Crue-TIC ha desarrollado una propuesta de catálogo de servicios informáticos de referencia, que debe ser la base sobre la que partir para definir nuestro catálogo de activos.
¿Cómo gestionar el catálogo de activos? Para ello hemos de definir el marco de gestión o de gobierno TI de la organización: será necesario establecer un procedimiento de gestión de las altas, modificaciones y bajas del catálogo (incorporadas en la gestión de los proyectos), o sea, definir un registro de activos; establecer una métrica de valoración de activos;

establecer una métrica de madurez del sistema; establecer los procedimientos que permitan la privacidad por diseño y por defecto; y establecer un conjunto de prácticas de control que garanticen el cumplimiento normativo, la prestación de servicio y el buen uso de la información. Todo en cumplimiento del artículo 4 del ENS ***Principios básicos del Esquema Nacional de Seguridad que determina el objetivo último de la función de seguridad de la información.***

Para más detalle ver el informe en Universitic 2017, *Marco de gobierno TI/SI basado en la innovación y la auditoría TI. Gestionando la transformación digital*.

Análogamente a tener un catálogo común de servicios informáticos, sería conveniente apostar en CRUE-TIC por unificar criterios a tener en cuenta entre las universidades a la hora de desarrollar valoraciones, medidas de seguridad, políticas de seguridad y sistemas de gestión de la seguridad de la información. E incluso, modelos de gestión de activos, para obtener un modelo de referencia de gobierno TI basado en la gestión de los activos que incluye la prestación del servicio y su control.

Un primer paso, muy importante, dado en esta dirección, ha sido la de establecer como anexo 1 a la guía 803 de CCN la elaboración de criterios para la valoración de activos en las universidades. El anexo:

- Introduce criterios de valoración específicos para el ámbito universitario, o extienden con criterios concretos más específicos, los criterios de valoración definidos en el cuerpo principal de la guía.
- Incluye un catálogo de tipos de información habituales en el ámbito universitario, detallando un nivel mínimo de seguridad recomendado.

De igual modo, ofrece un catálogo de servicios habituales prestados por las universidades, detallando también para ellos un nivel de seguridad mínimo recomendado.

4. Auditoría interna en universidades

Analizada la función de la Auditoría como el control del correcto funcionamiento del SGSI y vista su necesaria separación e independencia de la prestación de los servicios, es momento ya de adentrarse en especificar cómo se puede implementar la función de Auditoría de Seguridad de la información en las Universidades.

La auditoría de la seguridad de la información es el examen, la entrevista y/o la prueba formal de los tratamientos de la información para determinar si:

- Se cumplen las leyes, reglamentaciones y contratos aplicables y/o pautas de la industria.
- Los datos e información tienen niveles de confidencialidad, integridad y disponibilidad adecuados.
- Las operaciones de tratamiento de la información se están realizando de forma eficiente y se cumplen los objetivos de efectividad.

Conforme al artículo 34 del ENS «Auditoría de la seguridad», los Sistemas de Información categorizados como de nivel MEDIO y ALTO según lo dispuesto en el anexo I y de acuerdo con lo previsto en el anexo III del RD, serán objeto de una auditoría regular ordinaria, al menos cada dos años y, con carácter extraordinario, siempre que se produzca modificaciones sustanciales en el sistema de información que puedan repercutir en las medidas de seguridad requeridas.

En relación a la revisión de la medida [mp.info.2] del anexo II del ENS referente a datos personales, se deberán realizar auditorías de los tratamientos según lo establecido en la legislación vigente sobre Protección de Datos Personales.

Rol de auditor interno en las universidades

La función de auditoría interna de la seguridad de la información debe establecerse en la Universidad mediante un estatuto de auditoría aprobado por el Consejo de Gobierno. El auditor interno debe ser independiente y reportar a un Comité de Auditoría, si existe, o al Consejo de Gobierno.

Cuando en la Universidad no exista una función diferenciada de auditoría el rol de auditor interno podrá recaer en las personas que tienen delegada la Responsabilidad de la Seguridad de la información en aquellas tareas que no hayan sido de su propia competencia. Éstas asumen las tareas de control y evaluación continua, análisis de riesgos y revisión del estado de la seguridad de la información.

La seguridad se auditará, como parte de la mejora continua, en los términos establecidos en el anexo III del ENS, en la legislación vigente para la Protección de datos personales y en los estándares de buenas prácticas ISO.

El ENS y el RGPD obligan a las universidades a contar con un Responsable de Seguridad de la Información y un Delegado de Protección de Datos respectivamente. Ambas figuras están implicadas en la protección de la información y deben realizar informes periódicos sobre el grado de cumplimiento normativo, asumiendo de forma implícita tareas de auditoría interna.

El **Responsable de Seguridad** es la figura del ENS implicada en la seguridad de los sistemas de información que prestan servicios de la Universidad para el ejercicio de derechos y cumplimiento de deberes. Tiene un perfil más tecnológico, si bien debe conocer la legislación que le aplica.

El Delegado de Protección de Datos es la figura del RGPD que participa en todas las cuestiones relativas a la protección de datos personales tratados por la Universidad. Su perfil es más jurídico, aunque debe asesorar a los responsables de los tratamientos acerca las medidas de seguridad que deben aplicar para proteger los datos.

Puesto que la medida «Datos personales [mp.info.1]» del anexo II del ENS remite a lo dispuesto en la legislación vigente (RGPD) y el RGPD permite delegar la protección de los SI que contienen datos personales en las medidas del anexo II del ENS, el Responsable de Seguridad de la Información y el DPD, cuando sean personas distintas, deberán estar al mismo nivel de responsabilidad y tener una alta coordinación.

Aunque la AEPD recomienda separar la función del DPD del Responsable de Seguridad de la Información una persona con doble perfil jurídico y tecnológico podría asumir ambos roles.

El informe Universitic 2017 analiza los roles de seguridad de la información en universidades y recomienda que el **rol de Responsable de Seguridad lo ostente un cargo o funcionario, a nivel ejecutivo, designado formalmente por el Rector o el Equipo de Dirección. No debe 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. Estas mismas recomendaciones aplicarían al Delegado de Protección de Datos**.

Puesto que ambos roles son responsables de la auditoría continua de la seguridad de la información en la Universidad necesitan un cierto nivel de autoridad dentro de la organización para evaluar y resolver situaciones conflictivas, y promover la utilización del proceso y los estándares.

Deben tener conocimientos relacionados con los Sistemas de información, la seguridad y el cumplimiento normativo, además de ciertas habilidades personales, tal como se detalla en los apartados 4.3 y 4.4.

En materia de auditorías de seguridad de la información el Responsable de Seguridad de la Información y el Delegado de Protección de Datos de la Universidad deberán plantear la auditoría del RGPD y del ENS de manera conjunta.

No existen restricciones para que, al menos de una forma temporal, ambos roles puedan externalizarse y contratarse como servicios a empresas especializadas.

Equipo auditor y su capacitación

El Artículo 15 del ENS hace referencia a la Profesionalidad del equipo de auditoría: «la seguridad de los sistemas será auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento».

El equipo auditor, independientemente de que pertenezca o no a la organización, deberá estar compuesto por profesionales que dispongan de los conocimientos y experiencia suficientes, de acuerdo al alcance establecido, para asegurar la adecuada y ajustada realización de la auditoría.

Este equipo podrá estar compuesto por auditores internos y/ o externos o una combinación de ambos, pero en todo caso, es necesario cumplir con los requisitos que se especifican en el artículo 22 de la Guía CCN-STIC-802 sobre Auditoria ENS.

Los componentes del equipo de auditoría deberán tener una formación suficiente en auditoría de sistemas de información, y en seguridad, según se establece en los requisitos mínimos reflejados en el Anexo A de la Guía CCN-STIC-802 sobre Auditoria ENS.

Si se considera necesario por la complejidad tecnológica o dimensiones del entorno a auditar, se podrán incorporar expertos en determinadas materias según se establece en el Anexo B de esta misma Guía.

En todo caso al Auditor Jefe o líder del equipo auditor se le exige como requisito la «*acreditación de formación y experiencia en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional, o bien a través de experiencia verificable y evidenciada*».

Habilidades personales

La auditoría se basa en el principio de independencia, fundamental para la imparcialidad y objetividad de las conclusiones, y en un enfoque basado en la evidencia que es el método racional para alcanzar conclusiones de auditoría fiables, y reproducibles en un proceso de auditoría sistemático.

Para ello, en base a las directrices para la auditoría de los sistemas de gestión de la norma ISO 19011, los auditores internos deben demostrar:

- Una conducta ética en la que la confianza, integridad, confidencialidad y discreción son esenciales para auditar.
- Una presentación ecuánime que les obliga a informar con veracidad y exactitud de los hallazgos, conclusiones, informando de los obstáculos significativos encontrados durante la auditoría y de las opiniones divergentes sin resolver entre el equipo auditor y el auditado.
- El debido cuidado profesional, aplicando la diligencia y juicio al auditar, de acuerdo con la importancia de con la importancia de la tarea que desempeñan y la confianza depositada en ellos por los auditados.
- Esto se traduce en una serie de habilidades personales el auditor, que debe ser:
- Ético, es decir, imparcial, sincero, honesto y discreto
- De mentalidad abierta, es decir, dispuesto a considerar ideas o puntos de vista alternativos.
- Diplomático, es decir, con tacto en las relaciones con las personas.
- Observador, es decir, activamente consciente del entorno físico y las actividades
- Perceptivo, es decir, instintivamente consciente, capaz de entender las situaciones.
- Versátil, es decir, se adapta fácilmente a diferentes situaciones.
- Tenaz, es decir, persistente, orientado hacia el logro de los objetivos.
- Decidido, es decir, alcanza conclusiones oportunas basadas en el análisis y razonamiento lógicos para la detección de mejoras.
- Seguro de sí mismo, es decir, actúa y funciona de forma independiente a la vez que se relaciona eficazmente con otros porque tiene capacidad de trabajo en equipo, habilidad de comunicación y capacidad de mediación.

5. Auditoría externa en universidades

Después de toda la exposición anterior es el momento de hacerse algunas preguntas: ¿Cómo están afrontando las universidades la Auditoría de SI? ¿Cuál es el panorama en estos momentos? ¿Hay alguna iniciativa para afrontar este asunto de una forma conjunta y coordinada? Según la última edición (año 2018) del Informe Estado Seguridad en universidades (Informe INES CCN-CERT IT 18/18) un 84% de las universidades (43 de las 51 que han respondido a la encuesta a partir de la que se elabora el informe) han valorado sus Sistemas de información como de categoría media, a lo que hay que sumarle el 4% que los ha considerado como de categoría alta.

Por otro lado, el citado informe resalta también **que «La certificación es completamente residual»**, habiendo sólo dos universidades (un 4%) que ya disponen de la certificación ENS. Por ello, por segundo año consecutivo, la primera recomendación que se da a las universidades en materia de gestión de la seguridad es:

> *Promover la conformidad con el Esquema Nacional de Seguridad, fomentando la certificación de la conformidad a través de la realización de auditorías independientes, de acuerdo con lo previsto en el artículo 41, en la Instrucción Técnica de Seguridad (ITS) de conformidad con el ENS y en la guía CCN-STIC-809 (Declaración y Certificación de Conformidad con el ENS y distintivos de cumplimiento).*

Por lo tanto**, la realización de auditorías externas para certificación en el ENS, empieza a ser una necesidad para que las universidades puedan cumplir con lo establecido en el marco legal**.

Iniciativa "auditorías cruzadas" en CRUE-TIC

Este es un tema que ya se viene debatiendo en la Sectorial CRUE-TIC en los últimos años. En la reunión de la Sectorial CRUE-TIC de octubre de 2016, ya se presentó la "**Iniciativa AIDA**"[1], en la que el objetivo principal era, citando textualmente, "La realización de auditorías informáticas mediante el intercambio de auditores internos de forma cruzada entre universidades".

En esta presentación, se enumeraban varias ventajas que este planteamiento podría aportar a las universidades, entre las que podemos destacar las siguientes:

- Homogeneidad de criterios en las auditorías.
- Benchmarking y valor del conocimiento que se genera e incorpora directamente en nuestras instituciones.
- Minimizar costes pues, al ser cruzadas, no es necesario contratar a ninguna empresa externa.
- Mejorar de la formación y el grado de especialización profesional de nuestros técnicos.

Esta idea fue acogida con gran interés por parte de las universidades y de la propia Ejecutiva de CRUE-TIC, lo que desembocó en el «**Curso de Auditoría tecnológica, de seguridad y legal de sistemas de información**», impartido en la UNIA y patrocinado por CRUE-TIC, cuya finalidad era: «*Formar a profesionales de los Servicios de Informática de las Universidades en la gestión de la seguridad informática, dadas las múltiples obligaciones legales que están surgiendo sobre la misma, y la conveniencia de adaptarse a estándares internacionales. De esta forma, a la finalización del curso, deberán ser capaces de administrar la política de seguridad de*

la universidad mediante la definición de normativas, el despliegue y el seguimiento, tanto desde el punto de vista tecnológico como de cumplimiento legal, incluyendo estándar ISO 27000, Esquema Nacional de Seguridad, y Legislación sobre Protección de Datos Personales».

A este curso semipresencial, de 7 meses y 15 créditos ECTS de duración, asistieron unos 30 profesionales de varias universidades tanto públicas como privadas; con su finalización se puede considerar cubierto el objetivo de tener un grupo de personas con la formación requerida para formar parte de equipos de auditorías de certificación de ENS.

Pero antes de que el personal formado en el curso citado pueda dirigir auditorías, es necesario que complemente esta formación con la colaboración en auditorías reales formando parte del equipo auditor.

Además, hay que tener en cuenta lo que se establece la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad (BOE 265 de 2 de noviembre de 2016); en su apartado V.1 indica que:

> *«La Certificación de Conformidad con el Esquema Nacional de Seguridad, de sistemas de categorías MEDIA o ALTA, será expedida por una entidad certificadora y se completará mediante un Distintivo de Certificación de Conformidad cuyo uso estará condicionado a la antedicha Certificación de Conformidad».*

Como complemento a esto, la ITS de Auditoría de Seguridad (BOE 81, de 3 de abril de 2018) tiene un apartado (el VII) dedicado a lo que se denomina "Entidades Auditoras del Sector Público", que indica lo siguiente:

> *Entidades Auditoras del Sector Público: La presente Instrucción Técnica de Seguridad también será de aplicación a las actividades de auditoría y a la emisión de los correspondientes informes que se realicen por entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias se correspondan con el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.*

En definitiva: para poder cumplir el objetivo planteado, o sea, realizar auditorías cruzadas entre universidades y que éstas tengan validez para una certificación de cumplimiento del ENS, no sólo necesitamos auditores formados, sino que además es necesario:
Que el equipo de auditoría esté liderado por un auditor jefe que tenga una experiencia previa mínima según unos requisitos establecidos.

Que la auditoría sea llevada a cabo por una entidad externa debidamente acreditada.
Así nos encontramos con dos posibles escenarios para cubrir estos requisitos:
Realizar las auditorías de la mano de empresas debidamente acreditadas (ver https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/entidades-de-certificacion) en las que dentro del equipo auditor se incluya a algún auditor universitario, de una universidad distinta, que tenga la formación adecuada.

Constituir un grupo de auditores dentro de CRUE que pueda ser considerado como una «Entidad Auditora del Sector Público» dentro del ámbito de las universidades.

Para seguir avanzando en la primera de las opciones indicadas CRUE-TIC está manteniendo contactos con empresas que han obtenido la acreditación correspondiente y se están estudiando fórmulas de colaboración que faciliten las prácticas necesarias para constituir un grupo de auditores jefes que podrían dirigir auditorías externas en universidades distintas a la suya de origen.

Por otro lado, también se ha consultado al CCN-CERT sobre la viabilidad de constituir un grupo que pueda considerarse como «Entidad auditora del Sector Universitario» y su respuesta ha sido afirmativa e incluso muy favorable, con el único requisito de que dicho grupo sea debidamente reconocido por CRUE. En cualquier caso, los integrantes de este grupo deben haber participado previamente en un número suficiente de auditorías.
No debemos olvidar que esta iniciativa supone también un compromiso de colaboración entre universidades y que determinadas universidades van a «ceder» a un técnico cualificado de forma temporal, por el tiempo de duración de la auditoría (estimado en 5 días laborables) a otras universidades. Pero entendemos que las ventajas ya indicadas de esta iniciativa deben compensar de sobra esta dedicación.

6. Conclusiones y recomendaciones

Las universidades son un entorno específico donde la seguridad de los Sistemas de Información está supeditada a otros aspectos: operativas abiertas, colaboración y compartición de recursos, acceso libre a servicios, etc.

Esto no quiere decir en absoluto que no haya también información y tratamientos sensibles. Además, hoy día la práctica totalidad de la actividad universitaria (investigación, docencia y gestión) se soporta sobre sistemas automatizados y en muchos casos sin apenas intervención humana; por ejemplo, en aplicación de lo que se denomina «Actuación administrativa automatizada», un estudiante podría solicitar y obtener un certificado académico firmado electrónicamente que tendría validez legal a todos los efectos. La información contenida en este certificado se ha obtenido directamente de la base de datos, por un programa (ERP) y ha sido firmado usando un sello de órgano en un servidor, todo ello sin intervención humana alguna.

Estas particularidades hacen incluso que se refuerce la necesidad de realizar una «Gestión de la seguridad». Por «gestionar» la seguridad se entiende:

- Conocer los riesgos a los que están expuestos los Sistemas de Información y determinar cuáles de ellos deben ser asumidos y cuáles habrá que mitigar.
- Establecer y aplicar las medidas de toda índole (organizativas, de operación del sistema y técnicas) encaminadas a mitigar y reducir los riesgos.
- Controlar que las medidas se están aplicando correctamente y evaluar los resultados.

El primer punto requiere de la toma de decisiones por parte de la Dirección de la Universidad; el segundo es fundamentalmente competencia de los responsables de los servicios y de los sistemas; y el tercer aspecto es el objetivo de la función de auditoría.

La confianza en un Sistema de Información se basa en que éste desarrolle correctamente las tareas para las que ha sido implantado, incluso en presencia de anomalías y errores (intencionados o no) en sus entradas (*inputs*) o en el tratamiento de la información. Por ello, no basta con tener un sistema de gestión integral de la seguridad; también se requiere un control del mismo, para generar la confianza de que las cosas se están haciendo como deben. Ahí es donde entra la función de auditoría. Y ese control debe estar diferenciado y ser independiente de la prestación de los servicios.

La auditoría externa asegura esa diferenciación e independencia, siendo necesaria para los procesos de certificación (para cumplimiento legal o para estándares); pero no bastaría para asegurar el proceso de mejora continua que está en la base de todo sistema de gestión de la calidad. Para ello, se debe complementar con una «Auditoría interna».

El auditor interno de SI debe tener una capacitación y un perfil específico, pero también es fundamental que se asegure que:

- Debe reportar al más alto nivel dentro de la organización.
- Se debe garantizar su independencia con respecto a los responsables de los servicios y entornos auditados.

La legislación vigente (Esquema Nacional de Seguridad y Reglamento UE de Protección de Datos Personales - RGPD) y los estándares y marcos de buenas prácticas apuntan también a la necesidad de realizar auditorías de la Seguridad y los Sistemas de Información y, más que una obligación, constituyen un marco de ayuda para la generación de confianza.

Hoy día, hemos observado casos muy relevantes y mediáticos en los que ha habido un daño reputacional muy importante al mundo universitario debido a la pérdida de confianza en el desarrollo de las funciones universitarias. Un control eficaz habría mitigado gran parte de estos riesgos. Los autores de este documento consideramos que un sistema global de control y auditoría universitaria no puede ser completo y eficaz si no incluye una auditoría de Seguridad de los Sistemas de Información. La auditoría de SI no debe verse como un nicho para técnicos; antes bien, debe ser parte del sistema global de control en las universidades para prevenir y detectar posibles fallos en la confidencialidad, integridad o autenticidad de los tratamientos de información.

Actualmente pocas universidades, sean públicas o privadas, están convencidas de la importancia de la Auditoría de Seguridad de los Sistemas de Información para el Gobierno de las TI, e incluso para el Gobierno corporativo y en apenas ninguna existe la figura del "auditor interno". Esta figura sería perfectamente compatible con el rol de Responsable de Seguridad (que establece el ENS), al que habría que capacitar debidamente además para la realización de la función de auditoría interna. Además, dado el carácter peculiar del tratamiento de la seguridad de los SI en las universidades y el alto grado de colaboración y afinidad entre ellas, disponer de un grupo interuniversitario de auditores de seguridad de los sistemas de información puede contribuir a facilitar y a uniformizar la implantación de las auditorías de SI en el Sistema Universitario Español.

La Sectorial CRUE-TIC es consciente de la importancia creciente de la Auditoría de seguridad de los sistemas de información y está desarrollando iniciativas para liderar este proceso en el entorno universitario español.

Finalmente, como conclusión a este artículo, proponemos unas recomendaciones concretas para aplicar en nuestras Universidades y generar la confianza necesaria en nuestros Sistemas de Información:

- Separar la función de seguridad de la de prestación de los servicios.
- Designar un Responsable de seguridad que reporte directamente al Equipo de Dirección, que se encargue de controlar el funcionamiento del Sistema de gestión de la seguridad.
- Desarrollar la función de auditoría de seguridad de los sistemas de información con un auditor interno independiente, debidamente cualificado y que reporte directamente al Equipo de Dirección. Esta función de auditoría podría recaer también sobre el Responsable de Seguridad.
- Integrar las medidas técnicas para protección de datos personales en el "Sistema de gestión de la seguridad de la información", con un alto grado de coordinación entre el Delegado de Protección de Datos y el Responsable de Seguridad.
- Creación de un grupo de auditores de Sistemas de Información universitarios con capacidad para realizar auditorías de certificación.

El Responsable de Seguridad, el Delegado de protección de datos y el Auditor interno deberán tener en cuenta que el Esquema Nacional de Seguridad es el marco de referencia para la aplicación de las medidas de seguridad, incluidas las requeridas por el RGPD, en el ámbito de toda la Universidad.

Bibliografía y referencias:

A lo largo de este documento hemos referenciando otras fuentes (normativas, informes, estándares, etc.), que nos han servido de base a la hora de realizar nuestra exposición; creemos que estas referencias constituyen una ayuda muy importante para entender el papel de la Auditoría de Seguridad de los Sistemas de Información y pueden constituir una guía de gran valor para el lector. Por eso hemos querido finalizar este documento con esta bibliografía que a nuestro entender constituye el marco de referencia básico a tener en cuenta por las Universidades.

- 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 y Real Decreto 951/2015, de 23 de octubre, de modificación 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.
- Norma ISO 19011.
- Normas ISO 27001 y 27002.
- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Guía de Seguridad de las TIC CCN-STIC 801- «Responsabilidades y funciones en el ENS».
- Guía de Seguridad de las TIC CCN-STIC 802 «ENS. Guía de auditoría».
- Guía de Seguridad de las TIC CCN-STIC 803 «ENS. Valoración de los sistemas». ANEXO I: Valoración de los sistemas en Universidades.
- Instrucción Técnica de Seguridad de conformidad con el ENS (Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas).
- Instrucción Técnica de Seguridad de Auditoría de la seguridad de los sistemas de información (Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública).
- Informe CCN-CERT IT 18/18 del estado de la Seguridad de los sistemas de información en las Universidades (informe INES).
- La Gestión de la Seguridad de la Información en las Universidades Españolas. Universitic 2017: Análisis de las TIC en las Universidades Españolas.
- Marco de gobierno TI/SI basado en la innovación y la auditoría TI. Gestionando la transformación digital. Universitic 2017: Análisis de las TIC en las Universidades Españolas (pags. 132 a 146).
- La Gestión de la Seguridad de la Información en las Universidades Españolas. Universitic 2017: Análisis de las TIC en las Universidades Españolas (pags. 151 a 163).
- Sectorial CRUE-TIC: iniciativa AIDA, presentada por Elisa Ramírez (Universidad Miguel Hernández)en http://tic.crue.org/wp-content/uploads/2016/11/AIDA-Acuerdo-Interuniversidad-de-Auditor%C3%ADas-TIC-Ramirez-Navalon-Elisa.pdf
- «Principios y recomendaciones básicas en ciberseguridad – 2017» publicado por el CCN-CERT (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html)

Nota final:

Coincidiendo con la finalización de la redacción del presente documento, se ha hecho público el Informe emitido por la Ponencia sobre el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (con fecha de 9 de octubre de 2018) que sustituirá a la actual LOPD.

Es significativo que se ha modificado el nombre de la Ley, pasándose ahora a denominar «**Ley Orgánica de Protección de datos personales y Garantía de los derechos digitales**», incluyendo un título completo (el Título X) sobre «Garantía de los derechos digitales», que reconoce y garantiza un conjunto de «Derechos digitales» de los ciudadanos, entre los que nos encontramos, entre otros: derecho a la Seguridad digital, derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, derecho a la desconexión digital en el ámbito laboral, Derecho al olvido en búsquedas de Internet, etc.

Esto eleva el marco de exigencia normativa y nos debe hacer reflexionar aún más sobre la necesidad de establecer e implantar en nuestras universidades las herramientas y estructuras que garanticen la seguridad de nuestros Sistemas de información y generen la confianza suficiente en los ciudadanos que usen nuestros servicios.

crue
Universidades
Españolas

TIC