María Elisa Vivancos Cerezo

Departamento de Patrimonio Artístico y Documental
Programa 108: «Gestión del Conocimiento en las Organizaciones»
Universidad de León. Junio 2008.

# La seguridad en Bibliotecas universitarias: normas y auditoría

*Trabajo de investigación tutelado*

***Tutora: Dra. D. ª María Marsá Vila***

# Resumen

*Justificación del planteamiento del trabajo*

La Biblioteca Universitaria cobra un papel esencial en el marco de la Sociedad de la Información como depósito y canal de comunicación del conocimiento universitario. También es trascendental su papel para la comunidad universitaria como fuente y vehículo de apoyo para la docencia, el aprendizaje y la investigación. Dado el creciente uso de las tecnologías de la información y la comunicación para soporte de estas actividades, se plantea un estudio sobre las necesidades específicas de estas unidades de información para la **gestión de la seguridad de la información**. Tras analizar las normas existentes en materia de seguridad de la información y auditoria de seguridad, se evalúa la capacidad de la dirección de las bibliotecas universitarias para adaptar su gestión de seguridad de las TIC a estos estándares. Se estudian el estado actual y las medidas necesarias para implantar estrategias de gestión de la seguridad de la información en las bibliotecas universitarias españolas, tomándose como «caso de estudio» la Biblioteca Universitaria de la Universidad de León. Concluye el trabajo con la propuesta de un estudio del asunto a nivel nacional.

## Palabras clave

Bibliotecas universitarias; Tecnologías de la información y la comunicación; TIC; Gestión de la seguridad de la información; Auditoria de seguridad; Seguridad de la información.

# Índice

# 1. INTRODUCCIÓN

Los servicios de las bibliotecas universitarias se basan en las tecnologías de la información y la comunicación (TIC). En su evolución y en su entorno, se plantean retos que las promueven como instrumento esencial para la *Gestión del Conocimiento* universitario en la Sociedad de la Información: bibliotecas digitales, objetos de aprendizaje, herramientas de colaboración *en línea*, etc. Para conseguir afrontar con éxito estos retos y servir a la comunidad universitaria en este entorno dinámico, su gestión ha de incorporar los elementos que permitan garantizar la seguridad de la información asociada a los servicios, recursos y documentos que ofrece.

El objetivo de este trabajo es analizar la situación de la gestión de la seguridad en las bibliotecas universitarias, basándose en el caso de estudio de la Biblioteca de la Universidad de León.

## Contexto

La seguridad de la información es uno de los objetos de impulso de la Sociedad de la Información iniciados por el Ministerio de Industria, Turismo y Comercio para fomentar la confianza en los servicios que se ofrecen, tanto por la empresa privada como por la Administración, a través de Internet.

También en la actualidad la Gestión de la Seguridad de la Información está recibiendo atención de los agentes encargados de establecer estándares y normas como se refleja en las recientes publicaciones de AENOR y organismos internacionales.

La presencia de las universidades en Internet y la oferta de enseñanzas a distancia y semi-presenciales van a ser elementos esenciales para su prosperidad dada la *movilidad virtual* que la red otorga a los estudiantes. La biblioteca universitaria se convierte, junto con las aulas virtuales, en el núcleo de la enseñanza virtual. Por otra parte, la evolución de la enseñanza hacia el EEES[1], enfocada en el aprendizaje, comporta un mayor uso de recursos de información, repositorios digitales y entornos de colaboración, que residirán en las bibliotecas universitarias. La confianza en los servicios que ofrecen las bibliotecas universitarias descansa en la garantía de seguridad de la información que puedan demostrar.

## Beneficios

El análisis de la situación de la gestión de la seguridad de la información en el entorno de las bibliotecas universitarias va a reportar un conocimiento que permitirá abordar con éxito proyectos de implantación de sistemas de gestión de seguridad de la información.

En paralelo el estudio conlleva un germen de sensibilización y concienciación en la materia, al despertar la conciencia de la importancia de la gestión de la seguridad en la dirección de las bibliotecas universitarias que va a revertir en toda la comunidad universitaria.

[1] Espacio Europeo de Educación Superior

# 2. SITUACIÓN ACTUAL

*Bibliotecas universitarias y Seguridad TIC*

Este capítulo contiene una revisión del contexto y de los avances en materia de seguridad de la información para las bibliotecas universitarias.

En primer lugar se describe la situación actual de las bibliotecas universitarias en lo referente al impacto producido por las tecnologías de la información y la comunicación (TIC) en las mismas. Se hace referencia someramente a la realidad nacional, envuelta en el proceso de convergencia con el Espacio Europeo de Educación Superior, con el soporte de los informes y encuestas de la Red de Bibliotecas Universitarias: REBIUN.

Se repasan los modelos organizativos universitarios, propuestos por investigadores, que dan a las bibliotecas de estas instituciones un papel esencial en la gestión del conocimiento universitario y, por extensión, para la educación en la nueva sociedad.

Finalmente, se señalan los estudios recientes en materia de seguridad de las TIC en entornos bibliotecarios y académicos, enfatizando en los nuevos servicios y sus formas de acceso y utilización, las bibliotecas digitales y la forma de abordar gestión de la seguridad.

A lo largo de este trabajo se toma como caso de estudio la Biblioteca Universitaria de la Universidad de León. El desarrollo del caso se inicia en este apartado, señalando las características organizativas de esta biblioteca y su entorno, así como los servicios que ofrece y el uso que hace de las TIC. Como colofón de esta primera parte se describe la organización de las TIC en las Bibliotecas Universitarias y en el caso de estudio.

## 2.1. Las Bibliotecas Universitarias y las TIC

### *Introducción*

La información digital ofrece muchas posibilidades en todos los campos del saber, y sus aplicaciones, en el mundo actual. La propagación del uso de las tecnologías de la información ha revolucionado la existencia humana en todos los ámbitos: la educación, la economía, la cultura, la democracia, sociedad, etc. Es lo que se conoce como *Sociedad de la Información* (Masuda, 1981) o como *Sociedad del Conocimiento* (Druker, 1974), situando a la información o al conocimiento en el centro de producción de riqueza. En un sentido más amplio se la ha denominado *Sociedad Red* (Castells, 2002) aplicando la metáfora de que Internet se convierte en «el tejido de nuestras vidas».

En este entorno cambiante y globalizado, los sistemas y servicios bibliotecarios tradicionales están siendo reemplazados por nuevas prácticas: colecciones digitales, automatización de bibliotecas, redes y consorcios de bibliotecas, iniciativas de acceso abierto, etc.

Las bibliotecas universitarias, orientadas al soporte a la docencia, el aprendizaje y la investigación, se ven fuertemente afectadas por los desarrollos, la diversificación y la expansión de las tecnologías de la información, que ofrecen nuevas formas de comunicación y de difusión. Sus servicios clásicos se ven desbordados por las posibilidades tecnológicas y los vertiginosos cambios que la Sociedad de la Información impone. También se vislumbran para las bibliotecas universitarias nuevas oportunidades como gestoras del conocimiento universitario, en lugar del tradicional papel que tenían como depositarias del mismo.

Inmersas a su vez y, en parte por el mismo motivo, —el advenimiento de esta nueva Sociedad—, en el marco del Espacio Europeo de Educación Superior (en adelante EEES), las bibliotecas universitarias y sus profesionales se enfrentan pues a nuevos retos en su función y quehacer.

En España las bibliotecas universitarias se encuentran en un importante proceso de cambio que afecta al núcleo de su actividad, como puede apreciarse en el Plan Estratégico de la Red de Bibliotecas Universitarias (REBIUN, 2007-2010), cuyo condicionante principal es la implantación del EEES basado en el aprendizaje permanente y activo.

En este Plan Estratégico destaca la importancia que se otorga a: los repositorios institucionales, la biblioteca digital, la integración de ésta en los campus virtuales, el aprendizaje en red, las habilidades de información (ALFIN), el desarrollo e implantación de nuevas tecnologías y servicios, etc.

## Tendencias de las Bibliotecas Universitarias en la Sociedad de la Información

Desde hace años las bibliotecas en general, y las bibliotecas universitarias en particular, experimentan cambios sustanciales como consecuencia de las nuevas tecnologías. Desde los primeros pasos en la automatización, a los que siguieron los catálogos en línea y las bibliotecas digitales, hasta los proyectos actuales que incluyen la integración en las bibliotecas de servicios propios de la *Web 2.0*, entre otros: *blogs*, sindicadores de contenidos, etiquetado social, *chats*, foros, espacios *wiki* y *podcasting*.

Las bibliotecas universitarias van incorporando los cambios que ofrecen las tecnologías de acuerdo a su idiosincrasia particular, sus necesidades y los objetivos del entorno universitario en el que están inmersas.

En los siguientes párrafos se destaca la interrelación entre la educación y el nuevo paradigma social y cómo este se manifiesta en los planteamientos de futuro de las bibliotecas universitarias.

### *La Educación y la Sociedad de la Información*

La Educación ha tenido a lo largo de la historia un papel «clave» (Majó, 1988) en el desarrollo de la sociedad, con una función múltiple: contribuir a que las nuevas generaciones asimilen el progreso alcanzado, se incorporen activamente a la vida en sociedad, reconozcan y promuevan sus valores éticos y culturales, y puedan aportar nuevas soluciones socio-económicas y científico-tecnológicas.

En la *Sociedad de la Información,* la Educación, y en particular la educación universitaria, sigue siendo esencial. Su necesidad se amplía en profundidad y extensión: en profundidad, debido a la velocidad de los avances en todos los campos; y en extensión debido a la demanda de renovación de conocimientos y la necesidad de adquirir nuevas destrezas durante toda la vida. Se modifican a su vez las formas de transferencia y adquisición de conocimientos, alteradas por la generalización de las tecnologías de la información y la comunicación.

Se pone de manifiesto que de la educación y del acierto de su adaptación depende el futuro de la sociedad. El éxito de la implantación de los nuevos métodos y sistemas de aprendizaje que permiten las TIC reside en que han de estar acompañados de nuevos modelos de enseñanza-aprendizaje y de la renovación de las instituciones educativas. De esto se hace eco el Documento Marco del MEC (2003) *La integración del Sistema Universitario español en el EEES,* fomentando la colaboración entre las instituciones, la calidad universitaria y el desarrollo de una Europa del Conocimiento.

Dentro del entorno universitario español, las bibliotecas universitarias tienen por misión, según el citado Plan Estratégico de REBIUN (REBIUN, 2007-2010), ser un servicio a disposición del sistema universitario en el marco de EEES basado en el aprendizaje a lo largo de toda la vida (*LLL: Long Life Learning*). Su objetivo incluye un conjunto de necesidades que han de satisfacer, entre las que se encuentran:

- la biblioteca como agente difusor de los conocimientos de su universidad: los repositorios institucionales
- la biblioteca como Centro de Recursos para el Aprendizaje y la Investigación (CRAI) para conseguir los fines propuestos.
- la oferta de nuevos servicios: integración de bibliotecas digitales en los campus virtuales para potenciar el aprendizaje en red, las habilidades en información (programa ALFIN), etc.
- los servicios de la biblioteca como marca de calidad y la fidelización del usuario por la calidad ofrecida.

## Las Bibliotecas Universitarias y la *Gestión del Conocimiento*

En el epígrafe anterior se describe la importancia del papel que van a jugar las universidades en la nueva Sociedad. Se exponen a continuación las ideas de algunos investigadores que otorgan a las bibliotecas universitarias un papel fundamental en la *Gestión del Conocimiento* universitario.

Unos consideran a las universidades «Organizaciones intensivas en conocimiento» (Serradell y Juan, 2003) y otros «Empresas del conocimiento» (Rowley, 2003; Malone y Yohe, 2002), considerándose esencial su aportación a la Sociedad actual. Los modelos de *Gestión del Conocimiento* que estos investigadores proponen para la Universidad incluyen «Repositorios o Espacios de Conocimiento» con sede en la biblioteca universitaria.

También se subyace la idea (Rius, 2007) de que los «Repositorios o Espacios de Conocimiento» *en abierto* son claves para impulsar la calidad y excelencia de las universidades.

Por otra parte los «Espacios de Conocimiento» comparten contenidos con las «Aulas Virtuales» que reposan en plataformas de *e-learning*. Los contenidos son el vehículo para la transferencia del conocimiento. Con la creación y difusión de contenidos, aparecen elementos de seguridad a considerar para permitir a los usuarios y creadores de los mismos depositar su confianza en estos medios. Entre estos elementos están: la gestión de derechos de autor, la garantía de confidencialidad de los datos de usuario y de sus actividades, y la integridad y disponibilidad de documentos y servicios.

### *Las universidades y la Gestión del Conocimiento*

Estudios sobre *Gestión del Conocimiento* (Rowley, 2003; Malone y Yohe, 2002) sugieren que las universidades van a ser claves en la creación de una sociedad sostenible, equitativa y estable, convirtiéndose en «empresas de conocimiento». Sostienen que en las universidades reside un gran capital de conocimientos ya que con la investigación —y sus publicaciones— contribuyen a la creación de conocimiento, y con la docencia —y el aprendizaje— se comprometen a compartirlo y difundirlo. Para estos investigadores, en las bibliotecas universitarias reside la función de «repositorios de información publicada»; y en los académicos la capacidad de formar «comunidades de conocimiento» que sobrepasen los límites de la universidad.

Según Serradell y Juan (2003), las universidades se han de considerar «organizaciones intensivas en conocimiento», porque localizan y crean, estructuran, almacenan y distribuyen el conocimiento. Estos investigadores proponen un modelo de gestión universitaria basado en cinco pilares esenciales: un Sistema de información EIS

*(Enterprise Information System)*, una Red de colaboración, un Espacio de conocimiento, un Sistema CRM *(Customer Relationship Management)* de gestión de relaciones con clientes y una Cultura organizativa innovadora. Las bibliotecas universitarias serán esenciales para concretar el «Espacio de conocimiento» de este modelo.

Otros investigadores inciden en que las bibliotecas universitarias tendrán una función fundamental en los procesos derivados de la *Gestión del Conocimiento* (Townley, 2001) además de creando «Repositorios de conocimiento», mejorando el acceso al mismo —redes de expertos, comunidades de interés, bibliotecas virtuales—, enriqueciendo el entorno para la creación y transferencia de conocimiento y gestionándolo como un activo para la organización.

### *Contenidos de aprendizaje en abierto: Open CourseWare*

También se otorga protagonismo a los contenidos de aprendizaje en abierto, los llamados *Open CourseWare* en la *Sociedad del Conocimiento* en un mundo globalizado, acuñándose el término «Meta-universidad» (Vest, 2006) para definir el movimiento emergente desencadenado a partir de las iniciativas *Open CourseWare,* (en adelante *OCW*). Otros estudios (Jonhstone, 2005) defienden que los *OCW* aportarán también mejoras para las instituciones académicas además de para la sociedad.

Los *OCW* son publicaciones digitales abiertas y de libre distribución de materiales educativos de alta calidad organizados en cursos. Los materiales —programas docentes, materiales usados en clase, ejercicios propuestos o videograbaciones— de las clases son puestos a disposición pública para su visualización e utilización. Se autoriza su redistribución y transformación bajo licencias *Creative Commons* «Reconocimiento-No Comercial-Compartir Igual». Son de libre disposición, el autor asume la reutilización o adaptación de los mismos siempre bajo unas condiciones de respeto y nunca con ánimo de lucro.

La iniciativa *Open CourseWare* comenzó en el año 2002 (MIT-OCW [2]), fundada conjuntamente por el Instituto Tecnológico de Massachusetts (MIT) en colaboración con la Fundación William y Flora Hewlett[3] y la Fundación Andrew W. Mellon[4], personifica dos tendencias universitarias: la responsabilidad social y la búsqueda de la excelencia (Pernias y Marco, 2007).

Desde el comienzo de esta iniciativa, el MIT ha puesto —en línea— todo el material docente de los cursos de nivel de grado *(graduate)* e inferiores al grado *(undergraduate)*, ofreciendo acceso libre, sencillo y coherente a los materiales docentes para educadores, estudiantes y autodidactas de todo el mundo.

En el año 2005, el *OCW* del MIT y otros proyectos líderes en *OCW* fundaron el Consorcio *OCW Consortium* que persigue extender el alcance e impacto de estos materiales, fomentar la creación de nuevos contenidos y desarrollar modelos sostenibles para la publicación de *OCW*.

El Consorcio *OCW* es una red internacional de colaboración que comprende a más de cien instituciones y organizaciones universitarias que participan de un extenso conjunto de contenidos educativos abiertos y un modelo común de compartirlos. La misión del Consorcio es difundir la educación y potenciar a los individuos de todo el mundo mediante *OCW*.

El consorcio tiene entre sus miembros universidades de Austria, Canadá, China, Colombia, Francia, Japón, Corea, México, Holanda, Arabia Saudí, Sudáfrica, España, Portugal, Tailandia, Reino Unido, Estados Unidos, Venezuela y Vietnam.

[2] http://ocw.mit.edu/OcwWeb/index.htm
[3] http://www.hewlett.org/Default.htm
[4] http://www.mellon.org/

En España, Iberoamérica y Portugal, *Universia* [5] encabeza la incipiente iniciativa del Consorcio en Iberoamérica. En un primer paso los contenidos fueron sólo traducciones del material elaborado por el MIT-OCW Universia[6]. Actualmente hay catorce universidades españolas, las promotoras del proyecto, dispuestas a crear su propio *«OCW site»*, en el que incorporarán un mínimo de diez asignaturas de las que imparten.

### *Repositorios o Espacios de Conocimiento*

Los «Repositorios o Espacios de Conocimiento» se concretan en almacenes centralizados de información digital. En el entorno de la Educación Universitaria tienen una doble funcionalidad de apoyo a la docencia y a la investigación.

En las bibliotecas universitarias residen muchos de los repositorios «abiertos», como los anteriormente citados OCW entre cuyos objetivos es fundamental la libre distribución de los contenidos educativos. Esta finalidad de los repositorios abiertos, además de su labor social, puede convertirse en la mejor publicidad para las universidades (Rius, 2007) y en la fuerza motriz de la calidad de las mismas.

Los llamados «Repositorios Institucionales» de las universidades son en realidad bases de datos o de archivos informáticos que contienen artículos de investigación, tesis, informes técnicos, literatura gris, en algunos casos documentos administrativos y recientemente «objetos de aprendizaje». Su propósito general es la publicación, el auto-archivo, la libre disposición y la conservación de estos documentos.

Ya que estos Repositorios acumulan cantidades cada vez mayores de información, sus infraestructuras organizativas y tecnológicas han de estar sometidas a un importante control. Tanto los que depositan la información, como los que la ponen a disposición de los que la consultan y estos últimos precisan altos niveles de confianza en los procedimientos que se utilizan para su tratamiento. La calidad, y la seguridad, de este y otros servicios de la biblioteca son esenciales para dar el soporte correcto a la función que desempeñan.

### *Aulas virtuales y objetos de aprendizaje*

Hemos visto que uno de los pilares de la *Gestión del Conocimiento* (Serradell y Juan, 2003) es la creación de un «Espacio de conocimiento» que sirva como repositorio de documentos y archivo, y que sea fácilmente indexable y accesible para cualquier miembro de la organización.

Por otra parte, como consecuencia tanto de la necesidad de aprendizaje a lo largo de toda la vida (*LLL: Long-Life Learning*) como de las nuevas herramientas y plataformas de enseñanza, se hace patente que las tecnologías son imprescindibles para la alfabetización en la Sociedad de la Información. Como consecuencia surge una revolución de las aplicaciones educativas a través de Internet, lo que se conoce como *e-learning*.

Ambas realidades, los «Espacios de conocimiento» y las Plataformas de *e-learning*, comparten contenidos: los objetos de aprendizaje. Al igual que con los «Espacios de conocimiento», las plataformas *e-learning* y los contenidos educativos, y otros «objetos de aprendizaje», descansan en aplicaciones TIC en las que los usuarios tienen que asegurarse que se garantizan los derechos de autor, los derechos del individuo (datos personales) y la confidencialidad, disponibilidad e integridad de los documentos y servicios ofrecidos.

Alrededor del *e-learning* han surgido paquetes de software para administrar, distribuir y controlar las actividades de formación: los *LMS* (*Learning Management Systems*) también

[5] http://ocw.universia.net/es/
[6] http://mit.ocw.universia.net/

conocidos como «Aulas virtuales». Sus funciones son: gestionar usuarios, recursos y actividades de formación, administrar el acceso, controlar y hacer seguimiento del proceso de aprendizaje, realizar evaluaciones, generar informes y gestionar servicios de comunicación como foros de discusión y videoconferencias.

Sin embargo, los *LMS* no incluyen la posibilidad de crear contenidos, centrándose en gestionar los contenidos creados por otros medios. La creación de los contenidos para los cursos se realiza en otros paquetes software, denominados ***LCMS*** (*Learning Content Management Systems*). Los *LCMS* son sistemas de gestión de contenidos específicos para enseñanza. Proporcionan a los autores, a los diseñadores de cursos y a los expertos en las materias los medios para crear, aprobar y publicar cursos con mayor eficiencia, manejando contenidos reutilizables a su disposición.

Además del software necesario para crear los cursos, son necesarios los propios contenidos, los «objetos de aprendizaje», que se almacenarán en repositorios de objetos de aprendizaje. Existen muchas iniciativas para compartir objetos de aprendizaje entre las que se cabe destacar: Merlot[7], Ariadne[8] , EdNA Online[9] y SMETE[10].

El desarrollo de contenidos educativos de calidad es una labor costosa que exige generalmente la colaboración de expertos de distintas áreas (contenidos, tecnología, didáctica). Existen iniciativas para sistematizar la creación de contenidos que quedan fuera del ámbito de este estudio. Las bibliotecas universitarias tienen un importante papel en este campo: proporcionando mecanismos y experiencia para gestión de los objetos de aprendizaje y la coordinación de comunidades de expertos para su elaboración.

## Uso de las TIC en las bibliotecas universitarias: usuarios, servicios y tecnologías

Las bibliotecas universitarias son un reflejo de la sociedad en la que están integradas y adaptan sus servicios a los usuarios a los que van destinadas. Así, se ven afectadas por factores sociales, políticos, económicos y tecnológicos. Algunos de estos ya se han tratado los párrafos anteriores.

Entre los factores sociales que afectan a la universidades españolas podemos destacar: la disminución del número de alumnos; el aumento de la movilidad y del número de estudiantes extranjeros; la necesidad de reciclaje profesional y de aprendizaje durante toda la vida (*LLL: Long-Life Learning*); el apoyo a la investigación; los cambios en la docencia; el incremento de la producción científica y la creciente demanda de servicios *en línea*.

Como ya se ha mencionado, las bibliotecas universitarias españolas están intensamente involucradas en la convergencia e integración de las universidades con el EEES. Además de éste, hay otros factores políticos que inciden de lleno en su gestión como la legislación actual (Ley Orgánica de universidades, LOU, 2001) que enfoca la Universidad hacia la Investigación o el desarrollo e implantación de planes de evaluación de calidad universitaria, que incluyen la calidad en las bibliotecas universitarias.

También factores económicos inciden en la gestión de las bibliotecas universitarias. Así, su ubicación geográfica, la idiosincrasia de la provincia y la Comunidad Autónoma de sus sedes; el nuevo entorno bibliotecario protagonizado por los Consorcios de Bibliotecas y la Cooperación Interbibliotecaria; los acuerdos con editores y distribuidores; la necesidad de rentabilizar y justificar las inversiones; la problemática de los derechos de autor; y el aumento del precio de suscripciones impresas.

[7] http://www.merlot.org/
[8] http://www.ariadne-eu.org/
[9] http://www.edna.edu.au/
[10] http://www.smete.org/

Por último inciden sin duda las características particulares de la Universidad a la que pertenecen: su historia, tamaño, estructura, cultura corporativa, recursos, etc.

Los usuarios, tecnologías y servicios de las Bibliotecas Universitarias españolas son tan variados como las propias universidades que las albergan, si bien existe una composición básica compartida por todas, como reflejan los indicadores de REBIUN. Sobrepasa el alcance de este trabajo el análisis pormenorizado de las bibliotecas universitarias españolas. El propósito del presente trabajo es formular un modelo de estudio básico para la gestión de la seguridad de las TIC en las mismas y para ello se toma como caso de estudio los servicios y procesos de la Biblioteca Universitaria de la Universidad de León. [Una descripción tanto de la ULE como de su biblioteca y servicios se incluye en los anexos 8.1 y 8.2].

Las Bibliotecas Universitarias tienen como público objetivo la comunidad universitaria. Formando parte de ésta podemos distinguir: los alumnos clasificados por el ciclo de estudios que cursan, los profesores e investigadores y el personal de administración y servicios. Otros usuarios que habitualmente se contemplan son los usuarios en tránsito con los mismos perfiles mencionados pero con una relación esporádica con la institución.

Las tecnologías TIC utilizadas son estándares entre las bibliotecas universitarias para los procesos técnicos, los servicios básicos y los servicios a través del web con especial atención al acceso remoto a los recursos electrónicos. Además de las tecnologías básicas cabe destacar que recientemente se ha incorporado el acceso inalámbrico (Wi-Fi) en las universidades y que algunas bibliotecas incorporan mecanismos de *RFID* (Identificación por Radio Frecuencia) para los servicios de préstamo.

Mención singular, por su importancia para la seguridad de la información, merece la preservación de documentos digitales y la gestión de derechos de autor. Esta última ha de implementarse mediante sistemas específicos: *ERM (Electronic Rights Management).* Más adelante en este trabajo se comentan las iniciativas existentes para preservación de documentos digitales.

### *Acceso remoto a los recursos electrónicos*

Es un hecho constatado (REBIUN) que está creciendo la contratación de recursos electrónicos por parte de los servicios de bibliotecas universitarias, motivada por la demanda de los mismos. Este hecho, además del coste elevado de estos recursos, ha obligado a las universidades a establecer mecanismos para **controlar el uso** de estos **y facilitar el acceso autorizado** a los mismos, incluso desde fuera de los límites de la red corporativa de la universidad.

El informe sobre los principales sistemas utilizados por las bibliotecas REBIUN para gestionar el acceso remoto a los recursos electrónicos coordinado por la universidad de Valencia y la universidad Pablo de Olavide entre sus conclusiones incluye que:

- el método de acceso más utilizado por las bibliotecas son las redes privadas virtuales (VPN) frente a integradores basados en tecnologías Proxy y control del recurso mediante usuario y contraseña
- el método de autenticación[11] más frecuente es *LDAP (Lightweight Directory Access Protocol)* con servicios de directorio centralizado
- en el futuro el control de accesos y la identificación de usuarios se realizará mediante un sistema federado ofertado por la Fundación Española para la Ciencia y la Tecnología (FECYT)

[11] En seguridad informática, la autenticación es el proceso mediante el cual se intenta verificar la identidad digital del remitente de una comunicación como parte de una petición para conectarse.

- es esencial la colaboración entre las bibliotecas, los centros de informática y la FECYT para poder extrapolar el modelo de licencias nacionales a otros productos (proyecto Biblioteca Electrónica de Ciencia y Tecnología: BECyT)

- los sistemas de metabúsqueda e integración de recursos de información utilizados en las bibliotecas REBIUN son variados aunque se concentran en dos o tres productos del mercado

- la mayoría de las bibliotecas utilizan tecnología de enlace OpenURL (estándar Z39.88 [12]), tanto de forma remota como local. Esta tecnología utilizada por editores y proveedores de información, permite interconectar directamente todos los componentes de una biblioteca digital (acceso a texto completo, consultas a catálogo, formularios de préstamo interbibliotecario, descarga de referencias, etc.)

### *Bibliotecas digitales y derechos de autor*

Las bibliotecas digitales son en sentido amplio colecciones organizadas de contenidos multimedia digitales de alta calidad accesibles mediante redes de ordenadores. Incluyen ayudas de navegación y búsqueda que permiten el acceso a la información almacenada en la propia colección y a recursos en otras colecciones.

Los contenidos responden a la siguiente tipología:

- contenidos creados en ordenador

- contenidos convertidos a digitales (originales en papel, sonido analógico, etc.)

- acceso a contenidos externos mediante punteros a otras colecciones digitales

Los contenidos digitales están sometidos a los mismos procesos que los analógicos: selección y adquisición, catalogación, almacenamiento, recuperación, mantenimiento y gestión de derechos de autor con mecanismos adaptados al carácter digital de los contenidos. En particular el mantenimiento y conservación de los mismos hace necesarios: la adecuación del equipamiento, el control de versiones, la actualización del software, la comprobación de URLs y herramientas para la gestión de los derechos de autor.

Los derechos de propiedad intelectual y la seguridad de la información son cuestiones interdependientes. La primera promueve la producción intelectual con incentivos mientras que la segunda protege a las creaciones digitales de accesos no autorizados a la vez que garantiza la veracidad y autoría de los objetos de información digital. Las soluciones técnicas que protegen los derechos de autor incluyen: protección anti-copia, mecanismos de facturación automática, algoritmos de encriptación y marcas de agua digitales. Las bibliotecas digitales deben implantar sistemas específicos de gestión de derechos de autor.

### *Retos actuales y futuros*

Se han mencionado a lo largo de este apartado algunos de los retos a los que se enfrentan las bibliotecas universitarias en cuanto al uso de las TIC. Además de los servicios tradicionales, hoy en día automatizados y los servicios que se ofrecen a través de la página web, se hace patente un creciente uso de los recursos electrónicos que obligan a mejoras en su adquisición, organización y acceso. También, aunque no en todas las universidades por igual, se plantean nuevos servicios derivados del aprendizaje permanente (los objetos de aprendizaje, la alfabetización, OCW, etc.), las bibliotecas

[12] NISO Z39.88 -2004 *The OpenURL framework for context-sensitive services; National Information Standards Organization*; Se puede descargar gratuitamente de: http://www.niso.org/standards/index.htm

digitales, los repositorios institucionales, el acceso remoto de usuarios y la incorporación de tecnologías de circulación basadas en RFID.

A consecuencia de la ubicuidad de Internet, los usos de los espacios de bibliotecas se transforman para ofrecer a la vez acceso a materiales impresos y digitales convirtiéndose en espacios sociales, lugares de trabajo en grupo, de acceso inalámbrico a Internet, de utilización de portátiles y dispositivos móviles (teléfonos, *PDAs*) para comunicarse mediante *chats* y correo electrónico (Chandorkar, 2005).

Además, son comunes para esta y otras organizaciones otros retos que se presentan a raíz de la generalización de las tecnologías de la información: uso del *DNIe* y la factura electrónica y la obligación de cumplimiento legislativo (LOPD[13], LISI[14] y LPI[15], etc.).

## Organización de las TIC en las Bibliotecas Universitarias

Hasta ahora se ha descrito el impacto de las TIC en la educación y en las bibliotecas universitarias, los planteamientos de futuro y la realidad de estas instituciones en España.

### *El entorno universitario y las TIC*

Los entornos universitarios tienen ciertas características que afectan a la forma en la que aceptan e incorporan las tecnologías de la información:

- son abiertos y flexibles por naturaleza (Templeton, 2005) facilitando la equidad en la distribución del conocimiento sin imponer límites a su difusión;
- tanto si son de financiación pública como privada están sujetos a las regulaciones nacionales y regionales;
- su estructura organizativa es mixta (administración y servicios, y docencia), con estamentos con niveles de autonomía dispares que hacen compleja la uniformidad de equipamiento y procesos informáticos.

Estas características influyen también en las bibliotecas universitarias en cuanto que forman parte de una universidad y contribuyen a los objetivos de ésta.

De todo lo expuesto se desprende que la complejidad de los entornos universitarios se traslada a la organización de las TIC en las Bibliotecas. El caso más general en estas instituciones, las universidades, es que los recursos informáticos estén a cargo de un área específica en su organización que ofrecen sus servicios al resto de la estructura. Tal es el caso de la Universidad de León y su biblioteca, cuyos servicios reposan en el apoyo y soporte físico y lógico que presta el Servicio de Informática, con personal dedicado específicamente a la Biblioteca.

Es muy dispar entre las universidades, y fuente de complejidad añadida, la financiación de los fondos bibliográficos de las Bibliotecas Universitarias como reflejan los indicadores de las estadísticas de REBIUN. Sus fondos son adquiridos con presupuesto directo de la universidad o a través de los Departamentos Docentes, la Biblioteca y las Facultades, siendo en ocasiones fruto de subvenciones externas.

[13] Ley 15/1999 de Protección de Datos de Carácter Personal
[14] Ley 58/2007 de medidas de Impulso de la Sociedad de la Información
[15] Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril.

## Caso de estudio: La Biblioteca de la Universidad de León

### *Introducción*

La Biblioteca de la Universidad de León se define como:

> «centro de recursos para el aprendizaje, la docencia, la investigación y las actividades relacionadas con el funcionamiento y la gestión de la universidad en su conjunto.»

Está formada por la Biblioteca General, cuatro Bibliotecas de Área temática (que engloban a las Bibliotecas de Centro) y una Biblioteca de Campus en Ponferrada.

Dentro de la Universidad de León (en adelante ULE) y según su Estatuto[16] es «una unidad funcional cuya principal misión es la de servir de apoyo a las tareas docentes, discentes e investigadoras de la comunidad universitaria». Orgánicamente depende del Vicerrectorado de Innovación Tecnológica.

Al ser una Biblioteca de una universidad pública está integrada dentro del Sistema Español de Bibliotecas[17], siendo la Biblioteca Nacional la cabecera del sistema.

### *Nuevos servicios*

En el Anexo 1 se incluyen datos específicos de la ULE y su Biblioteca incluyendo los servicios que ofrece según su Reglamento.

Además de los servicios tradicionales de las bibliotecas universitarias ofrece un Centro de Apoyo al Aprendizaje y la Docencia (CAAD) (Barrionuevo y Marsá, 2007) que físicamente se ubica en el edificio CRAI-TIC de la universidad, con personal y equipamiento específicos para las funciones que tienen asignadas. Los objetivos de este servicio son potenciar las actividades de la Biblioteca como servicio integrador de los recursos de información en sus diferentes soportes, y como centro de gestión y aprovechamiento de las posibilidades de las nuevas tecnologías en el ámbito de la docencia y el aprendizaje. Para ello cuenta con personal especializado (bibliotecarios y técnicos) que analizan las necesidades y se ocupan de integrar los recursos de la Biblioteca en los proyectos docentes, así como de la gestión y aprovechamiento de las colecciones digitales, repositorios de nuevos materiales docentes y recursos electrónicos propios o compartidos, etc.

También recientemente se ha reformado y mejorado la página web de la Biblioteca Universitaria, con especial énfasis en el apartado de Recursos electrónicos incorporando un buscador específico y nuevos recursos de acceso abierto. Este apartado incluye ahora accesos a Repositorios temáticos (*e-prints*), «Repositorios institucionales» o archivos abiertos nacionales e internacionales, e Información complementaria (directorios de repositorios institucionales, directorios de revistas de acceso abierto, etc.)

Como compromisos de futuro reflejados en el Plan estratégico de esta biblioteca se destacan: la puesta en marcha del Repositorio Institucional de la Universidad de León, la creación de espacios abiertos para la alfabetización y el aprendizaje permanente; el desarrollo de herramientas útiles para desenvolverse en el mundo de las TIC; la creación de servicios y productos de valor añadido según las demandas de la comunidad universitaria; y la oferta continua de contenidos actualizados y organizados para la investigación.

[16] Estatuto de la ULE, Art. 38
[17] R.D. 582/1989 de 19 de mayo: Reglamento de Bibliotecas Públicas del Estado y del Sistema Español de Bibliotecas, Art. 22.d

*Datos estadísticos de la Biblioteca de la ULE*

Analizados los datos estadísticos de REBIUN desde el año 2000, se obtiene, junto con la descripción de los servicios del anexo, un punto de partida sobre el uso de las TIC en esta biblioteca. Se puede concluir que para el periodo 2000-2006:

- se mantienen los puestos informatizados sobre el total de puestos y disminuye el número de estudiantes por puesto informatizado
- aumenta ligeramente el uso de revistas electrónicas por investigador
- se triplica (desde 2001) el gasto en recursos electrónicos sobre el total de adquisiciones
- disminuye el gasto en recursos electrónicos por uso (2004-2006)
- aumentan el número de visitas al web por usuario y se duplican las consultas al catálogo por usuario (desde 2003)
- disminuye ligeramente el número de artículos electrónicos por investigador (desde 2005)
- hay que destacar el aumento espectacular del número de consultas a bases de datos por investigador (desde 2004)

## 2.2. Estudios previos sobre Gestión de la Seguridad de las TIC para BU

*Introducción*

Tradicionalmente la Seguridad en las bibliotecas ha tenido como eje la seguridad física enfocada en el cuidado de colecciones y personas: control de accesos, sistemas anti-hurto, anti-incendios, etc.

Actualmente, además del enfoque tradicional, se han ido incorporando elementos de seguridad para proteger la información y los sistemas que la soportan. Adaptándose a la legislación, a las nuevas demandas de servicios y al cambiante entorno universitario en que están inmersas, las bibliotecas universitarias van adquiriendo cada vez más conciencia de que **la seguridad de la información** es un **aspecto clave en su gestión**. Se desarrollan en este apartado algunas iniciativas y estudios en materia de seguridad TIC que afectan a las bibliotecas universitarias y los servicios que ofrecen.

Un reciente trabajo de la asociación americana EDUCAUSE subraya por una parte la necesidad de la integración de las herramientas de gestión de contenidos, *e-learning* y gestión de repositorios que permita un óptimo aprovechamiento de estos elementos por las bibliotecas universitarias para ofrecer sus servicios; por otra, señala la importancia de permitir al usuario un acceso flexible y seguro adoptando soluciones tecnológicamente híbridas y cooperativas que minimicen y den una respuesta rápida a los ataques de intrusos y al acceso no autorizado. Para ello propone la creación de una **infraestructura mínima de seguridad**.

Estudios de la universidad de Glasgow (McHugh et al, 2007) exponen que la seguridad de las bibliotecas digitales reside en la confianza en sus repositorios. Para garantizar las capacidades de conservación de las bibliotecas digitales proponen una metodología, DRAMBORA, de auditoría de repositorios digitales, basada en **gestión de riesgos**.

Además las bibliotecas universitarias (Thomson, 2006) se convierten en objetivos de hackers por su infraestructura y activos TIC. Para enfrentarse las amenazas y a los retos

tecnológicos, se propone (Lane, 2007) un **enfoque de continuidad negocio** para abordar el problema de la seguridad en los entornos universitarios.

### Infraestructura mínima de seguridad: EDUCAUSE

En el ámbito académico en Estados Unidos la asociación sin ánimo de lucro EDUCAUSE proclama como misión el progreso de la educación superior promoviendo el uso inteligente de las tecnologías de la información. Una de sus iniciativas principales es la encomendada al *Security Task Force* o grupo de trabajo de Seguridad cuyo propósito es ser el punto focal de información y recursos sobre seguridad en red y en ordenadores para la comunidad universitaria.

En un reciente trabajo el Comité de tecnologías emergentes (EDUCAUSE, 2004) investiga sobre las tecnologías que mayor impacto tienen en el ámbito universitario, destacando:

- la gestión del *spam* (correo electrónico no solicitado),
- las redes *P2P* (descarga de música, películas,…) legales,
- los objetos de aprendizaje,
- la *nomadicity* o acceso remoto electrónico (dispositivos móviles, redes inalámbricas,…) a los servicios y software de la universidad,
- la creación de redes regionales y
- la convergencia de las bibliotecas, los repositorios institucionales y la gestión de contenidos web.

Sobre este último punto el estudio expone la aproximación de los mercados de gestión de contenidos, *e-learning* y gestión de repositorios y concluye apuntando la necesidad de alineación entre los líderes académicos y financieros para hacer posible la integración de estas herramientas que **garantice la seguridad en el uso y la gestión de los sistemas y servicios ofrecidos** mediante tecnologías de la información por la biblioteca.

Un estudio anterior (Hurley, 2002) también publicado en EDUCAUSE basándose en las mencionadas características de los entornos universitarios, busca una **infraestructura mínima de seguridad** para que las universidades, y también sus bibliotecas, participen con confianza de la *Sociedad de la Información*. Los retos que se le piden a esta infraestructura son:

- aunar el uso de mecanismos de seguridad locales diferentes y con frecuencia incompatibles
- tener en cuenta las ineficiencias de las tecnologías actuales y adecuar los nuevos recursos a la variedad de lenguajes, plataformas y dispositivos existentes.
- aportar flexibilidad y control para incluir las nuevas formas de intercambio (*P2P*, *single sign-on*[18],…)
- incorporar credenciales y políticas que permitan agregar múltiples organizaciones
- ser modular, interoperable, global y dinámica
- tener la posibilidad de evolucionar
- proporcionar seguridad de extremo a extremo

[18] Inicio de sesión único en recursos relacionados.

- soportar implementaciones múltiples y coherentes

Concluye que el éxito en el ámbito de la seguridad de las TIC en las universidades reside en **adoptar soluciones tecnológicamente híbridas y cooperativas** que permitan un acceso flexible, desde múltiples plataformas, y seguro, minimizando y dando una respuesta rápida a los ataques de intrusos y al acceso no autorizado a los datos y los recursos.

## Repositorios digitales confiables: DRAMBORA

Los repositorios digitales acumulan cantidades de información en continuo crecimiento. Las características de un repositorio confiable son aquellas que garanticen su capacidad para recibir, preservar y difundir sus contenidos.

### *DRAMBORA*

Investigadores (McHugh et al., 2007) del instituto HATII (*Humanities Advanced Technology and Information Institute*) la universidad de Glasgow (Reino Unido) plantean el uso de una metodología basada en gestión de riesgos para asegurar la sostenibilidad de los contenidos de repositorios digitales a largo plazo. DRAMBORA (*Digital Repository Audit Method Based on Risk Assesment*) es la metodología que permite la valoración de la exposición al riesgo mediante una auditoría interna de forma que los administradores del repositorio puedan evaluar sus capacidades, identificar sus debilidades y reconocer sus fortalezas.

DRAMBORA contempla los diez principios del consorcio CRL [19] (*Center for Research Libraries*). Este consorcio tiene por misión adquirir y preservar recursos en formato tradicional y digital para la investigación y la enseñanza y ponerlos a disposición de sus miembros por medio de préstamo interbibliotecario y distribución electrónica. Los diez principios de los repositorios «confiables» fueron acordados en enero de 2007 por cuatro proyectos: *Digital Curation Center*[20] *(DCC)*, *DigitalPreservationEurope*[21]*(DPE)*, *Nestor*[22] y el mencionado *Center for Research Libraries (CRL).*

De acuerdo con estos principios, con independencia de su misión, modelo de negocio y fuente de financiación, todos los **repositorios digitales confiables** deben cumplir:

1. el compromiso de mantenimiento continuo de los objetos digitales para sus comunidades;

2. demostrar la adecuación de la organización (incluso financiera, de plantilla, estructura, procesos) para alcanzar este compromiso;

3. adquirir y mantener requisitos contractuales y derechos legales, y cumplir las responsabilidades adquiridas;

4. disponer de un marco de políticas efectivo y eficiente;

5. adquirir e ingresar objetos digitales basándose en criterios fijados que correspondan con sus compromisos y capacidades;

6. mantener / asegurar la integridad, autenticidad y usabilidad a lo largo del tiempo de los objetos digitales que contienen;

[19] CRL consorcio norte americano de bibliotecas universitarias y de investigación http://www.crl.edu/
[20] DCC http://www.dcc.ac.uk
[21] DPE: *DigitalPreservationEurope* http://www.digitalpreservationeurope.eu
[22] Nestor: *Network of Expertise in Long-term STOrage of Digital Resources* http://www.langzeitarchivierung.de

7. crear y mantener los *metadatos* precisos para las acciones que se tomen sobre objetos digitales durante su conservación, y para permitir su acceso y su utilización en el contexto previo a la conservación;

8. cumplir los requisitos para las obligaciones de difusión;

9. disponer de un programa estratégico para planificar y ejecutar la preservación;

10. disponer de la infraestructura técnica adecuada para asegurar el mantenimiento y la seguridad de los objetos digitales.

Para cumplir estos principios se debe asegurar que los repositorios sobre los que descansa la biblioteca digital están diseñados, conservados y gestionados de forma que se reduzcan los riesgos de pérdida de sus contenidos y relaciones en el seno de la biblioteca digital.

La herramienta de auditoría DRAMBORA diseñada por DCC y DPE está disponible en línea (http://www.repositoryaudit.eu/). Consta de una descripción extensa del método y unas plantillas para su utilización. Sirve para evaluar la gestión de la seguridad en repositorios digitales y de guía de diseño para minimizar el riesgo. Contempla la gestión de los riesgos asociados al funcionamiento y al soporte del repositorio: adquisición e ingreso, preservación y almacenamiento, gestión de metadatos, acceso y difusión, organización y gestión, personal, gestión financiera e infraestructura técnica y de seguridad.

El procedimiento es el siguiente a grandes rasgos:

1. se recaban los datos del repositorio, sus obligaciones, objetivos, planificación estratégica, marco contractual, etc.;

2. para cada una de las áreas de funcionamiento y soporte se registran las actividades y los activos asociados;

3. posteriormente se han de identificar, valorar y gestionar los riesgos de cada activo procedentes del entorno físico, de los procedimientos de gestión y administración o del personal, de la oferta de servicios y de la operación de los mismos y del equipamiento hardware, software o de comunicaciones.

Está prevista una versión con interfaz web cuya utilidad se va a comprobar en bibliotecas internacionales con el objetivo de **valorar su aplicabilidad en el contexto de las bibliotecas digitales** y modificarla si fuera necesario para su aplicación práctica.

## La seguridad TIC como estrategia y el proyecto LOVE

### *Bibiotecas Universitarias: objetivo de hackers*

Una tesis (Simons, 2005) que estudia los retos de seguridad virtual[23] a los que se enfrenta la Universidad expone como estas instituciones son el objetivo de los ataques de hackers que las utilizan como campos de entrenamiento para obtener el reconocimiento de sus colegas. Este hecho se debe en parte a que esta seguridad no ha sido un tema prioritario en la gestión universitaria, principalmente por razones de presupuesto. Esta tesis concluye con una serie de recomendaciones que se resumen en el desarrollo y aplicación de políticas de seguridad.

Especialmente atractivas para los hackers resultan las bibliotecas universitarias (Thomson, 2006) por sus bases de datos personales, sus suscripciones a caras bases de datos propietarias, el amplio ancho de banda de sus conexiones —que permite gran

[23] Seguridad de la información almacenada en ordenadores, los mensajes transmitidos en redes y los recursos que se acceden mediante comandos en-línea (Schneier, 2000)

capacidad de descarga— y su amplia base instalada de ordenadores —que pueden ser comprometidos y utilizados como «zombies».

### *Seguridad en el diseño de los sistemas de información*

Hasta ahora se han planteado algunas cuestiones que afectan a la seguridad de la información en bibliotecas universitarias. Además del cumplimiento con el marco legislativo, los retos que suponen la adaptación tecnológica y los cambios en la enseñanza universitaria, las bibliotecas universitarias se enfrentan al desafío de incorporar en su gestión mecanismos que proporcionen la seguridad a los activos informacionales que ostentan y a los usuarios que los utilizan.

En los trabajos analizados se pone de manifiesto que la seguridad de los sistemas de las bibliotecas varía dependiendo de los activos que los mecanismos de seguridad deben proteger. El principal objetivo de estos mecanismos es que los activos desplieguen su funcionalidad de acuerdo con las expectativas de los usuarios autorizados, a la vez que se mantiene la confidencialidad, integridad y disponibilidad de la información.

Los mecanismos de seguridad pueden por tanto clasificarse según los activos que protegen (Inmor, Esichaikul y Batanov, 2003): seguridad del hardware, del software, seguridad en red, seguridad de los sistemas de información. La siguiente lista detalla estos conceptos:

- la seguridad del hardware es la relativa al equipamiento informático y requiere mecanismos para el control del acceso físico;
- la seguridad del software es la relativa a la seguridad de los programas de aplicación, los sistemas de gestión de bases de datos y los sistemas operativos y requiere mecanismos tanto de control de acceso físico como lógico (autenticación);
- la seguridad en red es necesaria cuando los sistemas realizan su actividad a través de conexiones en red. Esta seguridad requiere mecanismos para proteger las comunicaciones tales como protocolos de transmisión segura y encriptación de datos;
- la seguridad de los sistemas de información trata de cómo se analizan y diseñan los sistemas de información de las organizaciones de forma que sus datos de valor estén protegidos ante exposiciones y modificaciones inapropiadas.

Estos investigadores sugieren que **la integración de la seguridad en los sistemas de información debe comenzar en el diseño de los mismos** y proponen un modelo de diseño orientado a la seguridad.

### *Dominios de información vs. dominios en red*

Además, dada la difusión de Internet, está cambiando el modelo de la seguridad informática (Chen, Choo y Chow, 2006) tradicionalmente basada en autenticación y autorización de usuarios en dominios de red, ya que ahora tiene que lidiar con nuevos retos planteados por usuarios, contenidos informacionales y sistemas de aplicación en *dominios de información*. La seguridad en los **dominios de información** comprende aspectos tan variados como: procesos de flujos de trabajo, gestión de *records*, interoperabilidad de datos (especificaciones XML), metadatos y formatos de datos (abiertos y otros). **La seguridad se convierte** (Chen, Choo y Chow, 2006) por tanto **en una de las tecnologías estratégicas que permitirán el incremento del valor y la utilidad de las aplicaciones basadas en Internet.**

Basado en este concepto de *dominio de información*, el proyecto LOVE (*Learning Object Virtual Exchange*) implementado en una biblioteca digital (NDSL http://www.ndsl.org) de la universidad de Florida-Gainesville (Chen, Choo y Chow, 2006), proporciona un entorno

colaborativo bajo el que se desarrollan: la preservación de información en Internet, la privacidad del usuario y del contenido, y mecanismos de acceso, autenticación y autorización a los contenidos. El resultado es una arquitectura de *middleware*[24] completa y amplia para el acceso seguro y la preservación robusta de las aplicaciones basadas en Internet de bibliotecas digitales que podría ser objeto de estudio previo ante la perspectiva de incorporar entornos colaborativos en las bibliotecas universitarias.

### *Continuidad del negocio*

Aplicar la seguridad de la información a las TIC es estratégicamente importante para salvaguardar la continuidad del negocio[25] en las universidades. A esta conclusión llegó Tim Lane (2007) tras un estudio sobre la gestión de la seguridad en treinta y ocho universidades australianas.

Este estudio distingue en sus conclusiones entre las universidades que adoptan una perspectiva holística con una visión de negocio cuando se enfrentan al reto de la seguridad de las TIC, de las que no lo hacen. Las primeras desarrollan políticas de seguridad de la información y planifican la gestión de la seguridad. Son conscientes de que a medida que los riesgos aumentan y la dependencia en la información y en los sistemas se hace más crítica, se incrementan las necesidades en seguridad. Las segundas no están aún sensibilizadas sobre los daños que los incidentes de seguridad pueden acarrear a su negocio y consideran que la seguridad es solo un problema de tecnología.

El investigador recomienda a las universidades adoptar una aproximación empresarial de la gestión de la seguridad de la información para atraer los apoyos de la comunidad universitaria y sus dirigentes y facilitar la implementación efectiva de la seguridad TIC.

Este estudio y los anteriores ponen de manifiesto la necesidad de implementar sistemas de gestión de la seguridad de la información en las organizaciones en las que la consecución de los objetivos dependa de sus activos de información. Las bibliotecas universitarias son organizaciones cuyos activos de información no solo constituyen la base de su negocio sino también su principal producto y servicio.

[24] Software utilizado para soportar aplicaciones distribuidas: servidores web, servidores de aplicaciones y gestión de contenidos. Es esencial para tecnologías orientadas a servicios y servicios web.

[25] La gestión de la continuidad del negocio consiste en gestionar los riesgos para asegurar siempre que una organización pueda continuar operando, como mínimo, a un nivel predeterminado.

# 3. Objeto de estudio

*Gestión y auditoria de la seguridad en bibliotecas universitarias*

## 3.1. Normas y estándares para la gestión de la seguridad de la información

*Marcos normativos para la gestión de la seguridad*

El capítulo anterior ha puesto de manifiesto que las bibliotecas universitarias deben afrontar el reto de la gestión de la seguridad de la información desde una perspectiva empresarial. Se analiza en este capítulo el marco normativo actual sobre la materia en España.

Algunos de los marcos normativos relativos a la gestión de la seguridad de las tecnologías de la información de actualidad internacional son los siguientes:

- AICPA (*American Institute of Certified Public Accountants*) y CICA (*Canadian Institute Of Chartered Accountants*), institutos americano y canadiense respectivamente que desarrollan los «Principios y criterios de servicios confiables» (*Trust Services Principles and Criteria*) para abordar los riesgos y oportunidades de las tecnologías de la información. Otorgan sellos de confiabilidad web o de sistemas y su marco puede utilizarse para servicios de consultoría y de asesoría (http://www.aicpa.org/trustservices).

- CICA *Canadian Institute Of Chartered Accountants* (http://www.cica.ca): es una iniciativa canadiense que propone un marco de criterios de control (CoCo) enfocados a la información financiera. Publica unas recomendaciones internacionalmente reconocidas para el diseño, implementación y evaluación de controles en tecnologías de la información (*IT Control Guidelines*).

- COSO (http://www.coso.org): es una iniciativa independiente del sector privado con base en el AICPA (*American Institute of Certified Public Accountants*) dedicada a la mejora de la calidad de la información financiera. Propone entre otros un marco para la gestión de riesgos corporativos.

- GAISP, *Generally Accepted Information Security Principles* recoge las mejores prácticas de otros marcos similares, dotándoles de una jerarquía que sirve de guía para asegurar la información y la tecnología que la soporta. Está en desarrollo por la asociación ISSA *Information System Security Association* (http://www.issa.org) que es una organización internacional sin ánimo de lucro de profesionales de la seguridad

- El Instituto americano IIA (*Institute of Internal Auditors*) aporta un modelo llamado SAC (*Systems Assurance and Control*) que sirve a las empresas de marco para evaluar la seguridad en un entorno de e-business. (http://www.thelia.org)

- ITGI (http://www.itgi.org) El instituto americano *IT Governance Institute* proclama que su razón de ser es facilitar a las empresas el alineamiento de las tecnologías de la información con sus negocios y publica los *Control Objetives for Information Technology* CobiT. Estos controles son una forma de implementar el *Buen Gobierno TI*, definiendo éste como el conjunto de relaciones y procesos para dirigir y controlar las empresas hacia la consecución de sus objetivos, añadiendo valor, pero sopesando riesgos y retornos de inversión en las TI y sus procesos asociados.

- ISF *Standard of Good Practice for Information Security* (http://www.isfsecuritystandard.com) es un estándar de buenas prácticas para seguridad de la información del *Information Security Forum* (http://www.securityforum.org) foro internacionalmente reconocido en este campo.

- UNE-ISO/IEC 27001: literalmente según la propia norma (AENOR, 2007) «[…] proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI)».

El análisis comparativo de estos estándares escapa del ámbito de este trabajo y podría ser objeto de posteriores estudios. Sin embargo, en una primera aproximación se comprueba que estos marcos proponen el establecimiento de **buenas prácticas y controles** para medir la efectividad de los mecanismos de seguridad implementados a nivel físico, lógico y empresarial. Los controles afectan a toda la organización desde los niveles operativos hasta los niveles estratégicos de la organización. En particular cabe reseñar que es común que estos estándares dediquen un apartado al factor humano (sensibilización, fallo intencionado o no intencionado, etc.)

Para este trabajo se toma como referencia la norma recientemente aprobada por AENOR, UNE-ISO/IEC 27001 y las normas asociadas. Esta norma es certificable y está siendo implantada en las empresas españolas que consideran adecuado disponer de un Sistema de Gestión de la Seguridad de la Información. También se considera el carácter abierto de esta norma en cuanto a los controles que pueden implementarse, ya que puede completarse con controles de otros referentes generales o específicos.

Otro apartado analiza un modelo de madurez específico de seguridad de la información ISM$^{3}$ (*Information Security Management Maturity Model*)[26], si bien son aplicables junto con la citada norma otros modelos de competencia como el modelo CMM (*Capability Maturity Model*) originalmente desarrollado por la universidad Carnegie-Mellon.

Dada la generalización de la gestión de riesgos se incluye un apartado sobre este tema. Aunque existen muchas metodologías para gestión de riesgos[27] en este trabajo se introduce, a modo de ejemplo, la utilizada en el entorno de las administraciones públicas: MAGERIT.

## SGSI: Sistema de Gestión de Seguridad de la Información

*UNE-ISO/IEC 27001 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Especificaciones.*

Esta norma especifica los requisitos para establecer un plan de seguridad constituido por un Sistema de Gestión de Seguridad de la Información, en adelante **SGSI**, dentro del contexto de los riesgos totales de una organización.

La norma adopta un enfoque por procesos para la gestión de la seguridad de la información siguiendo el modelo «planificar-hacer-verificar-actuar» conocido por sus siglas en inglés PDCA (*plan-do-check-act*).

Este **enfoque por procesos** anima a los usuarios de la norma a enfatizar la importancia de:

[26] http://www.ism3.com/

[27] Las metodologías y herramientas de gestión de riesgos pueden consultarse, además de una comparativa entre ellas, en el Inventario de métodos y herramientas de gestión y valoración de riesgos (http://www.enisa.europa.eu/rmra/rm_home.html) de la Agencia Europea ENISA (*European Network and Information Security Agency*).

- «comprender los **requisitos de seguridad** de la información de una organización y la necesidad de establecer una política de seguridad de la información y sus objetivos;
- implementar y operar los **controles** para administrar los riesgos de seguridad de la información de una organización en el marco de sus riesgos empresariales generales;
- **supervisar y revisar** el rendimiento y la eficacia del SGSI; y
- asegurar la **mejora continua** sobre la base de la medición objetiva.»

### *Las normas 27000*

La serie de normas 27000 tienen sus orígenes en la norma técnica BS 7799 de seguridad del instituto británico de normas técnicas, *British Standard Institute* (BSI), publicada inicialmente en 1995. En el año 2000 fue adoptada y publicada por la organización internacional de estándares, *International Standards Organization* (ISO), bajo el nombre de ISO 17799. Actualmente forma parte de la serie 27000. Esta serie está compuesta por las siguientes normas:

- ISO 27000: define el vocabulario técnico y específico; (propuesta).
- ISO 27001: versión ISO de la norma BS 7799-2. Requisitos SGSI; (publicada en 2005 y también norma UNE en 2007). Es certificable.
- ISO 27002: versión actualizada de la ISO 17799:2005; Código de buenas prácticas para la gestión de la seguridad de la información; (publicada, traducción por AENOR en curso).
- ISO 27003: guía general de implementación; (borrador).
- ISO 27004: métricas y mediciones para la gestión de la seguridad; (borrador).
- ISO 27005: evaluación y gestión de riesgos; (borrador, en AENOR prevista como UNE 71504)
- ISO 27006: especificaciones para organismos certificadores de SGSI (publicada)
- ISO 27007: guía para Auditar un SGSI (borrador)
- ISO 2701x: guías sectoriales (Telecomunicaciones, etc.); (borrador)
- ISO 27xxx: futuras normas

La norma UNE-ISO/IEC 27001 es certificable, es decir, su cumplimiento puede ser reconocido por organismos certificadores que otorgarán el sello correspondiente.

### *Conceptos*

La norma UNE-ISO/IEC 27001 se construye sobre el concepto del Sistema de Gestión de la Seguridad de la Información, como «parte del sistema de gestión general, basado en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, los procesos y los recursos».

El propósito de un SGSI es[28] garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados de forma sistemática, estructurada,

[28] http://www.iso27000.es/sgsi.html

repetible, eficiente, documentada y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La norma define la información como un activo que posee valor para la organización y requiere por tanto la protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la **continuidad del negocio**, **minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio**.

La seguridad de la información se define como la **preservación de**:

- **la confidencialidad**: «propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados»
- **la integridad**: «propiedad de salvaguardar la exactitud y completitud de los activos»
- **la disponibilidad**: «propiedad de ser accesible y utilizable por una entidad autorizada»

Como ha quedado constancia en el capítulo anterior para las bibliotecas universitarias, como para otras organizaciones, son extremadamente importantes los activos de información y los procesos y sistemas que la utilizan. También se han comentado algunas de las amenazas a estos activos que, aprovechando las vulnerabilidades existentes, pueden atacarlos con actos de: sabotaje, vandalismo, espionaje o fraude. Además se han de tener en cuenta los riesgos de incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la organización y los provocados por fallos técnicos y catástrofes naturales.

La adopción de un SGSI favorece el control sobre estas amenazas además del adecuado cumplimiento con la legislación y la adaptación flexible a las condiciones del entorno, protegiendo así los objetivos del negocio.

### *Implementación*

La implementación del SGSI comienza con la determinación del **alcance** del proyecto. El alcance es el ámbito de la organización que queda sometido al SGSI. Este documento debe incluir una identificación clara de las dependencias, relaciones y límites que deban ser tenidos en cuenta.

A continuación se debe redactar una **Política de Seguridad**, un documento que incluye el alcance y otras consideraciones y que debe ser refrendado por los responsables de la organización. En este documento se exponen las intenciones, objetivos, responsabilidades, directrices, etc. que han de regir el SGSI.

Es importante al comienzo de este proceso identificar los **requisitos de seguridad** de la organización. Según la norma ISO/IEC 27002 hay tres posibles fuentes de estos requisitos:

1. Una fuente es la que resulta de la evaluación de riesgos de la organización, considerando fundamentalmente los objetivos y estrategias de negocio de la misma. Mediante la evaluación de riesgos, se identifican las amenazas contra los activos, se valoran las vulnerabilidades y las probabilidades de ocurrencia y se estima el impacto potencial.
2. Otra fuente son los requisitos legales, normativos, regulatorios y contractuales que tiene que satisfacer la organización, sus socios comerciales, subcontratas y proveedores de servicios en su entorno socio-cultural.

3. Una fuente más es el conjunto particular de principios, objetivos y requisitos de negocio para el procesamiento de la información que la organización ha desarrollado para el soporte de sus operaciones.

La siguiente fase consiste en la selección e implementación de controles de seguridad. Los **controles** son prácticas, procedimientos o mecanismos que garantizan que cada aspecto que se ha valorado que conlleva cierto riesgo, queda contemplado y puede ser auditado. La norma ISO 27002 es un compendio de buenas prácticas que explica la aplicación de los controles. Estos no son los únicos controles que se pueden utilizar, existen y pueden utilizarse controles adicionales de otras fuentes. La norma contiene un listado con 134 controles agrupados en 39 objetivos de seguridad o resultados que se esperan obtener al implementar los controles. Estos objetivos pertenecen a 11 dominios:

1. Política de seguridad
2. Aspectos organizativos de la seguridad de la información
3. Gestión de activos
4. Seguridad ligada a los recursos humanos
5. Seguridad física y ambiental
6. Gestión de comunicaciones y operaciones
7. Control de acceso
8. Adquisición, desarrollo y mantenimiento de los sistemas de información
9. Gestión de incidentes de seguridad de la información
10. Gestión de la continuidad del negocio
11. Cumplimiento

El gráfico siguiente ilustra la distribución en la pirámide organizativa de estos dominios de control:

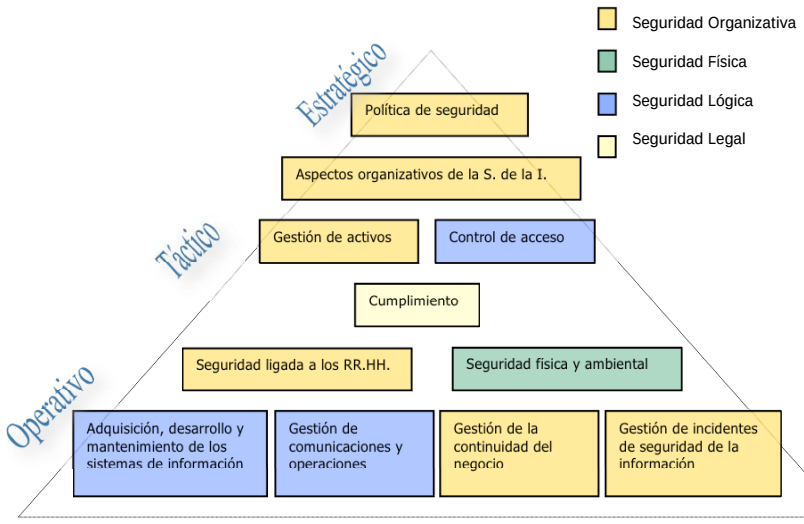


*Ilustración 0: Dominios de Control UNE-ISO/IEC 27001 Adaptado de Díaz (2005)*

La selección de controles debe realizarse según la norma en base a un **análisis de riesgos**. Para ello se han de determinar los activos de la organización, evaluar las vulnerabilidades que les afectan y valorar los riesgos que hay que afrontar. La norma no especifica la selección de metodología ni herramienta ninguna para realizar la evaluación

de riesgos. En un futuro otra norma (ISO 27005) determinará el marco de trabajo para este análisis. Los resultados de la evaluación de riesgos se contrastan con la situación de seguridad existente mediante un proceso de auditoría que se conoce como «análisis gap». Así se determinan los controles que han de aplicarse que se incluyen al redactar la «**Declaración de Aplicabilidad**», documento que junto con el alcance ha de servir para la certificación del SGSI. Para la correcta selección de los controles se utilizará la norma ISO/IEC 27002.

Finalmente se ha de **documentar el SGSI**. Esta documentación incluirá documentos a distintos niveles organizativos: políticas, normas y estándares; procedimientos y guías; tareas, operaciones, evidencias y registros. Además de la Política de seguridad con el alcance y la Declaración de Aplicabilidad, se han de documentar: las acciones realizadas para planificar y diseñar el sistema, los procedimientos adoptados para implantar los controles y los de gestión y operación del SGSI. Toda la documentación debe estar controlada con procedimientos que garanticen que estará disponible, será comprensible y podrá ser revisada cuando se necesite. También se ha de mantener un control de versiones y ha de retirarse la documentación que esté obsoleta. Igualmente se han de disponer de los procedimientos adecuados que permitan identificar, mantener, conservar y destruir los registros que evidencien el cumplimiento del SGSI.

El siguiente gráfico muestra de forma esquemática el proceso creación de un SGSI.

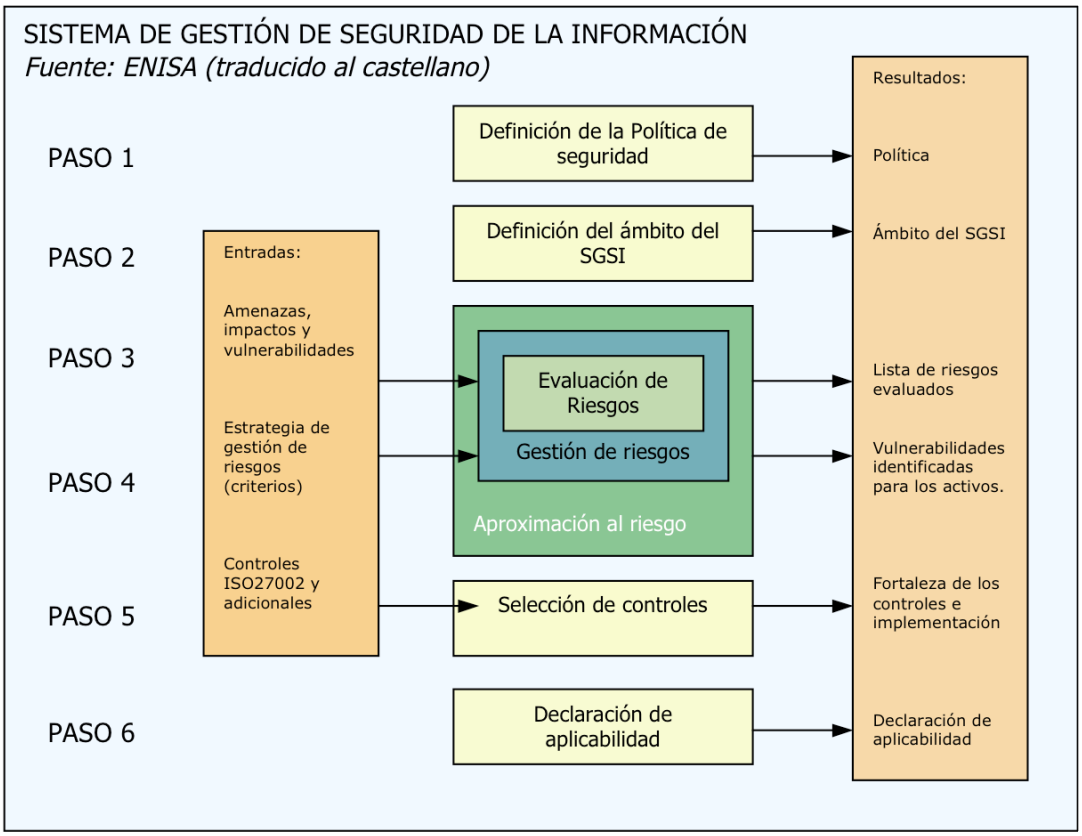


*Ilustración 0: Establecimiento de un SGSI. Fuente: ENISA (http://www.enisa.europa.eu/)*

La UNE-ISO/IEC 27001 no es una norma tecnológica, ha sido redactada de forma flexible e independiente de cualquier solución específica de seguridad, proporcionando buenas prácticas (ISO/IEC 27002) tecnológicamente neutras. Estas características hacen posible su implantación en todo tipo de organizaciones, con independencia de su tamaño y sector de negocio.

### *Ciclo de mejora continua*

Para establecer y gestionar un SGSI en base a la norma UNE-ISO/IEC 27001, se utiliza el ciclo de mejora continua PDCA. Las fases son las siguientes:

- *Plan* (planificar): establecer del SGSI
- *Do* (hacer): implementar y operación del SGSI
- *Check* (verificar): supervisión y revisión del SGSI
- *Act* (actuar): mantenimiento y mejora del SGSI

El siguiente esquema muestra gráficamente este proceso:

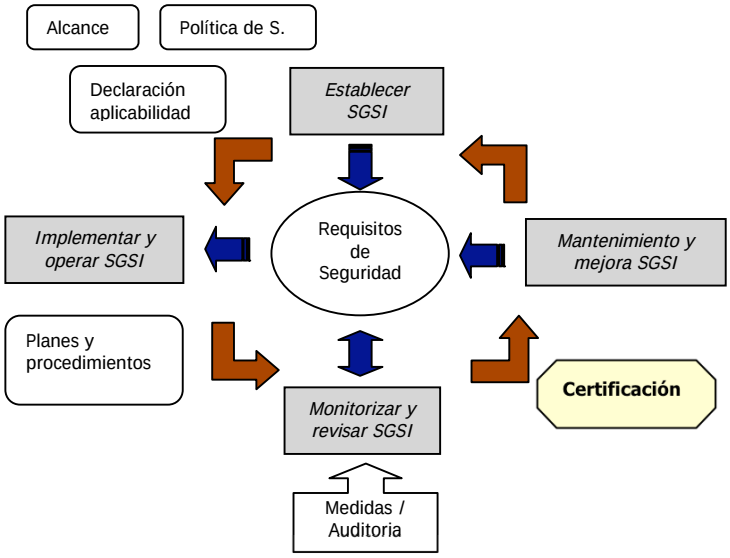


*Ilustración 1: Ciclo PDCA para SGSI*

La fase de establecimiento (*Plan*) ha sido descrita en el apartado anterior. La fase de implementación (*Do*) consiste en definir e implantar los planes de tratamiento de riesgos, implementar los controles seleccionados, definir el sistema de métricas para medir la eficacia de los controles, implantar acciones de formación y concienciación, gestionar operaciones y recursos e implantar procedimientos para la detección y respuesta a incidentes.

En la fase de monitorización y revisión (*Check*) se han de ejecutar los procedimientos que permitan detectar y prevenir los incidentes. Se mide en esta fase la efectividad de los controles, se realizan revisiones periódicas de las evaluaciones de riesgos y del propio SGSI. Es en esta fase dónde se actualizan los planes de seguridad. También se registran las acciones y los eventos que impactan sobre el rendimiento del SGSI y se realizan auditorias internas.

Finalmente en la fase de mantenimiento y mejora (*Act*) se implementan las mejoras identificadas asegurándose de que contribuyen a alcanzar los objetivos previstos, se realizan acciones preventivas y correctivas y se comunica a las partes interesadas.

### *Ventajas de implantar un SGSI*

Según menciona Díez (2005) la adopción de la norma, y por tanto la implantación de un SGSI proporciona las siguientes ventajas:

- aumento de la seguridad efectiva de los sistemas de información,
- correcta planificación y gestión de la seguridad,
- garantías de continuidad del negocio,
- alianzas comerciales y comercio electrónico (*e-commerce*) más seguros,
- mejora continua a través de un proceso de auditoria interna,
- incremento de los niveles de confianza de nuestros clientes y socios comerciales,
- aumento del valor comercial y mejora de la imagen de la organización,
- auditorias de seguridad más precisas y fiables y
- menor responsabilidad civil.

## Ciclo de vida de la gestión de la seguridad de la información

La gestión de la seguridad de la información consiste en un ciclo con planificación, ejecución, monitorización y realimentación (PDCA). Este ciclo afecta a todos los niveles de la organización y se considera (Nyanchama, 2005) el Ciclo de vida de la gestión de la seguridad de la información, ***ISMLC*** de sus siglas en inglés, *Information Security Management Life Cicle*.

El objetivo de este «ciclo de vida» ISMLC es asegurar la correcta **comprensión de las necesidades del negocio y sus riesgos asociados** de forma que se diseñen formas de buen gobierno, estrategias, tácticas y operaciones de seguridad sólidas.


*Ilustración 2: SGSI; Fuente: Korean Information Security Agency http://www.kisa.or.kr*

### *Estrategias de seguridad*

Los elementos estratégicos comprenden el buen gobierno y las políticas de seguridad. El buen gobierno en seguridad proporciona medios para garantizar que la organización aprovechará las inversiones en seguridad de la información. Es un medio para definir, dirigir y controlar un programa de seguridad que abarque a toda la organización.

Basándose en la visión, la misión y los objetivos del programa de seguridad, se definen las políticas generales (prioridades, presupuestos, etc.) y estándares que han de regir el programa de seguridad. Toda política debe responder a las preguntas: qué es (ámbito de aplicación), por qué es necesaria, cuándo debe aplicarse, quién es responsable de hacerlo y cómo debe aplicarse (procesos, procedimientos, estándares)

También son elementos estratégicos las políticas de concienciación, desde la definición de los públicos objetivo (técnicos, personal, usuarios) hasta las medidas que se tomen de su efectividad.

### *Tácticas de seguridad*

Los elementos tácticos están dirigidos a asegurar que los requisitos de seguridad identificados se concretan en proyectos específicos, desde su diseño hasta su implementación. Estos elementos incluyen los procedimientos y directrices basados en buenas prácticas, la evaluación y gestión de riesgos y las métricas de rendimiento.

### *Operativa de seguridad*

La parte activa de la seguridad es la operativa. Incluye la monitorización de la infraestructura de seguridad, las evaluaciones proactivas y la respuesta a incidentes. Entre otros son elementos de la operativa de seguridad: la detección de intrusiones, el análisis de los registros de alertas, la gestión anti-malware, la gestión de accesos, la gestión de claves y certificados, etc.

## Modelos de madurez de seguridad de la información

### *SSE-CMM*

Además de la norma UNE-ISO/IEC 27001, otros estándares pueden servir, independientemente o en paralelo, como marco de referencia para la gestión de la seguridad, entre ellos los llamados modelos de madurez. Uno de ellos está descrito en la norma ISO/IEC 21827 *Information technology—Systems Security Engineering—Capability Maturity Model (**SSE-CMM®**)* o Ingeniería de Seguridad de Sistemas—Modelo de madurez de capacidad. Esta norma fue desarrollada por la *International Systems Security Engineering Association* (ISSEA), organización sin ánimo de lucro patrocinada por compañías dedicadas a la seguridad de sistemas.

Es un marco de referencia para el seguimiento del nivel de madurez de los procesos relacionados con los riesgos y el aseguramiento de la seguridad. Esta norma trabaja con el modelo *CMM®*, desarrollado por la universidad Carnegie-Mellon que tiene una amplia difusión en otras áreas de la tecnología, aunque no así en los proyectos basados en la ISO/IEC 27001. El modelo de madurez *CMM®,* consta de cinco niveles: inicial, repetible, definido, gestionado y optimizado. Entre las críticas a este modelo destaca la falta de métricas para la correcta práctica profesional.

También denominado por sus siglas en inglés, el SSE-CMM[29] describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de sus sistemas informáticos. El modelo fue diseñado para su uso como:

- herramienta para que las organizaciones evalúen sus prácticas en proyectos de seguridad y definir mejoras aplicables;
- mecanismo estándar para que los consumidores evalúen la capacidad de los proveedores de proyectos de seguridad;
- base para la evaluación de los proyectos de seguridad en una organización (p.ej. certificadores de sistemas y evaluadores de productos) para establecer la confianza basada en la capacidad de la organización (como ingrediente de un sistema o proyecto de garantía de seguridad).

El SSE-CMM aborda las actividades del proyecto de seguridad que abarcan el ciclo de vida completo del producto o sistema, incluyendo la definición conceptual, el análisis de requisitos, su diseño, desarrollo, integración, instalación, operaciones, mantenimiento y desmantelamiento.

[29] http://www.sse-cmm.org/model/model.asp

Este modelo está destinado a todo tipo y tamaño de organizaciones con proyectos de seguridad: comerciales, gubernamentales y académicas.

Este modelo está enfocado en proyectos de seguridad no en la gestión de la seguridad por parte de las organizaciones.

### *El modelo de madurez de la gestión de seguridad de la información ISM³ (Information Security Management Maturity Model)*

Otro modelo de madurez es el patrocinado por el *ISM³ Consortium*[30]. ***ISM³*** o *Information Security Management Maturity Model.* Es un marco de referencia sobre la madurez de los sistemas de gestión de la seguridad de la información. Define cinco niveles de madurez de seguridad adaptados a la misión del negocio y al retorno de inversión (ROI). Este modelo está **basado en procesos**, incluye métricas y es compatible con los estándares UNE EN-ISO 9001:2000, UNE-ISO/IEC 27001, CobiT e ITIL[31], entre otros.

El *ISM³ Consortium*, impulsado por un español, fue constituido para la promoción de esta iniciativa y su aceptación por ISO (*International Standards Organization*). Este modelo de madurez es acreditable por el consorcio.

El modelo *ISM³* es un estándar de ISECOM [32] y tiene licencia de «código libre». Actualmente ISECOM tiene en proyecto la evolución de este modelo para estructurar y medir con precisión y sencillez la seguridad operacional y el proceso de gestión. El proyecto, aún en desarrollo, se denomina SOMA [33] (*Security Operations Maturity Architecture*). Sus objetivos son evitar los métodos basados en productos, análisis de riesgos y buenas prácticas no específicos de la organización a la que se aplican.

El modelo *ISM³* aplica los principios de gestión de la calidad de la norma UNE EN-ISO 9001:2000 a los sistemas de gestión de la seguridad de la información. Está más enfocado a los procesos generales en seguridad de la información, compartidos en cierta medida por todas las organizaciones, que a los controles. Este modelo describe estos procesos dotándoles de objetivos de rendimiento y de métricas. Los objetivos de rendimiento dependen de los requisitos de negocio y de los recursos disponibles. Estos objetivos en conjunto forman la Política de seguridad de la información. La originalidad de este modelo reside en el énfasis en ser práctico y conmensurable y su adaptabilidad a los cambios tecnológicos y a los riesgos.

Describe cinco configuraciones de procesos (estratégicos, tácticos y operativos) básicos, equivalentes a niveles de madurez, que se utilizan para orientar a las organizaciones al escoger el SGSI más adecuado a sus necesidades.

Los objetivos de este modelo son:

- permitir la creación de SGSIs completamente alineados con la misión del negocio y las necesidades de cumplimiento (legislativo y normativo);
- ser aplicable a cualquier organización sin importar su tamaño, contexto o recursos;
- permitir a las organizaciones priorizar y optimizar sus inversiones en seguridad de la información;

[30] http://www.ism3.com/
[31] Information Technology Infrastructure Library, Estándar mundial de de facto en la Gestión de Servicios Informáticos.
[32] Instituto para la Seguridad y las Metodologías Abiertas (ISECOM) es una iniciativa internacional sin ánimo de lucro dedicada a definir estándares técnicos y éticos en seguridad de la información desde enero de 2001.
[33] http://www.isecom.org/research/soma.shtml

- permitir la mejora continua de los SGSIs utilizando métricas; y
- admitir el *outsourcing* o externalización de procesos de seguridad.

Este modelo considera dos tipos de madurez: capacidad y cobertura. La capacidad es una propiedad de cómo los procesos son gestionados. Por otra parte, los procesos se sitúan en un nivel de cobertura de acuerdo a un espectro, desde básico a avanzado de cinco niveles. El estándar basa su clasificación de los niveles de cobertura en la paradoja de Mayfield[34] y en un estudio de la universidad Carnegie-Mellon[35]. Estos estudios definen la capacidad de supervivencia o *survivability* como «la capacidad de un sistema para cumplir su misión a tiempo, en presencia de ataques, fallos o incidentes» y demuestran que a medida que mejora la actitud ante la seguridad, el coste correspondiente a mejoras adicionales también se incrementa.

Los cinco niveles de cobertura que una organización puede elegir implementar, de acuerdo con sus objetivos de seguridad específicos son los siguientes:

| | |
|---|---|
| **Nivel 1**: Este nivel debería suponer una reducción significativa de los riesgos de amenazas técnicas, con una inversión mínima en procesos de gestión de seguridad básicos. | Está recomendado para organizaciones con pocos objetivos (*targets*) de seguridad de la información, en entornos de bajo riesgo y que tengan recursos muy limitados. Las métricas de los procesos no son obligatorias en este nivel. |
| **Nivel 2**: Este nivel debería suponer una reducción mayor del riesgo frente a amenazas técnicas, con una inversión moderada en procesos de seguridad. | Está recomendado para organizaciones con objetivos normales (*targets*) de seguridad de la información, en entornos de riesgo normales y que necesiten demostrar buenas prácticas a socios y estén dispuestos a evitar incidentes de seguridad. Las métricas de los procesos no son obligatorias en este nivel. |
| **Nivel 3**: Este nivel debería suponer una reducción aún mayor del riesgo frente a amenazas técnicas, con una inversión considerable en procesos de seguridad. | Está recomendado para organizaciones con objetivos altos (*targets*) de seguridad de la información, en entornos de riesgo normal o alto, por ejemplo organizaciones que dependen de servicios de información y comercio electrónico. Las métricas de los procesos no son obligatorias en este nivel. |
| **Nivel 4**: Este nivel debería suponer la más alta reducción del riesgo frente a amenazas técnicas e internas, para una inversión alta en procesos de seguridad. | Está recomendado para organizaciones maduras afectadas por requisitos específicos por ejemplo organizaciones muy sometidas a regulación, que coticen en bolsa, administraciones e instituciones financieras. Las métricas de los procesos no son obligatorias en este nivel. Certificable ISO 27001. |
| **Nivel 5**: La diferencia de este nivel con el anterior es el uso obligatorio de las métricas. | Está dirigido a organizaciones maduras que tengan cierta experiencia en el nivel 4 y puedan optimizar y aplicar la mejora continua en este nivel. Certificable ISO 27001. |

*Tabla 1: Niveles de madurez de ISM³*

Los niveles de capacidad de los procesos son:

- Indefinido: el proceso ha de usarse pero no está definido;
- Definido: el proceso está definido y en uso;
- Gestionado: el proceso está definido y los resultados del mismo se utilizan para compensarlo y mejorarlo.

[34] La paradoja de Ross Mayfield es un hecho empíricamente observado de que el coste de permitir/restringir el acceso a un sistema informático es una curva, con forma de U, función del porcentaje de población que tiene acceso.
[35] Citado en *ISM³ Information Security Maturity Model: Carnegie-Mellon Univ. (2000) The Survivability of Network Systems: An Empirical Analysis.*

- Controlado: el proceso está gestionado pudiéndose preveer con precisión hitos y necesidades de recursos.

- Optimizado: el proceso está controlado y las mejoras conducen al ahorro de recursos.

Para superar certificación con la norma UNE EN-ISO 9001:2000 (Sistemas de Gestión de la Calidad) se debe alcanzar el nivel «Gestionado». Los sistemas de gestión basados en ISM$^3$ son acreditables bajo los esquemas de ISO 9001 o ISO 27001. De la misma forma, ISM$^3$ puede ser utilizado como una herramienta para implantar el sistema de gestión de seguridad sugerido por la norma UNE-ISO/IEC 27001. Esto resulta particularmente atractivo para organizaciones que ya se encuentran certificadas en Calidad o han tenido experiencia con ISO 9001.

En resumen, es un modelo tecnológicamente neutro, diseñado para cualquier tipo de organización con independencia de su tamaño. Permite gestionar la seguridad de la información de la organización resaltando las diferencias entre el nivel actual y un nivel deseado de madurez. Emplea un enfoque cuantitativo para evaluar la madurez del sistema y su entorno de control de la seguridad y puede utilizarse como guía para gestionar inversiones en seguridad. *ISM$^3$* pretende cubrir la necesidad de un estándar simple y aplicable de calidad para sistemas de gestión de la seguridad de la información.

Existen diferencias con la norma UNE-ISO/IEC 27001 entre las que se pueden citar: la existencia de métricas; la orientación en este modelo desde el principio a las necesidades técnicas, de cumplimiento y del negocio (calidad, estabilidad, prioridad, control de accesos) como objetivos de seguridad, en lugar de los típicos confidencialidad, integridad y disponibilidad; la distribución de las responsabilidades granular y específica en los distintos niveles organizativos; la dependencia del coste de implementación del nivel de madurez y el ámbito elegido; la posibilidad de gestionar también servicios en externalización o *outsourcing* de seguridad; una selección de procesos ajustada a los objetivos y metas de seguridad; el uso de ciclo de Deming (PDCA) en cada proceso; y el enfoque *Top-Down* basado en procesos fácilmente integrable con ISO 9001, CobiT e ITIL[36].

## Gestión de riesgos

En un capitulo anterior se analizó una herramienta de gestión de riesgos aplicada a repositorios institucionales y bibliotecas digitales. Son muchas las aplicaciones de la gestión de riesgos utilizadas por los gerentes de organizaciones para determinar qué y cómo puede afectarles en el logro de sus objetivos, para con este conocimiento, tomar las medidas que aporten la seguridad e integridad adecuadas para el negocio.

En el caso de la gestión de la seguridad, en el apartado anterior se describen someramente dos enfoques posibles para abordarla: uno orientado a controles y otro orientado a procesos. El primero, la norma UNE-ISO/IEC 27001 recomienda una gestión de riesgos en su fase inicial. El último de estos modelos analizados, *ISM$^3$* proclama que permite la gestión de las inversiones en seguridad con un modelo de seguridad contextual. Otros estudios (Arora et al., 2004) proponen un marco para valorar las inversiones en seguridad en TI basándose en mecanismos de gestión de riesgos, calculando un retorno de inversión basado en riesgos, RROI (*Risk based Return of Investment*), en el que comparan el coste del riesgo (valor de los daños) frente al coste de implementación, para cada solución de seguridad, como medida de eficiencia.

Existe actualmente una fuerte controversia en cuanto al Retorno de Inversión aplicado a la seguridad. El llamado ROSI (*Return of Security Investment*) compara la cantidad ahorrada al reducir el riesgo con la cantidad invertida, es por tanto una medida de

[36] ITIL: Biblioteca de Infraestructura de Tecnologías de la Información, estándar mundial de de facto en la Gestión de Servicios Informáticos.

efectividad. Algunos estudiosos del tema (Pols, 2008) sostienen que no puede haber retorno donde no hay ingresos. También Parker (2006) sostiene que la seguridad basada en la gestión, reducción y valoración de riesgos es un concepto erróneo. Estos detractores del ROSI declaran que no hay tal retorno de inversión sino una prevención de pérdidas e introducen la idea de que la seguridad TI debe ser tratada por compañías aseguradoras, desplazando a estas la función de auditar la seguridad.

Toda esta controversia, que reside en la dificultad de calcular el coste del valor de la pérdida de activos y la probabilidad de que esto ocurra, está en parte justificada por la carencia de modelos de referencia maduros. Las metodologías de gestión de riesgos en seguridad abordan también análisis cualitativos a la vez que cuantitativos, siendo conscientes de que no todos los riesgos pueden ser cuantificables.

### *Metodologías de gestión de riesgos: MAGERIT*

A pesar de la controversia actual, el análisis de riesgos se utiliza en proyectos de gestión de la seguridad de la información. Mediante su aplicación se obtiene información sobre los activos, la valoración del impacto que para la organización tiene la pérdida de los mismos y la identificación de las amenazas a las que están expuestos. También en el capítulo anterior se ha comentado la aplicación de la gestión de riesgos en bibliotecas y repositorios digitales.

Existen varias metodologías de gestión de riesgos aplicables a la seguridad de la información. Dada la importancia que tiene la gestión de riesgos para la aplicación de un SGSI según la norma UNE-ISO/IEC 27001, se expone brevemente a modo de ejemplo la metodología de carácter público MAGERIT [37] elaborada por el Ministerio de Administraciones Públicas.

Las actividades para aplicar esta metodología se agrupan en dos grandes fases:

- análisis de riesgos: para determinar los activos de la organización y los hechos que les pueden afectar; y
- gestión de riesgos: organizar la defensa para hacer frente a emergencias, resistir ante los incidentes y seguir operando en las mejores condiciones.

En el análisis de riesgos se distinguen las siguientes actividades:

1. Determinar los activos relevantes, sus interrelaciones y su valor (coste que supondría su degradación). Los activos pueden ser: servicios, aplicaciones informáticas, equipos informáticos, soportes de información, equipamiento auxiliar, redes de comunicaciones, instalaciones y personas. El valor cuantitativo o cualitativo de los mismos se calibra atendiendo a las siguientes dimensiones: autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad.
2. Determinar a que amenazas están expuestos los activos y estimar cuán vulnerable es cada activo en dos sentidos: degradación y frecuencia.
3. Determinar que salvaguardas hay dispuestas y cuán eficaces son frente al riesgo, tanto si reducen la frecuencia de las amenazas como si limitan el daño causado.
4. Estimar el impacto, como daño sobre el activo, en caso de materializarse la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (expectativa de materialización) de la amenaza.

[37] http://www.csi.map.es/csi/pg5m20.htm

Del análisis de riesgos se obtiene un Informe de Insuficiencias o asuntos pendientes para reducir los riesgos a niveles aceptables. En esto consiste la gestión de riesgos. Para cada riesgo identificado hay que seleccionar el tratamiento (UNE-ISO/IEC 27001): asumirlo, eliminarlo, transferirlo o reducirlo (mitigarlo).

En caso de asumirlo hay que reflejar este hecho documentalmente. Si se elimina, se actúa para que desaparezca el riesgo sobre el activo, el propio activo o la causa que lo provoca. Si se transfiere, se ejecutan acciones como externalización o contratación de seguros que palien este riesgo o sus efectos. Para concretar la forma de reducirlos o mitigarlos se establece una forma profesional de afrontarlos:

1. establecer políticas (directrices generales) de la organización al respecto,
2. establecer normas (objetivos),
3. establecer procedimientos (instrucciones),
4. desplegar salvaguardas técnicas y
5. desplegar controles para comprobar que todo lo anterior funciona

Estas actividades conforman el establecimiento ya mencionado de un SGSI.

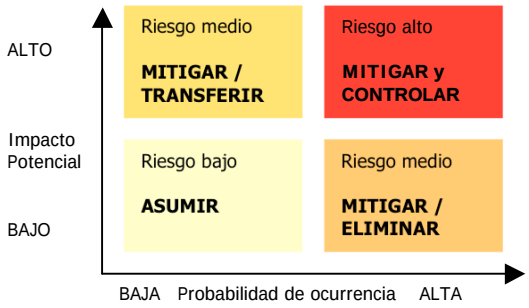


*Ilustración 3: Matriz de gestión de riesgos*

El gráfico muestra los tratamientos posibles de los riesgos según su impacto y probabilidad de ocurrencia.

## 3.2. Auditorias de seguridad

Las auditorías constituyen el mecanismo para revisar, verificar y comprobar la gestión de la seguridad o la seguridad de los sistemas de información, mediante un proceso sistemático y metódico, generalmente de carácter independiente. Existen por tanto dos tipos de auditorias: las auditorías de gestión de seguridad y las auditorías técnicas.

### *Auditorías de gestión de la seguridad*

En estas auditorías se comprueba el cumplimiento de las políticas de seguridad. En ellas se verifica el cumplimiento de los procesos operativos de seguridad; se verifica el estado de la información en cuanto a su confidencialidad, integridad y disponibilidad; se comprueba la adecuación de la organización a las políticas; se recogen evidencias del funcionamiento de los procesos implementados y se identifican mejoras de seguridad.

La norma UNE-ISO/IEC 27001 contiene un apartado dedicado a la obligatoriedad de realizar auditorías internas del SGSI «a intervalos planificados, para determinar si los objetivos de control, los controles, los procesos y los procedimientos de este SGSI:

1. cumplen los requisitos de esta norma internacional, así como la legislación y normativa aplicables;

2. cumplen los requisitos de seguridad de la información identificados;

3. se implantan y mantienen de forma efectiva; y

4. dan el resultado esperado.»

También otra norma la ISO/IEC 27006 contiene las directrices para la auditoria del SGSI previa a su certificación. Estas auditorías generalmente se materializan en entrevistas con los responsables de la seguridad, el personal técnico y los usuarios de los sistemas.

### *Auditorías técnicas de seguridad*

Las auditorías técnicas se ocupan de los riesgos existentes en los sistemas de información de la organización y en la calidad técnica de las medidas de seguridad introducidas.

Estas pueden ser intentos de *hacking* controlados, *test* de intrusiones, auditorias a nivel de aplicación y auditorías de vulnerabilidades. Bien tratan de explotar errores de programación, de la arquitectura de red, debilidades de los protocolos de comunicación y de los controles de acceso, o bien tratan de localizar configuraciones erróneas o no suficientemente estrictas y agujeros de seguridad en el software directamente explotables. Este tipo de auditorías puede clasificarse en auditorías de caja negra o de caja blanca. Las primeras buscan debilidades desde el exterior de los sistemas y las segundas realizan una revisión de seguridad analizando la configuración del propio sistema, accediendo al mismo.

Las auditorías de caja negra intentan ganar algún tipo de acceso a los sistemas para una vez conseguido, examinarlo y tomar el control. Se apoyan en herramientas y procedimientos de metodologías estándar: *OSSTMM* (*Open Source Security Testing Methodology Manual*) de ISECOM[38] o en el documento SP 800-42[39] del instituto de estándares americano NIST (*National Institute of Standards and Technology*).

Las auditorías de caja blanca tienen por objetivo revisar las medidas de seguridad implementadas en el sistema y su conformidad o no con estándares reconocidos de *buenas prácticas* como por ejemplo los del mencionado instituto de estándares americano NIST. Estas pruebas incluyen:

- análisis de la configuración de los sistemas operativos,
- análisis de la robustez de las contraseñas,
- análisis de la configuración del software base (correo electrónico, web, etc.)
- análisis de las aplicaciones instaladas o del código fuente de las aplicaciones desarrolladas *ad hoc*,
- revisión de los parches y de la actualización de los sistemas y aplicaciones.

[38] http://www.isecom.org/osstmm/ (véase también nota 28)
[39] Wack, J., Tracy, M. y Souppaya, M. (2003) Guideline on network security testing: recomendation of the National Institute of Standards and Technology. *NIST Special Publication 800-42. Computer security.* http://www.nist.gov/

## 3.3. Elementos para gestión de la seguridad de las TIC en las BU españolas

En el desarrollo de este trabajo se ha mostrado la dependencia de la actividad de las bibliotecas universitarias de las TIC, las iniciativas existentes para abordar la seguridad en relación con los procesos y servicios de la biblioteca en el nuevo marco de la educación en la sociedad de la información y la normativa de uso habitual en organizaciones que buscan una mejora en la gestión de la seguridad. En este apartado se abordan distintos aspectos que pueden influir en la forma de afrontar esta necesidad por las bibliotecas universitarias españolas.

### Calidad y Seguridad

Los servicios bibliotecarios cuentan con un reconocimiento a sus esfuerzos en cuanto a calidad que se materializa en el Certificado de Calidad de los Servicios Bibliotecarios, iniciativa de la Dirección General de Universidades. Hasta el momento son veinticinco las universidades españolas que tienen este reconocimiento que también las faculta para optar a subvenciones para la financiación de propuestas de mejora. Si bien estos esfuerzos no contemplan de momento iniciativas en cuanto a seguridad de la información, si son indicativos tanto del compromiso con la calidad como de la orientación hacia la gestión por procesos de estas unidades de información.

Según Balagué, Rey y Falomir (2006) las bibliotecas universitarias (BU) españolas pueden clasificarse en tres grupos:

- BU con sistemas de gestión de la calidad consolidados basados en la evaluación continua,
- BU con sistemas de gestión de la calidad en fase de consolidación, que han realizado la primera evaluación institucional
- BU que aún no ha pasado por ningún proceso de autoevaluación ni evaluación externa.

Sin embargo, aunque la iniciativa está en marcha, el grupo más numeroso, según el citado estudio, es el que no han iniciado ningún proceso de autoevaluación. No obstante, este tema es también motivo de una de las líneas estratégicas del Plan estratégico de REBIUN. La biblioteca del caso de estudio se encuentra en el grupo intermedio.

Estas iniciativas y orientaciones estratégicas suponen áreas de sinergia con la gestión de la seguridad de la información.

#### *Sinergias de la gestión de la seguridad con otros instrumentos de gestión*

Por una parte las iniciativas orientadas a la calidad proponen un modelo de gestión por procesos que supone un paso organizativo importante para la adopción de sistemas de gestión de la seguridad.

Por otra parte el esquema de SGSI de la norma UNE-ISO/IEC 27001 comparte con la norma UNE-EN ISO 9001:2000 (Sistemas de gestión de calidad. Requisitos), y con otras normas ISO, el ciclo *PDCA* (o círculo de Deming: *Plan-Do-Check-Act*). Las etapas de este modelo: planificar, hacer, verificar y actuar, forman parte de la estrategia de mejora continua compartida por ambas normas. También el modelo ISM$^3$ comparte con las normas ISO el ciclo de Deming (PDCA) aplicándolo a cada proceso.

Estas sinergias facilitan la integración de la gestión de la seguridad con los sistemas de gestión de la biblioteca universitaria. La integración se verá favorecida por el alineamiento en áreas comunes como documentación, auditoría, etc. que facilita una implementación consistente, con la consiguiente reducción de costes y esfuerzos.

## Cumplimiento legislativo

*LOPD, LPI y otras leyes.*

Ya se ha hecho mención a las obligaciones legales que afectan por igual a todas las organizaciones y en particular a aquellas que como las bibliotecas universitarias utilizan **datos personales**, elementos con **propiedad intelectual** y disponen de **página web**. La generalización de la factura electrónica o del uso del DNIe también pueden ser objeto de tratamientos especiales de seguridad. Sean estas o no exigencias legales van a tener especiales consecuencias en el tratamiento de la información que requerirán políticas, formación, concienciación y utilización de aplicaciones y tecnologías de seguridad.

También desde otra perspectiva y según el Manifiesto de Alejandría (IFLA, 2005) «Las bibliotecas y los servicios de información contribuyen a la adecuada puesta en práctica de una **Sociedad de la Información incluyente**. Capacitan para la libertad intelectual dando acceso a información, ideas y obras de imaginación en cualquier medio y por encima de fronteras. Ayudan a conservar los valores democráticos y los derechos civiles universales con imparcialidad y oponiéndose a cualquier forma de censura.»

El cumplimento con la LOPD de la biblioteca universitaria está incluido en las obligaciones de la Universidad para con esta ley. No obstante, el carácter de los servicios bibliotecarios y la proliferación de las nuevas tecnologías puede dar lugar a la toma de datos de carácter personal de mayor nivel de protección que los que manejan otras unidades de la Universidad para los que el cumplimiento legislativo tiene exigencias mayores en cuanto a los requisitos de seguridad. Por este motivo deben garantizar una especial atención al derecho a la intimidad de las personas mediante una política específica de confidencialidad y privacidad de los datos personales que manejan en los servicios que ofrecen de forma presencial y virtual.

Es recomendable que se tomen también las precauciones técnicas si fueran necesarias: software para la encriptación de la información confidencial y control de acceso a la información de carácter personal, usuarios restringidos, usuarios y contraseñas que caducan según exige la LOPD, y otros sistemas orientados a evitar el mal uso, alteración, acceso no autorizado y robo de los Datos Personales facilitados.

Dada la tendencia de las bibliotecas universitarias a integrar «Repositorios o espacios de conocimiento» a lo que se añade el crecimiento de las iniciativas de contenidos abiertos, es trascendental que estas unidades de información garanticen, en los términos que la LPI obligue (reproducción, distribución, comunicación pública y transformación), los derechos de propiedad intelectual de los que depositan sus creaciones. La biblioteca universitaria puede convertirse en una vía de estímulo a los creadores de contenido asesorando a los autores (investigadores, docentes, alumnos) sobre la gestión de los derechos de autor, la utilización de los recursos «copyleft» y la liberación de sus creaciones.

Finalmente las organizaciones que disponen de servicios a través de Internet, están sujetas en mayor o menor medida a la legislación que regula y fomenta un correcto uso de la Sociedad de la Información (LISI, LAECSP[40] y LSSICE[41],…). Por poner un ejemplo, sus páginas han de ser accesibles para personas con discapacidad y edad avanzada. La LISI además de reforzar los derechos de los usuarios de los servicios públicos o no a través de Internet, también introduce innovaciones normativas en materia de facturación electrónica para favorecer la contratación electrónica que en un plazo breve será de uso común en la administración y que previsiblemente será adoptada por las bibliotecas universitarias en su relación con terceros.

[40] Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos

[41] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Con la adopción de un sistema de gestión de seguridad, la biblioteca universitaria integrará el cumplimiento legislativo que le corresponda en sus procesos de gestión.

## El factor humano

### *Concienciación, formación y capacitación*

Una de las funciones de los sistemas de gestión de la seguridad es asegurarse que los usuarios, los operarios y los responsables de las TIC tienen la motivación y los conocimientos necesarios para utilizar, operar y gestionar respectivamente la seguridad de las TIC en la biblioteca universitaria.

Una política de seguridad ha de incluir las directrices para el alineamiento con los objetivos y estrategias de gestores, técnicos y usuarios para que la gestión de la seguridad sea efectiva, protegiendo los activos ante errores humanos y fallos por falta de competencia, entre otros.

Por extensión, la realización de actividades de concienciación en seguridad hacia la comunidad universitaria revertirá en la mejora de la utilización de otros servicios dependientes de las TIC.

### *Perspectivas y actitudes*

La seguridad de las TIC no se entiende por igual por los distintos colectivos que acceden a la biblioteca universitaria. Se pueden identificar (Templeton, 2004) actitudes y perspectivas diferentes según procedan de gestores, técnicos, personal de biblioteca, docentes e investigadores y estudiantes.

Para los directivos de las bibliotecas, la seguridad puede convertirse en una cuestión de imagen o reputación y de presupuesto. A este nivel, se han de equilibrar todos los aspectos de la seguridad con las necesidades y objetivos de la biblioteca.

La preocupación de los técnicos se centra en la disponibilidad, la confidencialidad y la integridad de los sistemas, desde el diseño de los sistemas hasta su operación y mantenimiento con cierto sentimiento de propiedad sobre los equipos y aplicaciones que operan.

La plantilla no técnica de la biblioteca se plantea la dificultad de la operativa diaria y del hacer cumplir las normas que se dicten. También sienten la seguridad como una restricción a la libertad en su actividad o bien se sienten observados y monitorizados. La autenticación y la accesibilidad son los efectos de la seguridad que más impacto tienen sobre este colectivo.

Como usuarios de la biblioteca, los docentes e investigadores estarán más sensibilizados con el reconocimiento de la propiedad de los conocimientos o los derechos de autor. Por otra parte para este colectivo es fundamental la disponibilidad de los recursos de la biblioteca.

Los estudiantes por su edad se revelan a toda restricción o regulación de sus libertades. También es habitual que los estudiantes tiendan a no respetar la propiedad intelectual.

### *Responsabilidad*

En todo sistema de gestión de la seguridad se han de determinar con claridad los responsables de cada proceso o actividad. La responsabilidad ha de estar distribuida en todos los niveles organizativos: estratégico, táctico y operativo.

A nivel estratégico, es necesaria para la elaboración de las directrices y políticas. Es también indispensable el **apoyo incondicional de la dirección** y su **coordinación** con

los departamentos legales y de calidad de la Universidad para el éxito de un proyecto de implantación de un sistema de gestión de la seguridad. A nivel táctico, la responsabilidad estriba en el diseño y ejecución de los planes de seguridad. Los responsables a nivel operativo rendirán cuentas sobre los eventos registrados, las intervenciones necesarias, las actualizaciones, etc.

La práctica en la introducción de sistemas de gestión de seguridad en las organizaciones revela que es imprescindible la existencia de **perfiles o roles de seguridad** que han de desempeñar personas con la capacidad y los conocimientos suficientes para, entre otros, apoyar a la dirección en el análisis de riesgos y en la confección de presupuestos. También entre estos roles se define el papel de los técnicos en el desarrollo de planes de seguridad de la información adecuados para proteger la biblioteca universitaria.

## Requisitos de seguridad de las TIC en bibliotecas universitarias

### *Líneas generales*

En el apartado sobre las TIC en las bibliotecas universitarias se hace una breve exposición de las características de estas unidades de información en cuanto a la forma en la que estas adoptan las TIC, con diferencias sustanciales entre ellas.

A pesar de estas diferencias, después de estudiar las tendencias que se apuntan en cuanto a los servicios que han de ofrecer, los avances tecnológicos y la seguridad que se espera de las mismas, las necesidades de seguridad de las TIC de las bibliotecas universitarias se pueden resumir, parafraseando las de Templeton (2004) para las TIC de las universidades en:

- aportar un entorno de confianza en el que se pueda fomentar el intercambio de ideas y la libertad académica
- proveerse de una infraestructura de seguridad que sea capaz de soportar las demandas y expectativas de la comunidad universitaria
- proteger la infraestructura y los contenidos contra actividades no deseables o prohibidas, tanto internas como externas
- dotarse de políticas de seguridad de amplia perspectiva y de procedimientos prácticos y aplicables
- cumplir con sus obligaciones legales

Solventar estas demandas no sería posible sin un planteamiento de gestión de los recursos TIC que incluya la gestión de la seguridad de la información.

### *Factores técnicos*

En este apartado se han mencionado los aspectos relativos a calidad, cumplimento legislativo, factor humano y requisitos generales de las bibliotecas universitarias que tienen influencia en la gestión de la seguridad de las TIC. Además de éstos, se han identificado a lo largo del trabajo otros factores técnicos que afectan en la adopción de la gestión de la seguridad por estas unidades de información.

Un grupo de requisitos técnicos ya mencionados son los que hacen posible una infraestructura mínima de seguridad (Hurley, 2002), válidos tanto para la universidad en su conjunto como para su biblioteca. Y la integración (Inmor, Esichaikul y Batanov, 2003) de la seguridad en el diseño de los sistemas de información.

Por otra parte considerando la evolución que se apunta en el primer capítulo para estas instituciones se incluyen otros parámetros que ya se consideran claves actualmente y cobrarán más importancia en el futuro:

- los retos específicos de seguridad debidos a la existencia de repositorios institucionales o espacios de conocimiento,
- la seguridad en el desarrollo de sistemas de información específicos para bibliotecas y
- la seguridad en entornos colaborativos a través de Internet (seguridad en dominios de información).

Finalmente para completar los requisitos de seguridad de las bibliotecas universitarias, la biblioteca universitaria debe **gestionar los incidentes** de seguridad y tener una respuesta organizada ante estos sucesos para que su impacto sea menor y se puedan evitar incidentes similares en el futuro. Además dado el impacto que puede tener en el servicio que prestan las bibliotecas a la comunidad universitaria un evento de seguridad de carácter grave que degrade o deje inutilizable una parte sustancial de sus activos, se han de proveer de las medidas técnicas necesarias que garanticen la **continuidad del negocio**.

# 4. Métodos

## *Introducción*

Para determinar la capacidad de las bibliotecas universitarias en la adopción de un sistema para la gestión de la seguridad se utiliza un método exploratorio, basado en el caso de estudio, utilizando tres instrumentos: un cuestionario, un ensayo de análisis de riesgos y una entrevista. Con el resultado de estas acciones se determinará la disponibilidad y predisposición de los órganos directivos y la adecuación a los distintos planteamientos a la gestión de estas unidades de información considerándose dos opciones para su análisis: SGSI según UNE ISO/IEC 27001 o el modelo de madurez de *ISM*[3].

La elaboración del cuestionario se basa en el estudio y adaptación de herramientas utilizadas en estudios similares. Esta encuesta, o su evolución, podría servir para un estudio de este tema a nivel nacional.

El ensayo del análisis de riesgos consiste en un ejercicio de ejemplo para un proceso de la biblioteca del caso de estudio con dos enfoques. El primer enfoque combinado, siguiendo las directrices de las normas UNE y un segundo enfoque cualitativo siguiendo la metodología propuesta en el modelo ISM[3].

Las entrevistas tienen por objeto completar y valorar la información obtenida del cuestionario y del ensayo con observaciones *in-situ*. Consistirán en preguntas abiertas para recoger elementos contextuales no contemplados y concretar aquellas cuestiones o aspectos que susciten dudas sobre el cuestionario y el ensayo.

Estos métodos tendrán también el valor inherente de concienciación que puede suponer el autoanálisis de la dirección de la biblioteca sobre los diferentes aspectos de la seguridad.

## 4.1. Análisis de herramientas utilizadas en estudios similares

Se analizan a continuación los cuestionarios utilizados para el estudio de las necesidades en gestión de la seguridad y auditoría en las organizaciones con el objetivo de valorar los enfoques adoptados y su adecuación a los fines expuestos.

### *Herramienta de evaluación de EDUCAUSE*

Esta herramienta[42] elaborada por EDUCAUSE (www.educause.edu/security) está dirigida a universidades y organizaciones sin ánimo de lucro aunque inicialmente fue concebida para empresas. Tiene su origen en la preocupación del gobierno de Estados Unidos de extender la seguridad de la información de los directores de informática a los directores generales.

El propósito de esta herramienta es determinar el grado de implementación de un programa de buen gobierno corporativo en seguridad de la información, en el nivel estratégico en la organización. Indica que también puede ser utilizada por una parte de la organización. Intenta servir de ayuda a la dirección para identificar las áreas en las que es importante establecer un marco de seguridad, en lugar de detallar las prácticas y políticas que han de seguirse.

[42] http://www.educause.edu/ir/library/pdf/SEC0421.pdf

Una primera sección ayuda a la institución a valorar su dependencia en la tecnología de la información. Las siguientes secciones pretenden ayudar a determinar la madurez de marco de seguridad a nivel estratégico. Consta de cien preguntas de respuesta ponderada. Las primeras dieciséis dan un valor de dependencia en las tecnologías de la información (cinco niveles). Otras cinco secciones cubren aspectos de gestión de riesgos, factor humano, procesos y tecnología; las respuestas de cada una de estas cuestiones está ponderada de cero a cuatro (desde no implementada a totalmente implementada). Del cruce de estos con el primero se obtiene una valoración de cada aspecto (insuficiente, necesita mejoras, bueno).

Su aplicación para las bibliotecas universitarias es alta como análisis individual y como análisis global. Se plantea adaptar las cuestiones para obtener mayor precisión. Como debilidad se apunta que no contempla los niveles táctico y operativo.

### *Análisis exploratorio en las universidades australianas*

Esta encuesta forma parte de la mencionada tesis de Lane (2007) y está dirigida a directores de informática o coordinadores de la seguridad TIC de las universidades australianas.

El propósito de la encuesta fue determinar los factores clave que influyen en la gestión efectiva de la seguridad de la información para identificar cómo mejorarla. Tiene aspectos cuantitativos y cualitativos, incluyendo preguntas abiertas para favorecer la discusión. Consiste en una encuesta de cuarenta preguntas que se completa con una entrevista telefónica.

Consta de una sección inicial para determinar los indicadores básicos (tamaño, tipo de universidad, etc.) y cinco áreas: compromiso de la alta dirección, enfoque de la gestión de la seguridad, política de seguridad, concienciación y conformidad.

Su aplicación para bibliotecas universitarias es alta como parte de un análisis general que englobe a todas las universidades españolas. El principal inconveniente es la dificultad de tratamiento sistematizado de los datos cualitativos y de las respuestas a las preguntas abiertas.

### *Metodología de pruebas de auditoría de ISECOM*

ISECOM es una organización independiente y sin ánimo de lucro dedicada a la investigación y también una autoridad de certificación. Dispone de una metodología de pruebas de seguridad para apoyo a auditorías que se realicen para obtener la certificación OSSTMM.

Se analiza un informe de auditoría cuyo propósito es dotar de un esquema estándar para la auditoría, basado en una metodología científica y servir de conjunto de directrices para conseguir la certificación.

Esta formada por quince secciones. En la sección inicial se revisan los objetivos, políticas y normas que aplican y contra las cuales se verifican las otras secciones. Estas secciones incluyen entre otros: logística, verificación de accesos, de procesos, de controles, de la configuración/formación y privilegios.

Al ser un modelo para realizar un informe de auditoría, su interés reside en evaluar la aplicación de una serie de medidas. No es aplicable, en una primera aproximación, para medir la capacidad para la gestión.

### *Lista de verificación del instituto ITC*

El instituto de conformidad IT, ITC (http://www.itcinstitute.com/) pretende servir a los profesionales de las tecnologías de la información de un recurso útil para ayudar a sus

negocios en el cumplimiento de requisitos de privacidad, confidencialidad, auditoría financiera y otros.

Del análisis de la lista de chequeo de Auditoría en Seguridad de la Información, se concluye que está pensada para comprobar que se controlan los riesgos, que los controles se ejecutan de forma efectiva y consistente y que los niveles de gestión y operativos de la organización tienen la capacidad para reconocer y responder a nuevas amenazas y riesgos.

Es una lista de chequeo extensa y está dividida en tres grandes grupos: controles de gestión, controles operativos y controles técnicos. Cada uno de ellos cuenta con distintas áreas en las que se comprueban los controles que han de cumplirse. Para el grupo de controles de gestión estas áreas son: evaluaciones de certificación, acreditación y seguridad, planificación, evaluación de riesgos y adquisición de sistemas. El grupo de controles operacionales contiene las siguientes áreas: concienciación y formación, gestión de la configuración, planes de contingencia, respuesta a incidentes, mantenimiento, protección de medios, protección física y del medioambiente, seguridad del personal e integridad de sistemas e información. Finalmente, el grupo de controles técnicos está formado por las áreas de: control de acceso, auditoría y auditabilidad, identificación y autenticación, protección de sistemas y comunicaciones.

Esta lista de chequeo es también una herramienta de auditoría, no aplicable en una primera aproximación para medir la capacidad de gestión.

### *Comparativa*

Tras el análisis de las herramientas se concluye que la orientación de las dos primeras es las más acertada para el enfoque de este trabajo, además de que están dirigidas al entorno universitario.

El enfoque de las dos restantes hacia la auditoría, supone ya el establecimiento de alguna forma de gestión de la seguridad, no siendo válidas en una primera aproximación del asunto que es el objeto de este trabajo.

## 4.2. Diseño del cuestionario

Para el diseño del cuestionario se parte del análisis comparativo de las herramientas utilizadas en estudios similares realizada en el capítulo anterior que se complementará con la adecuación de las cuestiones planteadas al propósito de la misma que es:

| |
|---|
| determinar la capacidad de las bibliotecas universitarias en la adopción de un sistema para la gestión de la seguridad |

Este cuestionario se dirigirá a los directores de bibliotecas universitarias. Los apartados que forman este cuestionario son:

**[A.]** Indicadores básicos de referencia: el propósito de este apartado es poder analizar en conjunto los datos de las bibliotecas universitarias que participen en una futura encuesta a nivel nacional.

**[B.]** Dependencia de la BU de las TIC: se persigue identificar el grado de subordinación de los procesos y servicios de la biblioteca a los sistemas de información basados en las TIC.

**[C.]** Aspectos a evaluar:

1. responsabilidad de los mandos: se analizará la disposición de las direcciones de la Biblioteca, del Servicio de informática y de otras unidades relacionadas para abordar la gestión de la seguridad;

2. enfoque organizativo de la gestión de la seguridad (personas y procesos): se analizará la disposición y preparación de la organización para asumir las responsabilidades asociadas a la gestión de la seguridad; y se analizará el impacto organizativo a nivel de procesos que puede suponer introducir la gestión de la seguridad;

3. cumplimiento legislativo: se analizará si se conoce y contempla la legislación aplicable a la actividad de la biblioteca universitaria;

4. tecnología: se evaluará someramente la percepción de la dirección de algunos aspectos de la seguridad tecnológica.

En el anexo se detalla la propuesta del cuestionario. Se omiten los resultados del caso de estudio para preservar la confidencialidad de la BU.

El resultado será puntuable y permitirá obtener para cada apartado una valoración de la capacidad de la BU para abordar la gestión de la seguridad y de la predisposición para abordar una aproximación basada en una de los modelos estudiados.

El cuestionario está inspirado en el de EDUCAUSE y en la tesis de T. Lane. Se simplifican el número y complejidad de las preguntas, adaptándose al entorno universitario y normativo español. La selección de las preguntas se realiza de forma que permitan conocer el grado de aproximación en cada apartado a los modelos estudiados. Se intercalan preguntas que se corresponden con los apartados de la norma UNE-ISO/IEC 27002 con preguntas que se corresponden con procesos de los distintos niveles de madurez de ISM[3].

*Entrevista*

El cuestionario se completa con preguntas abiertas a la dirección de la biblioteca para confirmar los resultados obtenidos y valorar las conclusiones que de ellos se deducen.

No se reproducen los resultados de la entrevista para preservar la confidencialidad de la BU. La entrevista versa sobre los aspectos del cuestionario de difícil respuesta o sobre aquellos que no pudieron responderse al no ser responsabilidad directa de la BU.

## 4.3. Valoración de riesgos para el caso de estudio

En el capítulo anterior se ha analizado el objeto de estudio presentando dos modelos de gestión de la seguridad y tipologías de auditorías. También se ha establecido la necesidad de la gestión de la seguridad en las BU e indicado la forma que otros estudios similares han escogido para analizar la idoneidad de abordar este tipo de gestión.

A continuación se realiza un ensayo de valoración de riesgos según dos modelos para un macroproceso de la BU con objeto de estimar la dificultad que puede entrañar este elemento de la gestión de la seguridad para la dirección de la BU y seleccionar el enfoque más adecuado para esta organización.

### Ejemplos de valoración de riesgos

Realizar un análisis de riesgos queda fuera del alcance de este trabajo, no obstante y con objeto de ilustrar algunas aproximaciones con las que se podría abordar este análisis se incluyen dos ensayos de cómo sería un análisis de riesgos para un macroproceso (según anexo) definido en la biblioteca universitaria.

El riesgo es una función que depende de: la **probabilidad** de que una **amenaza** explote una **vulnerabilidad** y del **impacto** resultante de dicho evento externo en la organización.[43]

Es función de la dirección aprobar los niveles de riesgo aceptables, escoger el enfoque y metodología para la gestión de riesgos y las herramientas de soporte para esta actividad.

### *La valoración de riesgos: enfoque combinado*

Según la norma UNE 71501-3 hay cuatro enfoques que la dirección puede elegir para abordar un análisis de riesgos: básica o de mínimos, informal, detallada y combinada. Cada enfoque tiene según la norma sus ventajas y desventajas.

Este último, el enfoque combinado, permite caracterizar inicialmente y de forma sencilla el riesgo para luego abordarlo de forma básica para riesgos de tipo general, o detallada para riesgos especiales. Consta de las siguientes fases algunas de las cuales aplicamos a modo de ejemplo a nuestro caso de estudio:

1. Establecimiento de los límites de la revisión.

| |
|---|
| Para nuestro ejemplo, las actividades del macroproceso MP2 (según anexo) de la BU del caso de estudio y los equipos e instalaciones necesarias para su operación (se excluyen las personas para este caso). |

2. Identificación de los activos (datos, aplicaciones, equipos, servicios, edificios, soportes y personas). Ejemplos de activos son: los ficheros y soportes en los que se almacenan los datos, las aplicaciones que se utilizan, los equipos de usuario, electrónica de red y servidores que proporcionan el soporte a las aplicaciones con su software base, la documentación administrativa y contable (facturas, pedidos, contratos,…), los servicios que se ofrecen, los servicios de comunicaciones que son necesarios, las salas y los edificios.

| |
|---|
| Para nuestro caso de estudio son ejemplos de activos: los servidores de la intranet, del catálogo y el OPAC, el servidor web y el de FTP y respaldo, las listas de selección de publicaciones, los pedidos y documentos de tramitación, los registros de entradas, los registros del catálogo, las aplicaciones para reserva de salas, las aplicaciones para proceso técnico, las aplicaciones para formación y evaluación de la colección, la sala del CPD, las salas de proceso técnico, el edificio de la biblioteca central, los soportes en los que se realizan copias de seguridad,… |

3. Valoración de activos y establecimiento de dependencias entre ellos. Para la valoración de los activos se ha de contactar con los propietarios y los usuarios de los mismos. Los valores representan la importancia que cada activo tiene para la organización. La valoración puede ser cuantitativa o cualitativa y se ha de realizar en relación a las variables: confidencialidad, integridad, autenticidad, disponibilidad y coste de sustitución. Es habitual establecer escalas de valoración, por ejemplo: despreciable, bajo, medio, alto, muy alto y crítico. Es obligación de la dirección establecer los criterios (coste de reposición, daños al servicio,…) para la valoración de los activos de manera que se contemple de forma homogénea por los distintos responsables.

   La dependencia de los activos entre sí puede influir en la valoración que se propaga entre activos dependientes de acuerdo a distintas fórmulas y criterios. El establecimiento de las dependencias ayuda a establecer los activos críticos.

4. Evaluación de las amenazas que tengan la potencialidad de dañar al sistema y a sus activos. Se han de identificar tanto las amenazas accidentales como las deliberadas.

[43] NIST 800-30 Risk Management Guide for IT Systems

Existen listados y catálogos de amenazas que pueden servir de referencia. Son ejemplos de amenazas: inundaciones, fuego, fallo hardware, robo, uso no autorizado de soportes, fallo software, errores de transmisión, acceso no autorizado a la red, análisis de tráfico con fines ilícitos, etc. La experiencia en un sector hace que se puedan elaborar catálogos de amenazas específicos. Una posible aplicación de estudios posteriores sobre este tema puede llevar a la elaboración de este catálogo de amenazas para bibliotecas universitarias.

Las manifestaciones de las amenazas son: errores y omisiones, fraude, robo, sabotaje, pérdida de soportes físicos o de infraestructura, intrusión malintencionada, códigos maliciosos, etc. Para cada amenaza sobre un activo se ha de considerar: frecuencia, motivación de los atacantes, habilidades necesarias y factores geográficos y ambientales.

5. Valoración de las vulnerabilidades, es decir la identificación del grado con que las debilidades pueden ser explotadas por las fuentes de amenaza, causando daño a los activos y a la actividad que soportan. Las vulnerabilidades pueden ser del entorno y la infraestructura (puertas, ventanas, red eléctrica, etc.), del hardware (mantenimiento insuficiente, falta de actualización, etc.), del software (contraseñas, permisos, descargas incontroladas, etc.), de las comunicaciones (tráfico no protegido, deficiencias en la gestión de red, etc.), de la documentación (copias incontroladas, falta de destrucción, etc.) o del personal (formación insuficiente, falta de sensibilización, uso incorrecto de equipos, etc.)

6. Identificación de las salvaguardas existentes o planificadas. Este paso da como resultado un listado con las salvaguardas existentes y planificadas, su estado de implantación y uso. Tiene por objeto, no duplicar protecciones existentes y evitar la colisión entre medidas de protección nuevas y existentes.

7. Valoración de riesgos. Con los datos anteriores, las distintas herramientas de gestión de riesgos ofrecen un listado de los riesgos sin salvaguarda y sus impactos. Existen distintos métodos de análisis de riesgos que se escapan del ámbito de este trabajo.

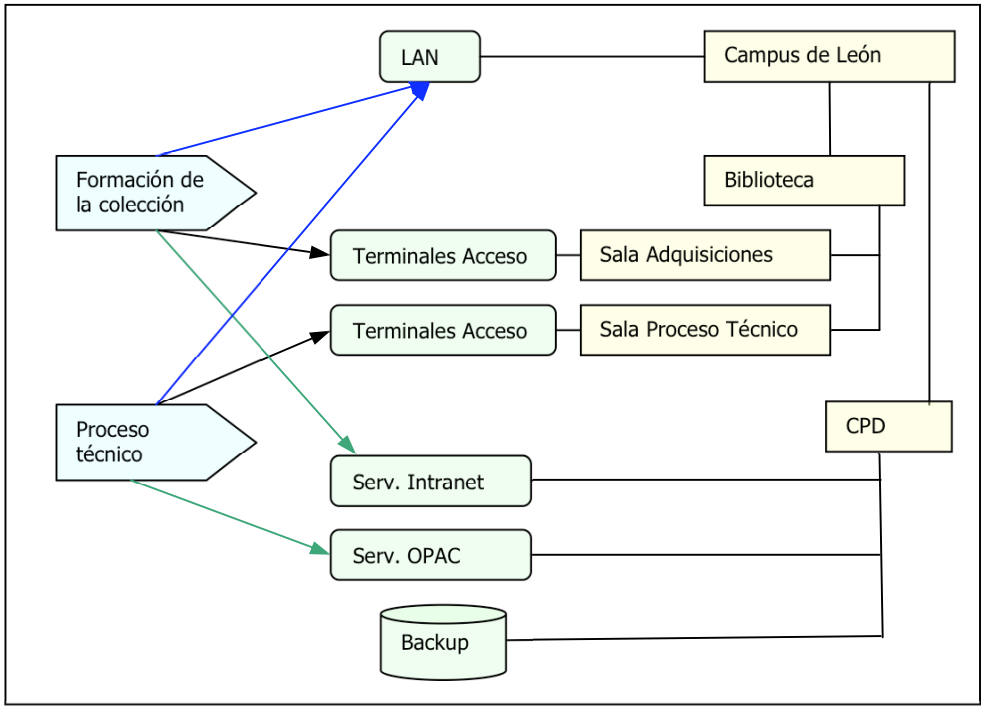


*Ilustración 3: Ejemplo dependencias entre activos*

### *Valoración al estilo de ISM³*

Se realiza a continuación un ejercicio de primera aproximación de gestión de riesgos siguiendo la metodología propuesta por *ISM³* [44]:

1. Listado de todas las **funciones de negocio** de la organización.

   Para el macroproceso del caso de estudio estas funciones son: formación de la colección, proceso técnico, mantenimiento de recursos de la información, evaluación de la colección y gestión de espacios de aprendizaje.

2. Valorar la importancia de cada función del negocio según la escala: muy poco importante (0), poco importante (1), importante (10) y muy importante (100).

   En el ejemplo: formación de la colección (100), proceso técnico (100), mantenimiento de recursos de la información (1), evaluación de la colección (10) y gestión de espacios de aprendizaje (10).

3. Se identifican los sistemas de información que soportan cada una de las funciones de negocio y se valoran sus dependencias según la escala: Ninguna (0), parcial (1), relativa (10) y absoluta (100).

   a. Ninguna (0): hay alternativas, es un requisito esporádico

   b. Parcial (1): hay alternativas asequibles (coste), es un requisito a tiempo completo

   c. Relativa (10): no hay alternativas asequibles (coste), es un requisito esporádico

   d. Absoluta (100): no hay alternativas asequibles (coste), es un requisito a tiempo completo

Para el ejemplo y los sistemas identificados:

| | **Catalogo y OPAC** | **Intranet y BB.DD.** | **FTP y Backup** | **Portal Web** |
|---|---|---|---|---|
| **Formación de la colección** | 0 | 100 | 10 | 0 |
| **Proceso técnico** | 100 | 1 | 1 | 10 |
| **Mantenimiento RR.II.** | 0 | 1 | 0 | 0 |
| **Evaluación de la colección** | 0 | 1 | 0 | 0 |
| **Gestión de espacios de aprendizaje** | 0 | 10 | 0 | 1 |

*Tabla 2: Ejemplo de valoración de dependencias entre activos*

4. Se realiza un listado con los sistemas de información/ubicación y se contestan para cada uno las siguientes preguntas:

   a. De los controles de la norma UNE-ISO/IEC 27001 cuantos son aplicables a cada sistema de información y ubicación

   b. Si un control es aplicable, se utiliza la siguiente escala para valorarlo: bajo (1, proceso indefinido), medio (10, proceso gestionado), alto (100, proceso controlado u optimizado), no aplicable (1000).

[44] Aboobacker, M. (2007) Implementing ISO 27001 using ISM³ Risk Analysis Methodology [en línea] [www.ism3.org] [consulta 29/04/2008]

5. Se utiliza una fórmula simple (sumas ponderadas y división) para calcular la escala de valores e identificar el riesgo en cada entrono de información.

# 5. Resultados

El capítulo anterior recoge los métodos que se emplean en este tipo de estudios en trabajos análogos su adaptación y aplicación para este trabajo. En el caso del análisis de riesgos se incluye a modo de ejemplo su concreción en el caso de estudio.

En este apartado se analizan los resultados obtenidos del cuestionario, la entrevista y el ejemplo de análisis de riesgos. También se comentan las aplicaciones de un estudio a nivel nacional y los elementos que pueden servir de germen para otras líneas de investigación.

Tras el estudio de los datos obtenidos se plantea un modelo preliminar para abordar la gestión de la seguridad en la BU del caso de estudio. La concreción definitiva de este modelo está sujeta a los resultados de un estudio a nivel nacional.

El modelo que se presenta es teórico. Está basado en el análisis de la documentación realizado en este trabajo de investigación y en los datos obtenidos de los métodos exploratorios empelados. Está enfocado, aunque de forma genérica, a la BU del caso de estudio.

## 5.1. Análisis del caso de estudio

El caso de estudio, la BU de la Universidad de León, se describe en el anexo.

### Resultados del cuestionario y la entrevista para el caso de estudio

Del análisis de la respuesta al cuestionario y la entrevista a la dirección de la BU del caso de estudio se obtienen los siguientes datos:

La BU del caso de estudio corresponde al **grupo de referencia** número **2** de cuatro grupos en los que se ha valorado el gasto del servicio, la utilización de su página web, su plantilla y la densidad de puestos de lectura. Este grupo de referencia servirá para establecer comparativas y agrupaciones en el caso de un estudio a nivel nacional.

La **dependencia de las TIC** ha dado como resultado el valor intermedio (**MEDIO**) de cinco valores, con posibilidades de que aumente a ALTO cuando se incorpore el repositorio institucional.

La **responsabilidad de los mandos** al igual que la **organización de la seguridad** dan como resultado valores **MUY BAJOS**, con algunas preguntas sin respuesta**.** Sin embargo, destaca el hecho de que ya se trabaja con procesos y se han identificado los activos críticos. También se pone de manifiesto una fuerte dependencia de la BU en aspectos básicos de seguridad del Servicio de Informática y Comunicaciones (SIC). Por este motivo algunas respuestas no se completan o se realizan de forma orientativa.

El resultado del **cumplimiento legislativo** es entre **MEDIO** y **ALTO** constatándose que muchas de las cuestiones planteadas se realizan de forma centralizada. Igualmente el apartado de **tecnologías** el resultado es **MEDIO** siendo las respuestas del Director del SIC debido a la mencionada dependencia de los aspectos planteados del citado Servicio.

La valoración global indica la existencia de una dependencia creciente de las TIC, y un recorrido pendiente considerable en cuanto a responsabilidad de los mandos, organización y concienciación para implementar un Sistema de Gestión de Seguridad. Sin embargo, se destaca un cumplimiento legislativo alto y una implantación considerable de tecnologías de la seguridad por lo que se exhorta a los mandos a cargo de la BU y sus sistemas de información a tomar mayor conciencia sobre la importancia del control de la seguridad de sus activos y servicios. Se propone la creación de una Comisión de seguridad en la que se

involucre personal de la BU y del SIC y de la unidad responsable del cumplimiento legislativo, con los objetivos iniciales de organización de la seguridad, concienciación y sensibilización interna y de análisis de la situación.

### Resultados del ejemplo de valoración de riesgos

La valoración de riesgos es un proceso en sí laborioso y complejo, que ha de documentarse para permitir hacer el seguimiento de los riesgos necesario para la gestión de la seguridad. En este proceso intervienen varias personas responsables de los activos por lo que es importante que la dirección establezca unos criterios de valoración para el análisis, que permita que ésta valoración sea homogénea.

La dedicación de tiempo necesaria para esta tarea y su necesidad le otorga un tratamiento particular dentro de la Gestión de la Seguridad de la Información. Para su realización ha de estar creada la Comisión que vaya a coordinar el Sistema de Gestión de la Seguridad.

Dado que tanto el listado de activos como el número de controles en muy amplio, si se realiza una valoración cualitativa o cuantitativa con el enfoque recomendado en la UNE ISO/IEC 27001 es conveniente la utilización de herramientas de gestión de riesgos que faciliten la labor y que implementan las distintas metodologías existentes.

El estilo de gestión de riesgos de ISM[3] estudiado es un enfoque cualitativo más sencillo que otras metodologías siendo también compatible con la norma UNE ISO/IEC 27001. Una hoja Excel podría servir para su realización. Este enfoque es similar al estudiado para la herramienta DAMBRORA si bien ésta no contempla el entronque con los controles de la norma.

### Propuesta de estudio a nivel nacional

El análisis de un caso de estudio aislado supone un pequeño avance en este campo. Un estudio a nivel nacional permitiría un examen de los cinco parámetros medidos en el cuestionario, la agrupación de las distintas universidades según los clusters de referencia y el análisis individual de las respuestas a las cuestiones planteadas.

Las aplicaciones de este estudio servirían para realizar el planteamiento definitivo de un modelo de gestión de la seguridad adaptados a estas organizaciones y a los distintos clusters resultantes y la posible evolución entre ellos.

También este estudio serviría para elaborar indicadores de REBIUN sobre la seguridad de las BU y para la solicitud de apoyo económico para la mejora de este aspecto de la gestión de las BU que tan alto impacto puede tener en el futuro universitario.

## 5.2. Propuesta de un modelo de gestión de la seguridad para BU

*Requisitos*

Para la integración de la gestión de la seguridad en las bibliotecas universitarias se propone un modelo que cumpla los siguientes requisitos:

1. que sea integrable en los sistemas de gestión de la biblioteca y con su organización interna;

2. que contemple la seguridad de la información tanto para la gestión interna como de cara a los servicios que se ofrecen;

3. que sea escalable y adaptable a los cambios que puedan darse en cuanto a organización interna y creación de nuevos servicios;

4. que sea proporcional a las necesidades actuales y pueda evolucionar cuando estas se modifiquen;

5. que permita cumplir con las obligaciones de la biblioteca con la comunidad universitaria y con la gestión de la universidad: y

6. que pueda ser abordada por personal de la biblioteca con el apoyo técnico necesario de los servicios de informática de la universidad.

### *Gestión por procesos en la Biblioteca Universitaria*

Dado que las bibliotecas universitarias se están gestionando cada vez más con un enfoque basado en procesos y para cumplir estos requisitos, se propone la integración de la gestión de la seguridad de la información como un macroproceso estratégico más en un supuesto mapa general de macroprocesos de la biblioteca universitaria.

La integración en los procesos de la BU de un macroproceso estratégico dedicado a la gestión de la seguridad es importante para garantizar el cumplimiento del primer requisito de los mencionados en el apartado anterior. Es también una garantía del compromiso de la dirección con las actuaciones que de este macroproceso se deriven.

La siguiente imagen muestra la situación de este macroproceso en ese supuesto mapa de macroprocesos genérico de una biblioteca universitaria.

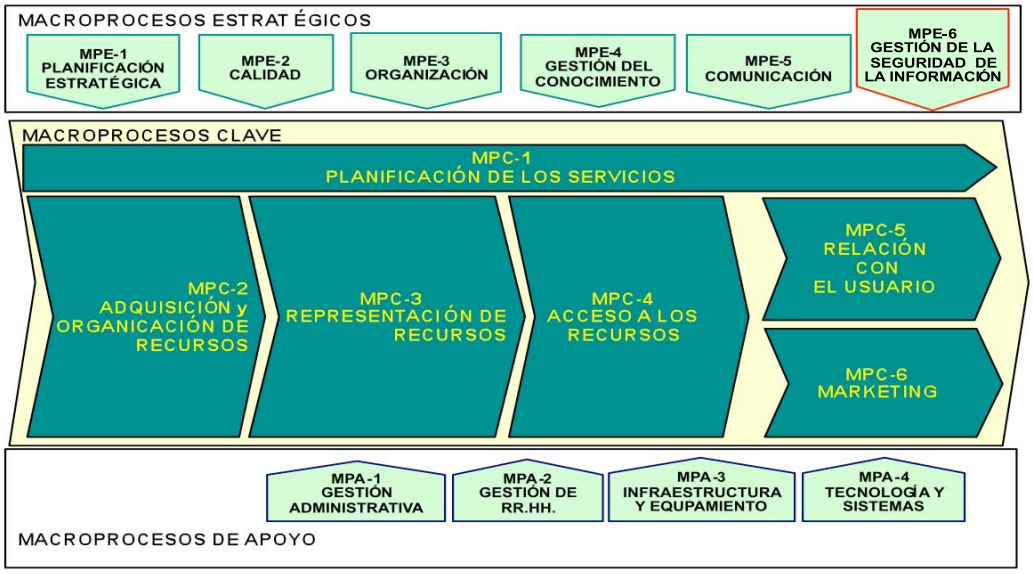


*Ilustración 3: Mapa de macroprocesos de la Biblioteca Universitaria*

### *Macroproceso de Gestión de la Seguridad de la Información*

La siguiente imagen muestra la ficha genérica del macroproceso de gestión de la seguridad de la información. Se indican además de su objetivo, y su ámbito, los procesos genéricos que podrían integrar este macroproceso. Estos estarán a su vez formados por subprocesos para cumplir los objetivos de seguridad que se establezcan.

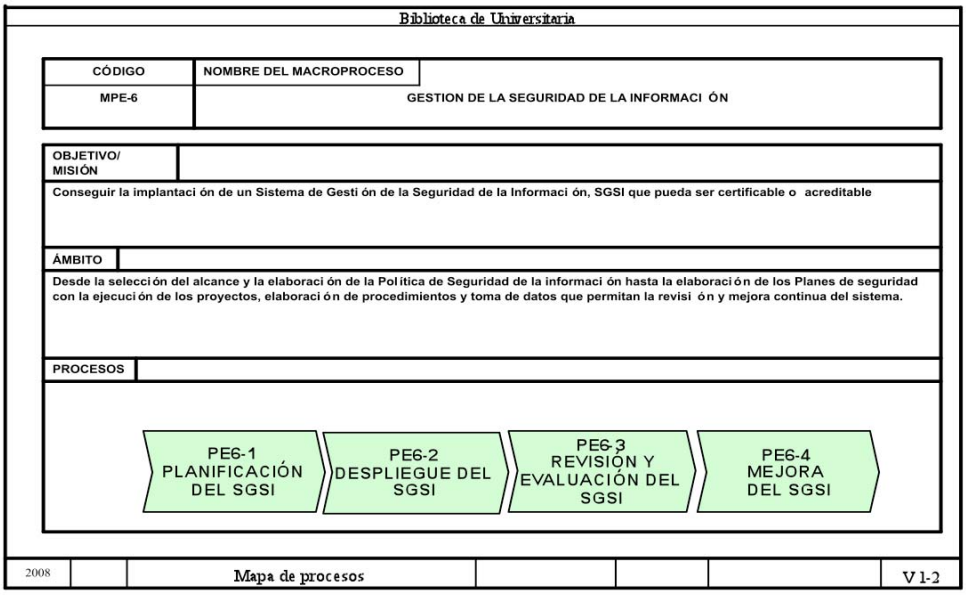


*Ilustración 3: Ficha Macroproceso Gestión de la Seguridad de la Información*

La integración en los procesos de la BU, supone también la explotación de las sinergias con el sistema de gestión de la calidad que ya está desplegado entre las BU.

### *Seguridad de la gestión interna y de los servicios*

Para caracterizar el modelo de seguridad de la biblioteca universitaria de manera que esté alineado con el segundo de los requisitos se ha de adoptar una visión general de su sistema de información. Se identifican los siguientes módulos o servicios (de gestión interna y externos) para los que se han de identificar responsabilidades sobre la información que contienen y los equipos que la soportan o transportan.

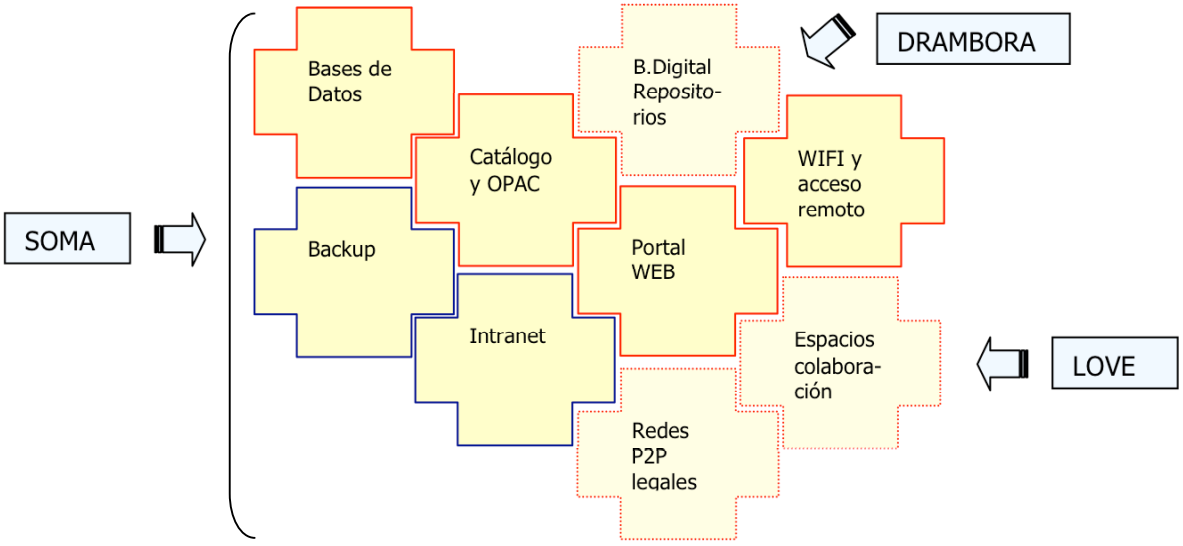


*Ilustración 3: Módulos a proteger en la Biblioteca Universitaria*

Se delimitan con colores sólidos los módulos ya establecidos en la BU del caso de estudio y en línea discontinua los módulos de evolución de futuro según la documentación analizada. Delimitados con línea azul están los módulos de uso interno y en línea de color rojo los módulos de uso externo que actualmente requieren protección.

Se apuntan las posibles implicaciones en proyectos introducidos a lo largo de este trabajo que se explicarán en el apartado de Conclusiones y Discusión.

### *Modelo de gestión de la seguridad integral*

Para cumplir los requisitos restantes, el modelo de gestión de la seguridad para BU debe abarcar los tres planos de la organización: estratégico, táctico y operativo con un **enfoque progresivo**, de forma que se vayan consiguiendo los objetivos de seguridad que se planteen de forma gradual.

Los objetivos de seguridad han de ser alcanzables y medibles, asignándose responsables para cada subproceso que se identifique. Estos subprocesos pueden seguir el estándar ISM$^3$ o su evolución SOMA como referente.

Se plantea un arranque en el plano estratégico que defina los aspectos organizativos (grupo de trabajo, responsabilidades) y las directrices generales de la **política de seguridad**. También en un primer paso ha de considerarse la puesta en marcha de un subproceso de **concienciación y formación**. Una vez se valore la estabilidad de estos procesos se ha de proceder con los procesos relativos al cumplimiento legislativo y la seguridad física y ambiental. A continuación se han de integrar los subprocesos restantes de seguridad lógica con especial énfasis en la evolución de los servicios y sistemas que los soportan. Estos procesos ya existen en gran medida, por lo que su integración será sencilla para los niveles más bajos de madurez ISM$^3$. Por último se han de considerar los aspectos de continuidad de negocio y gestión de incidentes.

Se ha de tener en cuenta el tratamiento que para la gestión de la biblioteca tengan las inversiones en soluciones técnicas y de gestión y la búsqueda de ayudas económicas para acometer los proyectos que de aquí se deriven.

# 6. Conclusiones y Discusión

## 6.1. Conclusiones

El caso de estudio es una BU que cuenta con una recientemente incorporada gestión por procesos y ha iniciado su gestión de la calidad. Hemos visto que estos factores colaboran con la integración de un sistema de gestión de la seguridad.

La BU analizada es una organización estable y en crecimiento como demuestran sus perspectivas de incorporar un repositorio institucional. Adopta, al ritmo que le permite su presupuesto, las recomendaciones de REBIUN.

El análisis de la gestión de la seguridad refleja una creciente dependencia de las TIC, la existencia de mecanismos de seguridad implantados a nivel general por la universidad y la ausencia de una organización de seguridad propia de la BU y del control de gestión por parte de la dirección de la BU.

La gestión de riesgos puede suponer un considerable esfuerzo para una organización enfocada a los usuarios. Debe realizarse de forma sencilla y utilizar herramientas adaptadas a las necesidades específicas de los servicios que se quieran proteger.

Según los resultados obtenidos, para una organización como la BU estudiada, sería recomendable el enfoque planteado por ISM$^3$. Este enfoque permite una introducción gradual y adaptada a las circunstancias organizativas a la gestión de la seguridad. El reparto de procesos entre las distintas áreas implicadas sería posible y facilitaría a la dirección una visión de conjunto sobre la seguridad de los servicios de la BU.

También es recomendable en una primera aproximación reducir el ámbito de aplicación del SGSI a un servicio determinado que ha de ser seleccionado por su alto nivel de riesgo.

Se propone un modelo que debe concretarse tras el análisis a nivel nacional y que comprende los elementos organizativos para la consecución de los objetivos de seguridad de acuerdo con consideraciones de negocio. Por tanto, además del compromiso de la dirección se han de reunir en un grupo de trabajo transversal o Comisión de seguridad, las personas correspondientes a las áreas organizativas dentro y fuera de la BU con responsabilidad directa sobre activos de la BU.

Del cuestionario a la BU del caso de estudio se deduce que dada la dependencia de los activos de la BU del servicio SIC, se ha de contar con la presencia en el citado grupo de trabajo del responsable de estos activos. Así mismo, aquellos aspectos (p. ej.: cumplimiento legislativo) de la seguridad de la BU que se gestionen de forma centralizada en la Universidad deben estar representados en el grupo que se reúna para este cometido.

Dada la interrelación de la seguridad de las TIC de la BU con otras áreas de la Universidad, la gestión de la seguridad de la misma debe pertenecer a un programa más amplio de gestión de la seguridad de las TIC a nivel de la universidad en general. No obstante, la acreditación de la seguridad puede realizarse exclusivamente para el ámbito que se defina, es decir para la biblioteca o alguno de sus servicios.

## 6.2. Discusión

Después del análisis del caso de estudio y del objeto de estudio se plantean distintas formas de ampliar este estudio en investigaciones posteriores.

Referente a la gestión de la seguridad el apartado anterior concluye con la necesidad de extender este **análisis a nivel nacional** lo que favorecería el desarrollo y completitud del modelo propuesto.

Otra opción, muy interesante si las BU se decantan por la utilización de un modelo de madurez, reside en la colaboración con ISECOM en el mencionado **proyecto SOMA** (*Security Operations Maturity Architecture*) dirigido a estructurar y medir con precisión y sencillez la seguridad operacional y el proceso de gestión.

Se ha mencionado también la elaboración de un **catálogo de amenazas** propias de la BU que sirva para un análisis de riesgos específico. Igualmente y enfocadas a gestión de riesgos en repositorios y bibliotecas digitales se abren vías de estudio sobre la aplicación de la herramienta **DAMBRORA**.

Por otra parte es también una alternativa de estudio con un contenido más técnico la profundización en el proyecto de entorno colaborativo **LOVE** (*Learning Object Virtual Exchange*) para bibliotecas digitales, implementado en la biblioteca NDSL (http://www.ndsl.org) de la universidad de Florida-Gainesville (Chen, Choo y Chow, 2006).

Estas alternativas no son excluyentes e individualmente o en conjunto van a favorecer la visibilidad de la BU en los entornos de investigación en este campo. Adicionalmente, involucrarse en cualquiera de estos proyectos va a reportar los beneficios de contribuir a una estandarización en el campo de la gestión de la seguridad que contemple el caso particular de las organizaciones intensivas en información que son las BU.

En cualquier caso, se pone de manifiesto la necesidad de incorporar de forma gradual una gestión de la seguridad a las bibliotecas universitarias que cumpla los objetivos de: conseguir una acreditación que va a ser esencial para la promoción de la BU y de la Universidad en el nuevo entorno universitario globalizado; y contribuir a la difusión de la utilización de las medidas de seguridad por la comunidad universitaria y por ende, dada su imbricación en la sociedad, favorecer una Sociedad de la Información más confiable.

# 7. Bibliografía


1. AENOR (2001) Informe UNE 71501-1 IN. Tecnología de la Información (TI). Guía para la gestión de la seguridad TI. Parte 1: Conceptos y modelos de seguridad TI.

2. AENOR (2001) Informe UNE 71501-2 IN. Tecnología de la Información (TI). Guía para la gestión de la seguridad TI. Parte 2: Gestión y planificación de la seguridad TI.

3. AENOR (2001) Informe UNE 71501-3 IN. Tecnología de la Información (TI). Guía para la gestión de la seguridad TI. Parte 3: Técnicas para la gestión de la seguridad TI.

4. AENOR (2007) Norma española UNE-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

5. Arora, A. et al. (2004) An ounce of prevention vs. a pound of cure: how can we measure the value of IT security solutions? *Lawrence Berkeley National Laboratory. Paper LBNL-54549.* [en línea] http://repositories.cdlib.org/lbnl/LBNL-54549[Consulta 24/04/2008]

6. Balagué, N., Rey, C. y Falomir, V. (2006) Evaluación y Gestión de la Calidad de las Bibliotecas Universitarias. Marketing y Comunicación: Estado de la cuestión y propuestas de mejora. Universidad Politécnica de Cataluña.

7. Barrionuevo, L. y Marsá, M. (2007) La biblioteca universitaria de León: pasos hacia la convergencia europea. *Actas del VIII Congreso ISKO-España*. Universidad de León.

8. Castells, M. (2002) La Era de la Información. Vol. I: La Sociedad Red. México, Distrito Federal: Siglo XXI Editores.

9. Cebrian, J. L. (1988). La red. Barcelona. Círculo de Lectores

10. Chandorkar, T.G. (2005) Users, Technology and Space in Libraries in the Digital Age. [Tesis] Massachusetts Institute of Technology.

11. Chen, S-S., Choo, C-Y y Chow, R.Y. (2006) Internet Security: A Novel Role/Object Based Access Control for Digital Libraries. Journal of Organizational Computing and Electronic Commerce, 16(2), 87-103 University of Florida.

12. Comisión internacional sobre la educación para el siglo XXI, presidida por Jaques Delors, Informe a la UNESCO, 1996. La educación encierra un tesoro.

13. Declaración de Bolonia desde la página el Ministerio de Educación y Ciencia para el Espacio Europeo de Educación Superior. [en línea] http://wwwn.mec.es/univ/jsp/plantilla.jsp?id=3501][consulta: 11/05/2008]

14. Díaz, R. (2005) Seguridad en Redes Telemáticas. SGSI: Sistemas de Gestión de la Seguridad ISO 17799 y UNE 71502.universidad Politécnica de Madrid.

15. Druker, P. (1974) La sociedad post-capitalista. http://www.sans.org/reading_room/whitepapers/policyissues/1570.php

16. EDUCAUSE (2004) Surveying the digital landscape evolving Technologies 2004. *The EDUCAUSE Evolving Technologies Committee* [en línea] [http://www.educause.edu/EvolvingTechnologiesReports/869] [consulta: 22/05/2008]

17. Hurley, J.S. (2002) Overview of Security. *EDUCAUSE Evolving Technologies Commitee*

18. IFLA (2005) Manifiesto de Alejandría sobre Bibliotecas: la Sociedad de la Información en Acción. International Federation of Library Associations and Institutions. [en línea] [http://www.ifla.org/III/wsis/AlexandriaManifesto-es.html][Consulta 24/04/2008]

19. Inmor, S., Esichaikul, V. y Batanov, D.N. (2003) A Security-Oriented Extension of the Object Model for Development of an Information System. *Information System Security; Application and System Development security. May / June*

20. ISM3 Consortium (2007) Information Security Management Maturity Model V2.0. ISM3 Consortium [en linea] [www.ism3.com][Consulta 24/04/2008]

21. ISO/IEC (2005) International Standard ISO/IEC 27002:2005 E. Information technology—Security techniques—Code of practice for information security Management.

22. ISO/IEC (2007) International Standard ISO/IEC 27006:2007 E. Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management Systems.

23. Jonhstone S.M. (2005) Open educational resources serve the World: Sharing educational resources over the Internet provides multiple benefits, from academic collaboration to economic developement [en línea]. *Educause Quaterly, n. º 3* [http://www.educause.edu/ir/library/pdf/EQM0533.pdf] [consulta: 02/05/2008]

24. Krause, M. y Tipton, H.F. (1999) Handbook of Information Security Management. *Auerbach Publications*

25. Lane, T. (2007) Information Security Management in Australian Universities: an exploratory analisys. Queensland University of Technology. [en línea] http://adt.library.qut.edu.au/adt-qut/public/adt-QUT20071109.083418/[consulta: 11/05/2008)

26. MacHugh, A. et al. (2007) Risk Management foundations for digital libraries: DRAMBORA (Digital Repository Audit Method Based on Risk Assessment). HATII, University of Glasgow. [en línea] http://www.hatii.arts.gla.ac.uk/research/publications.html [consulta: 11/05/2008]

27. Majó, J. (1997). Chips, cables y poder. Barcelona. Planeta

28. Majó, J. (1998). Educación, ciencia y tecnología.

29. Majó, J. (200?) Nuevas Tecnologías y Educación [en línea] http://www.uoc.edu/web/esp/articles/joan_majo.html [consulta: 11/05/2008]

30. Malone, T.F. y Yohe, G.W. (2002) Knowledge partnerships for sustainable, equitable, and stable society. *Journal of Knowledge Management, Vol. 6, n. º 4.*

31. Margaix Arnal, Dídac (2007) Conceptos de web 2.0 y biblioteca 2.0: origen, definiciones y retos para las bibliotecas actuales. *El Profesional de la Información 16(2):pp. 95-106.*

32. Masuda, Y. (1981)The Information Society as Post-Industrial Society. Ed. World Future Society, Estados Unidos.

33. MEC (2003) La integración del Sistema Universitario español en el Espacio Europeo de Educación Superior: documento marco.

34. Ministerio de las Administraciones Públicas, (2006) MAGERIT V2.0 Metodología y Análisis de Gestión de Riesgos en los Sistemas de Información: 1- Método. MAP. [en línea][http://www.csi.map.es/csi/pg5m20.htm] [consulta 22/04/2008]

35. Nyanchama, M. (2005) Enterprise Vulnerability Management and its Role in Information Security Management. Information Security Management (July/August)

36. Parker, D. (2006) Making the Case for Replacing Risk-based Security. *ISSA Journal.*

37. Pernias Peco, P. y Marco Such, M. (2007) Motivación y valor del proyecto Open Courseware: la Universidad del S.XXI. *En Contenidos educativos en abierto* [monográfico en línea] *Revista de universidad y Sociedad del Conocimiento (RUSC). Vol. 4, n. º 1 UOC.* [en línea] http://www.uoc.edu/rusc/4/1/dt/esp/pernias_marco.htm] [consulta: 02/05/2008]

38. Pols, J. (2008) The Fallacy of Security ROI. *ISSA Journal*.

39. REBIUN (2006) Anuario de las bibliotecas universitarias y científicas españolas [en línea] [http://www.rebiun.org/] [consulta: 22/03/2008]

40. REBIUN, Plan estratégico 2007-2010

41. Rius, C. (2007) El contenido abierto es una publicidad potentísima para las universidades, entrevista a David Willey. *Món UOC, n. º 26* [en línea] [http://www.uoc.edu/prensa/entrevistas/wiley.html] [consulta: 11/05/2008]

42. Rowley, J. (2003) Knowledge management" the new librarianship? From custodians of history to gatekeepers to the future. *Library Management, Vol. 24, n. º 8-9, p. 433-440*

43. Schneier, B. (2000) Secrets and Lies: Digital Security in a Networked World. Whiley Computer Publishing.

44. Serradell López, E. y Juan Pérez, A.A. (2003) La gestión del conocimiento en las organizaciones intensivas en conocimiento: El caso de la universidad, en *La gestión del conocimiento en la nueva economía. Cap.8* [en línea] *Fundación UOC.* [http://www.uoc.edu/dt/20133/index.html#8][consulta: 10/04/2008]

45. Simons, W. R. (2005) The Chalenges of Network Security Remediation at a Regional University. [Tesis] East Tennessi State University

46. Tedesco, J. C. (Buenos Aires, 2003). Los pilares de la educación del futuro. [en línea] [http://www.iipe-buenosaires.org.ar/pdfs/pilares-educacion-futuro.pdf] [consulta: 11/05/2008]

47. Templeton C. (2004) Security in an open envirnoment such as University. SANS Institute

48. Thomson, S.T.C. (2006) Helping the hacker? Library Information, Security and Social Engineering. *Information Technology and Libraries. December*

49. Townley, C.T. (2001) Knowledge Management and academic libraries. *College and Research Libraries. Enero, p. 44-55*

50. Vest, C.M. (2006) Open Content and the emerging Global Meta-University [en línea]. *Educause review, mayo-junio* [http://www.educause.edu/ir/library/pdf/ERM0630.pdf] [consulta: 02/05/2008]

# 8. Anexos

## 8.1. La Universidad de León

Con objeto de situar la biblioteca en la organización a la que pertenece se incluyen a continuación datos sobre la ULE:

La ULE según su anterior Rector "por ser joven tiene la pujanza de la edad y la experiencia acumulada del buen hacer de sus progenitores...". Por el número de alumnos está entre las universidades españolas en el rango de 10-20 mil alumnos, junto con otras 15 universidades de las 48 U. públicas y 20 privadas. Según la estadística del MEC sobre universidades del curso 2006-2007 tiene 13.850 alumnos; en su mayoría jóvenes menores de 25 años y españoles.

En su organización docente e investigadora, la ULE cuenta con 8 Facultades, 2 Escuelas Superiores y 5 Escuelas Universitarias y 26 departamentos y tiene adscritos 6 Institutos de Investigación, 2 Cátedras, 1 Centro de formación avanzada, 4 Fundaciones y 4 Centros Tecnológicos. Además de los órganos de gobierno comunes en las universidades públicas (Rectorado, Gerencia, Secretaría General, Consejo Social, Claustro, Juntas...), su gestión está repartida en 10 Vicerrectorados. La Biblioteca está adscrita al Vicerrectorado de Innovación Tecnológica.

En cuanto a su funcionamiento interno, se caracteriza por los parámetros de los organismos públicos. Su plantilla se divide en Profesorado y PAS (Personal de Administración y Servicios), ambos regulados por la legislación correspondiente. Se rige por la LOU y su desarrollo, con la supervisión de los organismos correspondientes de la Junta de Castilla y León y del Ministerio; y está sometida a los avatares políticos de los equipos rectorales elegidos en referéndum. Administrativamente se rige por su reglamento interno y conserva la inercia característica de estas instituciones.

Recursos corporativos y recursos físicos: La ULE cuenta con dos Campus uno en León y otro en Ponferrada. El Campus de León está formado por 11 edificios para Facultades y Escuelas y 8 edificios anexos (rectorado, clínica veterinaria, animalario, CRAI-TIC, aulario, pabellón deportivo, centro de idiomas y Biblioteca General).

El Campus de Ponferrada está ubicado en el antiguo complejo hospitalario, dividido en tres edificios llamados A, B, y C. Consta también de un Complejo de Servicios, con tres partes diferenciadas: Edificio de Servicios Múltiples y Salón de Actos, Edificio de Cafetería y Comedor y Edificio de Biblioteca. Otros edificios del Campus contienen un Aulario, un Centro de Investigación, un Plató 2 (Cine). También dispone de un Complejo Deportivo (piscina cubierta, gimnasio, pabellón deportivo, campos de atletismo y fútbol). Así mismo, está próximo a finalizar un edificio de guardería.

En cuanto al uso de la tecnología, tiene los recursos necesarios para el desarrollo de sus tareas docente, investigadora y administrativa. Las redes telefónica e informática permiten la conexión entre todos los centros, servicios y usuarios y con el exterior. Cuenta con redes WAN separadas para Profesorado, PAS y Estudiantes. Utiliza para su gestión interna programas específicamente diseñados para la Administración.

Con objeto de facilitar el acceso de la Comunidad Universitaria a la Sociedad de la Información, tiene centralizadas una serie de actividades de apoyo para el aprendizaje y la investigación: el despliegue de tecnologías inalámbricas, la apertura de aulas multimedia, la creación y fortalecimiento del campus virtual, la elaboración de contenidos docentes digitales, la generalización de protocolos de tutorías en red y el desarrollo de programas de formación del PDI, de los alumnos y del PAS en el uso de las TIC.

Los presupuestos y financiación son los propios de las universidades públicas, Puntualmente pueden existir acuerdos con empresas para la financiación de las actividades de Institutos de Investigación.

Su plantilla está formada (datos aproximados) por 1120 profesores (funcionarios y contratados) y 450 PAS (entre funcionarios y laborales).

## 8.2. La Biblioteca Universitaria de la ULE

En cuanto a la Biblioteca Universitaria, está constituida por una Biblioteca General, 4 Bibliotecas de áreas temáticas y una biblioteca de Campus (Ponferrada). La Biblioteca General está ubicada en un edificio de diseño reciente –inaugurado en 1995– de 4 plantas. Tiene encomendadas la realización de tareas centralizadas, como adquisiciones, proceso técnico, préstamo interbibliotecario, gestión de recursos electrónicos, mantenimiento de los servicios electrónicos (catálogo automatizado, gestión de la web y la intranet); está integrada por las siguientes unidades:

- Unidad de Adquisiciones
- Unidad de Publicaciones Periódicas
- Unidad de Proceso Técnico y Normalización
- Unidad de Préstamo Interbibliotecario y Acceso al Documento
- Unidad de Atención al Usuario
- Unidad de Recursos Digitales y Audiovisuales
- Unidad de Automatización
- Unidad de Gestión Administrativa y Económica

Las bibliotecas de áreas temáticas son cuatro:

- Ciencias Experimentales (con 4 puntos de servicio)
- Humanidades y Ciencias Sociales (con 2 puntos de servicio)
- Ciencias Económicas y Jurídicas (con 3 puntos de servicio)
- Ingenierías (con 3 puntos de servicio)

En los puntos de servicio o bibliotecas de Centro, se realizan las tareas de gestión y evaluación de la colección (tanto de los fondos que se hallan en las propias bibliotecas como los que permanecen todavía en los Departamentos) y la atención y formación de usuarios.

En el Campus de Ponferrada, sólo hay una Biblioteca, que atiende a todos los usuarios del Campus, y cuyo fondo abarca todas las disciplinas que se imparten en él.

Según su reglamento para su funcionamiento tienen los siguientes órganos colegiados: Comisión General de Bibliotecas, Comisiones de Áreas Temáticas y Consejo de Dirección

Infraestructuras. La Biblioteca Universitaria dispone de casi 2.800 puestos (en la General 590 y en las restantes Bibliotecas, 2.200. En conjunto dispone de 70 puestos informatizados para consulta de OPAC's y 15 ordenadores conectados a Internet a disposición de los usuarios. En la Biblioteca General hay, además, 40 despachos

individuales de investigación con toma de red. De estos, la mayoría están equipados con PC con conexión a la red y con software de acceso a Internet y edición.

Para el servicio de Reprografía cuenta con fotocopiadora, lector-reproductor de microformas, escáner, acceso directo a Internet, OCR, software para digitalizar documentos, convertidor de papel a microfilm, etc.

En el CAAD (Centro de Apoyo al Aprendizaje y a la Docencia) hay 15 puestos equipados para edición/grabación de video y audio. Los equipos audiovisuales incluyen pletinas de casetes, giradiscos, amplificador, DVD's, Laser disc, mesa mezcladora y edición SVHS, proyectores (video, diapositivas, transparencias, opacos), televisores, pantallas acústicas y sistema de megafonía.

La Sala de Conferencias tiene capacidad para 70 personas y 5 ponentes y está equipada con equipos para la proyección, visionado y audición colectivos, PC y videoconferencia. También hay disponible una sala con capacidad de hasta 10 personas para videoconferencia.

Algunos depósitos cuentan con estanterías Compactus (en la Biblioteca General, Educación, Biológicas).

Colección. El fondo bibliográfico está compuesto por 450.000 volúmenes, 13.300 títulos de revistas en papel, y casi 9.000 recursos electrónicos (libros, revistas y bases de datos).

La gestión automatizada de la colección se hace, desde septiembre de 2002, mediante un programa de la empresa Innovative INNOPAC Millenium.

Cuenta con una página web remodelada que proporciona información y acceso a sus servicios en línea, mediante formularios interactivos.

Recursos humanos: Los servicios de la biblioteca cuentan con la plantilla[45] de personal funcionario (23) y laboral (48). Los puestos de los funcionarios son: Director (1), Facultativos y Ayudantes de Biblioteca (18), Gestores responsables (2) y técnicos (1) y Subalterno (1). Los laborales son Técnicos Especialistas (20) y Oficiales (28).

Los fondos de los libros y revistas ubicados en los Departamentos, están adscritos a las bibliotecas de Centro correspondientes.

Recursos económicos: Según el Reglamento de la Biblioteca (Art. 14.4) el presupuesto de la BU debe adecuarse a los planes estratégicos y objetivos de la ULE, para que el servicio sea un instrumento eficaz del desarrollo académico y científico de la institución. La BU es también responsable de la gestión de los recursos que le correspondan y de su ejecución.

En el presupuesto general anual de la universidad, no existe ninguna partida específica para la biblioteca, es decir los gastos de personal, mobiliario, equipamiento, etc. no están separados del resto de la Universidad. Las únicas partidas que pueden atribuirse a la biblioteca son las relativas al Fondo bibliográfico (422D-624) y Equipos para procesos de Información (422D-627) ambas dentro de la Inversión nueva asociada al funcionamiento operativo de servicios (422D-62); y en los Servicios Complementarios a la enseñanza (423B) la relativa a Prensa, revistas, libros y otras publicaciones (220.01). La adquisición de fondos bibliográficos y documentales está cofinanciada por Caja España.

[45] Según RPT de 2004 publicada en BOCyL el 16 de febrero.

*Servicios y productos que presta la unidad.*

Según el Reglamento de la Biblioteca universitaria de la ULE pueden agruparse en:

1. Acceso al documento

   - Consulta en sala: el horario es de 9 a 21 h. en la Biblioteca General y las bibliotecas de Centro, con horarios especiales en vacaciones y exámenes.

   - Préstamo domiciliario: pueden acceder a este servicio los usuarios que cuenten con carné universitario (alumnos, profesores, investigadores, alumnos de doctorado, becarios, PAS...) o bien tarjeta de usuario externo. Los plazos de devolución y condiciones del préstamo están regulados en la Normativa de Préstamo. Existe la posibilidad de realizar reservas y consultar on-line el estado de los préstamos realizados. Hay documentos excluidos de este servicio.

   - Préstamo Interbibliotecario: es un servicio (no gratuito) que consiste en la obtención de documentos de otras bibliotecas nacionales o extranjeras (monografías, tesis, congresos, fotocopias de artículos de revistas o capítulos de libros y reproducciones en microforma) por un tiempo determinado. La duración y condiciones del préstamo son variable, y los originales deben consultarse en sala.

   - Reproducción de documentos: escáner, reprografía, edición, digitalización y copia de los documentos que no pueden prestarse. Copias de artículos de revista.

   - Acceso al documento en línea: acceso a bases de datos referenciales y a texto completo, y a libros y revistas electrónicos.

2. Acceso a la información

   - Información general de la biblioteca de la ULE: desde su página web, con guías y en las propias bibliotecas. Servicio 24 horas «Pregunte al bibliotecario» y «Preguntas más frecuentes».

   - Información bibliográfica de fondos: mediante el OPAC, acceso al catálogo general automatizado y mediante un servicio de Bibliografía recomendada: acceso a los libros recomendados por los profesores en cada una de las asignaturas. Se puede buscar por el nombre de la asignatura o del profesor, y da información sobre el número de volúmenes existentes y el lugar donde se encuentran.

   - Información bibliográfica externa: soporte, información y localización de bibliografía de fondos externos. Acceso a catálogos de bibliotecas vía Z39.50

   - Difusión de la Información: Catálogo general, de publicaciones periódicas, de recursos electrónicos, de Novedades y nuevas adquisiciones, y Tesis doctorales en microficha

3. Formación de Usuarios: tienen como objetivo enseñar a los miembros de la comunidad universitaria a utilizar de manera eficaz la Biblioteca de la Universidad de León y sus recursos de información. Consisten en seminarios, cursos generales y específicos y visitas guiadas.

4. Extensión bibliotecaria: tiene como objetivo la difusión a la comunidad universitaria y a la sociedad en general de los fondos y actividades de la Biblioteca.

Sugerencias, quejas, reclamaciones, etc. mediante formularios en la web o en los buzones de todas las bibliotecas.

## 8.3. Datos para el ensayo de evaluación de riesgos

*Macroproceso MP2*

Los procesos que forman este macroproceso son:

### Formación de la colección

- Selección de recursos de información: monografías, materiales especiales y publicaciones periódicas impresas
- Selección de recursos de información: recursos electrónicos
- Creación y mantenimiento de fondos de gasto
- Creación y mantenimiento de registros de proveedor
- Elaboración de listas de selección: publicaciones periódicas y recursos electrónicos
- Tramitación de órdenes de compra: monografías y materiales especiales
- Tramitación de órdenes de compra: publicaciones periódicas impresas y recursos electrónicos
- Elaboración y tramitación de pedidos desde listas de selección: monografías y materiales especiales
- Elaboración y tramitación de pedidos a partir de órdenes de compra: monografías y materiales especiales
- Suscripción de recursos de información gestionados fuera de concurso público
- Suscripción de recursos de información gestionados a través de concurso público
- Documento de reclamaciones para publicaciones periódicas
- Evaluación de proveedores de monografías y materiales especiales
- Recepción e ingreso de recursos de información pedidos a través de biblioteca: monografías y materiales especiales
- Recepción e ingreso de recursos de información: publicaciones periódicas impresas
- Itinerario de la documentación en la BG
- Tramitación de facturas de recursos de información gestionados fuera de concurso público
- Tramitación de documentación administrativa-contable de recursos de información gestionados a través de concurso público
- Tramitación de facturas de solicitudes procedentes de compra directa
- Recepción e ingreso de publicaciones editadas por la ULE

- Manual para la gestión de donaciones bibliográficas
- Canje e intercambio

### Proceso técnico

- Catalogación automatizada
- Creación de entradas de autoridad
- Clasificación sistemática
- Indización por materias
- Registro de copias
- Asignación de signaturas topográficas
- Actuaciones para identificación y seguridad
- Control de autoridades
- Mantenimiento de registros

### Mantenimiento de los recursos de información

- Ordenación y localización
- Recuento de la colección
- Encuadernación de fondos
- Mantenimiento de URLs en la colección electrónica
- Gestión de reclamaciones por enlaces rotos en recursos electrónicos suscritos.

### Evaluación de la colección

- Estudios de circulación de fondos.
- Reasignación de ubicaciones
- Expurgos de monografías.
- Expurgo de publicaciones periódicas.
- Bajas en recursos electrónicos

### Gestión de espacios de aprendizaje

- Uso de equipos
- Gestión de reserva de salas
- Gestión de los despachos de uso individual
- Identificación y señalización de espacios
- Gestión para la apertura 24 horas

## 8.4. Cuestionario

**[A.]** Indicadores básicos de referencia: el propósito de este apartado es poder analizar en conjunto los datos de las bibliotecas universitarias que eventualmente participen en una encuesta basada en este cuestionario.

| **INDICADORES BÁSICOS DE REFERENCIA**<br>**Puntuación: 0=muy bajo; 1=bajo; 2=medio; 3=alto; 4=muy alto.** | |
|---|---|
| Biblioteca de la universidad (opcional) | |
| A-1.- ¿Gasto total del servicio de biblioteca por usuario?<br>Muy bajo: 0-50 €; Bajo: 50- 100 € ; Medio: 100-200 €<br>Alto: 200- 300 €; Muy alto: > 300 € | |
| A-2.- ¿Visitas web por usuario?<br>Muy bajo: 0-20; Bajo: 20 - 50 ; Medio: 50-100<br>Alto: 100 - 300 ; Muy alto: > 300 | |
| A-3.- ¿% de técnicos sobre el total de la plantilla?<br>Muy bajo: 0-10%; Bajo: 10 - 30 %; Medio: 30-60 %<br>Alto: 60 – 80 %; Muy alto: > 80% % | |
| A-4.- ¿Índice del número de estudiantes por puesto de lectura informatizado?<br>Muy bajo: >400; Bajo: 300-400 ; Medio: 100-300<br>Alto: 40-100; Muy alto: 0-40 | |
| **PUNTUACIÓN** | |

**Comentarios a las preguntas anteriores**

| **GRUPOS DE REFERENCIA** | |
|---|---|
| De 0 a 4 | Grupo 1 |
| De 4 a 8 | Grupo 2 |
| De 8 a 12 | Grupo 3 |
| De 12 a 16 | Grupo 4 |

**[B.]** Dependencia de la BU de las TIC: esta sección servirá para identificar el grado de subordinación de los procesos y servicios de la biblioteca a los sistemas de información basados en las TIC.

| **DEPENDENCIA DE LAS TIC**<br>**Puntuación: 0=muy bajo; 1=bajo; 2=medio; 3=alto; 4=muy alto.** | |
|---|---|
| B-1.- Valor apreciado del repositorio institucional con sede en la BU para la comunidad universitaria | |
| B-2.- Valor apreciado de la propiedad intelectual almacenada o transmitida por los servicios de la biblioteca | |
| B-3.- Valor apreciado de los recursos electrónicos ofertados por la biblioteca por la comunidad universitaria | |
| B-4.- Impacto en el servicio de una caída total de la red de la biblioteca | |
| B-5.- Impacto en el servicio de una caída total de Internet | |
| B-6.- Sensibilidad apreciada de los usuarios a la privacidad de sus operaciones | |
| B-7.- Sensibilidad apreciada de los bibliotecarios hacia la confidencialidad de los datos que manejan en su actividad | |
| B-8.- Impacto en la reputación de la biblioteca de un incidente grave de seguridad | |
| B-9.- Planes de outsourcing de servicios informáticos de la BU | |
| B-10.- Valor apreciado del acceso a los servicios de la biblioteca fuera del campus | |
| **PUNTUACIÓN** | |

**Comentarios a las preguntas anteriores**

| **TOTAL PUNTUACIÓN DEPENDENCIA DE LAS TIC** | |
|---|---|
| De 0 a 8 | Muy baja |
| De 8 a 16 | Baja |
| De 16 a 24 | Media |
| De 24 a 32 | Alta |
| De 32 a 40 | Muy alta |

*Aspectos a evaluar:*

**[C.]** Responsabilidad de los mandos: se analizará la disposición de la dirección de la Biblioteca y de los Servicios Informáticos y otras unidades relacionadas para abordar la gestión de la seguridad.

| **RESPONSABILIDAD DE LOS MANDOS**<br>**Puntuación: 0=no definido;**<br>**1=planificado;**<br>**2=parcialmente implementado;**<br>**3=implementado;**<br>**4=optimizado.** | |
|---|---|
| C-1.- ¿Existe un programa escrito para abordar la seguridad de la información? | |
| C-2.- ¿Están identificados los activos críticos y las funciones que estos soportan? | |
| C-3.- ¿Existe un presupuesto asignado a la gestión de la seguridad TIC de la BU? | |
| C-4.- ¿Existe un informe periódico a la dirección del estado de la seguridad de la información de los activos de la BU? | |
| C-5.- ¿Existen controles en los procesos de la BU para garantizar la seguridad de la información que manejan? | |
| C-6.- ¿Existe en la BU un sistema de calidad según IS0 9001? | |
| C-7.- ¿Está organizada la gestión de la BU en torno a procesos? | |
| C-8.- ¿Existe en la BU algún proceso basado en gestión de riesgos? | |
| C-9.- ¿Existen políticas de seguridad de la información? | |
| C-10.- ¿Existe un proceso de gestión de las tecnologías de la información controlado por la dirección de la biblioteca? | |
| **PUNTUACIÓN** | |

**Comentarios a las preguntas anteriores**

| **TOTAL PUNTUACIÓN RESPONSABILIDAD DE LOS MANDOS** | |
|---|---|
| De 0 a 8 | Muy bajo |
| De 8 a 16 | Bajo |
| De 16 a 24 | Medio |
| De 24 a 32 | Alto |
| De 32 a 40 | Muy alto |

**[D.]** Enfoque organizativo de la gestión de la seguridad (personas y procesos): se analizará la disposición y preparación de la organización para asumir las responsabilidades asociadas a la gestión de la seguridad; y se analizará el impacto organizativo a nivel de procesos que puede suponer introducir la gestión de la seguridad.

| **ORGANIZACIÓN DE LA SEGURIDAD (PERSONAS /PROCESOS)**<br>**Puntuación: 0=no definido;**<br>**1=planificado;**<br>**2=parcialmente implementado;**<br>**3=implementado;**<br>**4=optimizado.** | |
|---|---|
| D-1.- ¿Existe un programa escrito para concienciar a los empleados sobre la seguridad de la información? | |
| D-2.- ¿Están identificados los responsables de los activos críticos de la BU? | |
| D-3.- ¿Se han identificado las necesidades formativas de los responsables de la seguridad de las TIC en la BU? | |
| D-4.- ¿Están identificados los responsables de los procesos críticos que se ven afectados por la seguridad de las TIC? | |
| D-5.- ¿Existe un programa escrito para concienciar a los usuarios sobre la seguridad de la información? | |
| D-6.- ¿Existe una arquitectura de seguridad definida para garantizar la seguridad de los sistemas dedicados a los servicios de la BU? | |
| D-7.- ¿Se controlan los procedimientos de seguridad aplicables a los servicios de la BU? | |
| D-8.- ¿Existe un procedimiento de actuación en caso de desastre? | |
| D-9.- ¿Existen copias de seguridad actualizadas y comprobadas, en lugar seguro para reiniciar la actividad en el menor tiempo posible en caso de desastre? | |
| D-10.- ¿Se comprueba el funcionamiento de los procedimientos de recuperación de desastres? | |
| **PUNTUACIÓN** | |

**Comentarios a las preguntas anteriores**

| **TOTAL PUNTUACIÓN ORGANIZACIÓN DE LA SEGURIDAD (PERSONAS /PROCESOS)** | |
|---|---|
| De 0 a 8 | Muy baja |
| De 8 a 16 | Baja |
| De 16 a 24 | Media |
| De 24 a 32 | Alta |
| De 32 a 40 | Muy alta |

**[E.]** Cumplimiento legislativo: se analizará si se conoce y contempla la legislación aplicable a la actividad de la biblioteca universitaria.

| **CUMPLIMIENTO LEGISLATIVO**<br>**Puntuación: 0=no definido;**<br>**1=planificado;**<br>**2=parcialmente implementado,**<br>**3=implementado;**<br>**4=optimizado;** | |
|---|---|
| E-1.- ¿Existen procedimientos en uso que garanticen la protección y privacidad en el tratamiento de datos personales conforme a la LOPD? | |
| E-2.- ¿Existe una política para estudiantes y personal que contemple el uso adecuado de materiales de propiedad intelectual depositados en la biblioteca? | |
| E-3.- ¿Existe un procedimiento para el tratamiento de contratos con terceros por vía telemática de forma segura? | |
| E-4.- ¿Existe un procedimiento que impida el uso de productos software propietario sin licencia en los equipos de la biblioteca? | |
| E-5.- ¿Existe una política que regule el uso autorizado de los documentos a disposición de los usuarios? | |
| E-6.- ¿Existen procedimientos en uso para la protección de las bases de datos de al biblioteca? | |
| E-7.- ¿Existen políticas para garantizar la seguridad de los recursos consorciados? | |
| E-8.- ¿Existe una política para fomentar el uso de buenas prácticas en cuanto al uso seguro y conforme a la ley de los recursos de la biblioteca? | |
| E-9.- ¿Existen y se aplican perfiles de autorización y mecanismos de autenticación de los usuarios autorizados para usos restringidos de los activos de la biblioteca? | |
| E-10.- ¿Existen informes periódicos de los incidentes sobre usos no autorizados de activos de la biblioteca? | |
| **PUNTUACIÓN** | |

**Comentarios a las preguntas anteriores**

| **TOTAL PUNTUACIÓN CUMPLIMENTO LEGISLATIVO** | |
|---|---|
| De 0 a 8 | Muy bajo |
| De 8 a 16 | Bajo |
| De 16 a 24 | Medio |
| De 24 a 32 | Alto |
| De 32 a 40 | Muy alto |

**[F.]** Tecnología: se evaluará someramente la percepción de la dirección de algunos aspectos de la seguridad tecnológica.

| **TECNOLOGÍA DE SEGURIDAD**<br>**Puntuación: 0=no definido;**<br>**1=planificado;**<br>**2=parcialmente implementado;**<br>**3=implementado;**<br>**4=optimizado;** | |
|---|---|
| F-1.- ¿Se actualiza cada equipo de la biblioteca regularmente con los parches y actualizaciones de las aplicaciones y sistemas que contiene? | |
| F-2.- ¿Se verifica en cada equipo regularmente que no hay infecciones de malware? | |
| F-3.- ¿Están todos los equipos protegidos con contraseña y automatizado el sistema que obliga su complejidad, su no reutilización y los tiempos de expiración? | |
| F-4.- ¿Se guarda registro (log) de todas las actividades relacionadas con cambios de configuración de hardware o software, intentos de acceso, asignaciones de privilegios y autorizaciones? | |
| F-5.- ¿Se monitoriza en tiempo real las redes, sistemas y aplicaciones para localizar accesos no autorizados, comportamientos anómalos como virus o código malicioso e intentos de intrusión? | |
| F-6.- ¿Se emplean medidas específicas para prevenir y detectar accesos indebidos a las redes inalámbricas? | |
| F-7.- ¿Existen mecanismos para informar y responder a los eventos e incidentes de seguridad? | |
| F-8.- ¿Se cifran los datos sensibles y se guardan las claves de cifrado con la protección adecuada? | |
| F-9.- ¿Disponen los sistemas de la biblioteca de mecanismos de autorización y autenticación que apliquen al acceso a los recursos más sensibles? | |
| F-10.- ¿Los sistemas de la biblioteca aplican las prácticas de gestión de usuarios/sesión que incluyen *timeouts*, bloqueo en caso de fallo en el *login* y revocación? | |
| **PUNTUACIÓN** | |

**Comentarios a las preguntas anteriores**

| **TOTAL PUNTUACIÓN TECNOLOGÍA DE SEGURIDAD** | |
|---|---|
| De 0 a 8 | Muy bajo |
| De 8 a 16 | Bajo |
| De 16 a 24 | Medio |
| De 24 a 32 | Alto |
| De 32 a 40 | Muy alto |