Ciberseguridad y bibliotecas: apuntes para una propuesta de formación sobre riesgo tecnológico en bibliotecas

Cybersecurity and libraries: notes for a training proposal on technological risk in libraries

Juan Vte. Oltra Gutiérrez
jvoltra@omp.upv.es
PDI Universitat Politècnica de València. Departamento de Organización de Empresas. Escuela Técnica Superior de Ingeniería Informática.
ORCID https://orcid.org/0000-0002-7765-1085

Rafael Ibáñez-Hernández
ribanez@aytoburgos.es
Ayudante de Biblioteca. Biblioteca Municipal de Burgos
ORCID https://orcid.org/0000-0001-5111-1833

Resumen

Se presenta una propuesta de formación para trabajadores en bibliotecas públicas sobre aspectos básicos de ciberseguridad y privacidad, mediante un listado de elementos a considerar y una apuesta por su impartición a distancia. De forma previa se delimitan los términos más significativos para evitar toda posible ambigüedad. Así mismo, se hace una previsión de nuevos riesgos tecnológicos a un corto y medio plazo.

Palabras clave

Privacidad; Ciberseguridad; Formación.

Abstract

A proposal for training for workers in public libraries on basic aspects of cybersecurity and privacy is presented, through a list of elements to consider and a commitment to distance education. In advance, the most significant terms are delimited to avoid any possible ambiguity, and a new technology risk forecast is made in the short and medium term.

Keywords

Privacy; Cybersecurity; Training.

Recibido: 16/12/2019
Aceptado: 27/12/2019
DOI: https://dx.doi.org/10.5557/IIMEI10-N19-075126
Descripción propuesta: Oltra-Gutiérrez, Juan Vte; Ibáñez-Hernández, Rafael. Ciberseguridad y bibliotecas: apuntes para una propuesta de formación sobre riesgo tecnológico en bibliotecas. *Métodos de Información*, **10**(19), 75-126

1. Estado actual

El mundo, la sociedad, está en permanente cambio, y éste parece haber sido acelerado vertiginosamente en los últimos años, en particular en lo que respecta al uso de las tecnologías de la información.

Una simple visita a los estudios de We Are Social (2019) nos dice que la penetración digital es algo que ya queda lejos de ser residual. Vemos en la siguiente tabla unos datos que nos permiten comparar la situación de España con la del resto del mundo.

	Población mundial	Números de telefonía móvil	Usuarios de internet	Usuarios activos de redes sociales	Usuarios de redes sociales desde teléfonos móviles
Mundo	7.734 billones	5.155 billones	4.479 billones	3.725 billones	3.660 billones
Penetración	-	67 %	58 %	48 %	47 %
España	46,42 millones	54,44 millones	42,96 millones	28 millones	24 millones
Penetración	-	117 %	93 %	60 %	52 %

Tabla 1. Datos referentes a la penetración TIC comparados España / totales mundiales. Fuente: elaboración propia, según datos de We Are Social (2019).

Un mayor uso de las tecnologías de la información implica que tanto el ciudadano como empresas y administraciones públicas van a gozar de muchas ventajas (sin ánimo de ser exhaustivo, pensemos tan solo en cómo la facilidad de difusión y acceso a la información ha cambiado en relativamente poco tiempo el modo de trabajar de nuestros escolares cuando realizan sus tareas, o el acceso universal a recursos tales como hemerotecas o colecciones clásicas de libros, desde el propio domicilio y a cualquier hora por todo interesado), pero también de nuevos inconvenientes. De todos los riesgos a cubrir nos interesan en esta ocasión particular aquellos que van ligados a la ciberseguridad.

A pesar de que la ciberseguridad es un asunto antiguo (una simple consulta a la Web of Sciencie (WOS) nos muestra resultados con esa etiqueta indexados desde el año 2002, aunque en revistas de divulgación es sencillo encontrar referencias anteriores[1]), adquirió notoriedad con la entrada en vigor en la Unión Europea de la llamada Directiva NIS[2] (Directiva (UE) 2016/1148). Las alarmantes noticias que publicaron los medios hace algunos meses sobre ataques masivos de *ransomware*[3] al sistema británico de salud (Walker-Roberts y otros 2018), además de a otras instituciones y empresas, generaron cierta alarma pública y el lógico desasosiego en las bibliotecas (Leal 2019). Por otra parte, la literatura que ha señalado la seguridad TIC como un elemento importante relacionado con las bibliotecas es extensa. Cabe señalar el texto de Vivancos-Cerezo (2008) dedicado a las bibliotecas universitarias, pero completamente extrapolable a las bibliotecas públicas, en el que se afirma que aplicar la seguridad de la información a las TIC es estratégicamente importante para salvaguardar la continuidad del negocio en las universidades, entendiendo por continuidad del negocio que una organización pueda continuar operando a un nivel mínimo predeterminado. Recordemos este párrafo para cuando definamos el término resiliencia.

[1] Sin pretender apuntar la referencia como la primera, sino a modo de simple ejemplo, encontramos el término en la cabecera clásica de los quioscos *PCManía* en el año 2000 (PCManía, 2000).
[2] Acrónimo de Network and Information Systems.
[3] Este término formado por la composición de *ransom*, «rescate», y *ware*, «software», responde a un tipo de *malware* o programa dañino (abreviación de *malicius software*, código informático maligno) que impide o restringe el acceso a un dispositivo de almacenamiento o a partes del mismo, situación cuya reversión exige el pago de determinada cantidad al causante.

El presente trabajo trata en primer término de abordar las confluencias entre ciberseguridad y bibliotecas. Es un tema tremendamente extenso, como demuestran el trabajo de Mendoza (2019) sobre la ciberseguridad de la Biblioteca General del Ejército del Perú o el interés por las bibliotecas en el trabajo de varios especialistas de la Unión de Informáticos de Cuba (Rodríguez Pérez y otros 2018), por lo que trataremos de centrar el foco en lo que parecen ser los elementos clave en esa intersección[4]: la formación en ciberseguridad de los trabajadores de las bibliotecas, la protección de la privacidad en la gestión de las mismas y el elemental blindaje ante los ataques más comunes (*ransomware*, etc.). Quede claro que no es propósito de los autores hacer una relación exhaustiva de las normas legales y técnicas vigentes, haciendo alusión tan solo a las que, más allá del marco general (Real Decreto 3/2010; Ley 8/2011), configuran la actividad diaria en una biblioteca. Tampoco pretendemos hacer una relación exhaustiva de la gran cantidad de normas o directrices técnicas existentes, destacando tan solo las de más interés. Intencionalmente hemos omitido las alusiones a la normativa sobre identificación electrónica (Reglamento (UE) 910/2014), por exceder las intenciones del presente trabajo.

Sobre la privacidad del usuario existe literatura reciente de alto interés, como el artículo de San Nicolas-Roca y Burkhard (2019), centrado en la formación en ciberseguridad para los trabajadores de la biblioteca. Reid (2019) centra su atención en la privacidad de profesores y estudiantes en una biblioteca universitaria, algo que de forma evidente puede de nuevo extrapolarse al resto de bibliotecas. Algo similar ocurre con el trabajo de Castillo Fonseca y Zavala Juárez (2019), que vincula privacidad y ciberseguridad, con los archivos mexicanos como campo de trabajo.

Por otra parte, cabe recordar su presencia en los principales códigos éticos y pautas profesionales. Así, el tercer principio del Código de Ética de la American Library Association (ALA 2008) exige el compromiso a la

[4] Para ayudar a determinar el foco, se realizó una encuesta abierta a los alumnos del Máster Oficial Universitario en Gestión de la Información (MUGI 2019) y a los del doble grado de Administración de Empresas e Informática (ETSINF 2017) de la Universitat Politècnica de València. Estos tres temas que se apuntan aparecieron en todas y cada una de las respuestas. La encuesta, carente de validez científica, sí marca al menos unos elementos de interés que, por otra parte, coinciden con la experiencia de los autores, uno como bibliotecario-documentalista y otro como docente e investigador.

protección del «derecho de cada usuario de la biblioteca a la privacidad y confidencialidad con respecto a la información buscada o recibida y los recursos consultados, prestados, adquiridos o transmitidos». Por su parte, el tercer punto del código de Código de Ética de la Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas (IFLA 2012) se refiere la privacidad, la confidencialidad y la transparencia en los siguientes términos:

> *Los bibliotecarios y otros trabajadores de la información respetan la privacidad personal, y la protección de datos personales, que por necesidad sean compartidos entre los individuos y las instituciones. La relación entre la biblioteca y el usuario se basa en la confidencialidad y los bibliotecarios y otros trabajadores de la información tomarán las medidas apropiadas para garantizar que los datos de los usuarios no sean compartidos más allá del proceso original. Los bibliotecarios y otros trabajadores de la información apoyan y participan en la transparencia para que el funcionamiento del gobierno, la administración y los negocios queden abiertos al escrutinio del público en general. Ellos también reconocen que están expuestos a la exención de esa confidencialidad aquellos casos de interés público que, por mala conducta, corrupción o crimen, sean requeridos por la autoridad judicial.*

Este compromiso se viene trasladando a otros instrumentos orientados hacia la normalización de equipamientos y servicios. Las *Pautas para el servicio de acceso a Internet en las bibliotecas públicas* (Jornadas de Cooperación Bibliotecaria 2006), por ejemplo, dictaminan que «las bibliotecas facilitarán entornos físicos que posibiliten la privacidad del usuario que accede a los recursos de información electrónica, y ubicarán los equipos informáticos, en lugares que permitan dicha privacidad. No obstante, el usuario debe ser consciente de que accede a Internet desde un espacio público.» Más allá aún, en la *Declaración de Lyon sobre el Acceso a la Información y el Desarrollo* (IFLA 2014)[5] se dice:

> *2. El desarrollo sostenible debe tener lugar en un arco basado en los derechos humanos, donde:*
>
> *[...]*
>
> *d. El acceso equitativo a la información, la libertad de expresión, la libertad de reunión y asociación y la privacidad se promuevan, protejan y respeten como elementos fundamentales para la independencia individual.*

[5] Promovida por IFLA con el fin de que se garantizase el acceso a la información, al conocimiento y la disponibilidad de las tecnologías de la información para la mejora de la calidad de vida de las personas a la hora de establecer los Objetivos de Desarrollo Sostenible en lo que ahora se conoce como Agenda 2030.

> *[...]*
> *6. Por lo tanto, los abajo firmantes pedimos a los Estados Miembros de las Naciones Unidas que reconozcan que el acceso a la información y las habilidades para utilizarla eficazmente, son obligatorios para el desarrollo sostenible; y que garanticen su reconocimiento en la agenda de desarrollo posterior al 2015 mediante:*
>
> > *a. La aceptación del derecho de las personas a acceder a la información y a los datos, respetando el derecho a la privacidad individual.*

En este punto cabe lanzar al menos una reflexión: hemos pasado de un lector que accedía a los fondos siempre de forma física, gestionando su préstamo en el mostrador de la biblioteca, a la convivencia de este modelo con una nueva generación que accede siempre que puede de forma telemática a los fondos y emplea como lector un dispositivo digital (un 10% de la población adulta (We Are Social 2019)). Ya en plena eclosión de la web 2.0 Álvarez Marañón (2011) alertó sobre los riesgos de la biblioteca transparente que debía construirse con las nuevas aplicaciones, poniendo especialmente el acento en la privacidad, puesto que el uso de esas herramientas deja un rastro que facilita la generación de perfiles personales, de modo que un atacante puede averiguar los intereses de los usuarios no sólo a costa de sus valoraciones y comentarios públicos, sino accediendo de forma fraudulenta a sus búsquedas en el catálogo o al tipo de información que consume, cuándo lo hace e incluso desde dónde y mediante qué dispositivo. No podemos por tanto dejar de tener en cuenta ciertas consideraciones sobre las bibliotecas digitales, esenciales hoy en día; tanto que Birnbaum (2004) apuntaba ya hace lustros algo que se está convirtiendo en realidad: que serán el eje para la difusión cultural, investigación y docencia y, por tanto de forma inevitable se convertirán en blanco de ataques maliciosos por delincuentes e incluso por terroristas que buscan distorsionar nuestro día a día, lo que no deja de tener ecos parecidos a nuestro Esquema Nacional de Seguridad (Real Decreto 3/2010).

Obviamente, resulta imprescindible tener una mínima idea de la situación actual de las bibliotecas españolas en lo que a servicios bibliotecarios electrónicos se refiere. Por sus características, nos fijamos inicialmente en las bibliotecas universitarias, por lo general más adelantadas en la implantación tecnológica. Según las estadísticas de REBIUN (2018), los fondos documentales de las 75 bibliotecas universitarias integradas en la red en 2018 sumaban las siguientes cantidades:

Monografías electrónicas de pago	14.512.533
Publicaciones periódicas electrónicas de pago	2.887.997
Bases de datos de pago	6.106
Objetos digitales en el repositorio institucional en acceso abierto	2.033.886

Tabla 2. Fondos documentales de las bibliotecas universitarias. Fuente: (REBIUN 2018).

Estas mismas bibliotecas contaban entonces con un parque informático para uso público compuesto por 22.047 equipos, aunque debe tenerse en cuenta que muchos de estos documentos son accesibles desde equipos y dispositivos privados conectados a la correspondiente red informática. Las consultas en recursos electrónicos de pago o con licencia contabilizadas a lo largo de dicho año conforme al estándar COUNTER[6] fueron 37.724.450 (algo más de 1.531 consultas cada uno de los 24.637 días de apertura anual), que se tradujeron en 48.248.292 documentos descargados.

Aunque con cifras muy diferentes, no debe desdeñarse en absoluto la situación de las bibliotecas públicas españolas. De las 4.600 bibliotecas recogidas en el informe estadístico *Bibliotecas públicas españolas en cifras* para 2017, 3.906 tenían automatizado su catálogo y, por lo tanto, la gestión del préstamo (Bibliotecas públicas españolas en cifras, 2017). Durante el mismo periodo, el parque de ordenadores del servicio de acceso a Internet en estas bibliotecas alcanzaba la cifra de 4,64 por cada 10.000 habitantes, proporcionando un total de 26.051.353 sesiones (cantidad que sostiene el progresivo crecimiento frente a las 19.912.987 sesiones de 2013), lo que se traduce en 114.355 sesiones de acceso a Internet por día de apertura. Pero acaso resulte más significativo para considerar la trascendencia de este servicio que el número de sesiones alcanza una media del 25% del total de visitas en estas bibliotecas[7]. En cuanto a las colecciones de documentos electrónicos de las bibliotecas públicas, su volumen resulta aún muy reducido[8], con una media

[6] Acrónimo de Counting Online Usage of NeTworked Electronic Resources (Contabilización del Uso en Línea de los Recursos Electrónicos en Red) es un código de conducta desarrollado por la Coalición Internacional de Consorcios de Bibliotecas (International Coalition of Library Consortia, ICOLC) lanzado en el 2002.

[7] Destaca Extremadura con una tasa de 72% frente al 4% del País Vasco, lo que indudablemente nos habla de la trascendencia de este servicio público en las áreas de menor desarrollo tecnológico.

[8] Tanto que el conocido informe de la Federación Española de Sociedades de Archivística, Biblioteconomía, Documentación y Museística (FESABID) *Las bibliotecas públicas en España:*

de apenas 192,93 documentos por cada 10.000 habitantes[9], situación que no tiene visos de variar en futuro próximo con un índice de adquisición de 7,54 documentos electrónicos por cada 10.000 habitantes (resultado de un descenso irregular pero progresivo desde los 11,59 de 2013), muy por debajo de los 114,5 documentos audiovisuales y, sobre todo, los 643,6 libros y folletos impresos. Con colecciones tan exiguas, no es sorprendente que frente a medias como la de 0,73 préstamos de libros y folletos o 0,22 documentos audiovisuales por habitante, los préstamos de documentos electrónicos resultan prácticamente insignificantes, con una media de 151,82 por cada 10.000 habitantes[10] (o, lo que es lo mismo, sólo 0,01 por habitante) durante 2017.

No obstante, merece la pena prestar algo de atención a los datos correspondientes a 2018 de las grandes plataformas de préstamo digital, eBiblio (eBiblio 2018), operativa en todo el territorio nacional excepto en el País Vasco, comunidad que cuenta con la suya propia, eLiburutegia (Servicio de Bibliotecas del Gobierno Vasco 2018), cuya disponibilidad y uso son crecientes. Entre ambas sumaron 598.990 licencias, contabilizándose 1.086.421 préstamos.

2. Objetivo: GRi tecnológico en bibliotecas

Si nuestro propósito es aportar unas líneas que faciliten el diseño de planes formativos sobre el riesgo tecnológico en las bibliotecas, es evidente que de alguna manera nos estamos refiriendo a un elemento fundamental de la gestión del riesgo (GRi) en estas unidades de información. Tradicionalmente se han señalado como objetivos de un plan de seguridad en una biblioteca los edificios e infraestructuras, las personas que los ocupan (usuarios y personal) y, claro está, los documentos (Prieto Gutiérrez 2009, p. 60). En relación con estos últimos, no es escasa la bibliografía sobre la protección y la conservación (en sus facetas preventiva y curativa, y aun restauradora) de los diferentes materiales que conforman una colección, con alusiones a la previsión de

diagnóstico tras la crisis económica (Arroyo-Vázquez, Hernández-Sánchez, Gómez-Hernández 2019) agrupa los datos de los documentos electrónicos junto con los sonoros y audiovisuales.

[9] En este caso destaca la comunidad de Castilla-La Mancha, con 415,83 documentos electrónicos por cada 10.000 habitantes.

[10] El máximo valor se alcanzó en Cataluña, con 340,54 préstamos de documentos electrónicos por cada 10.000 habitantes.

potenciales accidentes de catastróficas consecuencias y su recuperación (Tacón Clavaín 2008, p. 180-189). Sin embargo, el acelerado crecimiento de las tecnologías de la información y la comunicación ha generado una extensa variedad de amenazas (Sena, Tenzer 2004, p. 1) sobre las que, a pesar de la bibliografía existente, no parece haberse reflexionado aún lo suficiente. De hecho, cuando se habla de preservación digital se alude a la digitalización de materiales tradicionales o la preservación de recursos digitales, obviando por lo general los riesgos tecnológicos que deben afrontarse ante estas tareas, más allá de las inevitables alusiones a la obsolescencia (Keefer, Gallart 2007).

Obviamente, estamos planteando la necesidad de que los planes de seguridad en las bibliotecas contemplen los riesgos tecnológicos que las amenazan, puesto que resulta necesario garantizar no sólo el acceso y la preservación de los nuevos formatos electrónicos y digitales, sino también la gran cantidad de datos que gestionan y conservan sobre sus colecciones, sus usuarios, su comunidad y sus servicios. Por lo tanto, si aquellos planes deben basarse en una adecuada GRi, no debe en modo alguno eludirse la GRi tecnológica dado que, más allá de cual sea su causa (natural, accidental o intencional) u origen (interno o externo), esos riesgos pueden afectar al nivel físico (infraestructura), al nivel lógico (sistemas de información) e incluso al factor humano (medidas organizacionales) (Corda, Viñas, Coria 2017, p. 3).

Para minimizar en lo posible tales riesgos o sus consecuencias, puesto que no existe una seguridad absoluta (Chávez Flores 2009, p. 2), es imprescindible aplicar «un método un método lógico y sistemático para establecer el contexto interno y externo de la organización, con el fin de identificar, analizar, procesar, monitorear, comunicar y evaluar los riesgos asociados con cualquier actividad, función o proceso» (Corda, Viñas, Coria 2017, p. 4). Con estas palabras se alude a la GRi tecnológico, que no debe considerarse como una actividad independiente sino formar parte de la cultura de gestión de la biblioteca. En ella se pueden identificar diferentes fases, aunque no existe un sólido consenso sobre su enumeración. Tras analizar su aplicación a distintos ámbitos por diferentes autores, como Cóppola (2012, p. 44) al riesgo comunicacional o el Instituto Nacional de Ciberseguridad[11] (INCIBE 2015), optamos por describir hasta seis etapas:

[11] El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Economía y Empresa de España a través de la Secretaría de Estado para el Avance Digital.

- Identificación de los riesgos.
- Evaluación de los factores de riesgo, su probabilidad e impacto.
- Establecimiento de prioridades.
- Desarrollo de un plan de acción para prevenir, reducir o transferir el riesgo, o para reaccionar ante su desencadenamiento.
- Implementación del tratamiento planificado.
- Monitorización de la acción y medición de los resultados de los controles y tratamientos implementados, reevaluando los riesgos, para mejorar su gestión.

Además, en cualquiera de estas etapas la comunicación es fundamental para una toma de decisiones efectiva, así como para concienciar al personal sobre estos riesgos y las acciones adecuadas, con el fin de que se involucren en el proceso.

Atendiendo al GRi tecnológico de un sistema de información, debe considerarse que los riesgos que lo amenazan pueden afectar a (Corda, Viñas, Coria 2017, p. 12):

a. Los datos: la información guardada en las computadoras, cuyas características a proteger son la confidencialidad, la integridad y la disponibilidad.
b. Los recursos: el equipamiento en sí mismo.
c. La reputación: en nuestro caso, la de la biblioteca, pero también la de la institución a la que esté vinculada.

3. Consideraciones terminológicas

Para evitar confusiones, bien por la existencia de múltiples definiciones, bien por la posible ambigüedad generada por la polisemia de algunos términos, vamos a acotar los elementos más relevantes del presente trabajo.

3.1. Ciberseguridad

Hablamos con este popular término de la seguridad de las redes y de la información, algo que queda acotado por el Real Decreto 3/2010, de 8 de

enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en su anexo IV:

> *Seguridad de las redes y de la información, es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.*

Para la norma *UNE-EN ISO/IEC 27000:2019. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario* (AENOR 2019), la seguridad de la información sería la «preservación de la confidencialidad, la integridad y la disponibilidad de la información. Pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la fiabilidad». En la misma norma se entiende la información como:

> *un activo que, al igual que otros activos importantes del negocio, es esencial para el negocio de una organización y, por consiguiente necesita ser debidamente protegida. La información puede ser almacenada en muchas formas, incluyendo: formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato material (por ejemplo, en papel), así como la información intangible que forma parte del conocimiento de los empleados. La información puede ser transmitida por diversos medios: mensajería, comunicación electrónica o verbal. Independientemente del formato o del medio por el cual se transmite la información, es necesaria siempre una protección adecuada.*

Debemos destacar en este momento la aparición, que veremos repetida, de la palabra *confidencialidad*, que ligará indudablemente todos los esfuerzos hechos en pro de la ciberseguridad en mejora de la privacidad.

Estrechamente unidos a este primer término aparecen la idea del *riesgo* (*ciber-riesgo* en esta ocasión), el *incidente de seguridad*, la *resiliencia* y la *vigilancia tecnológica*. De la miríada de conceptos relacionados escogemos éstos por ser parte del núcleo duro de cualquier formación sobre ciberseguridad, siendo insoslayable una mínima alusión a ellos. Así, de modo informal, previo a las definiciones que acompañarán a la principal, parece obvio que, si en la seguridad en general

todo orbita en torno a los riesgos que se pueden sufrir, la ciberseguridad deberá orbitar en torno al ciber-riesgo. Estos riesgos pueden desatar incidentes de seguridad, que provocarán una respuesta conducente a minimizar los efectos y retornar a la situación de partida (resiliencia). Con todo, una de las mejores medidas preventivas para que estos incidentes no se lleguen a desatar es ejercer una oportuna vigilancia tecnológica.

Vamos con estos términos.

3.2. Ciber-riesgo

Íntimamente ligado al anterior queda el ciber-riesgo, que será elemento principal en lo que respecta a la ciberseguridad. Debemos partir de la definición que de riesgo en la seguridad de la información nos proporciona la norma *ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management* (ISO 2018): «Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.»

Dentro del campo de normas UNE que atañen a los sistemas de información nos encontramos con dos definiciones elementales de riesgo. Así, según la norma *UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información* (AENOR 2008), sería «estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.» Una definición más simplificada la encontramos en las normas *UNE-ISO Guía 73:2010 IN. Gestión del riesgo. Vocabulario* (AENOR 2010) y *UNE-ISO 31000:2018. Gestión del riesgo* (AENOR 2018b): «efecto de la incertidumbre sobre los objetivos.»

Centrándonos en los ciber-riesgos, Ybarra Malo de Molina (2019) los define como «los riesgos asociados a las Tecnologías de la Información y Comunicación que comprometen de algún modo (daños, confidencialidad, integridad, acceso, disponibilidad, etc.) redes, datos o servicios de información.» Por su parte, para la Asociación Española de Gerencia de Riesgos y Seguros (AGERS), el riesgo cibernético es (AGERS, ISMS Forum, 2017, p. 14):

> *aquel que puede producir un daño en los sistemas de información de una organización. El riesgo puede tener su origen en cualquier componente del sistema: equipos, aplicaciones, comunicaciones... Se puede producir como consecuencia de ataques de piratas informáticos o hackers y por fallos o errores no intencionados. Los daños pueden ser la alteración, modificación, destrucción o pérdida de información, el acceso indebido a la información y la falta de disponibilidad de servicio.*

Como señala Jimeno Muñoz (2019), para Cebula y Young (2010, p. 2-8) los elementos que dan paso a un ciber-riesgo son:

- La concurrencia de una acción u omisión humana.
- La concurrencia de una vulnerabilidad o fallo en los sistemas tecnológicos y procedimientos internos
- Como consecuencia de lo anterior, una serie de efectos externos que den paso a un daño efectivo.

3.3. Incidente de seguridad

Éste es otro término estrechamente relacionado que, para el INCIBE (2017, p. 24) es «cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.»

3.4. Seguridad de la información

El concepto de seguridad de la información puede verse reflejado en no pocos documentos no normativos ni oficiales (AGERS, ISMS Forum 2017, p. 13):

> *conjunto de controles cuyo propósito final es preservar la confidencialidad, integridad y disponibilidad de la información, colaborando a asegurar la competitividad, rentabilidad, el cumplimiento de la legalidad vigente y la buena imagen de la empresa.*

No obstante, parece imprescindible reforzar su definición distinguiéndolo sin ambages de otro aparentemente muy similar con el que se confunde en no pocas ocasiones. Tanto es así que no son pocos los autores que emplean de forma recurrente esta cita (Godoy Lemus 2014, p. 162)[12]:

[12] Sólo en este mismo volumen encontramos estos párrafos en otras dos ocasiones (Galindo López 2014, p. 100; Quilo Jáuregui 2014, p. 238).

> *La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permite resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.*
> *El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.*

Y ello es así porque (Corda, Viñas, Coria 2017, p. 9):

> *La seguridad de los sistemas de información es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de la información almacenada o transmitida, y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.*

No obstante, según se desprende de las palabras de Guerrero Julio y Gómez Florez (2011, p.198-199), tanto una como otra forman parte de la GRi en sistemas de información.

3.5. Resiliencia

La norma *UNE-EN ISO 22300:2015. Protección y seguridad de los ciudadanos* (AENOR 2015) nos la define doblemente:

> *Capacidad de adaptación de una organización en un entorno ambiental complejo y cambiante.*
> *[…]*
> *Es la habilidad de una organización para gestionar interrupciones relacionadas con el riesgo.*

Cabe señalar que la Estrategia Europea de Seguridad tiene en la ciber-resiliencia uno de sus ejes principales, señalándola como uno de los requisitos de los equipos de respuesta a incidentes de seguridad informática (CSIRT) (Directiva (UE) 2016/1148).

3.6. Vigilancia tecnológica

Aparecen dos definiciones bien diferentes pero no incompatibles entre sí. Así, mientras para la norma *Gestión de la I+D+i: terminología y definiciones de las actividades de I+D+i*, (AENOR 2006) vigilancia tecnológica es un:

> *proceso organizado, selectivo y sistemático, para captar información del exterior y de la propia organización sobre ciencia y tecnología, seleccionarla, analizarla, difundirla y comunicarla, para convertirla en conocimiento con el fin de tomar decisiones con menor riesgo y poder anticiparse a los cambios.*

Por su parte, en la norma UNE 166006, Gestión de la I+D+i: Sistema de vigilancia e inteligencia (AENOR 2018c) aparecen dos definiciones complementarias; mejor dicho, una es extensión de la anterior:

> *Vigilancia e inteligencia: Proceso ético y sistemático de recolección y análisis de información acerca del ambiente de negocios, de los competidores y de la propia organización, y comunicación de su significado e implicaciones destinada a la toma de decisiones.*
> *Vigilancia e inteligencia en red: Proceso de vigilancia e inteligencia compartida que se establece gracias a la interactuación de diferentes nodos pertenecientes a organizaciones distintas.*

3.7. Privacidad

Puede parecer sorprendente, pero en ninguno de los dos grandes textos legales que rigen este derecho, la Ley de Protección de Datos Personales (Ley Orgánica 3/2018) y el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679), aparece definida la privacidad. Para buscar un enunciado canónico acudimos al Diccionario del español jurídico (DEJ, 2019), que la define en su primera acepción como: «Facultad de una persona de prevenir la difusión de datos pertenecientes a su vida privada que, sin ser difamatorios ni perjudiciales, esta desea que no sean divulgados.» Lógicamente, esto enlaza de forma natural con la definición del derecho de protección de datos personales que ofrece el propio DEJ:

> *Derecho fundamental de toda persona física que la faculta para disponer y controlar sus datos de carácter personal, pudiendo decidir cuáles proporcionar a terceros, así como conocer quién posee esos datos y para qué, y oponerse a esa posesión o tratamiento.*

Obviamente, desde aquel artículo de Warren y Brandeis (1890)[13] que se asume como el origen, se han sucedido muchas definiciones de privacidad. Pero la

[13] La doctrina desarrollada por estos autores pretendió garantizar la protección de la privacidad, en ejercicio del «(el derecho a no ser molestado, a ser dejado solo», frente a la divulgación indiscriminada por la prensa norteamericana de información privada (Saldaña, 2012, p. 198).

simplicidad que proporciona el DEJ la convierte en la definición más apropiada para su divulgación.

3.8. Formación de usuarios

La definición que Corral Beltrán (1977, p. 28) ofreció en un artículo ya clásico fue en su día la más reconocida y utilizada para acotar lo que entendemos por formación de los usuarios: «cualquier tipo de esfuerzo tendente a facilitar la orientación al usuario, individual o colectivamente, a fin de lograr una utilización más eficaz de los recursos y servicios que la biblioteca ofrece.» Veinte años más tarde, Sánchez Paus (1997, p. 44) la recogió en otro artículo indicando la conveniencia de abandonar el término *esfuerzo* para hablar de *actividad y/o servicio*. Y profundizó añadiendo que ese concepto de formación de usuarios en realidad debería ser un conjunto de actuaciones clasificados en tres acepciones: orientación, educación e instrucción de los usuarios en la utilización de las bibliotecas y en los recursos informativos que éstas les pueden proporcionar. Estos tres conjuntos se presentan en la tabla siguiente:

Orientación	Acción de informar o asesorar al usuario sobre cuestiones puntuales.	Cómo funciona un servicio determinado, hacer una petición de préstamo interbibliotecario, cómo encontrar un libro y/o localizar una signatura en el libre acceso, etc.
Educación	Acción de enseñar a utilizar las técnicas bibliotecarias básicas.	Enseñar a buscar en las distintas opciones del OPAC propio y en otros catálogos en línea.
Instrucción	Ayuda a la adquisición por parte de un usuario con más o menos aptitud o habilidad, soltura, en la selección de fuentes bibliográficas y documentales.	Manejo de bibliografías, búsquedas en bases de datos en CD-ROM, recursos de información en Internet, etc.

Tabla 3. Formación de los usuarios, según (Sánchez Paus, 1997).

En cierto modo ligado a este concepto se encuentra el de *alfabetización informacional* (ALFIN), que nos permite reconocer cuándo se necesita información y capacita para ubicar, evaluar y usar de manera efectiva la información necesaria (ALA, 1989). Fundamental para los profesionales de la información en la medida en que crean, seleccionan y permiten el uso de

diversos tipos de información, según el británico Chartered Institute of Library and Information Professionals (CILIP, 2018), la ALFIN

> *incorpora un conjunto de habilidades y capacidades que todos necesitan para emprender tareas relacionadas con la información; por ejemplo, cómo descubrir, acceder, interpretar, analizar, administrar, crear, comunicar, almacenar y compartir información. Pero es mucho más que eso: se refiere a la aplicación de las competencias, atributos y confianza necesarios para hacer el mejor uso de la información e interpretarla con criterio. Incorpora pensamiento crítico y conciencia, y una comprensión de los problemas éticos y políticos asociados con el uso de la información.*
>
> *[...]*
>
> *La alfabetización informacional ayuda a comprender los problemas éticos y legales asociados con el uso de la información, incluida la privacidad, la protección de datos, la libertad de información, el acceso abierto / datos abiertos y la propiedad intelectual.*[14]

Por su parte, el Grupo de Trabajo de Alfabetización Informacional (GTALFIN) del español Consejo de Cooperación reconoció que, siendo a estas alturas imprescindible, el acceso a las tecnologías de la información y la comunicación no es suficiente Bibliotecaria (GTALFIN 2009, p. 4)[15]:

> *La tecnología por sí sola no sirve para mucho; es necesario aprender a usarla correctamente para obtener el mayor potencial posible. La alfabetización digital se ha de desarrollar como parte de la informacional. Es necesario un reconocimiento por parte de los educadores, bibliotecarios y de los gobernantes, de que la alfabetización informacional, y no solo la alfabetización digital, es la clave educativa de la tan llamada sociedad de la información.*

Con todo, para nosotros la ALFIN debe ser aún más amplia puesto que, dada la actual trascendencia de la tecnología en los sistemas de información, debería también incluir la alfabetización tecnológica precisa para su manejo y gestión. De hecho, ya en las *Pautas para el servicio de acceso a Internet en las bibliotecas públicas* (Jornadas de Cooperación Bibliotecaria 2006, p. 24) se habla de que la formación de usuarios debe orientarse tanto a la ALFIN como hacia la «instrucción en el manejo de las nuevas tecnologías, con el fin de que los usuarios sean capaces de manejar por sí mismos todos estos nuevos medios que se ponen a su alcance».

Para que esto sea posible planteamos una formación no dirigida en exclusiva a los usuarios, sino orientada en primer término hacia los propios trabajadores

[14] Traducción propia.
[15] En este documento se recopilan otras numerosas definiciones de ALFIN.

de la biblioteca. Esto debe nos obliga a tener presentes circunstancias como la dependencia administrativa y tecnológica de la institución a la que esté vinculada de biblioteca (Ayuntamiento, Comunidad Autónoma, Universidad…), con la consecuente necesidad de apoyo incondicional de la institución y la coordinación con sus departamentos técnicos, legales y de calidad.

La formación dirigida a este perfil, el de trabajador de la biblioteca, debe considerar una serie de criterios que van desde los temas a tratar (algo que en este caso, como queda claro, enfatiza los aspectos de privacidad y seguridad) al tipo de formación no orientada hacia lo académico-científico, sino hacia la integración en su propio conocimiento para adaptarlo a nuevas situaciones; el necesario apoyo en las tecnologías de la información; y la búsqueda del necesario compromiso de colaboración entre los alumnos (Orera-Orera 2002; Silvera Iturrioz 2005; Pinto, Uribe-Tirado 2011; Díaz Salazar 2018).

Acotados los términos, centrémonos en la propuesta.

4. Elementos clave a considerar en la seguridad en la operativa diaria

Como anticipábamos, trataremos de una terna de asuntos tremendamente relacionados entre sí:

- la formación en ciberseguridad de los trabajadores de las bibliotecas.
- la protección de la privacidad en la gestión de las bibliotecas.
- el blindaje ante los ataques más comunes.

Imagen 1. Elementos clave para la ciberseguridad en bibliotecas. Fuente: Elaboración propia.

En la imagen 1 vemos las relaciones entre los tres elementos, que desarrollamos a continuación.

Las relaciones que emanan de la cápsula *Formación* son evidentes: se trata de desarrollar un programa de mínimos para ser empleado con profesionales de las bibliotecas, centrado en los aspectos elementales de la ciberseguridad, pero destacando un aspecto como primordial: la protección de los usuarios, sobre todo de los usuarios, pero sin desdeñar la de los propios trabajadores. Y apuntamos que son evidentes porque no se puede desde el desconocimiento aplicar medida alguna que atienda debidamente las dimensiones canónicas de la seguridad (MAGERIT 2012, p. 9):

- *Disponibilidad:* acceso y utilización de la información y sus sistemas de tratamiento cuando se requiera.
- *Confidencialidad:* la información solamente se pone a disposición de individuos, entidades o procesos no autorizados.
- *Integridad:* mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

¿Qué elementos debería tener el curso? Esta elemental pregunta no tiene una respuesta sencilla. Tendríamos que hablar de *forma* (cómo ha de ser contada) y *fondo* (qué queremos que contenga).

Empecemos por la estructura. Tras identificar los elementos que hay que proteger en la biblioteca (y que ya conocemos: usuarios y personal, edificios e infraestructuras, y documentos), en su manual Prieto Gutiérrez (2013) describe los sistemas generales de seguridad y las medidas para protección del patrimonio bibliográfico (incluyendo sistemas electromagnéticos (EM) y de radiofrecuencia (RFID), proponiendo las grandes líneas del plan de seguridad. El último capítulo está dedicado a la seguridad de los documentos electrónicos, utilizando como base el modelo Open Archival Information System (OAIS), que se apoya en la norma UNE-ISO 14721 (AENOR 2015b). Pero, desde nuestro criterio, este manual no menciona la seguridad (prevención y protección) de los datos personales y privados de los usuarios, que hoy se gestionan por medios informáticos, y que son uno de nuestros ejes, a pesar de que él mismo ya señaló (Prieto Gutiérrez 2009) la conveniencia de

que se tratasen conjuntamente con la seguridad del continente y el acervo de las bibliotecas, pues eso «provoca que se forme un valioso mallado mejorando su efectividad».

Otro criterio similar es el que mantienen S. Inmor, V. Esichaikul, y D. N. Batanov (2003), que clasifican los mecanismos de seguridad según los activos que protegen: seguridad del hardware, seguridad del software, seguridad en red y seguridad de los sistemas de información. Hay un factor de mucho interés que adoptamos como propio: 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. Esto tiene unos ecos imposibles de soslayar con la privacidad desde el diseño y por defecto (AEPD 2019)[16].

Ya que ha aparecido la privacidad, ahondemos en el tema. El riesgo tecnológico que amenaza las bibliotecas no afecta, como ya hemos visto, solamente a sus colecciones (sean digitales o no), sino también a la privacidad de sus usuarios y trabajadores. Esto nos da paso a plantear uno de los primeros elementos a defender, pues es un vínculo seguro entre privacidad y seguridad: el método de acceso. El cartón que con poco más que una foto y un cuño se convertía en el carné que daba acceso al uso y disfrute de los recursos de la biblioteca convive (cuando no ha desaparecido definitivamente) con una miríada de métodos de acceso a los recursos, sean estos físicos o virtuales. Hablando del caso particular de los Estados Unidos, San Nicolas-Rocca y Burkhard (2019, p. 58-59) describen esa identificación oficial como un documento con fotografía que muestra información personal (nombre, dirección, número de teléfono y dirección de correo electrónico). Este documento permite conectar a los usuarios con elementos digitales vía web, y facilita la conservación de sus búsquedas, además de los elementos prestados o accedidos, lo que produce un efecto secundario: permite obtener una traza

[16] AEPD es el acrónimo de la Agencia Española de Protección de Datos. El principio de protección de datos desde el diseño tiene como objetivo cumplir los requisitos definidos en el RGPD (Reglamento (UE) 2016/679) procurando que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto; por ejemplo, incorporando la seudoanonimización temprana de los datos personales.
El concepto de privacidad por defecto alude a que sólo sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines de tratamiento, independientemente del conjunto de datos recogidos, por ejemplo, analizando los procesos asociados al tratamiento de los datos para que se acceda a los mínimos datos personales necesarios para ejecutarlos.

y, por lo tanto, potencialmente construir una imagen de un usuario concreto que podría usarse para evaluar su perfil. Esto provocó en su momento una respuesta de ALA, que desarrolló políticas sobre confidencialidad, extendida a «información buscada o recibida y recursos consultados, prestados, adquiridos o transmitidos» que incluye, pero no se limita a, registros de búsqueda en la base de datos y referencias digitales. Esta trazabilidad será uno de los principales puntos débiles que trataremos cubrir.

5. ¿Por qué formación al personal bibliotecario?

En este creciente y complejo entorno, en el que aumentan las amenazas, «los responsables de gestionar las herramientas tecnológicas deben poder diagnosticar adecuadamente los riesgos a los cuales se ven expuestos para poder mitigar de manera oportuna las pérdidas que puedan generase» (Sena, Tenzer 2004, p. 2). Pero si hace años estos responsables eran exclusivamente profesionales especializados en tecnología, en la actualidad los profesionales en otras áreas están obligados a comprender razonablemente las herramientas y recursos tecnológicos con los cuales cuentan, puesto que pueden responsables de la gestión de algún componente específico que soporta el proceso de negocio que les compete.

Como ya hemos señalado, en la actualidad la práctica totalidad de las bibliotecas son gestionadas o al menos están vinculadas a otras entidades o administraciones. El caso de las bibliotecas universitarias es palmario, como lo es también el de las bibliotecas públicas, dependientes de las administraciones locales, autonómicas y estatales, además de pertenecer a redes u otro tipo de agrupaciones con los que comparten servicios y herramientas tecnológicas. Por si esto no fuera suficiente, comúnmente se encuentran ubicadas (especialmente las más pequeñas y, por lo tanto, débiles) en el interior de edificios que albergan también instituciones con otras ocupaciones y obligaciones, con los que comparten redes informáticas. Esta realidad, que incrementa las vulnerabilidades tecnológicas de manera casi exponencial, dificulta la puesta en marcha de una unidad central dedicada a la seguridad informática (Prieto Gutiérrez 2009, pág. 1), lo que, unido a la responsabilidad de los bibliotecarios sobre la seguridad de la información, exige que adquieran un cierto grado de conocimientos y alguna capacidad para tomar decisiones.

Pero, ¿están los profesionales de la documentación, y muy particularmente los bibliotecarios, capacitados para esto?

La respuesta que nos viene a la mente puede parecer descorazonadora y preocupante. Pero, aun así, debemos prestar atención a la visión que el sector bibliotecario español tiene sobre sí mismo, para lo que recurrimos al *Informe de los resultados de la encuesta IFLA Global Vision en España* (FESABID 2017), en el que se han recogido las cinco respuestas más votadas a las siete cuestiones plateadas. En mayor o menor medida, los profesionales bibliotecarios participantes en la encuesta se han manifestado convencidos de que las bibliotecas son excepcionalmente buenas en el tratamiento y gestión de la información, característica fundamental para afrontar el desarrollo científico y tecnológico, uno de los principales desafíos para la sociedad. Sin embargo, se han mostrado ansiosos por dejar de centrarse en los trabajos técnicos, lo que (más allá de proporcionar oportunidades para otras funciones y tareas que desarrollen por otros caminos la práctica profesional) debe provocarnos cierta alerta dados los requisitos que exige el mencionado desarrollo tecnológico. Afortunadamente, son partidarios de que las bibliotecas potencien todavía más la formación de la ciudadanía al tiempo que, en clave interna, creen que la formación permanente sería una de las características principales de un sector bibliotecario unido.

Si los bibliotecarios se declaran propiciadores de la innovación digital, propia de una era que exige la actualización de los roles tradicionales, y se reconocen obligados a la adaptación a los permanentes cambios tecnológicos (IFLA 2019), resulta evidente de una formación capacitativa.

6. Propuesta de diseño de la formación

A continuación presentamos una propuesta de formación basada en las tres preguntas clásicas: ¿a quién? ¿el qué? y ¿cómo? En cuanto a la primera, la respuesta será rápida, inmediata: se trata de dar formación a trabajadores de bibliotecas públicas (aunque la propuesta puede ser extensible a otras, con leves modificaciones) y, como efecto dominó, que estos mismos trabajadores puedan dar consejos, cuando no directamente formación, a los usuarios de sus centros. Tan solo destacaremos un elemento que es de alta importancia: el *conocimiento previo* y la *percepción del riesgo*.

6.1. Quién: perfil y percepción del riesgo

La producción de literatura científica al respecto es parca, más considerando un breve lapso de tiempo para explorar en busca de artículos, dada la rápida caducidad de los datos que pueden hacerlos poco relevantes. Una búsqueda en las bases de datos WOS nos devuelve solo siete artículos al respecto en España durante los últimos dos años, ninguno de ellos con datos de interés para el presente trabajo. Las estadísticas que ofrece el Instituto Nacional de Estadística, por otra parte, devuelven un trazo muy grueso, como puede adivinarse en la figura siguiente (INEbase 2019).

Operaciones estadísticas que el INE elabora de forma periódica	Últimos datos
Encuesta sobre el uso de TIC y comercio electrónico en las empresas	Año 2019
Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares	Año 2019
Indicadores del sector de tecnologías de la información y las comunicaciones (TIC)	Año 2017
Operaciones elaboradas por otros organismos del sistema estadístico nacional	
Estadística sobre la Sociedad de la Información y la Comunicación en los Centros Educativos no Universitarios	
Estadística de Presupuestos de Tecnologías de la Información y las Comunicaciones en la AGE	
Las Tecnologías de la Información y las Comunicaciones en las Administraciones Públicas	

Ilustración 2. INE: Nuevas tecnologías de la información y la comunicación. (INE, 2019)

Por ello la percepción del grado de conocimiento de ciberseguridad por parte de la generación actual la hacemos descansar en dos fuentes principales. Uno, la tesis doctoral de José Ramón Díaz Sáenz (2015), que, aunque dotada de un magnífico aparato estadístico, puede presentar la indudable pega de su no inmediatez. Para paliar eso y contrastarlo con un trabajo más reciente, aunque de mucha menos entidad científica, recurrimos al trabajo de fin de grado de Oleguer Rocafull (2018).

La tesis de Díaz Sáenz tiene un elemento que la hace más significativa: sus datos descansan en una encuesta realizada a alumnos tecnológicos: alumnos que cursaban el grado de informática o de telecomunicaciones. La perspectiva *a priori*, intuitiva, decía que su percepción de los riesgos y su protección ante los mismos iba a ser muy elevada. Pero, como tantas ideas preconcebidas sin sólido apoyo en datos, resultó falsa. Hagamos una relación de algunos hallazgos que resultaron desoladores:

- Tan solo algo más del 4% de los encuestados utilizan contraseñas complejas, diferentes para cada acceso y renovadas con frecuencia.
- Alrededor del 40% tienen una *password* única para todos los accesos, el 70% las mantiene fijas en el tiempo y una cuarta parte deja que las genere el propio sistema.
- El 32% no protege el acceso a su propio ordenador.
- Una séptima parte de encuestados nunca ha hecho una copia de seguridad de sus datos y tan solo otra séptima parte tiene un sistema automático de actualización.
- Algo más del 25% abren correos de desconocidos, y una sexta parte no tienen inquietud por conocer las vulnerabilidades que se producen.
- Con respecto a las redes sociales, más del 60% se dan de alta sin leerse las condiciones de registro y casi la mitad (entre el 40 y el 45%) manifiestan libremente sus opiniones personales sobre temas sensibles.

Puede pensarse que este fenómeno era algo puramente español, pero estudios coincidentes en el tiempo en China (Jiang, Heng, Choi 2013) y en Estados Unidos (Marwick, Murgia Diaz, Palfrey 2010) obtuvieron unos resultados tremendamente similares.

En un trabajo posterior, aunque abierto a todo tipo de público, Rocafull no encontró datos mucho más esperanzadores: el 40% de los usuarios podría sucumbir ante un ataque técnicamente simple, porcentaje similar (39,7%) al de los que deja desprotegidas sus contraseñas.

No queda más que intentar dar la vuelta a estos datos desde la formación. Formación, como vemos, que debe empezar por un nivel muy elemental, a riesgo de perder al público potencial por carecer éste de base para asimilar conceptos tecnológicos densos.

6.2. Qué: contenidos

Los contenidos deben cubrir todas las esferas vulnerables. Eso implica dar un giro de 360º al ecosistema digital (véase la figura siguiente) que cubre tanto hardware y software, elementos clásicos, como las infraestructuras (accesos WiFi, accesos a Internet en general, bases de datos electrónicas, etc.) y, por

supuesto, el corazón del sistema y lo que debe ser objeto de máxima protección: las personas. El principal enfoque al tratar de éstas lo colocamos en lo que más puede dañar a la persona si se deja sin cubrir ese flanco: su privacidad.

Es fácil intuir que habrá elementos comunes. El más representativo puede ser la contraseña de acceso a un servicio: una contraseña violada puede afectar a la intimidad de la persona a la que va asociada, puede afectar al software y/o hardware de la máquina a la que se accede y causar estragos en las infraestructuras, sobre todo si la contraseña pertenece a alguien con permisos de acceso que puedan modificar las distintas configuraciones. Esto puede dar una idea del concepto holístico de la ciberseguridad, donde el todo siempre es mayor que la suma de las partes.

De forma esquemática, referiremos aquellos aspectos que deben ser, bajo nuestro criterio, incluidos en un plan de formación para el personal de bibliotecas. Sólo consideramos un curso básico, elemental, para personas con escasa o nula formación. Este curso podría (debería) ser complementado con otros posteriores más específicos.
En la figura siguiente vemos una representación gráfica de los posibles elementos a tratar.

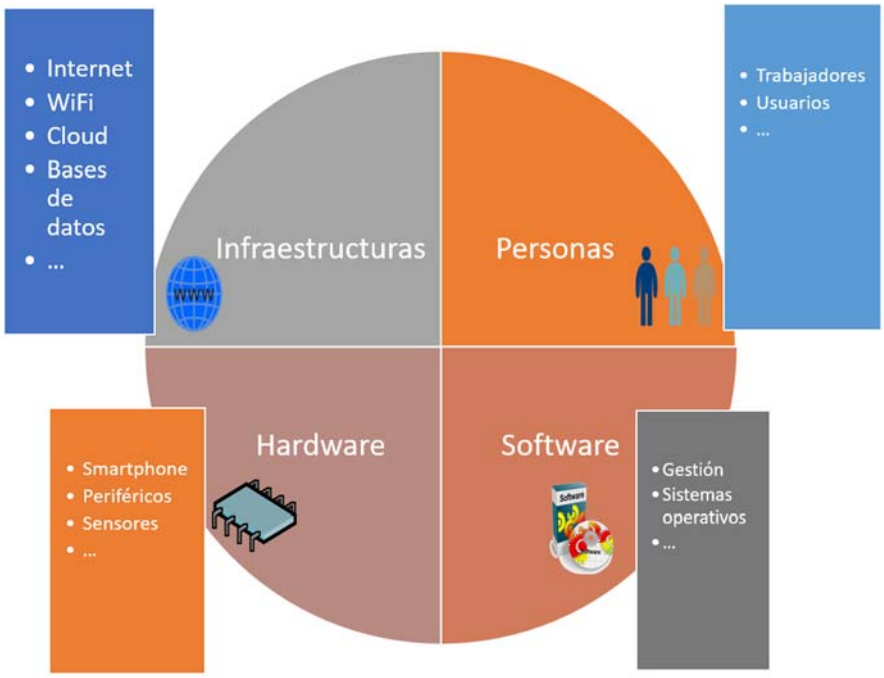

Ilustración 3. Ecosistema digital de la ciberseguridad. (Fuente: elaboración propia)

6.2.1. Seguridad básica

En este apartado aludimos a elementos centrados en la infraestructura: redes de comunicación, bases de datos digitales a las que se accede a distancia, facilitación al usuario de servicios de Internet, etc.

- Empecemos con la puerta de acceso: las contraseñas. Estas permiten al usuario acceder a sus datos personales en el Sistema Integrado de Gestión Bibliotecaria (SIGB), necesarios para la prestación de los servicios bibliotecarios (datos de contacto, renovaciones de préstamo, reservas, desideratas, valoraciones…) y emplear bases de datos restringidas y otros servicios vinculados (eBiblio, eFilm, proveedores de revistas…). Dado que una contraseña protege mucho más que recursos, como ya se ha dicho, pues tras ella está el propio individuo y su personalidad, la desarrollaremos en ese apartado. Podemos adelantar un elemento de alto interés para incluir en la formación: cómo se construye una contraseña segura y las normas para facilitar que lo siga siendo.
- Accesos seguros: mediante *Transport Layer Security* (TLS), túneles encriptados que permiten emplear bases de datos. En ocasiones, cuando el acceso se hace desde una red distinta y es preciso que el usuario aparente estar en las instalaciones (por el número de IP[17]), se recurre al empleo de redes virtuales privadas VPN[18]. Esto requiere un adiestramiento, pues su uso no es trivial.
- Vigilancia (captación de datos operativos). Una biblioteca precisa tomar decisiones, que siempre deben estar basadas en datos. Es preciso, pues, formalizar y estructurar el proceso de recogida de esos datos, previo a su análisis. Esto puede interpretarse como dar una formación muy elemental con la norma UNE 1666006 de base (AENOR 2018d). Tengamos en cuenta que una corrupción, intencionada o no de esos

[17] Permite identificar dispositivos (ordenador, tableta…) que usen el protocolo TCP/IP.

[18] Red Privada Virtual (VPN, *Virtual Private Network*) es una red, construida sobre la infraestructura de una red pública, que permite a usuarios remotos comunicarse de forma privada, transparente y segura. Estas conexiones permiten a los usuarios de una biblioteca acceder desde un lugar lejano a servidores como si estuvieran en la misma biblioteca.

datos, puede generar análisis incorrectos que den paso a malas decisiones en la gestión de la biblioteca.

- Vinculado con lo anterior, pero de igual modo con otras actividades de la biblioteca, existen otras dos normas más de interés: las dedicadas a la gestión y sistemas de gestión de documentos (AENOR 2011; AENOR 2016). Esto nos permite controlar la generación de documentos electrónicos a través de las cadenas de custodia o cadenas de valor codificado. Sobre el empleo de bases de datos electrónicas internacionales, véase el estupendo trabajo de García Mirete (2014).
- Resiliencia. Mediante una combinación adecuada de hardware y software se puede restaurar tras un ataque el funcionamiento con un comportamiento similar a los momentos previos al mismo. Si existen estos medios (algo más que aconsejable), el personal debe ser capaz de ejecutarlos.

6.2.2. Personas (y su privacidad)

De los muchos aspectos a gestionar, consideramos como el principal, el primordial, la solución encontrada para identificar al usuario. Hablamos del carné o identificador, y sus distintas modalidades.

- Carné clásico: la opción de un cartón con una foto, un plástico con una foto impresa, con o sin una banda magnética, un chip o… cualquier elemento adicional, sigue estando muy viva. En este caso la formación debería considerar no sólo los clásicos trámites de solicitud y gestión del carné. Pensemos que en ocasiones se trata de una tarjeta multiuso que da acceso también a servicios en centros cívicos o instalaciones deportivas, puede servir de tarjeta monedero para autobuses, fotocopiadoras y otros servicios municipales, universitarios, etc. Nos encontramos de plano con un abanico de riesgos que hasta ahora no habíamos mencionado: los que nacen de la interoperabilidad[19] (Real Decreto 4/2010).

[19] Capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. Esta definición es la que da el propio esquema nacional de interoperabilidad.

- Identificador digital: opción paralela o sustituta del carné físico, se identifica ante el sistema bibliotecario mediante la combinación de un nombre de cuenta (popularmente *login*) y su contraseña. Suele ser empleado para acceder de forma remota a determinados servicios (reservas, renovaciones de préstamo, etc.) y, muy especialmente, a recursos digitales y electrónicos. Y con esto volvemos al tema que dejamos pendiente: las contraseñas.
    - Contraseñas de nuestro propio sistema. Aquellas que entrega la biblioteca, tras generarlas ella misma o a través de otro organismo, que generalmente puede modificar el destinatario, ya sea usuario de la biblioteca o uno de sus trabajadores. En este caso la seguridad estriba en la autenticación, tanto para comunicaciones que salen como para las que entran. Dando por sentado que los problemas técnicos exceden el propósito de esta formación, el eje estriba en adiestrar sobre los mecanismos para generar contraseñas seguras, impidiendo así que se vulneren, y a su vez albergar conocimientos suficientes para hacer una difusión divulgativa sobre esto.
    - Contraseñas que son ajenas a nuestro sistema. Reid (2019) apunta que los bibliotecarios han velado tradicionalmente por el mantenimiento del derecho a la privacidad del usuario como un deber profesional. Sin embargo, en el caso de las bibliotecas académicas en particular (pero no sólo), su papel en la gestión de colecciones ha cambiado en gran medida desde el añejo de custodio local de contenidos al de intermediario de intermediario para el acceso a contenido alojado en otro lugar. Ese acceso a otro lugar implica contraseñas que pueden tomar muchas formas:
        - Empleo de un ID único por la institución. Este caso es muy simple: generalmente basta con que el usuario se conecte de manera transparente desde dentro de la institución para acceder, por ejemplo, a una colección de revistas.
        - Empleo de un ID de usuario personalizado. Aquí los problemas son comunes a los que teníamos con nuestro

propio identificador: cabe hacer apología de contraseñas seguras y poco más. Pero a la formación que se le dé a los usuarios no debemos olvidar el añadir una reflexión sobre la posible pérdida de privacidad: esa navegación puede permitir a los propietarios de los recursos accedidos perfilar a los usuarios. Pero ¿qué hace el proveedor de información con esos datos de navegación?

- ID delegada en terceros. Es común hoy acceder a sistemas mediante la validación de identidad a través de Facebook o Gmail. Determinadas revistas académicas, por ejemplo, hacen uso de un ID de usuario vinculado a LinkedIn Learning. Esto va acompañado de una invitación a los usuarios para que asocien su uso del recurso con una cuenta de LinkedIn preexistente. Bajo una idea positiva, la personalización de la experiencia de usuario, se esconde una realidad: se hace crecer el número de usuarios y la información sobre los mismos a una red social basada en datos, ligando así una identidad que responde a la vida del usuario más allá de los límites de su actividad en la biblioteca. Aquí cabría establecer unas reflexiones a compartir por todas las partes implicadas, como los potenciales peligros para la privacidad y las preguntas a formular sobre posibles ganancias económicas adicionales ligadas a ese modelo. En este punto cabe recordar lo fácil que es darse de alta en algunas plataformas y lo difícil que resulta darse de baja de ellas, lo que puede ilustrarse con el vídeo formativo *How Dark Patterns Trick You Online* (Nerdwriter 2018), insertado en un post de Justin Pot (2018).

- Formación específica sobre privacidad.
    - A los encargados y responsables del tratamiento de datos, la realización de una evaluación de impacto, la gestión y notificación de brechas de seguridad o la realización de un análisis de riesgos seguro que les es muy familiar (AEPD 2018;

AEPD 2018b; AEPD 2018c; AEPD 2018d; GT29[20] 2017; GT29 2018; ISO 2011; Reglamento (UE) No 611/2013). Pero para un trabajador no especializado, detectar una brecha que está surgiendo delante de ellos a veces no es fácil, como tampoco el saber informar a los usuarios de una situación delicada. Todo esto debería formar parte de ese conjunto de mínimos, incluyendo información sobre como apoyar las auditorías técnicas de seguridad, o cómo se realiza una petición de datos respetando el necesario consentimiento (GT29 2018b).

- Privacidad sobre los préstamos en los SIGB. En este apartado deberían considerarse, siquiera en forma rudimentaria, conceptos sobre la opacidad de los empleados, cómo actuar si se presenta una solicitud judicial (incluida la captación de evidencias (UNE 71505-1:2013) o las mejores prácticas para preservar la privacidad del historial de préstamos para usuarios.
- Colaboración. Los contactos con otras bibliotecas son frecuentes (desde el préstamo interbibliotecario a la organización de actividades conjuntas) y a menudo se comparte información. La manera de hacer seguro ese trasvase de información debería formar parte de esta formación básica.
- Digitalización de documentos para su empleo en archivos o hemerotecas digitales. Resultan imprescindibles las consideraciones sobre anonimización en buscadores y, por complejo que parezca, prestar atención al derecho al olvido (STS 4132/2015; STC 58/2018).

6.2.3. Hardware y software

Englobamos en una única categoría a dos elementos básicos pues, excepto en temas puntuales, dependerá de personal especializado, no siendo competencia del personal de sala. Así que excluimos, por entender que son asuntos de alto interés pero que exceden su cometido, aquellos que impliquen un conocimiento tecnológico especializado. No obstante, aportamos en la

[20] GT29 es el Grupo de Trabajo de Protección sobre Protección de Datos del Artículo 29 o de las Personas en lo que respecta al Tratamiento de Datos Personales de la Comisión Europea.

siguiente relación elementos en los que la infraestructura juega un papel esencial:

- La inclusión sistemática de un plan de seguridad informática en el Plan de Seguridad de la Biblioteca (que tradicionalmente vela por la protección de las instalaciones físicas y del patrimonio bibliográfico) y sus correspondientes planes de contingencia (UNE-EN ISO 22301:2015).
- La necesaria actualización del software (desde su actualización, parcheo de seguridad si es preciso y medidas elementales de seguridad primaria, tales como instalación y mantenimiento de antivirus y cortafuegos (UNE 71044:1999; ISO/IEC 33004:2015).
- Todo lo que gira en torno a la resiliencia y planes de contingencia. UNE-EN ISO/IEC 27000:2019; ISO/IEC 27005:2018).
- Empleo de discos duros y otros almacenamientos (INCIBE 2016).
- Si se empleara la nube[21], sea para uso de computación o almacenaje, tanto propia (por ejemplo, ownCloud) como ajena (por ejemplo Dropbox), el cumplimiento de los mínimos de seguridad y consideraciones sobre la privacidad (UNE 71380:2014; UNE 71381:2016).
- Vigilancia sobre los accesos a la WiFi y sus posibles usos fraudulentos, tanto pública como privada.
- Atención al catálogo en línea (OPAC) y las plataformas de descubrimento[22]. Una manipulación, accidental o malintencionada del mismo debería ser detectada con la máxima premura para poder revertir los efectos (CCN 2018).

Sobre esos temas puntuales que apuntábamos, quedará dar instrucciones sobre:

- Vigilancia ante el riesgo de que los servicios informáticos de uso público, como ordenadores de libre acceso, puedan ser empleados por

[21] La «computación en la nube», traducción de *cloud computing*, permite ofrecer servicios de computación a través de Internet.

[22] Para acercarse al conocimiento de estas herramientas resulta imprescindible el artículo de Alvite Díez (2012).

malos fines: desde el riesgo de su uso para accesos indebidos a servidores de la institución o de utilización como zombies[23].

- Vigilancia ante la suplantación de la personalidad (personas que se hacen pasar por otras personas) (Gámiz Mejías 2018).
- Destrucción de material confidencial (UNE-EN 15713:2010).
- Revisión de antivirus: detección de inactividad y posibles motivos, identificación y correcta interpretación de sus mensajes…

6.3. Cómo: forma

El diseño curricular del curso no puede ser, dada la elevada casuística entre centros y su personal, algo monolítico. Encontrarnos con una población compuesta por usuarios con distintos conocimientos previos y centros con unos u otros servicios, aconsejan a un diseño modular.

Puede parecer, y de hecho es así, que nos movemos en un terreno especulativo, debido a la falta de información concreta sobre el estado actual. San Nicolas y Burkhard (2019) nos hablan así de la escasez de investigación sobre prácticas de seguridad de la información en bibliotecas:[24]

> *Si bien los bibliotecarios y otros empleados de la biblioteca pueden comprender la importancia de la protección de datos, generalmente no tienen los recursos disponibles para evaluar el riesgo de seguridad de la información, emplear estrategias de mitigación de riesgos u ofrecer programas de educación, capacitación o concientización sobre seguridad […]. Esto es especialmente preocupante ya que las bibliotecas tienen cada vez más acceso a las bases de datos de información personal y con derechos a proteger. […] En las bibliotecas, los sistemas de información se utilizan para proporcionar servicios a los usuarios, sin embargo, se sabe poco sobre las prácticas de seguridad de la información en ellas. Dada la alta sensibilidad de los datos manejados en las bibliotecas y la falta de recursos de seguridad de la información disponibles para hacer frente a su protección, es importante para aquellos que [trabajen en bibliotecas adquirir] conocimientos para identificar riesgos y desarrollar y emplear estrategias de mitigación de riesgos.*

No vamos por tanto a cubrir de forma exhaustiva los diseños de programas, su temporización, medios de impartición, estrategias docentes o tan siquiera

[23] Ordenadores infectados por *malware*, usados para ejecutar actividades ilícitas o al menos hostiles.
[24] Traducción propia.

objetivos de aprendizaje. Tratamos solo de dar una serie de consejos que puedan resultar de utilidad.

El primero será sobre el canal a emplear. Básicamente la formación para profesionales sigue uno de los tres cauces: presencial, teleformación o, un paso intermedio entre ambos, la semipresencialidad. Esto no es en absoluto una novedad, pues ya Benito Morales y otros (2000) plantearon hace un par de décadas un curso con la comunicación basada en el software de gestión del propio curso, correo electrónico, videoconferencia, panel de discusión y videos pregrabados.

Descartamos el formato puramente presencial por dos razones básicas: los elevados recursos económicos precisos para ponerlo en marcha (desplazamiento de profesores, adecuación de aulas, etc.) y, lo principal, lo difícil que resulta encontrar un espacio y momento común para los implicados, potenciado por el escaso personal existente en algunas bibliotecas, que haría virtualmente imposible gestionar cursos a la carta.

Esto nos lleva a pensar bien en una telepresencialidad pura, bien en un formato donde coexista alguna sesión de lección magistral. Alguna charla invitada o la organización de jornadas que pudieran servir al tiempo de punto de encuentro cubrirían ese punto de presencialidad cuya carencia pueda ser problemático: la falta de contacto humano hace menos atractivos los cursos e incluso puede incrementar el índice de abandono. Aun así, si no fuera posible, puede ser de alguna manera paliado mediante el uso de herramientas online como foros o videoconferencias, algo que se viene estudiando desde largo tiempo atrás (Oltra Gutiérrez 1999; Ramón Fernández y otros 2013; Álvarez, Cardona, Padilla 2004) y ha comenzado tímidamente a aplicarse en el ámbito de la información y la documentación. Hoy por hoy, gracias a las redes sociales, el contacto se humaniza y flexibiliza, independientemente de variables espaciales y temporales (Garrigós-Simón y otros, 2016).

La opción elegida en esta propuesta para dotarla de una mayor adaptabilidad es la de los MOOC[25]: resultan adaptables pues permiten estructurar distintos

[25] MOOC, acrónimo de *Massive Online Open Courses*, cursos masivos y abiertos mediante Internet. Como características principales tienen su posible seguimiento desde cualquier lugar con una conexión internet por cualquier interesado, sin límite de matrícula, siendo abierto a todos y gratuito.

módulos, que serían cursados o no según las características de los usuarios (si ya conocen el tema, o no les interesa porque no corresponde a la realidad de su centro, pueden prescindir) y establecer distintos nieles, donde el interesado puede pasar desde un simple barniz en los términos a conocimientos más profundos. Esta flexibilidad no es algo exclusivo de los MOOC (Oltra Gutiérrez, Miguel Molina 2002), ni sería el único camino el aplicarlo sobre internet (Oltra Gutièrrez y otros, 2009), pero es accesible a todo tipo de alumno con el único requisito de poder disponer de un dispositivo conectado a internet.

Una ventaja adicional es poder emplear recursos externos (desde videos de YouTube a materiales desarrollados por el INCIBE), lo que reduciría considerablemente los costes de creación del mismo. Existen recursos gratuitos y/o puestos a disposición por las administraciones que son invisibles para toda persona sin una mínima indicación al respecto.

Un elemento de interés sería establecer mediante un test previo (que puede ser corregido de forma automática, sin intervención humana alguna) el grado de formación previa en aspectos de ciberseguridad y, una vez establecido éste, las características de su puesto de trabajo (también fáciles de recoger con un formulario automatizado). Este test permitiría generar una ruta de formación personalizada mediante la cual avanzar por los contenidos. De igual forma, sería conveniente conocer de manera previa sus conocimientos relativos a sus obligaciones con respecto a la privacidad de los usuarios y de las personas que en general participen en la biblioteca. No estaría de más, por último, efectuar comprobaciones sobre el estado de la seguridad de las bibliotecas (Ismail, Ngah Zainab 2013).

Como extra, sería un magnífico complemento a esta formación propuesta la incorporación de la formación en ciberseguridad en los programas ALFIN y aprovechar para hacer una difusión de los mismos desde las bibliotecas públicas (Pinto, Sales 2007).

La flexibilidad aludida puede lograrse con herramientas de contenido condicional o, de forma más simple, mediante la creación de microcursos que tengan independencia entre sí, o, en algún caso, tengan una prelación establecida.

7. Predicciones próximos años. Riesgos de TIC innovadoras

En un contexto de cambios acelerados como el de las tecnologías de la información y las comunicaciones escribir sobre el presente supone el riesgo evidente de quedar obsoleto en un periodo muy breve de tiempo, de forma que escribir sobre el futuro parece casi un ejercicio de adivinación.
Pero a riesgo de quedar en evidencia dentro de pocos años, si alguien rescata este artículo y lo contrasta con la actualidad del momento, existen una serie de aspectos que ya permiten atisbar futuros problemas, hoy no preocupantes en las bibliotecas, pero que pueden generar mucho daño a corto o medio plazo. Sin ánimo de exhaustividad, nos limitaremos a mencionar los que consideramos principales, destacando un último punto, ya presente, pero con potenciales vulnerabilidades crecientes: el empleo de dispositivos propios para acceder a los recursos de la biblioteca, algo válido para los usuarios como para trabajadores[26].

7.1. Internet de las cosas

Todos los aparatos que nos rodean paulatinamente irán incorporando sensores para recopilar datos e interconectarse entre ellos. Los primeros dispositivos que hablaron entre ellos fueron los cajeros automáticos, en 1974. En el año 2008 el número de dispositivos conectados a Internet superaron al número de habitantes del planeta (Caballero Velasco, Cilleros Serrano 2019) y si atentemos a la Internet Society (Rose, Eldridge, Chapin 2015), en el año 2025 tendremos 100 mil millones de conexiones de la Internet de las Cosas (IoT, por sus siglas en inglés).

La principal debilidad del IoT está justamente en esos sensores, que por distintas razones (reducción de costes, incremento de la velocidad…) no incorporan en general por sí solos medidas de seguridad tales como aquellas que permiten la encriptación de los datos, lo que puede provocar que alguien capture el tráfico y vulnere la privacidad de las personas. Pero pensemos qué dispositivos propios de la biblioteca (una pantalla en una zona de estudio

[26] «Trae tu propio dispositivo», usualmente conocido por sus siglas en inglés, BYOD (*Bring Your Own Device*), alude al empleo de los trabajadores de sus equipos privados en su puesto laboral.

aislado, un arco de seguridad…) o ajenos (una máquina de refrescos en una zona de descanso) pronto serán comercializados dotados de sensores. Puede parecer una exageración, pero recordemos que ya hemos visto ataques de denegación de servicios por medio de electrodomésticos[27], y eso en un estado incipiente de la IoT.

7.2. Identidad digital y biometría

El problema de la identidad, el modo de acceso a los servicios de la biblioteca, lo hemos tratado. Pero estos métodos pueden variar en muy poco tiempo. Los métodos biométricos (sensores de huella digital, identificación facial, reconocimiento de retina, etc.) son más precisos e implican por tanto un mayor acierto evitando suplantaciones de personalidad. Además, el abaratamiento del hardware necesario para tal fin parece auspiciar una viralización de estos sistemas.

Además de sus beneficios, presentan varios riesgos: por una parte, se puede recoger lo que llamaremos el *hash biométrico*[28] de un individuo o, incluso de forma más burda, duplicar lo captado (un molde de una huella digital en silicona, por ejemplo). Por otra parte, queda el riesgo de robo de datos para otros usos. Hay que dejar claro que lo que se protege es el dato en sí, no el uso del mismo. En este sentido hay una sentencia reciente de la audiencia nacional (STS 3675/2019).

7.3. Inteligencia Artificial

La inteligencia artificial (IA) ha escapado hace tiempo de las películas y novelas de ciencia ficción para vivir entre nosotros. La emplean videojuegos, sistemas de retocado fotográfico, traducción, automatización de fábricas y «bots» o sistemas de respuesta automática, muy empleados ya por bancos y aseguradoras y que, aunque tímidamente, comienzan a asomar en algunas bibliotecas[29]. Pero es que dentro de una biblioteca la IA puede tener muchos usos: desde esos *chatbots* a los que aludíamos para interactuar con los usuarios a resolver pequeñas dudas relativas a la logística, para facilitar una

[27] Saravia 2016.
[28] Una expresión fácil de calcular que resume una entrada más compleja: la distancia de los ojos, etc.
[29] Young 2019.

organización más eficiente de los volúmenes, para mejorar la climatización del edificio, para obtener pronósticos que permitan mejorar la adquisición de obras…

Un elemento fundamental para la IA es el *Machine Learning*, el aprendizaje automático, que permite a los ordenadores aprender por sí mismos. Y esto presenta fortalezas que pueden ser aprovechadas más allá de los riesgos, Siguiendo a Caballero Velasco y Cilleros Serrano (2019), encontramos entre aquellas el reconocimiento de patrones en los datos (características explícitas y ocultas en los datos que pueden servir para reconocer patrones) o la detección de anomalías (es decir, lo inverso: conocidos los patrones, buscamos algo «que no encaje»). Gracias a estos mecanismos podemos, por ejemplo, detectar el *spam* saliente y entrante de una organización, detectar intentos de instalación de *malware*, reconocer suplantaciones de usuario, controlar accesos, etc.

7.4. Uso de dispositivos propios

Esto, más que una amenaza futura, es algo muy presente. Son muchos ya los usuarios que emplean sus propios dispositivos para conectarse a las redes WiFi de una biblioteca. Y esto presenta una serie de problemas potenciales para la biblioteca, pero sobre todo para el usuario, en el que ponemos el acento.

Básicamente, al menos de momento, hay dos asuntos que generan un interés alto para las autoridades de protección de datos: uno, las aplicaciones móviles (responde esto a la pregunta ¿podemos forzar la instalación de una app en un dispositivo para que éste pueda tener acceso a nuestra red?) (GT29 2013) y la llamada huella digital de dispositivo (AEPD 2019b) : para identificar a los usuarios se utilizan diferentes técnicas de seguimiento, destacando las llamadas *cookies*[30]. Esto está suficientemente protegido por la ley y por la evolución de la técnica como para que los interesados en obtenerlos de forma irregular a toda costa busquen nuevos medios para saltarse esas protecciones y así poder recopilar datos de los usuarios. Destacan con este fin las técnicas *device*

[30] Ficheros almacenados en el ordenador del usuario que accede a la web.

fingerprinting, *browser fingerprinting* o *fingerprinting*, (huella digital del dispositivo o huella del dispositivo)[31] (AEPD 2019b).

Ese perfilado no se limita a recopilar y analizar los hábitos de navegación del usuario o las búsquedas que realiza en servidores, sino registrar los movimientos que realiza el usuario a través de la página web con el ratón, examinando en que partes de la pantalla se detiene por más tiempo. Si eso lo unimos a la facilidad técnica para recoger información concreta como tipo y versión de navegador y sistema operativo, resolución de la pantalla, dirección IP, etc., vemos que se permite obtener una huella digital que diferencia de forma univoca a cada usuario en internet, facilitando por tanto la elaboración de perfiles que reflejan el comportamiento privado de los mismos.

8. Conclusiones

Es un elemento clave en el día a día de nuestra sociedad tecnodependiente el mantenerse a salvo de ciber-riesgos. Y si eso es así en la sociedad en general, en el caso de las bibliotecas en particular, lugar transitado por muchos ciudadanos, el asunto cobra especial interés. Si a esto le sumamos el peso que ha ganado no solo de forma legal, sino también por concienciación social, la privacidad, la protección de los datos personales en suma, y consideramos que estos se pueden poner en juego tan solo accediendo a determinados servicios que ofrece una biblioteca, tenemos un escenario que necesita una actuación.

La propuesta presente pasa por reforzar, incluso ofrecer un primer acercamiento a temas tan sensibles. El proceso de formación a los trabajadores de una biblioteca no puede estar sujeto una receta única, tanto por la diversidad de servicios prestados por las distintas bibliotecas, como por el nivel de conocimientos previos de su personal. A esto se suma que se trata de temas con una evolución tan acelerada como la ciberseguridad, por razones tecnológicas, o la privacidad, con recientes cambios normativos de calado.

[31] El Grupo de Trabajo de Protección sobre Protección de Datos del Artículo 29 de la Comisión Europea (GT29 2014) hace propia la definición de la huella proporcionada por Cooper y otros (2013) como «un conjunto de elementos de información que identifica un dispositivo o una instancia de aplicación».

Como además los recursos económicos suelen ser escasos, el planteamiento pasa por un curso masivo, abierto y configurable, de modo que la preparación pueda ser realizada por un limitado número de personas, que únicamente deben estar atentos a posibles cambios que provoquen modificaciones en el material. Modificaciones que, por otra parte, afectarán siempre a unidades mínimas, siendo el resto de la formación reutilizable una y otra vez.

En cuanto al futuro inmediato, coincidimos con Reid (2019) en que el foco puede centrarse en la identificación del usuario: de la identificación institucional a la identificación social (sea ésta procedente de otras entidades públicas o de empresas privadas, como Google o Facebook). De igual manera, Reid, centrado en las bibliotecas universitarias pero con reflexiones válidas para todas, advierte que la tendencia histórica a hacer un uso liberal del consentimiento dado por los usuarios para el tratamiento de sus datos (tanto en lo que respecta a su cesión a terceros, tales como publicaciones electrónicas, como en el tratamiento propio, buscando mejorar los procesos de suscripción y renovación) debe ser reconsiderado a la luz de la legislación (Reglamento (UE) 2016/679; Ley Orgánica 3/2018), incluyendo las recomendaciones pertinentes que, a raíz de los cambios normativos, surgen en temas antes inexistentes, como la privacidad por diseño y por defecto (AEPD 2019) o en aquellos donde los cambios han sido profundos, como en el consentimiento (GT29 2018b).

En definitiva, se trata de crear una herramienta de formación frente a los riesgos tecnológicos en las bibliotecas, incorporando esos conocimientos a los procesos de información y gestión bibliotecaria, a la cultura de la seguridad propia de las bibliotecas.

9. Bibliografía

AENOR, 1999. *Tecnología de la información. Procesos del ciclo de vida del software.* UNE 71044:1999. Madrid: AENOR

AENOR, 2006. *Gestión de la I+D+i: terminología y definiciones de las actividades de I+D+i.* UNE 166000:2006. Madrid: AENOR

AENOR, 2010. *Gestión del riesgo. Vocabulario*. UNE-ISO Guía 73:2010 IN. Madrid: AENOR

AENOR, 2010b. *Destrucción segura del material confidencial. Código de buenas prácticas*. UNE-EN 15713:2010. Madrid: AENOR

AENOR, 2011. *Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario*. UNE-ISO 30300:2011. Madrid: AENOR

AENOR, 2013. *Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales*. UNE 71505-1:2013. Madrid: AENOR

AENOR, 2014. *Tecnología de la información. Computación en la nube. Vocabulario y definiciones*. UNE 71380:2014. Madrid: AENOR

AENOR, 2015. *Protección y seguridad de los ciudadanos. Terminología. (ISO 22300:2012)*. UNE-EN ISO 22300:2015. Madrid: AENOR

AENOR, 2015b. *Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones. (ISO 22301:2012)*. UNE-EN ISO 22301:2015. Madrid: AENOR

AENOR, 2015b. *Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia*. UNE-ISO 14721:2015. Madrid: AENOR

AENOR, 2016. *Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios*. UNE-ISO 15489-1:2016. Madrid: AENOR

AENOR, 2016b. *Tecnología de la información. Computación en la nube. Sistemas de etiquetado*. UNE 71381:2016. Madrid: AENOR

AENOR, 2018. *Metodología de análisis y gestión de riesgos para los sistemas de información*. UNE 71504:2008. Madrid: AENOR

AENOR, 2018b. *Gestión del riesgo. Directrices*. UNE-ISO 31000:2018. Madrid: AENOR

AENOR, 2018c. *Gestión de la I+D+i: Sistema de vigilancia e inteligencia*. UNE 166006:2018. Madrid: AENOR

AENOR, 2019. *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario. (ISO/IEC 27000:2016)*. UNE-EN ISO/IEC 27000:2019. Madrid: AENOR

AEPD, 2018. *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD* [en línea]. Madrid: AEPD. [Consulta: 19 noviembre 2019]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

AEPD, 2018b. *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD* [en línea]. Madrid: AEPD. [Consulta: 19 noviembre 2019]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

AEPD, 2018c. *Listado de cumplimiento normativo* [en línea]. Madrid: AEPD. [Consulta: 19 noviembre 2019]. Disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf

AEPD, 2018d. *Guía para la gestión y notificación de brechas de seguridad* [en línea]. Madrid: AEPD. [Consulta: 19 noviembre 2019]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

AEPD, 2019. *Guía de privacidad desde el diseño* [en línea]. Madrid: AEPD. [Consulta: 19 noviembre 2019]. Disponible en: https://www.aepd.es/media/guias/guia-privacidad-desde-diseno.pdf

AEPD, 2019b. *Fingerprint o Huella digital del dispositivo* [en línea]. Madrid: AEPD. [Consulta: 18 diciembre 2019]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf

AGERS; ISMS Forum, 2017. *Guía de terminología de ciberseguridad*. Madrid: Asociación Española De Gerencia de Riesgos y Seguros. ISBN 978-84-697-3492-6. Disponible en: https://agers.es/guia-terminologia-ciberseguridad/

ALA, 1989. *Presidential Committee on Information Literacy: Final Report*. Chicago: Association of College & Research Libraries. [Consulta: 12 octubre 2019]. Disponible en: http://www.ala.org/acrl/publications/whitepapers/presidential

ALA, 2008. El Código de Ética de la Asociación de Bibliotecas de los Estados Unidos (American Library Association-ALA). En: *American Library Association* [en línea]. 19 mayo 2017. [Consulta: 19 diciembre 2019]. Disponible en: http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/proethics/codeofethics/coespanishversion/codigodeetica.pdf

ÁLVAREZ MARAÑÓN, G., 2011. Amenazas 2.0 para la Biblioteca 2.0. [en línea]. En: *V Congreso Nacional de Bibliotecas Públicas: bibliotecas públicas y contenidos digitales: retos y oportunidades*. Madrid: Ministerio de Cultura, Subdirección General de Coordinación Bibliotecaria, p. 183-189. [Consulta: 6 diciembre 2019]. Disponible en: https://hdl.handle.net/10421/4975

ÁLVAREZ, F. J.; CARDONA, P.; PADILLA, A., 2004. Estrategias Educativas para la creación de cursos en Ambientes de Aprendizajes Virtuales. En: *Simposium Iberoamericano de Educación, Cibernética e Informática*. Orlando (FL, USA), 21-25 julio.

Disponible en: https://www.researchgate.net/publication/240620571_Estrategias_educativas_para_la_creacion_de_cursos_en_ambientes_de_aprendizajes_virtuales

ALVITE DÍEZ, M. L., 2012. Redefiniendo el catálogo: expectativas de las interfaces de descubrimiento centradas en el usuario [en línea]. *Investigación bibliotecológica*, **26**(56), 181-204. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2012000100009. ISSN 2448-8321

ARROYO-VÁZQUEZ, N.; HERNÁNDEZ-SÁNCHEZ, H.; GÓMEZ-HERNÁNDEZ, J.-A., 2019. *Las bibliotecas públicas en España: diagnóstico tras a crisis económica*. Madrid: FESABID. [Consulta: 9 diciembre 2019]. ISBN 978-84-939694-2-4. Disponible en: http://www.fesabid.org/sites/default/files/images/fesabid/Informe-fesabid-v12-digital.pdf

BENITO MOTALES, F., y otros, 2000. *Estrategias y modelos para enseñar a usar la información: guía para docentes, bibliotecarios y archiveros* [en línea]. J. A. Gómez Hernández, coord. Murcia: KR. Disponible en: [Consulta: 18 diciembre 2019]. ISBN 84-88661-63-0. Disponible en: http://eprints.rclis.org/6717/

Bibliotecas públicas españolas en cifras [en línea]. Madrid: Ministerio de Cultura y Deporte. [Consulta: 8 diciembre 2019]. Disponible en: http://www.culturaydeporte.gob.es/cultura/areas/bibliotecas/mc/ebp/portada.html

BIRNBAUM, J. S., 2004. Cybersecurity Considerations for Digital Libraries in an Era of Pervasive Computing. En: *Proceedings of the 4th ACM/IEEE-CS joint conference on Digital libraries*. New York: Association for Cumputing Machinery, p. 169. ISBN 1-58113-832-6. doi: 10.1145/996350.996352

CABALLERO VELASCO, M. A.; CILLEROS SERRANO, D., 2019. *Ciberseguridad y transformación digital*. Madrid: Anaya. ISBN 978-84-415-4162-7

CASTILLO FONSECA, J. M.; ZAVALA JUÁREZ, B., 2019. Ciberseguridad y vigilancia tecnológica: un reto para la protección de datos personales en los archivos [en línea]. *Tlatemoani*, 31, 218-246. [Consulta: 7 octubre 2019]. Disponible en: http://hdl.handle.net/20.500.11763/tlatemoani31ciberseguridad. ISSN 1989-9300

CCN, 2018. *Esquema Nacional de Seguridad: gestión de ciberincidentes*. CCN-STIC 817. Madrid: Centro Criptológico Nacional. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes.html

CEBULA, J. J.; YOUNG, L. R., 2010. *A Taxonomy of Operational Cyber Security Risks*. Pittsburgh: Software Engineering Institute, Carnegie Mellon University. [Consulta: 1 diciembre 2019]. Disponible en: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395

CHÁVEZ FLORES, A. T., 2009. *Seguridad informática (informe)*. Informe de pasantía. Consejo Latinoamericano de Ciencias Sociales. [Consulta: 10 noviembre 2019]. Disponible en: https://es.slideshare.net/mariorafaelquirozmartinez/seguridad-informtica-27231511

CILIP. Information Literacy Group, 2018. *CILIP Definition of Information Literacy*. London: CILIP Information Literacy Group. [Consulta: 12 octubre 2019]. Disponible en: https://infolit.org.uk/ILdefinitionCILIP2018.pdf

COOPER, A. y otros, 2013. Privacy Considerations for Internet Protocols [en línea]. *Request for comments*, 6973. [Consulta: 18 diciembre 2019]. Disponible en: https://tools.ietf.org/html/rfc6973

CÓPPOLA, G., 2012. Gestión del Riesgo Comunicacional. Puesta en práctica [en línea]. *Cuadernos del Centro de Estudios de Diseño y Comunicación*, **12**(40), 33-46. [Consulta: 7 diciembre 2019]. Disponible en: http://www.scielo.org.ar/pdf/ccedce/n40/n40a04.pdf. ISSN 1853-3523

CORDA, M.; VIÑAS, M.; CORIA, M., 2017. Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje [en línea]. *Palabra Clave*, **7**(1, e032). [Consulta: 8 diciembre 2019]. ISSN 1853-9912. Disponible en: https://doi.org/10.24215/18539912e032

CORRAL BELTRÁN, M., 1977. La biblioteca universitaria y la formación de usuarios en la Universidad [en línea]. *Boletín de la ANABA*, **27**(2), 28-36. [Consulta: 2 diciembre 2019]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/967596.pdf. ISSN 0044-9288

DEJ, 2019. Diccionario del español jurídico. En: *Real Academia Española* [en línea]. Madrid: Real Academia Española. [Consulta: 12 octubre 2019]. Disponible en: https://dej.rae.es/

DÍAZ SÁENZ, J. R, 2015. *Factores críticos en la adopción de las medidas de seguridad utilizadas por los alumnos de los Centros formativos universitarios de tecnologías TIC al usar herramientas 2.0*. Directores: Hermenegildo Gil Gómez, Juan Vicente Oltra Gutiérrez. Tesis doctoral. Universitat Politècnica de València. [Consulta: 1 noviembre 2019]. Disponible en: https://riunet.upv.es/handle/10251/56465

DÍAZ SALAZAR, C., 2018. *La formación de bibliotecarios en el buen trato hacia la comunidad a través del B-Learning*. Trabajo de Maestría en Informática Educativa. Universidad

de La Sabana. Directora: Ana Dolores Vargas Sánchez. [Consulta: 12 octubre 2019]. Disponible en: https://intellectum.unisabana.edu.co/handle/10818/34603

EBIBLIO, 2018. eBiblio, 2018. En: *eBiblio* [en línea]. Madrid: Ministerio de Cultura y Deporte. [Consulta: 10 diciembre 2019]. Disponible en: https://www.culturaydeporte.gob.es/dam/jcr:bd2243e2-5f17-431f-8ead-6990f1905355/ebiblio-2018-est.pdf

ESPAÑA, 2010. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. *Boletín Oficial del Estado* [en línea], 29 de enero de 2010, 25, 8089-8138 [Consulta: 24 octubre 2019]. ISSN 0212-033X. Disponible en: https://www.boe.es/eli/es/rd/2010/01/08/3/con

ESPAÑA, 2011. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *Boletín Oficial del Estado* [en línea], 29 de abril de 2011, 102, 43370-43380 [Consulta: 24 octubre 2019]. ISSN 0212-033X. Disponible en: https://www.boe.es/eli/es/l/2011/04/28/8/con

ESPAÑA, 2015. Tribunal Supremo (Sala de lo Civil, Sección 991). *Sentencia n. 4132/2015 de 15 de octubre*. ECLI:ES:TS:2015:4132. Disponible en: http://www.poderjudicial.es/search/AN/openDocument/4e8ef5015f4aeb90/20151019

ESPAÑA, 2018. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado* [en línea], 7 de diciembre 2018, 294, 119788-119857. [Consulta: 24 octubre 2019]. ISSN 0212-033X. Disponible en: https://www.boe.es/eli/es/lo/2018/12/05/3/con

ESPAÑA, 2018. Tribunal Constitucional (Sala Primera). *Sentencia n. 58/2018 de 4 de junio*. ECLI:ES:TC:2018:58. Disponible en: https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25683

ESPAÑA, 2019. Tribunal Supremo (Sala de lo Contencioso, Sección 1). *Sentencia n. 3675/2019 de 19 de septiembre*. ECLI: ES:AN:2019:3675. Disponible en: http://www.poderjudicial.es/search/AN/openDocument/19b8682810e3f39a/20191023

ETSINF, 2017. *Doble Grado en Ingeniería Informática y en Administración y Dirección de Empresas* [en línea]. València: Universitat Politècnica de València. [Consulta: 29 de octubre de 2019]. Disponible en: https://www.inf.upv.es/www/etsinf/es/doble-grado-en-ingenieria-informatica-y-administracion-y-direccion-de-empresas/

FESABID, 2017. *IFLA Global Visión: informe de los resultados de la encuesta en España*. Madrid: FESABID. [Consulta: 13 diciembre 2019]. Disponible en:

http://www.fesabid.org/sites/default/files/repositorio/informe_encuesta_espanola_ifla_global_vision.docx_.pdf

GALINDO LÓPEZ, C. M., 2014. La firma electrónica avanzada y su certificación. En: *Seguridad de la información*. Guatemala: Universidad San Carlos de Guatemala, Facultad de Ciencias Jurídicas y Sociales, Escuela de Estudios de Postgrado, p. 89-119. ISBN 978-9929-40-621-6

GÁMIZ MEJÍAS, M, 2018. *Suplantación de personalidad en Internet*. Director: Juan Vicente Oltra Gutiérrez. Trabajo Fin del Máster Universitario en Gestión de la Información. Universitat Politècnica de València. [Consulta: 1 noviembre 2019]. Disponible en: http://hdl.handle.net/10251/107789

GARCÍA MIRETE, C.M., 2014. *Bases de datos electrónicas internacionales*. Valencia: Tirant lo Blanch. ISBN 978-84-9033-951-0

GARRIGOS-SIMON, F. J., y otros, 2016. Ventajas y usos de Twitter, como herramienta de mejora de la educación universitaria. En: *In-Red 2016: II Congreso de Innovación Educativa y Docencia en Red* [en línea]. València: Editorial Universitat Politècnica de València. Disponible en: http://dx.doi.org/10.4995/INRED2016.2016.4430

GODOY LEMUS, R., 2014. Seguridad de la información. En: *Seguridad de la información*. Guatemala: Universidad San Carlos de Guatemala, Facultad de Ciencias Jurídicas y Sociales, Escuela de Estudios de Postgrado, p. 160-173. ISBN 978-9929-40-621-6

GT29, 2013. *Opinion 02/2013 on apps on smart devices: adopted on 27 February 2013*. WP202. [Consulta: 18 diciembre 2019]. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

GT29, 2014. *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*. WP224. [Consulta: 18 diciembre 2019]. Disponible en: https://www.dataprotection.ro/servlet/ViewDocument?id=1089

GT29, 2017. *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679: adoptadas el 4 de abril de 2017, revisadas por última vez y adoptadas el 4 de octubre de 2017*. WP248rev.01. [Consulta: 15 diciembre 2019]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

GT29, 2018. *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el reglamento 2016/679: adoptadas el 3 de octubre de 2017, revisadas por*

última vez y adoptadas el 6 de febrero de 2018. WP250rev.01. [Consulta: 15 diciembre 2019]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/wp250rev01-es.pdf

GT29, 2018b. *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679: adoptadas el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018*. WP259rev.01. [Consulta: 15 diciembre 2019]. Disponible en: http://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf

GTALFIN, 2009. *Hacia la alfabetización informacional en las bibliotecas públicas españolas*. Madrid: Ministerio de Cultura, Subdirección General de Publicaciones, Información y Documentación. [Consulta: 26 noviembre 2019]. Disponible en: http://hdl.handle.net/10421/1303

GUERRERO JULIO, M. L.; GÓMEZ FLÓREZ, L. C., 2011. Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información. *Estudios gerenciales*, **27**(121), 195-215. [Consulta:15 diciembre 2019]. ISSN 2665-6744. doi:10.1016/S0123-5923(11)70188-7

IFLA, 2012. Código de Ética de la IFLA para bibliotecarios y otros trabajadores de la información (versión completa). En: *IFLA* [en línea]. 5 septiembre 2019. [Consulta: 19 diciembre 2019]. Disponible en: https://www.ifla.org/files/assets/faife/codesofethics/spanishcodeofethicsfull.pdf

IFLA, 2014. Declaración de Lyon: versión en español. En: *IFLA Latin America and the Caribbean Section Blog* [en línea]. 18 agosto 2014. [Consulta: 19 diciembre 2019]. Disponible en: https://blogs.ifla.org/lac/2014/08/declaracion-de-lyon-version-en-espanol/

IFLA, 2019. *Visión Global: resumen del informe: 10 reflexiones destacadas y oportunidades*. La Haya: IFLA. [Consulta: 13 diciembre 2019]. Disponible en: https://www.ifla.org/files/assets/GVMultimedia/publications/gv-report-summary-es.pdf

INCIBE, 2015. *Gestión de riesgos. Una guía de aproximación para el empresario*. Madrid: INCIBE. [Consulta: 23 noviembre 2019]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

INCIBE, 2016. Guía de almacenamiento seguro de la información. Madrid: INCIBE. [Consulta: 12 diciembre 2019]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf

INCIBE, 2017. *Glosario de términos de ciberseguridad*. Madrid: INCIBE. [Consulta: 19 noviembre 2019]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

INEbase, 2019. Nuevas tecnologías de la información y la comunicación. En: *Instituto Nacional de Estadística* [en línea]. Madrid: INE. [Consulta: 29 octubre 2019]. Disponible en: https://www.ine.es/dyngs/INEbase/es/categoria.htm?c=Estadistica_P&cid=1254735576692

INMOR, S.; ESICHAIKUL, V.; BATANOV, D. N., 2003. A Security-Oriented Extension of the Object Model for the Development of an Information System. *Information Systems Security*, **12**(2), 21-36. ISSN 1065-898X. doi:10.1201/1086/43326.12.2.20030501/42584.6

ISMAIL, R.; NGAH ZAINAB, A., 2013. Assessing the Status of Library Information Systems Security. *Journal of Librarianship and Information Science*, **45**(3), 232-247. ISSN 0961-0006. doi:10.1177/0961000613477676

ISO, 2011. *Information technology, Security techniques, Privacy framework*. ISO/IEC 29100:2011. Geneva: ISO

ISO, 2015. Information technology. Process assessment. Requirements for process reference, process assessment and maturity models. ISO/IEC 33004:2015. Geneva: ISO

ISO, 2018. *Information technology. Security techniques. Information security risk management*. ISO/IEC 27005:2018. Geneva: ISO

JIANG, Z.; HENG, C. S.; CHOI, B. C. F., 2013. Privacy Concerns and Privacy-Protective Behaviorin Synchronous Online Social Interactions. *Information Systems Research*, **24**(3), 579-595. [Consulta: 1 noviembre 2019]. Disponible en: https://pdfs.semanticscholar.org/139e/0beb6f40340508f952fc2e3ec48f8ab4df84.pdf?_ga=2.89307099.1319683615.1576956375-612204107.1576956375

JIMENO MUÑOZ, J., 2019. *Derecho de daños tecnológicos: ciberseguridad e insurtech*. Madrid: Dyckinson. ISBN 978-84-1324-146-3

JORNADAS DE COOPERACIÓN BIBLIOTECARIA. Grupo de Trabajo de Bases Tecnológicas para la Gestión y Cooperación Bibliotecaria, 2006. *Pautas para el servicio de acceso a Internet en las bibliotecas públicas*. Madrid: Ministerio de Cultura, Subdirección General de Coordinación Bibliotecaria. [Consulta: 12 octubre 2019]. Disponible en: https://hdl.handle.net/10421/394

KEEFER, A; GALLART, N., 2007. *La preservación de recursos digitales: el reto para las bibliotecas del siglo XXI*. Barcelona: Editorial UOC. ISBN 978-84-9788-567-6

LEAL, F., 2019. Las bibliotecas blindan sus fondos ante las ciberamenazas. En: *Byzness* [en línea]. 7 octubre 2019. [Consulta: 20 noviembre 2019]. Disponible en: https://byzness.elperiodico.com/es/innovadores/20191007/bibliotecas-blindan-fondos-ciberamenazas-7667289

MAGERIT, 2012. *MAGERIT, versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: Ministerio de Hacienda y Administraciones Públicas, Centro de Publicaciones. [Consulta: 16 diciembre 2019]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

MARWICK, A. E.; MURGIA DIAZ, D.; PALFREY, P., 2010. *Youth, Privacy, and Reputation*. Cambridge, MA, USA: The Berkman Center for Internet & Society at Harvard University. [Consulta: 1 noviembre 2019]. Disponible en: http://ssrn.com/abstract=1588163

MENDOZA RAMOS, J. C. A., 2019. *Aplicación de un hacking ético para mejorar la ciberseguridad de una entidad del Estado*. Director: Director: Rembrandt Ubalde Enriquez. Trabajo de suficiencia profesional. Universidad Tecnológica del Perú. [Consulta: 24 octubre 2019]. Disponible en: http://repositorio.utp.edu.pe/handle/UTP/1880

MUGI, 2019. *Máster Oficial Universitario en Gestión de la Información* [en línea]. València: Universitat Politècnica de València. [Consulta: 29 octubre 2019]. Disponible en: http://mugi.webs.upv.es/

NERDWRITER, The [Nerdwriter1], 2018. *How Dark Patterns Trick You Online*. 28 marzo 2018. [Vídeo de YouTube]. [Consulta: 15 diciembre 2019]. Disponible en: https://youtu.be/kxkrdLI6e6M

OLTRA GUTIÉRREZ, J. V., 1999. Herramientas Internet como apoyo a la ingeniería. En: VII Congreso Universitario de Innovación Educativa en las Enseñanzas Técnicas. La Rábida: Escuela Politécnica Superior, p. 1111-1124. ISBN 84-931043-0-2

OLTRA GUTIÉRREZ, J. V., y otros, 2009. Recursos educativos abiertos: ¿una opción para TDT?. En: *Actas del 17 Congreso Universitario de Innovación Educativa en Enseñanzas Técnicas*. València: Editorial Universitat Politècnica de Valencia. ISBN 978-84-613-4617-2

OLTRA GUTIÉRREZ, J. V.; MIGUEL MOLINA, M., 2002. Un método flexible aplicando las Nuevas Tecnologías. En: *X Congreso Universitario de Innovación*

Educativa en las Enseñanzas Técnicas. València: Editorial Universitat Politècnica de Valencia. ISBN 84-9705-207-2

ORERA-ORERA, L., 2002. La evolución en la formación de los bibliotecarios. *Documentación de las Ciencias de la Información*, 25, 167 - 188. ISSN 0210-4210. Disponible en: http://hdl.handle.net/10760/15143

PINTO, M.; SALES, D., 2007. Alfabetización informacional para una sociedad intercultural: algunas iniciativas desde las bibliotecas públicas [en línea]. *Anales de documentación*, 10, 317-333. [Consulta: 20 noviembre 2019]. Disponible en: https://revistas.um.es/analesdoc/article/view/1221/1271. ISSN 1697-7904

PINTO, M.; URIBE-TIRADO, A., 2011. Formación del bibliotecario como alfabetizador informacional. *Anuario ThinkEPI*, 5, 13-20. [Consulta: 12 octubre 2019]. ISSN 2564-8837. Disponible en: http://hdl.handle.net/10760/15790

POT, J., 2018. Dark Patterns: When Companies Use Design to Manipulate You. En: *How-To Geek* [en línea]. 26 agosto 2018. [Consulta: 15 diciembre 2019]. Disponible en: https://www.howtogeek.com/363484/dark-patterns-when-companies-use-design-to-manipulate-you/

PRIETO GUTIÉRREZ, J. J., 2009. Seguridad en bibliotecas. *Seguritecnia*, 355, 60-64. ISSN 0210-8747. Disponible en: https://eprints.ucm.es/9505/

PRIETO GUTIÉRREZ, J. J., 2013. *Plan de seguridad en bibliotecas: la protección del patrimonio documental*. Gijón: Trea. ISBN 978-84-9704-696-1

QUILO JÁUREGUI, J. M., 2014. La Constitución política y la protección de la información. En: *Seguridad de la información*. Guatemala: Universidad San Carlos de Guatemala, Facultad de Ciencias Jurídicas y Sociales, Escuela de Estudios de Postgrado, p. 230-240. ISBN 978-9929-40-621-6

RAMÓN FERNÁNDEZ, F., y otros, 2013. La comunicación 2.0. En: V Jornada de Innovación Docente JIDINF'12. Valencia: Universitat Politècnica de València, Poster. ISBN 978-84-9048-030-4

REBIUN, 2018. Consulta de datos. En: *CRUE, Red de Bibliotecas REBIUN* [en línea]. Murcia: Universidad de Murcia. [Consulta: 9 diciembre 2019]. Disponible en: https://rebiun.um.es/rebiun/admin/ManageIndicatorsPage

REID, P., 2019. Usability and Privacy in Academic Libraries: Regaining a Foothold Through Identity and Access Management [en línea]. *Insights* **32**(33). Disponible en: http://doi.org/10.1629/uksg.487. ISSN 2048-7754

ROCAFULL, O., 2018. *Grado de conocimiento de ciberseguridad de la generación digital*. Trabajo de Fin de Grado en Seguridad. Institut de Seguretat Pública de Catalunya.

Barcelona. [Consulta: 1 noviembre 2019]. Disponible en: https://www.recercat.cat/handle/2072/338145

RODRÍGUEZ PÉREZ, Y., y otros, 2018. La ciberseguridad en el contexto actual. En: T. DELGADO FERNÁNDEZ, A. FEBLES ESTRADA coords. *Cibersociedad: soñando y actuando*. La Habana: Ediciones Futuro, p. 189-201. ISBN 978-959-286-067-4. Disponible en línea en: https://www.researchgate.net/publication/330618446_Cibersociedad_-_Sonando_y_Actuando

ROSE, K.; ELDRIDGE, S.; CHAPIN, L., 2015. *La Internet de las Cosas: una breve reseña*. Resto, VA, USA: Internet Society, 2015

ROSE, K.; ELDRIDGE, S; CHAPIN, L., 2015. *La Internet de las Cosas: una breve reseña*. Resto, VA, USA: Internet Society. [Consulta: 9 diciembre 2019]. Disponible en: https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf

SALDAÑA, M. N., 2012. «The right to privacy»: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis [en línea]. *Revista de Derecho Político*, 85. [Consulta: 12 octubre 2019]. ISSN 2174-5625. Disponible en: https://doi.org/10.5944/rdp.85.2012.10723

SAN NICOLAS-ROCCA, T.; y BURKHARD, R. J., 2019. Information Security in Libraries: Examining the Effects of Knowledge Transfer [en línea]. *Information Tecnology and Libraries* **38**(2), 58-71. [Consulta: 22 noviembre 2019]. ISSN 2163-5226. Disponible en: https://doi.org/10.6017/ital.v38i2.10973

SÁNCHEZ PAUS, L., 1997. Concepto de formación de usuarios: claves para un servicio de calidad [en línea]. *Educación y biblioteca*, 84, 44-47. [Consulta: 2 diciembre 2019]. ISSN 0214-7491. Disponible en: http://hdl.handle.net/10366/113429

SARABIA, D., 2016. Un ejército de dispositivos zombis, listo para destruir Internet [en línea]. *El Diario*, 24 octubre 2016. [Consulta: 29 octubre 2019]. Disponible en: https://www.eldiario.es/tecnologia/Millones-dispositivos-planean-destruir-Internet_0_572892955.html

SENA, L.; TENZER, S. M., 2004. *Introducción a Riesgo informático*. Montevideo: Universidad de la República, Cátedra Introducción a la Computación [Consulta: 12 noviembre 2019]. Disponible en: http://www.academia.edu/14745302/Estructura_del_documento_de_riesgos_inform%C3%A1ticos

SERVICIO DE BIBLIOTECAS DEL GOBIERNO VASCO, 2018. Estadísticas 2018 [en línea]. *Bibliotecas*, 2018, 3-16. [Consulta: 10 diciembre 2019]. Disponible en: https://www.euskadi.eus/contenidos/informacion/publicacion_profesional_biblio/es_def/adjuntos/Revista2018ES.pdf

SILVERA ITURRIOZ, C., 2005. Los bibliotecarios en la sociedad de la información. *ACIMED*, **13**(3). [Consulta: 12 octubre 2019]. ISSN 1024-9435. Disponible en: http://hdl.handle.net/10760/6674

TACÓN CLAVAÍN, J., 2008. *La conservación de archivos y bibliotecas: prevención y protección*. Madrid: Ollero y Ramos. ISBN 978-84-7895-252-6

UNIÓN EUROPEA, 2013. Reglamento (UE) 611/2013 de la Comisión de 24 de junio de 2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas. *Diario Oficial de la Unión Europea* [en línea], 26 de junio de 2013, L 132, 2-8 [Consulta: 12 octubre 2019]. ISSN 1977-0685. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:eS:PDF

UNIÓN EUROPEA, 2014. Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. *Diario Oficial de la Unión Europea* [en línea], 23 de julio de 2014, L 257, 73-114 [Consulta: 12 octubre 2019]. ISSN 1977-0685. Disponible en: http://data.europa.eu/eli/reg/2014/910/oj

UNIÓN EUROPEA, 2016. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. *Diario Oficial de la Unión Europea* [en línea], 19 de julio de 2016, L 194, 1-30 [Consulta: 12 octubre 2019]. ISSN 1977-0685. Disponible en: http://data.europa.eu/eli/dir/2016/1148/oj

UNIÓN EUROPEA, 2016b. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea* [en línea], 4 de mayo de 2016, L 119, 1-88 [Consulta: 12 octubre 2019]. ISSN 1977-0685. Disponible en: http://data.europa.eu/eli/reg/2016/679/oj

VIVANCOS-CEREZO, M.-E., 2008. *La seguridad en bibliotecas universitarias: normas y auditoría*. Trabajo de investigación tutelado. Directora: María Marsá Vila. Universidad de León. [Consulta: 7 octubre 2019]. Disponible en: http://hdl.handle.net/10760/16220

WALKER-ROBERTS, S; HAMMOUDEH, M.; y DEHGHANTANHA, A., 2018. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access*, 6, 25167-25177. doi: 10.1109/ACCESS.2018.2817560

WARREN, S. D.; BRANDEIS, L. D., 1890. The Right to Privacy. *Harvard Law Review*, **4**(5), 193-220. [Consulta: 12 octubre 2019]. doi: 10.2307/1321160

WE ARE SOCIAL, 2019. Digital. En: *We Are Social* [en línea]. [Consulta: 7 diciembre 2019]. Disponible en: https://wearesocial.com/global-digital-report-2019

WOS, 2019. Web Of Science. En: *Recursos científicos* [en línea]. Madrid: FECYT. [Consulta: 29 octubre 2019]. Disponible en: https://www.recursoscientificos.fecyt.es/

YBARRA MALO DE MOLINA, B., 2019. Responsabilidades en el ámbito cibernético. En: E. MONTERROSSO CASADO dir. *Inteligencia Artificial y riesgos cibernéticos: responsabilidades y aseguramiento*. Valencia: Tirant lo Blanch, p. 239-296. ISBN 978-84-1313-013-2

YOUNG, J. R., 2019. Bots in the Library? Colleges Try AI to Help Researchers (But With Caution). En: *EdSurge* [en línea]. Burlingame, CA, USA. 14 junio 2019. [Consulta: 18 diciembre 2019]. Disponible en: https://www.edsurge.com/news/2019-06-14-bots-in-the-library-colleges-try-ai-to-help-researchers-but-with-caution