Universidad de Alcalá

Trabajo Fin de Máster

Plan de implantación de medidas de ciberseguridad y de tecnología en la nube para una editorial

Máster Universitario en Dirección de Proyectos Informáticos

Presentado por:

Dª. Rocío Castellón Guerado

Dirigido por:

D. Pedro Castor Valcárcel Lucas

Alcalá de Henares, a 16 de septiembre de 2022

UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

Máster en Dirección de Proyectos Informáticos

Trabajo Fin de Máster

Plan de implantación de medidas de ciberseguridad y de tecnología en la nube para una editorial

Autor: Rocío Castellón Guerado

Director: Pedro Castor Valcárcel Lucas

TRIBUNAL:

Presidente:

Vocal 1º:

Vocal 2º:

CALIFICACIÓN: _____ **FECHA:**


Universidad
de Alcalá

Contenido

Índice de tablas

Índice de figuras

Resumen

El objetivo principal de este proyecto es diseñar un plan de Ciberseguridad y de seguridad en la nube para una empresa editorial que explota un gestor de contenidos a través de servicios *cloud* de tipo infraestructura como servicio o IaaS.

Para desarrollar ambos planes se ha estudiado la legislación vigente y aplicables, se han expuesto los riesgos generales de las empresas de este mercado y se han dado soluciones a la seguridad tanto en el puesto de trabajo como en la nube.

Además, se ha llevado a cabo un análisis de riesgos siguiendo una adaptación de la Metodología de Análisis y Gestión de Riesgos de los sistemas de la Información MAGERIT.

El proyecto trata de relacionar los conocimientos académicos adquiridos en diferentes asignaturas del máster en materia de seguridad de la información y cumplimiento normativo con un tipo de empresa con unas necesidades de seguridad muy concretas y únicas.

Palabras clave: Ciberseguridad, Seguridad en la nube, Mercado editorial, Propiedad intelectual, IaaS, MAGERIT, Análisis de riesgos.

Abstract

The main goal of this project is to design a Cybersecurity and cloud security plan for a publishing company that operates a content manager through cloud services such as infrastructure-as-a-service or IaaS.

To develop both plans, the current and applicable legislation has been studied, the general risks of companies in this market have been explained and solutions for the security have been given both in the workplace and in the cloud.

In addition, a risk analysis has been carried out after an adaptation of the MAGERIT Information Systems Risk Analysis and Management Methodology.

The project tries to relate the academic knowledge acquired in different subjects of the master's degree in information security and regulatory compliance with a type of company with very specific and unique security needs.

Keywords: Cybersecurity, Cloud Security, Publishing market, Intellectual property, IaaS, MAGERIT, Risk analysis.

A Teresa y Maria, por el empuje y la confianza.

A Pedro, por dejar que me divirtiera.

Y a Carmen, Irene, Lohanna y MJ, por todo lo demás.

1. Resumen ejecutivo

El presente trabajo tiene por objeto analizar las características de una empresa del mercado editorial, más concretamente, aquellas relacionadas con la seguridad informática y la protección de la propiedad intelectual.

Además, se propondrán soluciones a los problemas de seguridad encontrados y se creará un plan de seguridad en la nube. Mediante el uso combinado de ambos planes, se pretende aumentar la protección de los datos de la editorial.

Como fundamentos teóricos se estudiará el estado actual de la ciberseguridad, tanto en general como en el caso particular de las editoriales, y cómo operan los diferentes tipos de nubes informáticas y se programan en ellas. Se describirán las características del mercado editorial, cuál es la organización particular de las empresas dedicadas a ello, su infraestructura informática y las vulnerabilidades de seguridad que sufren.

También se ha llevado a cabo una búsqueda de la legislación vigente que se aplica en estos casos, sobre todo leyes de protección de datos y de propiedad intelectual.

Aparte de los planes de seguridad mencionados, uno en el puesto de trabajo y otro en la nube (ambos planes surgen de paliar amenazas cuyo origen son objeto de ataques informáticos), se propondrá un tercero enfocado a la continuidad del negocio para cuando ya se han producido actos de piratería que merman las ventas de la editorial.

El trabajo se completa con una discusión, una relación de las aportaciones, las conclusiones y sugerencias de acciones futuras.

2. Objetivos y campo de aplicación

2.1. Objetivos

El objetivo general de este trabajo es diseñar un plan de implantación de medidas de seguridad y de tecnología en la nube y en la infraestructura local para una empresa editorial.

Los objetivos específicos son, para este tipo de empresas:

a) Analizar las deficiencias de seguridad de la información.
b) Diseñar un plan de seguridad que prevenga de ataques maliciosos.
c) Crear un plan de seguridad para tecnologías en la nube.

2.2. Campo de aplicación

Este TFM se aplicará en una empresa común del área de la publicación editorial. Esta editorial busca protegerse de posibles ciberataques como los sufridos con anterioridad. Además, la migración a tecnologías en la nube hace preciso un plan de seguridad para proteger los datos de la empresa, los trabajadores, los autores y los manuscritos a publicar.

Los datos de la empresa son ficticios, pero se ha buscado un perfil típico para ilustrar el tema del trabajo de fin de máster.

3. Introducción

Decía Publio Siro que «la persona más segura está en guardia incluso cuando parece estar a salvo de todo peligro». Entonces, dado lo expuestos al peligro que estamos actualmente, se hace necesario hacerle caso al filósofo y estar preparados para cualquier amenaza.

Ese será el objetivo de este trabajo, preparar a una empresa de nueva formación para las amenazas de ciberseguridad que se han hecho tan frecuentes en el siglo XXI.

La industria editorial no es nueva en España, donde han llegado a concurrir más de tres mil quinientas editoriales activas en la primera década del presente siglo. Pero, sin duda, es un mercado que está renaciendo tras la crisis del libro sufrida entre los años 2010 y 2015. Como se apunta en [1], es precisamente desde este año que el número de editoriales activas ha subido de manera paulatina, llegando a estar en el 2019 en el punto más alto del último septenio.

En este marco de mercado renaciente, nos centraremos en una empresa editorial de tamaño entre pequeño y mediano. Esta empresa, que publica tanto en papel como en digital, quiere proteger sus manuscritos para que no sean leídos de forma ilegal. Esto lo conseguiremos, entre otras medidas, implantando un servicio en la nube.

Además, gran parte de las editoriales de un par de décadas hasta hoy tienen su núcleo de negocio en la *coedición* o en la *edición bajo demanda*. Esta última significa que se imprime el libro tras haber sido vendido, en contraposición a la edición impresa en la que se imprime una tirada de determinado número de ejemplares con la intención de venderlos después. Ambos casos, coedición y edición bajo demanda, están pensados para satisfacer a los escritores que quieren difundir sus libros sin tener que pasar por los filtros habituales de las grandes editoriales y que suelen desembocar en el rechazo del manuscrito. La coedición conlleva un reparto de los gastos entre empresa y «cliente», el cual se fija de forma habitual en el 50%. Si antes hemos entrecomillado la palabra «cliente», es porque el autor pasa a ser, a ojos de la editorial, un cliente al igual que el lector. De ambos obtiene beneficios.

Las modalidades de edición anteriores tienen como consecuencia que sea alto el número de autores que trabajan con las editoriales que las practican, aun cuando el volumen de negocio no sea grande, y por ende la cantidad de datos particulares que proteger.

En este trabajo plantearemos las características comunes y los riesgos generales de la empresa, tras lo cual expondremos los planes de seguridad y planificaremos las acciones futuras.

4. Metodología para el desarrollo del TFM

La metodología seguida para el desarrollo del presente proyecto se fundamenta en las actividades y fases descritas a continuación:

1. Análisis del estado del arte:

   En este primer apartado hemos hecho un resumen de la fundamentación teórica usada, así como una presentación del estado actual de la materia que nos ocupa. Nos centraremos en los siguientes puntos:

   - Seguridad informática y ciberseguridad.
   - Seguridad informática en el mercado editorial.
   - Computación en la nube. Tipos de nubes.
   - Legislación vigente y aplicable.

   En el trabajo se incluyen todas aquellas referencias bibliográficas que han sido consultadas para su elaboración, indicando autor, fecha y link de la fuente consultada.

2. Mercado editorial. Características comunes y riesgos generales:

   Aquí describiremos una empresa típica del mercado editorial, con sus características propias y aquello que la diferencia de una empresa de cualquier otro sector.

   Ahondaremos también en los problemas de seguridad más frecuentes en empresas de este tipo.

3. Metodología de la solución:

   En este apartado nos centraremos en, una vez descritos y analizados los riesgos, exponer las soluciones encontradas para mitigarlos. Esto lo haremos a través de varios proyectos, cada uno de los cuales se centra en un aspecto de la protección de los datos.

4. Plan de seguridad en el puesto de trabajo:

   Aquí detallaremos el proyecto correspondiente al plan de seguridad en el puesto de trabajo, mediante el cual se pretende mejorar la protección de la propiedad intelectual.

5. Descripción del plan de seguridad en la nube:

   Este apartado desarrolla el proyecto correspondiente al plan de seguridad en la nube, que refuerza la protección de la propiedad intelectual establecida en el apartado anterior.

6. Plan de continuidad de negocio:

En este apartado expondremos las acciones preventivas que se llevarán a cabo en caso de que se materialicen aquellos riesgos que hemos elegido no mitigar.

7. Discusión:

Aquí describiremos el ámbito de aplicación de este trabajo, así como sus posibles aplicaciones.

8. Aportaciones:

En dicho apartado hablaremos de las razones por las que este trabajo es original y novedoso, extractando las aportaciones del mismo a la seguridad informática.

9. Conclusiones y trabajos futuros:

Finalmente, en el presente documento se extractan las conclusiones del trabajo que son llevadas al apartado correspondiente al final de este.

Como parte de las conclusiones se propone una posible actividad de continuación del presente trabajo.

5. Fundamentación teórica. Estado del arte

5.1. Seguridad informática y ciberseguridad

En [2], se define la seguridad informática como «la seguridad que engloba la protección del factor computacional en los dispositivos, normalmente electrónicos». Es decir, es una seguridad enfocada en el aspecto lógico de una compañía más que en el físico.

Este tipo de seguridad es de carácter intangible, no es algo tan obvio como una alarma antiincendios o un control de acceso por huella digital, sino más bien programas antivirus o detectores de *malware*, entre otras herramientas.

Sin embargo, sobre todo en el caso que nos ocupa, la seguridad informática no debe limitarse solo a eso. En el mercado editorial, objeto de estudio de este trabajo, el bien más preciado de las empresas es la propiedad intelectual de los documentos, por tanto, todo plan de seguridad debe ir enfocado a protegerla a toda costa.

Pongamos un ejemplo: para una editorial es menos perjudicial un ataque de un troyano que borra los datos de los discos duros que un acceso ilícito a sus manuscritos originales que luego aparecen en webs de descargas piratas. En el primer caso, es relativamente sencillo obtener de nuevo los archivos, bien por una copia de seguridad almacenada fuera de la red, bien pidiendo de nuevo el documento a los autores. En cambio, en el segundo, cada descarga ilegal de la novela es una venta menos que realiza la editorial.

De esta forma, el foco se debe poner en un tipo de protección más específico contra la difusión de contenido en lugar de contra la pérdida. Sobre esto hablaremos en el apartado 8. Plan de seguridad en el puesto de trabajo.

5.2. Seguridad informática en el mercado editorial

A la hora de investigar sobre el estado actual de la seguridad informática en el mercado editorial, nos ha sido bastante costoso encontrar bibliografía específica al respecto.

Prácticamente toda la información encontrada ha sido sobre ciberseguridad en el sentido general, sin particularizar en ningún tipo de empresa en concreto.

Ante esta dificultad, nos hemos puesto en contacto con varias editoriales y les hemos preguntado si tienen implementados planes de seguridad como el que nos ocupa en este trabajo.

Para este contacto hemos elegido a varias editoriales de pequeño tamaño, las denominadas en el mercado como *indies*, a las que se les ha pasado un cuestionario acerca de las medidas de seguridad tomadas para proteger sus datos y, en especial, sus manuscritos.

Las editoriales *indies* se autocalifican como independientes, amantes de la buena edición y buscan rescatar a autores olvidados o encontrar nuevos valores literarios

entre escritores desconocidos que no logran superar las dificultades de admisión de manuscritos de las grandes empresas de la edición.

Este cuestionario lo detallamos en el Anexo II: Cuestionario a editoriales. Se ha dividido en cuatro áreas:

- Seguridad física.
- Seguridad en el puesto de trabajo.
- Protección de datos.
- Protección de la propiedad intelectual.

Ha incluido preguntas sobre la protección de datos de carácter general, la protección contra *malware* y ataques malintencionados y la protección de la propiedad intelectual.

Sobre la protección con contra *malware* y ataques externos, ninguna se aleja de las acciones típicas que puede llevar a cabo una empresa de cualquier tipo, así como cualquier particular: antivirus, cortafuegos comerciales y sistemas antispam. Además, se hace hincapié a los empleados en no descargar archivos o entrar en enlaces que provengan de fuentes desconocidas o poco fiables.

No todas han respondido, pero aquellas que lo han hecho nos han confirmado que no tienen implementado un plan de ciberseguridad específico. Varias han contestado que los archivos de los libros electrónicos llevan implantado un DRM que impide su copia, sin embargo, los archivos no están cifrados mientras se trabaja en ellos en su corrección o maquetación.

Los empleados suelen firmar una cláusula de confidencialidad en el contrato de trabajo con la que se intenta proteger a la compañía de posibles filtraciones. Todas las obras que se publican están debidamente registradas, aunque no es el caso de las obras que se están valorando, que en ciertos casos depende solo de la precaución del autor.

Por norma general, los empleados tienen permitido usar dispositivos de almacenamiento externo y no se hace un control de la salida de archivos. La mayoría de estas editoriales son pequeñas, con pocos empleados y se consideran casi empresas familiares, por lo existe plena confianza en la honestidad de los trabajadores.

Todas las editoriales encuestadas hacen un uso correcto de los datos personales y se adhieren a la LOPD y ninguna tiene un control físico de acceso a las instalaciones.

Es significativo, por ejemplo, que la empresa Libros Indie, en la sección de su página web dedicada a las instrucciones para la remisión de manuscritos [3], incluye el siguiente texto:

> *«En Libros Indie siempre trataremos tu obra con la mayor confidencialidad. Aun así, un buen consejo antes de proceder con el envío de manuscritos a una editorial es el registro de la obra. Existen varios niveles de licencias, que van desde la inscripción en el registro de la propiedad intelectual de tu provincia, (coste aprox. 12€); a licencias de internet gratuitas como Safecreative. El registro es una medida recomendable pero no obligatoria. Los escritores*

tienen garantizada por ley la propiedad intelectual de sus obras desde el momento de su creación.»

Es decir, la seguridad de poseer la autoría o la protección anti-plagio se fía, por un lado, a una iniciativa personal del autor, a la confianza que pueda entablar este con el editor y a las disposiciones legales. Como ya se verá varias veces a lo largo de este trabajo, estos niveles de seguridad son claramente insuficientes.

Por otro lado, la venta de libros por parte de estas editoriales indie, aparte de dotarse de redes de distribución y/o establecer convenios con librerías, se realiza directamente a través de sus páginas web o blogs necesitando para ello los datos del comprador y, con frecuencia, que estos se registren como usuarios o abran una cuenta. De ahí que en el cuestionario se hayan incluido preguntas sobre el tratamiento de datos personales y la protección de la propiedad intelectual.

Con frecuencia, las medidas de seguridad no son las adecuadas, ya que los recursos disponibles, en la mayoría de los casos, son limitados.

Fuera de estas editoriales, revisando las webs de otras empresas del mercado, la gran mayoría actúa de forma similar a como se ha descrito con anterioridad, esto es, limitar la protección de propiedad intelectual a recomendar o a exigir como requisito previo a la presentación del manuscrito la inscripción del mismo en el Registro de la Propiedad Intelectual o en alguna web de tipo SafeCreative.

En definitiva, en el momento actual, las editoriales tienen protegidas sus obras solo en terreno legal, de modo que, ante una suplantación de identidad o plagio, se pueda demostrar la autoría de la obra. Es un tipo de defensa reactivo. Por contraposición, en este trabajo vamos a proponer un tipo de defensa preventivo, protegiendo los archivos de los manuscritos para que no puedan ser copiados ni compartidos de forma ilegal.

5.3. Computación en la nube. Tipos de nubes

En informática, una *nube* o *cloud computing* es un concepto que se refiere a una nueva forma de pensar y ofrecer servicios de computación a través de Internet.

La computación en la nube ofrece servicios de almacenamiento, bases de datos y recursos como CPU, RAM o discos digitales, al igual que los VPS clásicos utilizados en la industria del alojamiento web de pago y anteriormente en el alojamiento gratuito. La diferencia es que la nube consta de miles de servidores interconectados que comparten recursos, lo que lo convierte en un servicio rápido, escalable y seguro.

5.3.1. Principales tipos de nube informática

A nivel de modos de servicio, existen tres tipos de nubes, tal como se describen en [4]:

1. **Software-as-a-Service (SaaS)**.
2. **Platform-as-a-Service (PaaS)**.
3. **Infraestructure-as-a-Service (IaaS)**.

Software-as-a-Service (SaaS)

El concepto de SaaS existe desde hace mucho tiempo, pero probablemente solo en los últimos años hayamos definido realmente lo que queremos decir. Básicamente, es cualquier servicio web. Tenemos claros ejemplos como Gmail Webmail, Online CRM. En este tipo de servicios, solemos acceder a él a través de un navegador sin prestar atención al software. Todo el desarrollo, mantenimiento, actualizaciones, copias de seguridad son responsabilidad del proveedor de servicios.

En este caso tenemos muy poco control, estamos en la parte superior de la capa de servicio. Si el servicio falla, es responsabilidad del proveedor de servicios reiniciarlo.

Los ejemplos populares de SaaS incluyen Google Docs, Salesforce, Dropbox, Gmail...

Platform-as-a-Service (PaaS)

PaaS es donde los desarrolladores comenzamos a aprovechar y desarrollar nuestras propias aplicaciones que se ejecutan en la nube. En este caso, solo nos preocupamos por construir la aplicación, ya que la infraestructura la proporciona la plataforma.

Es un modelo que reduce en gran medida la complejidad de implementar y mantener aplicaciones, ya que las soluciones PaaS administran automáticamente la escalabilidad mediante el uso de más recursos cuando es necesario. Los desarrolladores aún deben preocuparse por optimizar sus aplicaciones lo mejor posible para consumir la menor cantidad de recursos posible (número de solicitudes, escrituras en disco, espacio requerido, tiempo de procesamiento, etc.), todo sin profundizar en el nivel de la máquina.

Un ejemplo popular es Google App Engine, que le permite desarrollar aplicaciones implementando Java o Python en la infraestructura proporcionada por Google. Heroku también usa Rails y Django para hacer esto.

Esta es una opción para los desarrolladores que no entienden la infraestructura que necesitan configurar y solo quieren preocuparse por escribir software.

Infraestructure-as-a-Service (IaaS)

En este caso con IaaS tendríamos más control que con PaaS, aunque tendríamos que encargarnos de gestionar la infraestructura.

Un ejemplo perfecto es Amazon Web Services (AWS), que proporciona múltiples servicios como EC2 que nos permiten gestionar máquinas virtuales en la nube o usar S3 como almacenamiento. Podemos elegir el tipo de instancia que usamos, Linux o Windows, y la capacidad de memoria o procesador de cada una de nuestras máquinas. El hardware es transparente para nosotros, todo lo que hacemos es virtual.

La principal diferencia es que además de preparar todo el entorno en la máquina (aunque hay imágenes de instancia preparadas con las configuraciones más

habituales), escalamos nuestra aplicación según nuestras necesidades. Además de AWS, también encontramos ejemplos como Rackspace Cloud o vCloud de VMWare.

5.4. Legislación de protección de datos y de propiedad intelectual

El cumplimiento de la legislación vigente es de vital importancia para cualquier empresa, pero es particularmente crítico en el caso de una editorial ya que no solo maneja datos personales sino información sujeta a leyes de la propiedad intelectual. Por ello exponemos a continuación las normas aplicables a una empresa de este sector.

Por las características de la empresa, los planes de seguridad deben ajustarse a la legislación vigente en materia de protección de datos, derechos de autor y, sobre todo y muy especialmente, propiedad intelectual.

Es por ello por lo que debemos ajustarnos a lo dispuesto en la LPI [5] en referencia a la propiedad intelectual, así como en el Reglamento (UE) 2016/679 [6] y a la LOPDGDD [7] en materia de protección de datos, así como.

Por otra parte, la empresa debe ajustarse a los estándares ISO 27001 de Seguridad de la Información [8] y a la ISO 27002 de Protección de los Sistemas de Información [9].

6. Mercado editorial. Características comunes y riesgos generales

6.1. Riesgos generales de seguridad en el mundo editorial

El valor de un trabajo de análisis como éste es determinar los riesgos generales de seguridad de la información en el mundo editorial y, a partir de ahí, las medidas que se deben aplicar en materia de protección de datos.

De esta forma, los principales riesgos de una empresa del mercado editorial vienen dados por la mala distribución de los manuscritos, ya sea por la filtración de las obras inéditas o la subida a plataformas de descargas ilegales de aquellas ya publicadas.

Todo ello ocasiona un gran perjuicio a la compañía, que deja de ingresar el dinero correspondiente a esos libros Por ello, el bien más preciado del que dispone son los manuscritos de los cuales adquieren los derechos de publicación.

Para protegerlos, vamos a implementar tanto sistemas de seguridad para evitar el acceso a ellos de personas ajenas a la editorial, como sistemas de cifrado que impida que las obras se distribuyan de forma ilícita.

Todas estas medidas de seguridad las desarrollaremos en apartados posteriores de este trabajo.

A continuación, pasamos a describir las características generales de una empresa editorial dedicada a la publicación de libros, tanto en papel como en formato electrónico.

6.2. Descripción de una empresa editorial

Vamos a enfocar este trabajo en un modelo de empresa editorial de tamaño pequeño o mediano, lo que se conoce en el sector como editorial *indie*. Un ejemplo de estas editoriales podría ser Pato Ediciones [10], Editorial El Transbordador [11], Uzanza Editorial [12] o Cosecha Negra Ediciones [13], entre otras muchas.

Estas editoriales tienen pocos empleados, en ocasiones incluso es el propio editor el único trabajador, hacen tiradas de pocos ejemplares y su volumen de negocio no suele exceder los cincuenta mil euros.

La falta de empleados se suele suplir con la subcontratación de servicios como puede ser corrección, maquetación o diseño de portadas.

Las líneas de actuación comunes en una empresa de este tipo podrían ser:

- Librerías. Se trata del suministro de libros a tiendas de todo el país.
- Venta online. Es la venta a través de internet de libros a consumidores finales. A partir de pedidos, se envían a los clientes a través de una empresa de transporte.
- Libro electrónico. Es la venta a través de internet de libros en formato electrónico. Una vez comprados, el cliente puede descargarse el archivo.

- Recursos humanos. Se trata de las altas, mantenimiento y bajas de personal de todo el grupo, control de la asistencia, control y gestión de las horas extras, líneas de formación, compensaciones de horario, derechos sindicales, etc.
- Facturación y contabilidad. Esta línea abarca la facturación, la consolidación de cuentas y cierres contables, recaudación y pago de compromisos (servicios recibidos, nóminas, etc.).

El valor total de esta empresa, incluidos los valores activos, pasivos, sus instalaciones e infraestructuras y otro es del orden de 50000 euros. De ellos, el 25% de ese valor se atribuye a las tecnologías de la información y de las comunicaciones.

6.2.1. Infraestructura informática

6.2.1.1. Aplicaciones informáticas

Las aplicaciones informáticas típicas para dar soporte a los servicios anteriores son:

- Venta online, que sirve de soporte a la venta on-line de los libros, tanto físicos como electrónicos. Se trata de una página web donde los clientes solicitan los productos.
- Distribución, que contacta los departamentos de distribución y transporte para hacer llegar los pedidos a los clientes y las tiendas
- Facturación, que sirve como pasarela de pagos seguros a través de internet.

6.2.1.2. Servicio informático

La empresa tiene su sede central en España. Desde allí, presta servicio informático a librerías de todo el país y almacenes.

En la sede central existe un pequeño centro de proceso de datos con las siguientes características:

- Base de datos de sistemas abiertos (Oracle), donde se almacenan los datos de los almacenes, pedidos, etc.
- Programas de desarrollo propio en lenguaje Java.
- ERP (Enterprise Resource Planning) para la facturación de la empresa y los recursos humanos.
- Servidores de sistemas abiertos en entorno Linux.

Además, un departamento de desarrollo de web da servicio de desarrollo y mantenimiento a la web de la empresa.

El personal de la empresa dispone de diversos equipos informáticos personales:

- Para el personal administrativo, equipos Windows de sobremesa con ofimática y acceso a las bases de datos.
- Para los editores, ordenadores portátiles, *tablets* y teléfonos móviles corporativos.

Todos los equipos están conectados a unidades de red de área local, que almacenan información común de cada departamento.

6.2.1.3. Facturas

Esta aplicación informática da soporte a la venta on-line y presencial de los productos de la empresa. Una vez los clientes han elegido un producto, se conecta con tratamiento de datos en la nube

Ante el plan de expansión a una nueva sede en Barcelona, la empresa quiere contratar un servicio de Infraestructura como servicio ("IaaS"), puesto que ha visto que le sale más rentable contratar recursos informáticos que adquirirlos e instalarlos en su centro de proceso de datos.

En concreto, quiere acudir a un proveedor de servicios en la nube público que les proporcione espacio de almacenamiento de datos y procesamiento de datos, con un sistema de *backup* en el caso de que el servidor que actúe como suministrador principal sufra un ataque informático.

Las líneas de actuación de la compañía que se quieren subir a la nube son:

- Librerías.
- Venta online.
- Libro electrónico.
- Facturas.
- Recursos humanos.

6.3. Vulnerabilidades de seguridad

En este apartado describiremos los problemas de seguridad de la información que pueden afectar a una empresa del mercado editorial. Estas vulnerabilidades provienen de la encuesta realizadas.

1. No hay medidas preventivas de garantía de la propiedad intelectual.
2. No hay medidas reactivas de garantía de la propiedad intelectual.
3. La distribución de las empresas en varias sedes hace que la actualización de los sistemas informáticos (los sistemas operativos y los gestores de bases de datos), por ejemplo, en este ejemplo es Oracle, sea muy tardía, una vez al año.
4. Los servicios soportados por internet han avisado de un intento de ataque de fuga de información, a través de un phishing que ha llegado a un correo del departamento de administración de datos.
5. Se actualiza semestralmente el sistema operativo de los equipos de sobremesa de los empleados.
6. Los fragmentos de algunos libros aún no publicados por la empresa se han filtrado en algunas plataformas de contenido ilegal.
7. A las aplicaciones informáticas se accede a través de contraseñas que no se renuevan más que una vez cada cuatro meses.
8. Los equipos tienen liberados los pen-drives, lectores de CD-ROM, DVD y otros periféricos.

9. Este tipo de empresas puede sufrir ataques de *ransomware*.
10. También ha habido casos de empresas del sector que han tenido intentos de accesos remotos para obtener información de obras en edición, con el fin robar la autoría de las obras literarias.

7. Metodología de la solución

El estudio de los riesgos se ha llevado mediante la hoja Excel incluida en el apartado 15.1. Anexo I: Análisis de riesgos. Dicha hoja se compone de tres pestañas. En la primera de ellas, **Análisis de riesgos**, se han incluido los riesgos listados en el apartado anterior. Para cada riesgo se detalla qué amenaza supone y a qué activo afecta. A continuación, se le ha asignado una probabilidad y un impacto en función de lo frecuente que ese riesgo pueda materializarse y de lo dañino que resulte.

De esta forma, a la vulnerabilidad «No hay medidas preventivas de garantía de la propiedad intelectual», se le asignado probabilidad de 4 e impacto de 5, ya que, sin una medida preventiva de protección, es muy frecuente que los libros digitales acaben en webs de descargas ilegales y, como ya se ha comentado, cada descarga de estas páginas es una venta que pierde la editorial. De ahí su alto impacto.

Por esta misma razón, todas las vulnerabilidades que afectan a las obras literarias tienen asignado impacto 5, aunque no toda ellas son igualmente probables.

Una vez puntuadas todas estas vulnerabilidades, se calcula el valor del riesgo multiplicando el impacto por la probabilidad. Aquellas vulnerabilidades con mayor puntuación son las que debemos intentar mitigar. Esto lo haremos mediante la siguiente pestaña.

En la hoja **Planes de seguridad** se tratan las mismas vulnerabilidades de la pestaña anterior, ordenadas de mayor a mayor según el valor del riesgo. Además, se definen una serie de proyectos y acciones de seguridad que servirán para mitigarlas.

Para cada vulnerabilidad, se asigna un valor de la efectividad de cada una de las salvaguardas definidas. Una vez asignados estos valores, se calcula la efectividad de cada una de ellas multiplicando el valor de los riesgos por la eficacia asignada.

Aquellas con mayor efectividad serán las que se implementen, mientras que los riesgos que se elija no mitigar deberán ser tratados en el Plan de continuidad del negocio.

Este plan lo desarrollamos en la pestaña **PCN**, en la cual recuperamos de nuevo el listado de vulnerabilidades, con su probabilidad, impacto y valor del riesgo. A continuación, detallamos las acciones a llevar a cabo en caso de materializarse el riesgo. Estas medidas son:

- **Medidas de análisis**: acciones a ejecutar para detectar la amenaza.
- **Medidas de contención**: acciones para minimizar los daños causados.
- **Medidas de recuperación**: acciones correctivas para restablecer el estado inicial.

Analizando los resultados obtenidos, se decide implementar un proyecto de seguridad en el puesto de trabajo y otro de seguridad en la nube. Ambos proyectos, con sus correspondientes salvaguardas, se desarrollan en los siguientes apartados.

8. Plan de seguridad en el puesto de trabajo

8.1. Objetivo, ámbito y alcance

8.1.1. Objetivo

Diseñar el plan completo de seguridad en el puesto de trabajo para una empresa del mercado editorial.

8.1.2. Ámbito

El ámbito de este proyecto afecta al departamento de Seguridad de la empresa.

8.1.3. Alcance

El alcance de este proyecto consta de:

1. Diseño del plan de seguridad en el puesto de trabajo.

8.2. Arquitectura de la solución

En una empresa del mercado editorial, el mayor riesgo de seguridad que podría surgir es, sin duda, contra la propiedad intelectual. La exposición de datos personales de trabajadores o autores es grave, pero no tan perjudicial para los intereses de la compañía como una violación de estos derechos de propiedad. Al fin y al cabo, una brecha de seguridad en datos personales puede afectar, en mayor o menor medida, a su reputación, pero la filtración de contenido editorial inédito puede derivar en la publicación de estos en plataformas de descarga ilegales, lo que influye directamente en los beneficios económicos de la empresa.

La actividad que ha obtenido mayor puntuación en el análisis de riesgos es el DRM, por lo que será nuestra medida a adoptar. Un DRM, *Data Right Management*, según se define en [14], es un sistema que utilizan las tiendas de libros electrónicos (pero también las tiendas de música o películas) y restringe el acceso a los libros que compramos. «Gestión de derechos» es un eufemismo que evita la palabra «restricción» y ciertamente no suena muy atractivo comercialmente. Adobe, también creador de productos como Photoshop o Acrobat Reader, es el principal administrador del servicio.

La mayoría de los expertos en gestión de DRM están de acuerdo en que los mejores sistemas de permisos combinan mecanismos de acceso de software y hardware. Al vincular los derechos de acceso directamente a las CPU de las computadoras, discos duros u otros medios, los editores pueden controlar no solo quién lee la información, sino también en qué dispositivos. Este nivel de protección es importante para documentos particularmente confidenciales, como documentos de investigación de mercado privados o legales, donde la copia y el intercambio ilegales pueden causar un daño significativo.

De esta forma, un archivo protegido mediante esta tecnología no puede ser distribuido libremente, por lo que toda persona que tenga acceso a los manuscritos (editores, correctores, ilustradores, etc.) solo podrán leerlo pero no descargarlo ni compartirlo.

La siguiente medida que implantaremos es un DLP, *Data Lost Prevention*. En [15] se dice que las soluciones DLP se utilizan en el proceso de monitoreo de sucesos que pueden ocasionar la filtración de información. Los productos enfocados en DLP pueden prevenir y corregir vulnerabilidades cuando se diagnostican. Existen diferentes tipos de soluciones DLP, cada una con un propósito específico, pero con el mismo objetivo: evitar la pérdida de datos.

1. Network DLP:

   Disponible para plataformas de software o hardware, integrado en el punto de entrada de datos de una red empresarial. Una vez instalada, la solución monitoreará, rastreará e informará todos los datos de tráfico de la red. Esta es la forma ideal de DLP para escanear todo utilizando puertos y protocolos corporativos. Proporciona información importante que ayuda a mantener la información segura en su organización, como qué datos se utilizan, quién accede a ellos y adónde van. La información recopilada por Network DLP se almacena en una base de datos fácil de administrar.

2. Storage DLP:

   Este sistema le permite visualizar archivos confidenciales almacenados y compartidos por personas que tienen acceso a la red de la empresa. Esto puede identificar puntos sensibles y evitar la fuga de información. Por ejemplo, la gestión de datos almacenados en la nube es una gran solución.

3. Endpoint DLP:

   Disquetes, ahora pen drives: herramientas externas que ayudan a transferir archivos de manera fácil y rápida. Sin embargo, pueden comprometer la seguridad empresarial y son propensos a filtraciones de datos accidentales o intencionales. Para evitar esto, necesita una solución que ayude a prevenir la pérdida de datos al usar dispositivos extraíbles. La solución DLP más adecuada es la opción Endpoint. Se instalan en todas las estaciones de trabajo y dispositivos utilizados por los empleados de la empresa y se utilizan para monitorear y evitar la fuga de datos confidenciales a través de dispositivos extraíbles, aplicaciones compartidas o zonas de transferencia.

Todas estas acciones preventivas se han tomado teniendo en cuenta la naturaleza de la empresa y lo sensible de sus datos, pero también se ejecutarán otro tipo de actividades que pueden ser comunes a compañías de otro tipo. Estas actividades son:

1. Fortalecimiento del equipo de trabajo, con un control del software instalado y del uso de los puertos USB de los equipos informáticos personales.
2. Autenticación de la identidad del trabajador que accede.
3. Actualización de programas y de servidores con la frecuencia recomendada por los proveedores.

Al margen de todo esto, es muy frecuente en las editoriales que todo se contenido literario esté protegido mediante licencia. Lo usual es que el propio autor lo registre antes de distribuirlo, bien en el Registro de la Propiedad Intelectual [17], bien en organismos de licencia pública como Creative Commons [18] o similares. Sin embargo, si el autor no ha realizado este paso, debe ser la editorial quien lo lleve a cabo, aunque es usual que el registro de la obra sea requisito indispensable para presentar el manuscrito.

8.3. Tareas del proyecto

Para determinar las tareas del proyecto vamos a basarnos en las recomendaciones del INCIBE en [19]. Dichas tareas y su planificación vienen recogidas en la Tabla 8.1:

Nivel	Tarea	Responsable	Producto
1	**Situación actual**		
2	Toma de decisiones	Seguridad	
2	Elección de acciones	Seguridad	
2	Definir responsables	Seguridad	
1	**Implantación Fase I**		
2	Implantar DRM	Seguridad	
2	Implantar DLP	Seguridad	
2	Implantar ERP	Seguridad	
1	**Implantación Fase II**		
2	Control software	Seguridad	
2	Autenticación	Seguridad	
2	Actualización sistemas	Seguridad	

Tabla 8.1 - Tareas del proyecto Seguridad en el puesto de trabajo

Esta planificación puede verse de forma gráfica en el diagrama de Gantt de la Figura 8.1.

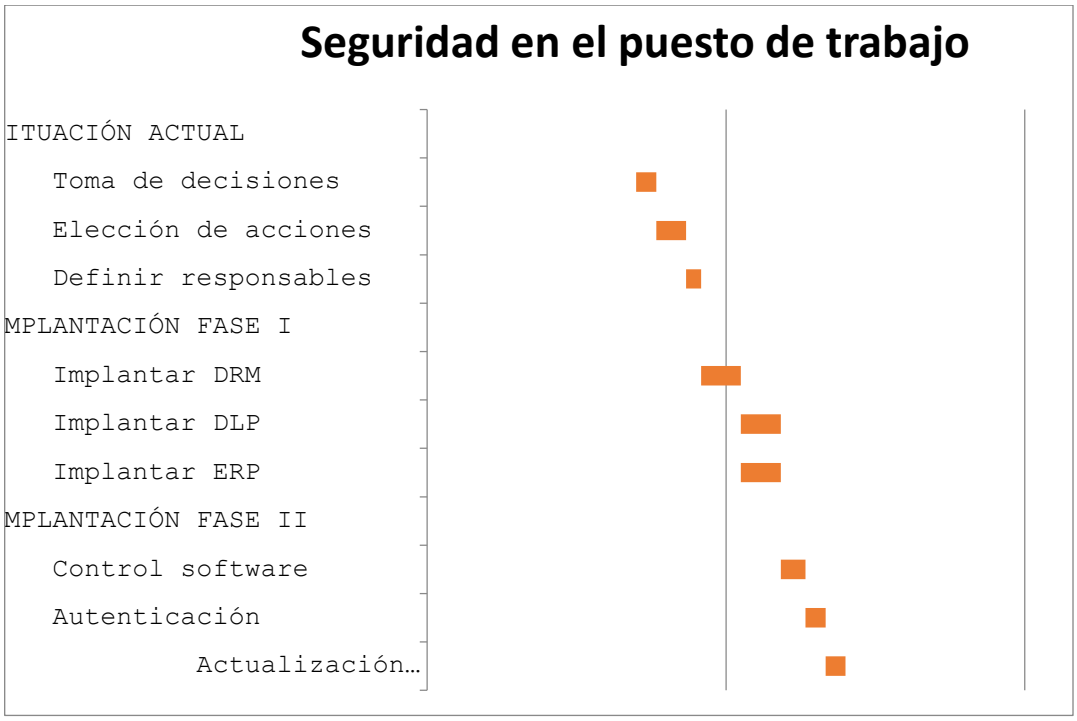

Figura 8.1 - Gantt del proyecto Seguridad en el puesto de trabajo

8.4. Actores el proyecto

Los actores de este proyecto son los listados en la Tabla 8.2:

Perfil	Objetivos (intereses)	Funciones	Recae en
Promotor del proyecto	Aportar recursos	Apoyar al jefe de proyecto	Directivo de la compañía
Jefe de proyecto	Impulsar las tareas	Gestión de alcance, tiempo y coste	Responsable de seguridad
Equipo de seguridad	Ejecutar las tareas	Ejecutar las tareas definidas en los planes	Equipo de seguridad

Tabla 8.2 - Actores del proyecto Seguridad en el puesto de trabajo

8.5. Análisis de los recursos necesarios

El desglose de los recursos necesarios está detallado en la Tabla 8.3. Se da este desglose en órdenes de magnitud:

Tipo	Concepto	Importe	
		1º año	Resto de años
Planes	DRM	9% facturación anual	
	DLP	5% facturación anual	

	ERP	4% facturación anual	
	Licencias	2% facturación anual	
Mantenimiento	10% de los planes		2% facturación anual
Total		**20% facturación anual**	**2% facturación anual**

Tabla 8.3 - Recursos del proyecto Seguridad en el puesto de trabajo

8.6. Análisis de los riesgos del proyecto

Además de los riesgos generales de la empresa, el proyecto puede acarrear a la organización los riesgos propios listados en la Tabla 8.4:

Descripción	Motivo	Contramedida para reducirlo
Pérdida de información	Las medidas de seguridad pueden resultar excesivas	Realizar pruebas suficientes antes de implantar las medidas de forma que la información protegida no se quede inaccesible

Tabla 8.4 - Riesgos del proyecto Seguridad en el puesto de trabajo

9. Plan de seguridad en la nube

9.1. Objetivo, ámbito y alcance

9.1.1. Objetivo

Diseñar el plan completo de seguridad en la nube para una empresa del mercado editorial.

9.1.2. Ámbito

El ámbito de este proyecto afecta al departamento de Seguridad de la empresa.

9.1.3. Alcance

El alcance de este proyecto consta de:

1. Diseño del plan de seguridad en la nube.

9.2. Arquitectura de la solución

A continuación abordamos el plan de seguridad para tecnologías en la nube. Este proyecto, con sus correspondientes acciones, sirve de salvaguarda a los riesgos relacionados con la fuga de información relativa a obras literarias.

Una empresa editorial usará principalmente una nube a modo de *backup* de su principal activo, que son los manuscritos de las obras de las cuales poseen los derechos de publicación.

Para ello, creemos que lo más apropiado es una Infraestructura como Servicio (IaaS), en la que un proveedor proporciona acceso a recursos como almacenamiento, red y servidores. De esta forma, se ahorra el coste de adquirir el hardware, ya que se paga por el IaaS bajo demanda [20].

Una primera alternativa podría ser Office 365, que no solo ofrece servicios de almacenamiento en la nube, sino también direcciones de correo empresarial y acceso a las aplicaciones de Microsoft, entre ellas Publisher, usado entre las editoriales para la maquetación. Con esto no haría falta pagar licencias de otros programas para este propósito, como Adobe InDesign o QuarkXPress.

Office 365 ofrece, además, la posibilidad de aplicar etiquetas de confidencialidad a los archivos, de forma que se mantienen en conformidad con las directivas de protección de información de la empresa [21]. Otra funcionalidad de Office 365 en materia de seguridad es el bloqueo de descarga de archivos. Mediante esta opción, los usuarios que accedan al archivo compartido no verán opciones para descargar, imprimir o copiar el archivo. Solo pueden ver archivos en la web y no pueden abrirlos en aplicaciones de escritorio o móviles [22].

De esta forma, por un coste reducido, se podría adquirir una infraestructura en la nube que estaría securizada por Microsoft y mantendría conectados a todos los

empleados de la compañía. Cada usuario tendrá acceso a una carpeta en la nube y, además, se podrá montar un sistema de SharePoint en el que podrán almacenarse los manuscritos.

Esta infraestructura, proporcionada por el proveedor Microsoft, además podrá reforzarse con un proveedor de identidad (IdP). Implementando un IdP con un sistema de inicio de sesión único (SSO) conseguiremos hacer más seguros los inicios de sesión de los usuarios, además de ser más cómodo para ellos [23].

Para mayor seguridad, se deberá implementar también un sistema de autenticación en dos fases. Dicho sistema, también conocido por 2FA, es un enfoque de seguridad para la gestión de acceso e identidad que requiere dos formas de identificación para acceder a recursos y datos. 2FA permite a las empresas monitorear y ayudar a proteger su información y redes más vulnerables [24].

Una de las ventajas de este sistema es que no hace falta transportar un generador de tokens, ya que la mayoría de sitios web utilizan un dispositivo móvil para enviar texto, realizar una llamada o utilizar una 2FA personalizada para que la empresa pueda verificar tu identidad. Es, en resumidas cuentas, una forma de proteger la información en caso de robo o pérdida del usuario y contraseña.

Además de todo lo anterior, implementaremos un sistema de *blockchain*, de forma que tanto la información como las transacciones con los clientes (lectores) esté registrada en el libro mayor de transacciones [25].

En los últimos años, la tecnología *blockchain*, como se indica en [26], se ha convertido en una herramienta innovadora para las empresas. A medida que se abordan los casos de uso de cadenas de bloques de gran potencia, los proveedores de servicios como NTT Data amplían sus ofertas para crear sistemas y generar resultados comerciales que les hagan ganar competitividad sumando esta tecnología en sus procesos internos.

La tecnología *blockchain* tiene propiedades que permiten gestionar la información de forma segura y trazable, garantizando la transparencia y privacidad de las operaciones. Es muy interesante para las empresas porque permite mejorar los procesos de negocio y definir nuevos modelos de entorno colaborativo basados en esta tecnología.

El aspecto principal de esta tecnología es su capacidad para garantizar la seguridad de los datos tratados y poder demostrarlo. Esto se llama el principio de responsabilidad activa.

En definitiva, la tecnología *blockchain* es una base de datos distribuida y segura (gracias al cifrado) que se puede aplicar a todo tipo de transacciones que no tienen por qué ser necesariamente económicas.

Los proveedores de servicios de almacenamiento en la nube proporcionan también un cifrado en la nube. Este servicio, según se define en [27], convierte los datos del cliente en texto cifrado mediante un algoritmo de cifrado y se almacenan en la nube. El cifrado es casi idéntico al cifrado local, con una gran diferencia: los clientes de la nube deben dedicar algún tiempo a comprender las políticas y los procedimientos de cifrado

de su proveedor de servicios, así como la gestión de claves de cifrado. Las capacidades de cifrado del proveedor de servicios deben coincidir con el nivel de sensibilidad de los datos alojados.

Microsoft 365 ofrece un servicio de cifrado en la nube mediante Microsoft Cloud [28], por lo que cumple con este requerimiento.

Dentro del plan de seguridad en la nube, una de las salvaguardas definidas es que el proveedor de servicios en la nube debe estar certificado, tal como se indica en [29]. Además, [30] detalla cuáles son estas certificaciones:

- La certificación SOC 1 da fe de la calidad del control de los informes financieros, mientras que los informes SOC 2 y SOC 3 abordan la seguridad, la disponibilidad, la integridad del procesamiento y otros factores relevantes para los sistemas de información.
- ISO 27001 es una familia de estándares de seguridad intersectoriales que abordan los requisitos, la implementación, la medición y los códigos de práctica.
- El programa de certificación STAR de Cloud Security Alliance es otro estándar de seguridad general. Está diseñado específicamente para proveedores de nube y se basa en dos componentes principales: la Matriz de controles de nube y el Cuestionario de iniciativa de evaluación de consenso (CAIQ).

9.3. Tareas del proyecto

La Tabla 9.1 recoge la descripción y planificación de las tareas del proyecto:

Nivel	Tarea	Responsable	Producto
1	**Situación actual**		
2	Toma de decisiones	Seguridad	
2	Elección de acciones	Seguridad	
2	Definir responsables	Seguridad	
1	**Implantación**		
2	Implantar IaaS	Seguridad	
2	Implantar IdP	Seguridad	
2	Implantar autenticación en 2 fases	Seguridad	
2	Implantación cifrado en la nube	Seguridad	
2	Implantar blockchain	Seguridad	

2	Instalación firewall y proxy	Seguridad	

Tabla 9.1 - Tareas del proyecto Nube

Esta planificación puede verse de forma gráfica en el diagrama de Gantt de la Figura 9.1.

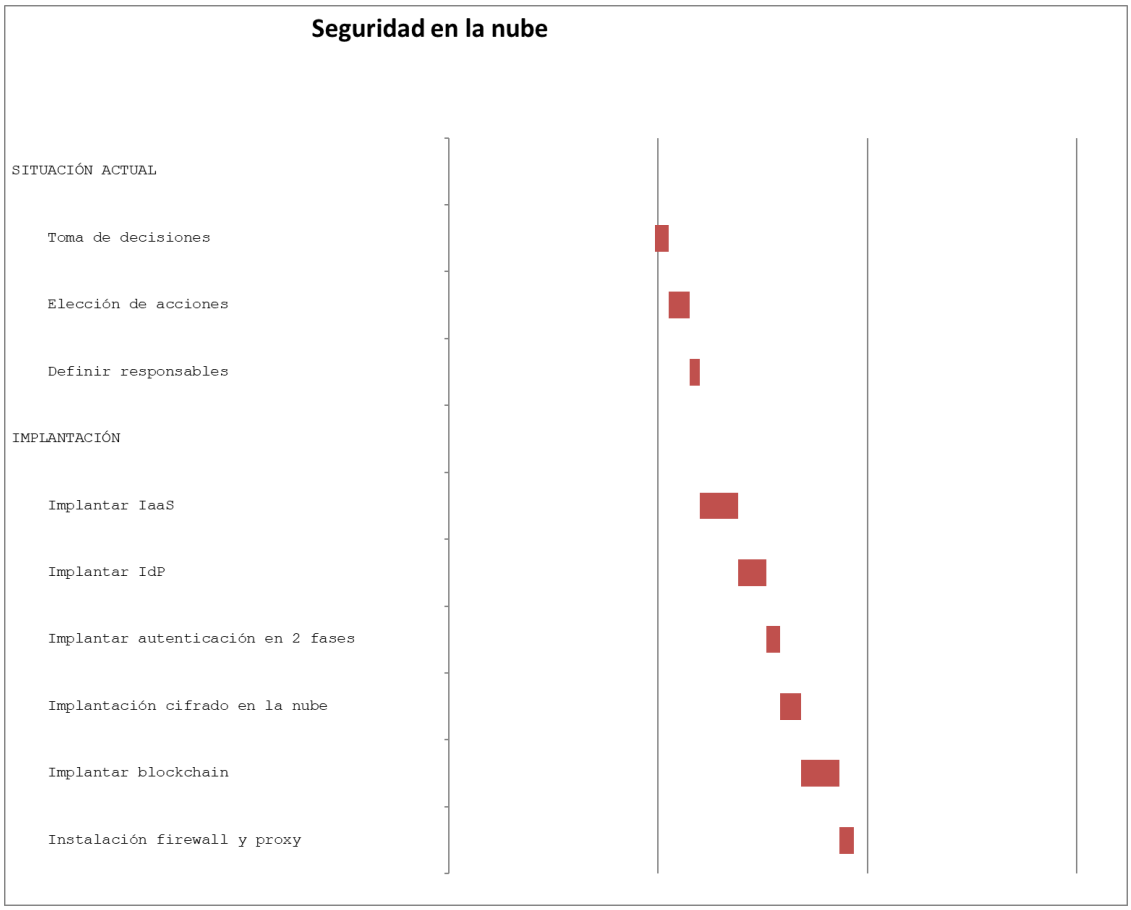

Figura 9.1 - Gantt del proyecto Seguridad en la nube

9.4. Actores el proyecto

Los actores de este proyecto son los listados en la Tabla 9.2:

Perfil	Objetivos (intereses)	Funciones	Recae en
Promotor del proyecto	Aportar recursos	Apoyar al jefe de proyecto	Directivo de la compañía
Jefe de proyecto	Impulsar las tareas	Gestión de alcance, tiempo y coste	Responsable de seguridad
Equipo de seguridad	Ejecutar las tareas	Ejecutar las tareas definidas en los planes	Equipo de seguridad

Tabla 9.2 - Actores del proyecto Nube

9.5. Análisis de los recursos necesarios

Para este proyecto no será necesario adquirir material, los recursos necesarios serán tan solo en concepto de personal durante la duración del proyecto. El desglose de estos recursos está detallado en la Tabla 9.3:

Tipo	Concepto	1º año	Resto de años
Inversiones	Hardware	10% facturación anual	
	Software	6% facturación anual	
	Base de datos	6% facturación anual	
Desarrollos	Cifrados	6% facturación anual	
	IdP	6% facturación anual	
	Blockchain	6% facturación anual	
Mantenimiento	10% de inversiones		2,20% facturación anual
	10% de desarrollos		1,80% facturación anual
Total		**40% facturación anual**	**4% facturación anual**

Tabla 9.3 - Recursos del proyecto Nube

9.6. Análisis de los riesgos del proyecto

Además de los riesgos generales de la empresa, el proyecto puede acarrear a la organización los riesgos propios listados en la Tabla 9.4:

Descripción	Motivo	Contramedida para reducirlo
Pérdida de claves del cifrado	La pérdida de la clave de cifrado hace que la recuperación de los datos sea imposible.	Realizar copias de seguridad con la frecuencia adecuada, de forma que la pérdida de datos se reduzca.
Código No Probado	La calidad del código de *blockchain* puede ser deficiente.	Implementar un plan de pruebas adecuado antes de implantarlo.

Tabla 9.4 - Riesgos del proyecto Nube

10.Plan de continuidad de negocio

En el mundo editorial, por desgracia, es muy frecuente que las obras literarias inéditas, en parte o completas, acaben en páginas ilegales de descargas o siendo víctimas de la piratería de una u otra manera. En más casos de los que a las empresas editoriales les gustaría contar, resultan indiferentes las medidas de protección que se hayan implantado en los archivos de los libros electrónicos. Estas medidas se rompen y los libros acaban pasando de mano en mano, produciendo un perjuicio a la editorial que deja de ingresar ese dinero.

Por eso, aunque en los apartados anteriores hemos expuesto medidas para proteger los manuscritos, vamos a exponer también un plan de continuidad del negocio en caso de que esas amenazas se materialicen. Dicho plan será el mismo para todas las amenazas que impliquen a las obras literarias.

Medidas de análisis:

La medida de análisis es escanear internet en busca de obras literarias disponibles para descargas ilegales. En principio, podría bastar con una búsqueda en Google o una navegación por algunas webs ya conocidas. También es interesante hacer lo mismo en grupos de Telegram o Facebook donde el intercambio de libros electrónicos es frecuente.

Esta medida no destaca por su eficiencia, pero es la única de que disponen las editoriales.

Medidas de contención:

Una vez detectada una obra literaria víctima de la piratería, se debe denunciar su publicación. Hay sitios webs, como por ejemplo Facebook [31], que prohíben la publicación de contenido protegido por derechos de autor, por tanto, una denuncia debería bastar para retirar el contenido ilegal e incluso cerrar el grupo o penalizar al usuario.

Las obras literarias ya publicadas sí que están protegidas por la Ley de Propiedad Intelectual, ya que están inscritas en el Registro de la propiedad o gozan de una licencia similar, por lo que se puede demostrar que la obra en cuestión está bajo derechos de autor y, por tanto, es ilegal su publicación fuera de los canales oficiales de la editorial.

Medidas de recuperación:

Puesta la denuncia por publicación de contenido ilegal, la medida de recuperación es solicitar la retirada del contenido ilegal publicado. Por desgracia, resulta imposible recuperar los archivos ya descargados y en poder de los usuarios, por lo que la editorial debe asumir esas pérdidas.

El siguiente paso debe ser reforzar la seguridad de todos sus archivos para prevenir una pérdida similar.

El resto de amenazas hacen referencia a datos generales de la empresa, como puede ser información de escritores o empleados. Dichas amenazas son menos frecuentes y, en el caso del mercado editorial, menos dañinas, ya que afectan más a la reputación de la empresa que a sus beneficios.

En este caso, el Plan de continuidad del negocio será también el mismo para todas las amenazas relacionadas con el mismo tipo de datos.

Medidas de análisis:

La primera medida a tomar en caso de fuga de información en general es determinar el grado de filtración producido, es decir, la cantidad de los datos expuestos o la confidencialidad de los mismos.

También se debe estudiar la integridad de estos datos, ya que es menos grave la pérdida de la confidencialidad que la modificación de información relevante. Pongamos por ejemplo el número de cuenta en el que un escritor está recibiendo sus regalías; no es tan malo la filtración de este número como su modificación, porque en este caso los beneficios los estaría percibiendo otra persona.

Medidas de contención:

Delimitado el alcance de la filtración, es importante comunicar la misma a los interesados de forma que se evite perjuicio sobre la reputación de la empresa. Además, sería conveniente realizar con ellos la comprobación de la integridad de los datos mencionada anteriormente.

Medidas de recuperación:

Contenidos los daños, el siguiente paso es reforzar la seguridad de la compañía, por ejemplo, haciendo un cambio general de las contraseñas de los empleados para prevenir una nueva fuga o actualizando el antivirus.

11. Discusión

La solución aportada es factible para empresas de pequeño o mediano tamaño que publican obras literarias. Este es un mercado muy afectado por las brechas de seguridad, donde cada venta perdida supone un gran perjuicio. Las empresas para las que se ha pensado este trabajo suelen tener un catálogo editorial pequeño, con menos de veinte publicaciones inéditas al año, y tiradas de menos de dos mil ejemplares. Esto quieren decir que cada libro vendido es un ingreso necesario para ellas, por lo que son bienes que se deben proteger a toda costa.

Nos hemos enfocado en implementar medidas para que esa protección sea la mayor posible, tanto en el puesto de trabajo como en la nube. También hemos desarrollado un plan en el caso de esas medidas fallen y se produzcan filtraciones.

Por otro lado, esta misma metodología será aplicable a empresas de mayor tamaño, con un mayor catálogo editorial y tiradas más grandes, con la salvedad de que este tipo de editoriales existen otros riesgos. En las mayores empresas del gremio, como pueden ser Planeta [32] o Penguin [33] por nombrar las más conocidas, publican autores de prestigio cuyas próximas publicaciones son muy esperadas, por lo que la probabilidad de sufrir filtraciones o ataques deliberados para obtener las obras antes de su fecha de salida al mercado es mayor.

También podría usarse un plan de características similares al expuesto en este trabajo en empresas que publican otro tipo de contenido audiovisual, como puede ser audiolibros.

Por último, una alternativa al alto coste de alguna de las medidas propuestas podría ser implementar este plan en asociaciones de editores, como podría ser la Federación De Gremios de Editores de España [34], de forma que nos adhiriéramos a una economía de escala y el desembolso económico para estas editoriales pequeñas sea menor.

12. Aportaciones

Una vez analizados los riesgos de esta empresa y diseñados los planes tanto de ciberseguridad como de seguridad en la nube, podemos hablar de las aportaciones que este trabajo hace a la seguridad de una empresa.

Para empezar, los riesgos que pueden afectar a la seguridad en la nube no son muy distintos de los que sufre la ciberseguridad, por lo que el hecho de paliar unos influye en el tratamiento de otros. Se han asignado valores de riesgo a cada posible vulnerabilidad, tanto en el puesto de trabajo como en la nube, diseñando medidas a tomar en cada caso en función del impacto que pueda tener en los ingresos o pérdidas de la editorial. También se ha calculado la efectividad de estas medidas a los efectos de facilitar la elección de cuáles son las que hay que tomar.

Para los casos en los que el daño ya está hecho por haber sufrido ataques de piratería, se han elaborado propuestas a seguir en el plan de continuidad de negocio.

Por otra parte, las características peculiares de este tipo de empresa nos permiten trabajar la confidencialidad de los datos en mayor medida que en otro tipo de compañía. Es un mercado que está muy afectado por la piratería, por lo que mantener los manuscritos en secreto hasta el momento de la publicación, es crucial para no perder ingresos.

Es por ello por lo que este trabajo puede usarse como modelo para otras editoriales de características similares e incluso, en una versión reducida, para autores autopublicados.

13. Conclusiones y trabajos futuros

13.1. Conclusiones

Para todos los tipos de compañía mantener un buen nivel de ciberseguridad es importante, pero para una editorial es particularmente crítico. Una filtración, por ejemplo, de una publicidad para una empresa de cosméticos no tiene por qué afectar a su nivel de ingresos. Un manuscrito inédito que se filtra antes de su publicación y acaba en plataformas de contenidos ilegales, sin embargo, disminuye los ingresos que la compra de ese libro genera en la editorial.

Los principales riesgos de una empresa del mercado editorial vienen dados por la mala distribución de los manuscritos. Ya sea por la filtración de las obras inéditas o la subida a plataformas de descargas ilegales de aquellas ya publicadas.

Todo ello ocasiona un perjuicio a la compañía, que deja de ingresar el dinero correspondiente a esos libros. Por ello, el bien más preciado del que dispone son los manuscritos de los cuales adquieren los derechos de publicación.

Para protegerlos, se han implementado tanto sistemas de seguridad para evitar el acceso a ellos a personas ajenas a la editorial, como sistemas de cifrado que impidan que las obras se distribuyan de forma ilícita.

Un buen cifrado de la información, además del resto de medidas de seguridad descritas, como una buena protección contra el personal externo es en especial importante para estas empresas. De esta forma, concluimos que toda editorial debería implementar un plan de ciberseguridad para evitar la fuga de información.

Todo esto lo hemos conseguido mediante una infraestructura en la nube, que, en esencia, consista en encontrar un proveedor de estos servicios que ofrezca garantías tanto en el cifrado, como en la ubicación y la certificación.

Estos riesgos son comunes a cualquier editorial, por lo que lo expuesto en este trabajo es extrapolable a todas las empresas que se dediquen al mismo mercado.

13.2. Trabajos futuros

Este trabajo de investigación se podría continuar con una encuesta más numerosa a otras empresas del sector, de forma que se obtenga una imagen más real del estado de la seguridad informática y la protección de la propiedad intelectual.

Como una segunda fase, se puede ampliar este plan para cubrir los riesgos adicionales que tendrían las editoriales de mayor tamaño y con autores más conocidos y demandado, y que ya han sido expuestos en el apartado 11. Discusión.

Además, se puede crear un plan de continuidad de negocio para todos esos riesgos que no se han contemplado en este trabajo.

14. Bibliografía

14.1. Trabajos citados

[1] Dirección General del Libro y Fomento de la Lectura, Panorámica de la edición española de libros 2018, Madrid: Ministerio de Educación, Cultura y Deporte, 2019.

[2] J. Llamas, «Seguridad informática - Qué es, definición y concepto | 2022 | Economipedia» [En línea]. Disponible: Aquí. [Último acceso: 10 08 2022].

[3] Libros Indie, «Envío de Manuscritos» 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[4] T. Rodríguez, «Entendiendo la nube: el significado de SaaS, PaaS y IaaS» 31 08 2012. [En línea]. Disponible: Aquí. [Último acceso: 01 09 2022].

[5] Gobierno de España, Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril., Madrid: Boletín Oficial del Estado, 2006.

[6] UE, REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 (Reglamento, Bruselas: Diario Oficial de la Unión Europea, 2016.

[7] Gobierno de España, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos, Madrid: Boletín Oficial del Estado, 2018.

[8] ISO, «ISO 27001,» 2013. [En línea]. Disponible: Aquí. [Último acceso: 31 07 2022].

[9] ISO, «ISO 27002,» 2022. [En línea]. Disponible: Aquí. [Último acceso: 31 07 2022].

[10] Pato Ediciones, «Pato Ediciones» [En línea]. Disponible: Aquí. [Último acceso: 01 09 2022].

[11] Ediciones El Transbordador, «Ediciones El Transbordador» [En línea]. Disponible: Aquí. [Último acceso: 01 09 2022].

[12] Uzanza Editorial, «Uzanza Editorial» [En línea]. Disponible: Aquí. [Último acceso: 01 09 2022].

[13] Cosecha Negra Ediciones, «Cosecha Negra Ediciones» 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[14] M. F, «Qué es el DRM y para qué sirve» 18 04 2011. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[15] OSTEC, «DLP qué es y cómo funciona» 22 09 2015. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[16] INICIBE, «Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa» 27 04 2021. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[17] Ministerio de Cultura y Deporte, «Registro de la Propiedad Intelectual» [En línea]. Disponible: Aquí. [Último acceso: 31 05 2022].

[18] Creative Commons, «Creative Commons» [En línea]. Disponible: Aquí. [Último acceso: 31 05 2022].

[19] INCIBE, «Plan director de seguridad» [En línea]. Disponible: Aquí. [Último acceso: 15 05 2022].

[20] IBM, «IaaS frente a PaaS frente a SaaS» 10 10 2018. [En línea]. Disponible: Aquí. [Último acceso: 07 06 2022].

[21] Microsoft, «Aplicar etiquetas de confidencialidad a los archivos y al correo electrónico en Office» 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[22] Microsoft, «Bloquear descargas de archivos de solo vista en SharePoint y OneDrive» 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[23] Cloudflare, «¿Qué es un proveedor de identidad (IdP)?» [En línea]. Disponible: Aquí. [Último acceso: 31 05 2022].

[24] Microsoft, «¿Qué es la autenticación en dos fases?» 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[25] IBM, «¿Qué es la tecnología de blockchain?» [En línea]. Disponible: Aquí. [Último acceso: 01 06 2022].

[26] MuyComputer, «Qué es la tecnología Blockchain» 08 09 2022. [En línea]. Disponible: Aquí. [Último acceso: 08 09 2022].

[27] Krypton Solid, «¿Qué es el cifrado en la nube? Cómo funciona el cifrado de almacenamiento en la nube» 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[28] Microsoft, «Cifrado en Microsoft Cloud» 06 07 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[29] INCIBE, «Certificación de la nube» 07 09 2012. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[30] Krypton Solid, «¿Qué certificaciones de seguridad en la nube deben tener los proveedores? » 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[31] Facebook, «Propiedad intelectual» 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[32] Editorial Planeta, «Editorial Planeta» 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[33] Penguin, «Penguin Libros» 01 01 2022. [En línea]. Disponible: Aquí. [Último acceso: 02 09 2022].

[34] Federación De Gremios de Editores de España, «Federación De Gremios de Editores de España,» 2019. [En línea]. Disponible: Aquí. [Último acceso: 01 09 2022].

14.2. Otras obras de referencia

[35] CCN, «Centro Criptológico Nacional» [En línea]. Disponible: Aquí. [Último acceso: 12 02 2022].

[36] ILIMIT, «ILIMIT» 19 11 2018. [En línea]. Disponible: Aquí. [Último acceso: 12 02 2022].

[37] INCIBE, «Instituto Nacional de Ciberseguridad» 01 02 2017. [En línea]. Disponible: Aquí. [Último acceso: 12 02 2022].

[38] ISO, «ISO 27005» 2018. [En línea]. Disponible: Aquí. [Último acceso: 12 02 2022].

[39] ISO, «ISO 31000» 2018. [En línea]. Disponible: Aquí. [Último acceso: 12 02 2022].

[40] ISO, «ISO 31010» 2019. [En línea]. Disponible: Aquí. [Último acceso: 12 02 2022].

[41] Consejo Superior de Administración Electrónica, MAGERIT – versión 3.0, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[42] INCIBE, Políticas de seguridad para la pyme: almacenamiento en la nube, Madrid: Ministerio de Energía, Turismo y Agenda Digital., 2017.

[43] INCIBE, Ransomware: una guía de aproximación para el empresario, Madrid: Ministerio de Energía, Turismo y Agenda Digital, 2017.

[44] S. Burns, «Computer Weekly» 09 03 2020. [En línea]. Disponible: Aquí. [Último acceso: 12 02 2022].

[45] Gobierno de España, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico., Madrid: Boletín Oficial del Estado, 2002.

[46] Gobierno de España, Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el

texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia., Madrid: Boletín Oficial del Estado, 1996.

15. Anexos

15.1. Anexo I: Análisis de riesgos

El análisis de riesgo descrito en el apartado 7. Metodología de la solución se ha llevado a cabo mediante la siguiente hoja Excel:

TFM Rocío Castellón. Análisis d

Esta hoja consta de las siguientes pestañas:

15.1.1. Análisis de riesgos

Aquí detallamos las vulnerabilidades descritas en el apartado 6.3. Vulnerabilidades de seguridad y les asignamos una probabilidad y un impacto para calcular el valor del riesgo.

Análisis de riesgos

Id	Vulnerabilidad	Amenaza	Activo	Probabilidad (P)			Impacto (I)			Riesgo (R)
				Valor	Descripción	Explicación	Valor	Descripción	Explicación	P x I
1	No hay medidas preventivas de garantía de la propiedad intelectual.	Fuga de información de obras literarias	Datos de obras literarias	4	Alta	Sin medidas hay mucha tentación de copiar contenidos	5	Muy alto	La fuga de una obra hace perder mucho dinero. Cada descarga de la web pirata significa un libro menos que	20
11	Datos de obras literarias que se suben a la nube para ser tratadas informáticamente	Fugas de información intencionadas	Obras literarias	3	Media	En la nube puede quedar accesibles para agentes malintencionados	5	Muy alto	La fuga de una obra hace perder mucho dinero. Cada descarga de la web pirata significa un libro menos que	15
10	Falta de fiabilidad del proveedor en la nube	Fugas de información intencionadas	Obras literarias	3	Media	Una nube poco fiable puede producir fugas de información	4	Alto	La fuga de una obra hace perder mucho dinero. Cada descarga de la web pirata significa un libro menos que	12
8	Este tipo de empresas puede sufrir ataques de ransomware.	Ciberataque	Datos en general de la empresa	2	Baja	Un ataque por ransomware deja inaccesible los datos	5	Muy alto	Un ataque podría desencadenar una fuga o una degradación de la información	10
9	También ha habido casos de empresas del sector que han tenido intentos de accesos remotos para obtener información de obras en edición, con el fin robar la autoría de las obras	Fugas de información intencionadas	Obras literarias	2	Baja	Los manuscritos no están protegidos durante el proceso de edicion, por lo que puede haber fugas	5	Muy alto	La fuga de una obra hace perder mucho dinero. Cada descarga de la web pirata significa un libro menos que se vende	10

Figura 15.1 - Análisis de riesgos

15.1.2. Planes de seguridad

En esta pestaña relacionamos cada vulnerabilidad con una salvaguarda, puntuando la efectividad de la misma sobre cada una de las amenazas.

						DLP ("Data Loss Prevention")	DRM	Fortalecimiento del equipo de trabajo	Autenticac
Análisis de riesgos						Bloqueo y auditoría de las nuevas obras literarias	Data Right Management	Control del software instalado y del uso de los puertos USB de los equipos informáticos personales.	Comprobación identidad del trabajador que accede
Id	Vulnerabilidad	Amenaza	Probabilidad	Impacto	Riesgo	80	144	44	45
1	No hay medidas preventivas de garantía de la propiedad intelectual.	Fuga de información de obras literarias	Sin medidas hay mucha tentación de copiar contenidos	La fuga de una obra hace perder mucho dinero. Cada descarga de la web pirata significa un libro menos que se vende	20		5		
11	Datos de obras literarias que se suben a la nube para ser tratadas informáticamente	Fugas de información intencionadas	En la nube puede quedar accesibles para agentes malintencionados	La fuga de una obra hace perder mucho dinero. Cada descarga de la web pirata significa un libro menos que se vende	15				
10	Falta de fiabilidad del proveedor en la nube	Fugas de información intencionadas	Una nube poco fiable puede producir fugas de información	La fuga de una obra hace perder mucho dinero. Cada descarga de la web pirata significa un libro menos que se vende	12				

Figura 15.2 - Planes de seguridad

15.1.3. PCN

Por último, aquí definimos el plan de continuidad del negocio para cada una de las amenazas definidas.

				PCN		
Id	Vulnerabilidad	Amenaza	Riesgo	Medidas de análisis	Medidas de contención	Medidas de recuperación
1	No hay medidas preventivas de garantía de la propiedad intelectual.	Fuga de información de obras literarias	20	Analizar internet	Denunciar	Pedir la despublicacion del contenido pirata
11	Datos de obras literarias que se suben a la nube para ser tratadas informáticamente	Fugas de información intencionadas	15	Analizar internet	Denunciar	Pedir la despublicacion del contenido pirata
10	Falta de fiabilidad del proveedor en la nube	Fugas de información intencionadas	12	Analizar internet	Denunciar	Pedir la despublicacion del contenido pirata
8	Este tipo de empresas puede sufrir ataques de ransomware.	Ciberataque	10	Determinar grado de filtración. Estudiar integridad	Comunicar	Cambiar contraseñas. Reforzar seguridad
9	También ha habido casos de empresas del sector que han tenido intentos de accesos remotos para obtener información de obras en edición, con el fin robar la autoría de las obras literarias.	Fugas de información intencionadas	10	Analizar internet	Denunciar	Pedir la despublicacion del contenido pirata

Figura 15.3 - PCN

15.2. Anexo II: Cuestionario a editoriales

Las preguntas enviadas a las editoriales sobre temas de seguridad se detallan en la Tabla 15.1:

Área	Pregunta	Respuesta
Protección de la propiedad intelectual	¿Los empleados firman un acuerdo de confidencialidad sobre el contenido de los manuscritos?	
	¿Los manuscritos está cifrados o protegidos mientras se trabaja en ellos?	
	¿Los libros electrónicos salen al mercado con algún tipo de protección contra copia?	
	¿Las obras publicadas están debidamente inscritas en el Registro de la propiedad?	
	¿Se permite a los empleados usar dispositivos de almacenamiento externo?	
	¿Se controla la salida de archivos de los equipos?	
Seguridad en el puesto de trabajo	¿Los equipos son nominativos y están protegidos por contraseña?	
	¿Existe una política de contraseñas fuerte? (Mínimo de caracteres, caracteres especiales, renovación periódica, etc.)	
	¿Los equipos tienen software antivirus?	

	¿Los equipos están protegidos por cortafuegos?	
	¿El proveedor de servicios en la nube (si lo hubiera) tiene las certificaciones requeridas?	
	¿El proveedor de servicios en la nube (si lo hubiera) pertenece al Espacio Económico Europeo?	
Protección de datos	¿Los empleados están informados sobre la LOPD?	
	¿Se da un tratamiento correcto a los datos personales?	
	¿Los datos personales están debidamente almacenados y anonimizados?	
	¿Hay designado un responsable de la protección de datos?	
Seguridad física	¿Tienen un control de acceso a las instalaciones?	
	Si existe este control de acceso, ¿usa datos biométricos (huella digital) o soporte físico (tarjeta de acceso)?	

Tabla 15.1 - Cuestionario a editoriales

15.3. Anexo III: Análisis de la seguridad de la empresa

15.3.1. Mapa de activos

Como primer paso, realizamos un análisis de los activos que componen la organización. Los clasificamos en procesos de negocio, procesos de IT y recursos de IT según la siguiente definición:

- Procesos o líneas de negocio. Son los servicios prestados por la organización sin tener en cuenta la informática necesaria para soportarlos.
- Procesos de IT. Entornos o programas informáticos en que se tratan los datos de la organización.
- Recursos de IT. Resto de activos, incluidos los programas informáticos, elementos de hardware e instalaciones de la compañía.

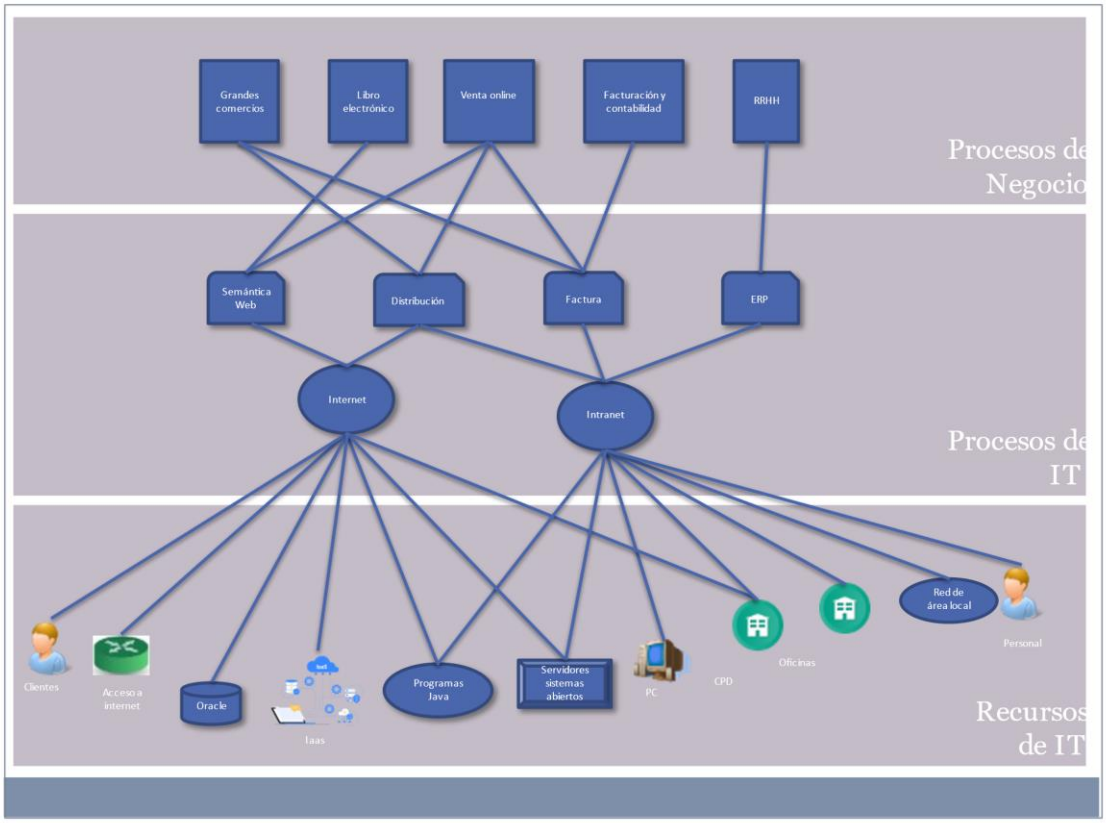

Figura 15.4 - Mapa de activos

15.3.2. Definición de activos y propagación de su valor

Como se observa en la Figura 15.4, los procesos de negocio son, en orden de importancia:

- Librerías.
- Libro electrónico.
- Venta online.
- Facturación y contabilidad.
- Recursos humanos.

Partiendo del valor de la compañía, esto es 500.000€, y considerando las prioridades anteriormente citadas, la herramienta de cálculo de riesgo arroja los siguientes datos sobre el valor del activo. Además, en la Tabla 15.2 también se valoran las dimensiones de seguridad.

Proceso de negocio	Valor del activo	Consideraciones para valoración DICATPd
Librerías	196.078 €	
Libro electrónico	132.026 €	
Venta online	100.000 €	
Facturación y	69.281 €	

contabilidad		
Recursos Humanos	2.614 €	

Tabla 15.2 - Definición de activos y consideraciones DICATPd

En la gráfica de la Figura 15.5 se puede observar la representación gráfica de todas las dimensiones de seguridad para todos los activos:

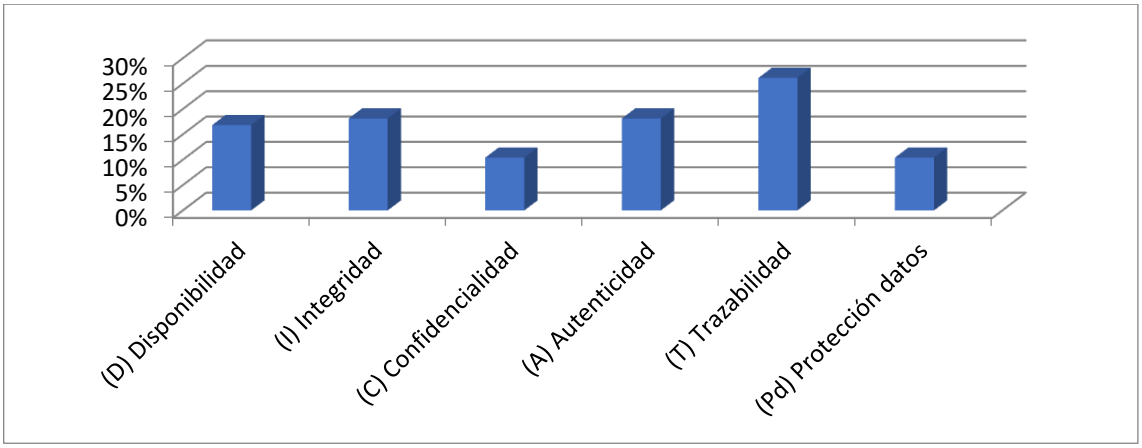

Figura 15.5 - Perfil DICATPd de la organización

A continuación, definimos la relación de los procesos de negocio con los procesos de IT. La herramienta de cálculo de riesgos nos da los datos listados en la Tabla 15.3.

Procesos IT	
Internet	999 €
Intranet	2.923 €

Tabla 15.3 - Procesos IT

De la misma manera, en la Tabla 15.4 desglosamos el resultado de relacionar los procesos IT y los recursos IT, siguiendo, de igual forma, lo indicado en el mapa de activos.

Recursos IT	
Clientes	1.458 €
Acceso a internet	1.259 €
Oracle	1.701 €
Programas Java	1.679 €
Servidores de sistemas abiertos	2.264 €
PCs	1.566 €
CPD	2.820 €
Oficinas	1.121 €
Tiendas	741 €
Red de área local	280 €
Personal	1.791 €

IaaS	1.458 €

Tabla 15.4 - Recursos IT

15.3.3. Vulnerabilidades, amenazas y riesgos

El análisis de riesgos de la organización se lleva a cabo en la pestaña **E60 Vulnerabilidades** de la herramienta de cálculo de riesgos. En ella especificamos la vulnerabilidad identificada, el activo al que afecta, su valor y el impacto que supone que dicho riesgo se materialice. Además, se incluye la salvaguarda que se debería llevar a cabo para tratar la vulnerabilidad. Esta información queda recogida en la Tabla 15.5.

Vulnerabilidad	Activo	Valor del activo	Riesgo	Salvaguarda
La actualización de los sistemas Oracle no es suficiente.	Oracle	167.393 €	425 €	Actualizar Sistemas Oracle
El CPD pierde suministro eléctrico.	CPD	334.362 €	1.880 €	Instalar sistema de emergencia en
Ciberataques por denegación de servicios	Acceso a internet	184.641 €	210 €	Actualizar antivirus
Posibilidad de daños por agua	CPD	334.362 €	470 €	Acondicionar CPD en caso de
La actualización de los sistemas operativos no es suficiente.	PCs	211.911 €	261 €	Actualizar SSOO
Filtración fragmentos de libros no publicados.	Servidores de sistemas abiertos	251.770 €	19 €	Cifrado información sensible
Mala política de contraseñas.	Personal	26.632 €	23 €	Mejora en la política de contraseña
Los equipos tienen liberados los pen-drives, lectores de CD-ROM, DVD y otros periféricos	Oficinas	106.527 €	28 €	Control sobre periféricos
Una empresa de la competencia ha sufrido un ataque de ransomware	Servidores de sistemas abiertos	251.770 €	1.132 €	Concienciación sobre phishing

Tabla 15.5 - Análisis de vulnerabilidades

Estas vulnerabilidades se identifican con el catálogo de amenazas de Magerit, como se puede ver en la gráfica de la Figura 15.6:

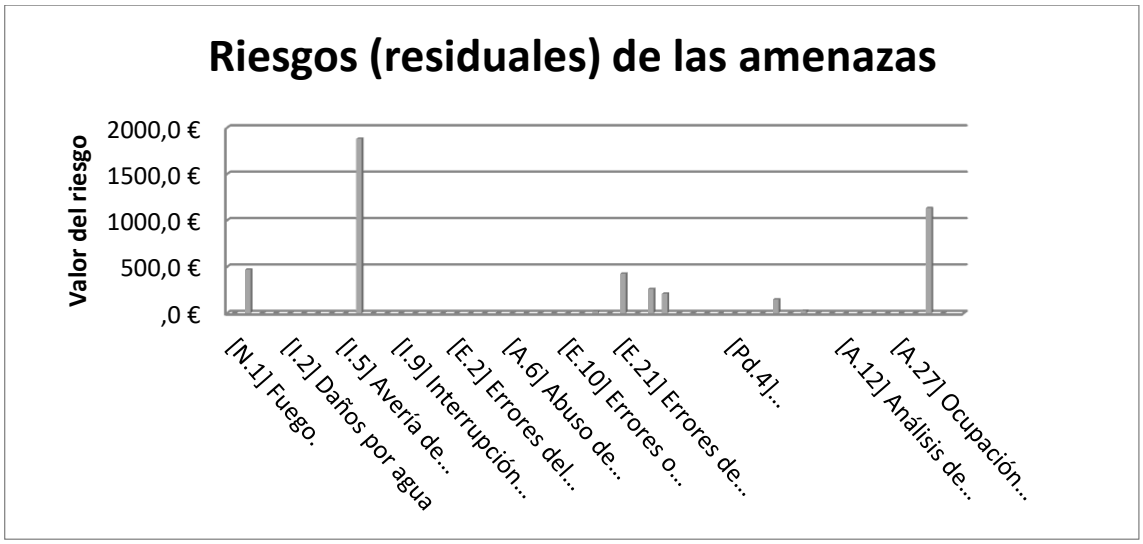

Figura 15.6 - Riesgos de las amenazas

Una vez aplicadas todas las salvaguardas anteriormente mencionadas, siguen quedando riesgos en cada una de las dimensiones de seguridad que no ha sido posible mitigar. A esto se le denomina riesgo residual. Este riesgo residual en cada una de las dimensiones queda reflejado en la gráfica de la Figura 15.7.

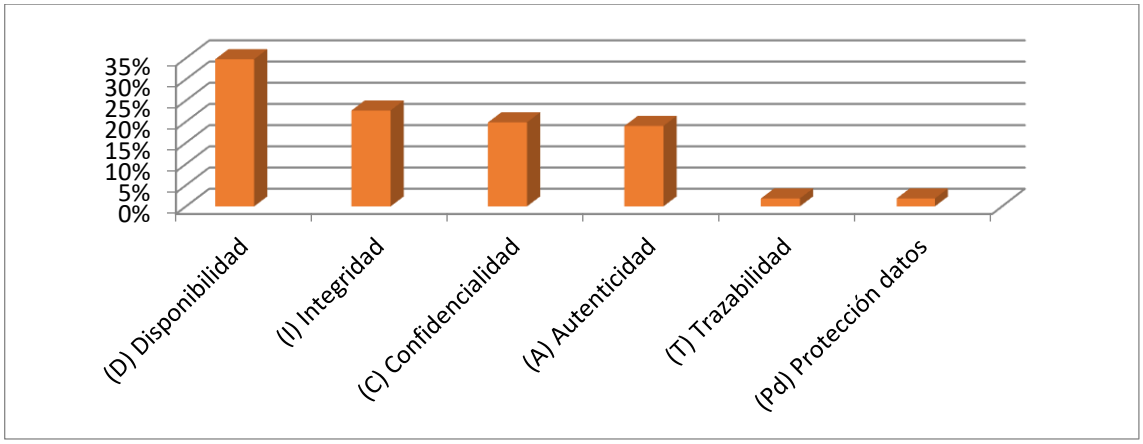

Figura 15.7 - Riesgo residual

Los costes del riesgo residual de la compañía sobre todos los activos ascienden a 4.574 €.