Estudio de herramientas de análisis y gestión de riesgos y propuesta de mejora de la herramienta PILAR

Autor: *Ángel Moreno Ontoria* ***Fecha:*** *8 de octubre de 2019*

Tutor: *Federico Simmross-Wattenberg*

Universidad de Valladolid
Ingeniería de Tecnologías Específicas de la Telecomunicación

Resumen

En el mundo cambiante en el que vivimos surgen imprevistos continuamente que afectan a particulares y organizaciones. Al género humano nos encantaría poder predecir el futuro con exactitud y anteponernos a los problemas que deriven de esos imprevistos. Saber con exactitud cuándo y dónde se desarrollará la próxima epidemia podría salvar muchas vidas o entender en qué momento concreto se va a caer un puente para remediarlo antes de que ocurra podría ahorrar mucho dinero. De igual manera sería muy útil saber donde atacarán unos hackers a una organización y cómo un incendio en cierto edificio supondrá un problema serio pues se perderán los datos de unos servidores clave.

Aunque en la práctica es imposible conocer el futuro a ciencia cierta sí que podemos determinar la probabilidad con la que se producirán eventos. En esto consiste el proceso de gestión de riesgos: en mantener un entorno controlado en el que se puedan analizar los riesgos y minimizarlos hasta niveles aceptables. Se realiza un modelado de la realidad centrándose en ciertos aspectos que interesen y simplificando otros. Se examina qué riesgos pueden afectar ese modelo y cuáles serían los más dañinos. Por último se tratan los riesgos, normalmente reduciendo su impacto, minimizando su probabilidad de ocurrencia o el daño ocasionado [1].

En distintos ámbitos de negocio se gestionan diversos tipos de riesgo: laboral, medioambiental, financiero, etc. El presente trabajo de fin de grado se centra en el riesgo de seguridad que afecta a empresas y administraciones públicas. En el mundo interconectado de hoy, ante la imposibilidad de participar en guerras entre países que hayan alcanzado tecnología nuclear, se ha ido cambiando el enfoque priorizando otros tipos de guerra: la guerra económica y la guerra cibernética. La gestión de riesgos de seguridad está muy enfocada hoy en día a la ciberseguridad pues la seguridad tradicional de guardia de seguridad y cámaras acorazadas es un ámbito muy maduro donde los delincuentes tienen difícil conseguir provecho alguno. La ciberseguridad, sin embargo, es un campo relativamente nuevo y cambiante en el que se están consiguiendo avances tanto por parte de atacantes como por la de defensores todos los días.

Para realizar un buen análisis de riesgos es importarte disponer de las herramientas y métodos adecuados. Este documento pretende mejorar una herramienta muy usada hoy en día en España: PILAR. Esta herramienta es de obligado uso en administraciones públicas y está empezando a ser usada por empresas. A pesar de lo extendida que está la herramienta y su gran utilidad en el proceso de análisis y gestión de riesgos, adolece de algunas carencias que dificultan el proceso de análisis de riesgos. Estas carencias retrasan el proceso de aprendizaje de la herramienta e incluso podrían interferir en el resultado del análisis de riesgos.

En este trabajo de fin de grado se busca identificar los puntos a mejorar en la herramienta para que puedan ser corregidos. Estos puntos de mejora se dividirán en cinco grandes categorías: *bugs*, mejoras de interfaz, mejoras de documentación, mejoras de funcionalidad y mejoras estructurales. Se intenta acercarse a estas posibilidades de mejora desde una perspectiva objetiva y concisa, detallando los pasos a seguir en el proceso de mejora. Los puntos propuestos podrán ser usados tanto para solucionar algun pequeño fallo como para reestructurar partes de la herramienta intentando mejorar fases del proceso de análisis y gestión de riesgos a través de PILAR. Para ayudar el proceso de mejora se analizarán dos herramientas que presentas funcionalidades de análisis y gestión de riesgos de las que PILAR no dispone. Se recomienda evaluar estos puntos detenidamente, pues aglutinan mejoras que son consideradas útiles por usuarios de la herramienta y funcionalidades nuevas que ayudarían a mejorar el proceso de análisis y gestión de riesgos.

Para valorar la utilidad de esta crítica, primero se encuestará a tres usuarios de la herramienta, para

recoger su punto de vista con respecto a las mejoras presentadas. A continuación se entrevistará a Jose Antonio Mañas, catedrático de la Universidad Politécnica de Madrid que ha sido el principal creador e impulsor de la herramienta. El punto central de estas entrevistas será determinar la utilidad de este trabajo de fin de grado.

Agradecimientos

En primer lugar me gustaría agradecer las enseñanzas de mi tutor de prácticas, Mariano J. Benito. Su guía me ha ayudado a entender mejor los entresijos del proceso de gestión de riesgos. Además su persistencia en *querer hacer las cosas bien* me ha impulsado a realizar esta crítica constructiva para mejorar, aunque sea un poco, este mundo en el que vivimos.

Me gustaría dar las gracias a Eduardo Hernández Perdiguero pues me ha enseñado a utilizar la herramienta con paciencia y buena fe. Me ha hecho ver que sin alguien con experiencia la herramienta se vuelve difícil de operar al principio. Además se ha preocupado porque este trabajo de fin de grado quedase bien pulido y estuviera orientado adecuadamente.

También me gustaría agradecer la participación de Manuel Jiménez Pérez-Yarza en la elaboración de este trabajo de fin de grado. Junto con las dos personas mencionadas anteriormente, ha participado en la evaluación del trabajo de fin de grado.

Quiero dar las gracias a la labor de *International Standardization Organization* por su trabajo en este ámbito. Concretamente me gustaría felicitar su estándar ISO 3100 que da una visión bastante útil de cómo se deben gestionar riesgos.

También quiero agradecer a José Antonio Mañas su ayuda prestada. Quiero remarcar que la herramienta PILAR me parece buena (pese a los puntos tratados) y necesaria para realizar una gestión de riesgos efectiva. Mi objetivo es ayudarla a ser aún mejor.

Por último (pero no menos importante), quiero agradecer el desempeño de mi tutor del trabajo de fin de grado, Federico Simmross Wattenberg. Su ayuda estructurando y revisando esta memoria ha sido muy útil. También quiero destacar su paciencia y afán de colaboración durante el desarrollo del trabajo de fin de grado.

Índice general

Capítulo 1

Introducción

1.1. Motivación

Desde la aparición de la herramienta PILAR en 2004 [2] ha sido señalada como herramienta estándar para realizar un análisis y gestión de riesgos por el Centro Criptológico Nacional. Año a año administraciones públicas, universidades y empresas han adoptado esta herramienta con buenos resultados. PILAR es la herramienta con la que mejor seguir la metodología MAGERIT [3], una metodología de análisis y gestión de riesgos elaborada por el Ministerio de Hacienda y Administraciones públicas. Además es especialmente útil por su compatibilidad con el Esquema Nacional de Seguridad, un estándar de nivel nacional que busca mejorar la seguridad de los sistemas de información de una organización mediante 75 controles.

Sin embargo la herramienta PILAR no es perfecta. Algunas de sus características existentes podrían ser mejoradas y se le podría añadir alguna funcionalidad nueva.

En concreto, de acuerdo a entrevistas realizadas a usuarios de la herramienta, el principal obstáculo que se encuentran los usuarios de la herramienta al empezar a usarla es una curva de aprendizaje bastante pendiente por su gran cantidad de opciones y diferentes configuraciones. Aunque es útil disponer de tantas formas de trabajar con el análisis y gestión de riesgos, tanta información puede ser un problema para un usuario no iniciado. El principal desarrollador de la herramienta, Jose A. Mañas, durante una entrevista realizada con motivo de este trabajo de fin de grado, afirma que lo que impide simplificar la herramienta es que quitar elementos dificulta realizar un buen análisis y gestión de riesgos. Como se puede ver, hacer menos pendiente la curva de aprendizaje de PILAR no es una tarea trivial.

Además al haberse desarrollado la herramienta originariamente en el 2004 hay elementos que hoy en día consideramos muy necesarios en el software, que no están implementados. Como por ejemplo una gestión modular de los estándares disponibles o la posibilidad de que la herramienta se actualice a sí misma.

1.2. Objetivos

En este trabajo de fin de grado se quiere proponer mejoras de la herramienta PILAR para que puedan ser implementadas por los desarrolladores de la herramienta si así lo consideran. El foco de las mejoras es mejorar la usabilidad (debido a la pendiente curva de dificultad) pero no acaban ahí las propuestas. Se ha decidido abarcar todo tipo de mejoras: desde cambios relativamente pequeños en la herramienta hasta modificaciones del modo de trabajar de la herramienta. Además de ello se sugieren características que, aunque difíciles de implementar, pueden suponer una gran mejora de uso de la herramienta, como por ejemplo adaptarla para poder acceder desde dispositivos móviles.

Se espera, además que dar contexto al análisis y gestión de riesgos y a la metodología MAGERIT ayude a entender cómo mejorarían la herramienta los puntos propuestos.

Por último, se busca comparar PILAR con otras herramientas de la misma índole para poder ver con mejor perspectiva las mejoras tratadas.

1.3. Estructura de la memoria

Además de criticar constructivamente a la herramienta PILAR, este trabajo de fin de grado también quiere introducir en el mundo de la Gestión de Riesgos a personas no iniciadas para que puedan compararla con otras herramientas y entiendan mejor los cambios propuestos.

Así pues tras la presente introducción se pasa al capítulo 2, un capítulo sobre el proceso de Gestión de Riesgos. En él, se explicará el proceso de acuerdo al ISO 31000 [4], un estándar considerado como guía por muchos en este ámbito. Se analizará el proceso paso a paso para entender cómo se afrontan cualquier tipo de riesgos en una organización.

Más tarde, en el capítulo 3 se hablará de MAGERIT; la metodología usada por PILAR para gestionar riesgos. MAGERIT proporciona un método sistemático para gestionar y analizar riesgos de Seguridad de la Información. Se puede considerar como una particularización del ISO 31000 para este tipo de riesgos.

Una vez tratados estos dos puntos se espera que el lector entienda la necesariedad de uso de herramientas de Gestión de Riesgos. Tras ello, en el capítulo 4, se pretende analizar otras herramientas de análisis y gestión de riesgos que consten de más madurez para poder entender mejor qué se podría mejorar de la herramienta.

Una vez entendido el contexto en el que se halla PILAR, en el capítulo 5 se desglosarán las propuestas de mejora en cinco grandes categorías: bugs, mejoras de interfaz, mejoras de documentación, mejoras de funcionalidad y mejoras estructurales. Se quiere estructurar todo de forma ordenada para facilitar la lectura. Las categorías de bugs, mejoras de interfaz y mejoras de documentación en general presentan cambios rápidos que se podrían hacer sobre la herramienta para corregir algún problema encontrado. Las categorías de mejoras de funcionalidad y mejoras estructuras se centran en añadir elementos nuevos a la herramienta para mejorar el proceso de análisis y gestión de riesgos a través de la misma. En concreto cabe destacar la última categoría, mejoras estructurales, porque presenta mejoras que se podrían hacer a la herramienta que requieren un cambio en su núcleo. No son mejoras fáciles de implementar pues modifican en gran manera su funcionamiento pero son las mejoras que más podrían beneficiar a PILAR.

A continuación, en el capítulo 6 se preguntará al creador y principal impulsor de la herramienta, Jose A. Mañas su opinión sobre el trabajo de fin de grado. También se encuestará a varios usuarios de la herramienta para que expresen su punto de vista con respecto a las distintas mejoras propuestas. Se busca evaluar la utilidad de esta memoria y determinar su impacto.

Por último, en el capítulo 7 se presentarán las conclusiones del estudio y se sugerirán líneas futuras de investigación en las que se pudiera entrar más adelante.

Capítulo 2

Gestión de riesgos

2.1. Introducción al proceso de gestión de riesgos

De acuerdo a la R.A.E., un riesgo es una contingencia o proximidad de un daño [5], aunque una forma más exacta de definir un riesgo en materia de análisis de riesgos sería afirmando que es un evento que tiene un impacto negativo sobre un elemento. Los riesgos se caracterizan por poder materializarse de acuerdo a una probabilidad de ocurrencia determinada [4].

Para entender cómo ayuda PILAR a la gestión de riesgos primero se ha de saber en qué consiste el proceso exactamente.

La gestión de riesgos, como se puede observar en la figura 2.1, es un proceso mediante el que primero se identifican posibles eventos que pudieran tener un impacto negativo en activos, entendiendo por activos a todo tipo de agentes presentes en el desarrollo del negocio (personas, servidores, edificios, procesos de negocio...). En segundo lugar se analizan los riesgos identificados intentando discernir cuáles son las consecuencias derivadas de los mismos más problemáticas basándose en la probabilidad de que los riesgos se materialicen. Por último se tratan los riesgos desarrollando controles destinados a corregirlos [4].

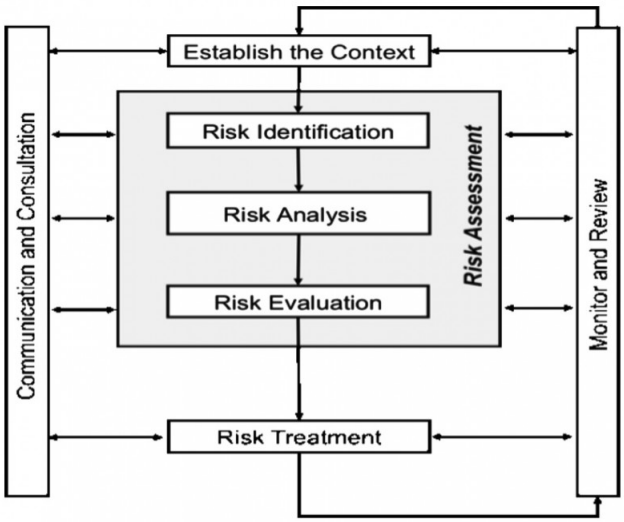

Figura 2.1: Proceso de gestión de riesgos según el ISO 3100:2018.

El proceso de gestión de riesgos se utiliza para decidir qué partes de una empresa son más vulnerables

y así poder asignar presupuesto a las mismas. Durante el proceso se tienen en cuenta salvaguardas ya implementadas para mitigar riesgos. Que un activo sea muy importante no quiere decir que sea más vulnerable que otro de menor importancia si está adecuadamente protegido.

La gestión de riesgos viene definida por las siguientes características [6]:

- Es un proceso continuo, pudiendo ser orientado como un proyecto de mantenimiento.
- Es realizado por el personal de una organización a todos los niveles.
- Está diseñado para identificar acontecimientos que pudieran pasar y, en el caso de ocurrir, afectarían a la entidad negativamente.
- Permite dar confianza al consejo de administración de una organización con respecto al estado de la misma.
- Está orientada al logro de objetivos.

2.2. Fases

Para llevar a cabo el proceso de gestión de riesgos se ha dividido el trabajo por hacer en fases. Las fases deben ejecutarse en orden como se describe a continuación, excepto la fase de *Monitorización y revisiones* que deberá estar presente durante todo el proceso.

2.2.1. Establecimiento de contexto

Antes de empezar a hacer nada conviene decidir de qué parte de la organización queremos gestionar los riesgos. A primera vista pudiera parecer que siempre se debe cubrir toda la empresa en su contexto, y en un mundo ideal así debiera ser. Sin embargo, a menudo existen limitaciones económicas que ponen trabas a perseguir ese objetivo. Por ejemplo, si se necesitara una certificación para hacer negocios con un determinado cliente por un requisito contractual lo más eficiente sería definir dentro del contexto los activos relacionados con el servicio que se le vaya a prestar.

No obstante, es altamente recomendable disponer de un estándar que abarque toda la organización. Siendo el ISO 27001 el principal candidato para esto pues es el más reconocido internacionalmente. El ISO 27001 permite establecer un Sistema de Gestión de la Seguridad de la Información (SGSI) que mejore el nivel de seguridad de la información de la organización. Se centra en la información por su criticidad en toda organización, por ejemplo si la lista de clientes de un empresa se *filtra* a otra empresa eso repercutiría negativamente en los ingresos de la primera.

Durante el proceso de establecimiento de un contexto se llegará a un acuerdo en cuanto a objetivos de la evaluación de riesgos, criterios de gestión de riesgos y el método de gestión de riesgos [7].

2.2.2. Apreciación del riesgo

Comprende el proceso de identificación, análisis y evaluación de riesgos. Los riesgos pueden ser vistos desde un punto de vista de la organización, de un departamento, de un proyecto o de una actividad individual.

El proceso de apreciación de riesgo proporciona como resultado información sobre las siguientes áreas [7]:

- Si una actividad debería ser llevada a cabo (como parchear cierto sistema).
- Cómo maximizar las oportunidades.
- Si los riesgos necesitan ser tratados.

- Cómo se deberán priorizar el tratamiento de riesgos.
- Las estrategias de tratamiento de riesgos que mejor se encargarán de rebajar el nivel de riesgos a una cantidad tolerable.

2.2.2.1. Identificación de riesgos

Una vez definido el contexto conviene saber a qué riesgos se enfrenta la organización. La identificación de riesgos consiste en el proceso de encontrar, reconocer y tomar nota de riesgos. Este proceso requiere ponerse en el lugar de *qué ocurriría si* el riesgo se materializa, identificando tanto las características claves del riesgo y como qué afectaría.

Conviene no solo identificar los riesgos a los que están espuestos los activos de la organización, sino también analizar sus causas y su probabilidad de que se materialicen en eventos reales. Todo esto debe ser hecho con la mayor imparcialidad posible.

Debido a la abundancia de riesgos a considerar, es fácil que alguno se pase por alto. Por ello es recomendable seguir alguno de los siguientes métodos [7]:

- Métodos basados en las evidencias, como por ejemplo datos históricos de un suceso.
- Análisis sistemático realizado por un equipo de expertos.
- Métodos de deducción inductiva como HAZOP [8].

Una incorrecta identificación de riesgos puede desencadenar un efecto dominó resultando en no implementar medidas de protección totalmente necesarias o gastar recursos en otras que no tengan demasiada utilidad.

2.2.2.2. Análisis de riesgos

Es una parte clave del proceso de gestión de riesgos. Un fallo en esta fase podría suponer que todo el proceso de gestión de riesgos perdiera su utilidad. Así pues, es muy importante que esta fase sea realizada con esmero. Por ello es la fase más difícil de realizar y en la que más se necesita una herramienta como PILAR. Esta herramienta ayuda durante todo el proceso de gestión de riesgos pero es en este ámbito donde es más útil.

El proceso de análisis de riesgos consiste en evaluar el impacto de los riesgos identificados en los activos de la organización. Para ello se tiene en cuenta el conocimiento adquirido sobre los riesgos del apartado anterior y se modifica este conocimiento en función de los activos de la organización. Se evalúa el impacto que tendría una materialización del riesgo en estos activos.

Para entender como el riesgo afecta a los activos se deben valorar normalmente en dimensiones de confidencialidad, integridad y trazabilidad, aunque no es raro que se usen otras dimensiones, como por ejemplo en MAGERIT, donde se añaden otras dos más a las *básicas*: trazabilidad y autenticidad [9].

Además de valorar los activos se deberá establecer una interdependencia entre activos. Una sala del edificio presenta unos riesgos por sí sola (incendio, acceso no autorizado...) pero el impacto de esos riesgos aumenta considerablemente si esa sala contiene servidores críticos para la organización. Así consideramos que los servidores dependen de la sala en la que se encuentran. Se puede identificar la relación de dependencia porque un problema con la sala es probable que afecte a los servidores mientras que lo contrario no es cierto.

Cada análisis de riesgos tiene sus particularidades y hay diferencias según quién lo desarrolle (aunque, si se modelase perfectamente la realidad, no debería haberlas). Pero, como norma general, se desarrolla un árbol de dependencias en el que los activos abstractos (servicios ofrecidos a clientes, procesos internos de la organización, etc.) se encuentran en la parte superior dependiendo de activos tangibles (servidores, salas, edificios, personal, etc.). Entrar en particularidades de cómo deberían depender unos de otros no es el objetivo de este documento pero cabe destacar que es un tema en el que se puede profundizar bastante.

Establecer una dependencia entre activos tiene la ventaja añadida de que hace más fácil revisar el análisis de riesgos. Si de repente un servicio ofrecido a un cliente cobra mucha relevancia, solo habrá que revisar el valor de este activo y su relación con los activos de los que dependa o que dependan de él; no hay que volver a revisar todos los activos.

Además, esta dependencia puede facilitar el proceso de valoración de activos. Si, por ejemplo, se tiene un árbol de 100 activos con 200 relaciones entre ellos, se puede valorar solo los activos superiores del árbol (15) y dejar que esa valoración se propague por el resto del árbol. Esto reduciría las 300 evaluaciones requeridas inicialmente a 215.

Otro método alternativo o complementario al descrito de dependencia entre activos es dividir los activos en diferentes dominios. Cada domino representa un conjunto de activos con unas características comunes; pueden ser propiedad de una misma persona, pertenecer a segmentos de red distintos, estar en una misma localización, etc. La valoración de estos dominios permite ajustar uniformemente el valor de los activos que pertenecen a los mismo.

2.2.2.3. Evaluación de riesgos

Durante esta fase del proceso de gestión de riesgos se intenta facilitar el proceso de decisión de qué hacer con los riesgos (ver siguiente fase). Para ello se evalúan los riesgos que tienen mayor prioridad y son candidatos a ser tratados con más detalle. También se revisan los resultados obtenidos evaluando el resultado del análisis de riesgos e intentando determinar si los riesgos encontrados tienen sentido (de lo contrario habría que volver a iterar la fase de *Apreciación del riesgo*.

2.2.3. Tratamiento de riesgos

Tras haber completado la evaluación de riesgos el proceso de tratamiento de los mismos cuyo objetivo es ponerse de acuerdo en qué hacer con los riesgos encontrados. Hay diversas formas de tratar un riesgo [7]:

- Evitarlo: este método implica dejar de hacer lo que genera el riesgo. Por ejemplo, es sabido que la mejor forma de que no se infecte un ordenador con código dañino es no tener ordenador. Se debe evaluar en detalle si interesa evitar un riesgo pues eso implica Cambios en el modo de funcionar de la organización.
- reducirlo: método preferido usado con los riesgos más críticos. Consiste en enfrentarse a él reduciendo su probabilidad de ocurrencia, sus efectos o ámbos. Esto deriva en una o varias acciones correctivas que *atacan* el riesgo.
- Transferirlo: método que busca que se encarguen otros del riesgo. Esto se puede conseguir subcontratando el servicio que presenta el riesgo. También se puede asegurar el riesgo. Una materialización del riesgo en el primer caso implicaría que no afecta a la organización y, en el segundo, que la organización no sufriría perjuicio (pues la aseguradora se haría cargo).
- Aceptarlo: para cuando todas las alternativas son demasiado costosas siempre se puede aceptar que ese riesgo existe y sus consecuencias en caso de que se materialice. Es arriesgado y desaconsejable seguir este camino con riesgos críticos para organización pero será el método usado para tratar todos los riesgos que no se puedan afrontar de otro modo.

Como se ha mencionado antes, de esta fase surgirán acciones correctivas que formarán parte del *plan de tratamiento de riesgos* de la organización. Este plan, a menudo aprobado por la Junta Directiva, pretende mejorar el nivel de riesgo de la organización tratando los riesgos más importantes identificados durante la fase de apreciación de riesgos.

2.2.4. Monitorización y revisiones

Los riesgos y controles deben ser monitoreados periódicamente para asegurar que no hayan cambiado. En caso de hacerlo se deberá reevaluar el estado del modelo de riesgos existente y adaptarlo como fuera conveniente. Esto podría, incluso, comenzar otro nuevo ciclo de gestión de riesgos si el cambio fuera significativo.

Durante el proceso de monitorización se deberá asegurar que [7]:

- Las suposiciones de riesgos siguen siendo válidas.
- Los pilares del análisis de riesgos no han cambiado, aún en caso de un cambio en el contexto.
- Se consiguen los objetivos proyectados.
- Las técnicas de análisis de riesgos estan siendo aplicadas correctamente.
- El tratamiento de riesgos es eficaz.

Capítulo 3

Gestión de riesgos de la seguridad de la información

3.1. Seguridad de la información

3.1.1. Introducción

La Seguridad de la Información consiste en la protección de la información poniendo especial interés en sus componentes críticos. Para ello, todo trabajo alrededor de ese concepto se centra en tres pilares: confidencialidad, integridad y disponibilidad [10].

La confidencialidad consiste en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. La confidencialidad es clave en estrategias de empresa, secretos de estado, secretos de sumario, etc. Un ejemplo de mejorar la confidencialidad de un documento sería cifrarlo mediante AES-512.

La integridad consiste en que el activo de información no ha sido alterado de manera no autorizada. A menudo interesa mantener una alta integridad cuando la confidencialidad también es alta aunque no es siempre el caso (como por ejemplo en un servidor DNS en el que la información es pública pero si es modificada podría dar lugar a ataques donde los cibercriminales hicieran apuntar un dominio conocido a una dirección ip propia en la que simulasen ser la página web legítima recogiendo credenciales de usuarios). Un ejemplo de mejorar integridad sería transmitir un código de redundancia cíclica (CRC) junto con la información de forma que una modificación no autorizada en la información crearía una disparidad entre el CRC y la información.

Por último, la disponibilidad consiste en que las entidades o procesos autorizados tienen acceso a los activos cuando lo requieren. A menudo esta carácterística es la priorizada con respecto a las otras pues una indisponibilidad del servicio puede tener consecuencias catastróficas en un negocio. Un ejemplo de mejorar esto sería crear un servidor de *backup* que sustituiría al principal en caso de fallo [11].

3.1.2. Estándares

Los siguientes estándares son los más conocidos en España en lo que se refiere a seguridad de la información. Indican unos controles a implementar que mejoran la seguridad de activos como información financiera, propiedad intelectual, datos de empleados o información proporcionada por terceros. Para probar que se están cumpliendo los controles de estos estándares las organizaciones se certifican mediante un proceso de auditoría.

A menudo las empresas disponen de controles de seguridad, pero han sido implementados como soluciones

a problemas específicos y tienden a estar desorganizados e inconexos entre sí. Estos estándares centraliza todos esos controles definiendo qué es recomendable en cada aspecto de la seguridad para una protección efectiva de la información en una organización.No solo tratan aspectos relacionados con tecnologías de la información, sino que abarcan todo lo referente a la seguridad de información desde revisiones de extintores hasta investigación previa a la contratación de empleados.

Una pieza clave común en estos estándares es la necesidad de realizar una gestión de los riesgos.

3.1.2.1. ISO 27001

ISO27001 es el estándar principal de la familia ISO 27000. Esta familia se centra en implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) en una organización. En concreto, ISO 27001 especifica los puntos a cubrir necesarios para establecer, implantar, mantener y mejorar un SGSI.

Cabe destacar que en la implementación de un SGSI es útil conocer las buenas prácticas comúnmente empleadas a través del ISO 27002. Este ISO entra en detalle en los puntos tratados en el ISO 27001.

3.1.2.2. NIST 800-53

Define un conjunto de controles a implementar para mejorar la seguridad y privacidad. Es usado principalmente en los Estados Unidos para sistemas de información federales. NIST dispone de guías para desarrollar e implementar este estándar.

3.1.2.3. Esquema Nacional de Seguridad

Estándar español en el que se especifica con detalle qué controles se deben implementar para securizar la información. Está orientado a un uso en administraciones públicas aunque también se usa en universidades y el sector privado.

Está constituido por los principios básicos y requisitos mínimos necesarios para proteger la información. Para ello añade dos dimensiones a las ya conocidas: autenticidad y trazabilidad [12].

3.1.3. Acercamientos a la seguridad de la información

El proceso de implantación de un sistema para aumentar la seguridad la información no es algo que sea rápido y puede resultar una tarea altamente compleja, especialmente si se dispone de escasos recursos. No es raro que una empresa quiera implantar un sistema de este tipo en un plazo de uno o dos meses se encuentre con que es prácticamente imposible llevar a cabo la tarea.

Existen dos métodos para implantar este tipo de sistema [10]:

Los administradores pueden ir mejorando la seguridad de los sistemas poco a poco. Al estar trabajando diariamente con los sistemas los administradores poseen información de primera mano de como funcionan y pueden ser mejorados. Entienden mejor qué se debe cambiar exactamente y se preocupan de que sea factible el cambio. Este método se denomina *bottom-up approach*.

Por otro lado el personal ejecutivo puede trazar un plan para mejorar la seguridad de la empresa cambiando las políticas de la misma. Los administradores podrán realizar los cambios convenientes siguiendo esas directrices. Lo mejor de este método es que es más difícil olvidarse de algún punto en comparación con usar un método *bottom-up*. Además es más probable que los cambios estén alineados con los objetivos estratégicos de la empresa. Este método se denomina *top-down approach*.

3.2. Metodologías de gestión de riesgos de seguridad de la información

Las metodologías de gestión de riesgos se encargan de enfrentarse a riesgos, siguiendo las directrices del ISO 31000 sección 4.4 (*Implementacion de la Gestión de Riesgos*). Normalmente vienen divididas en subprocesos a seguir, a veces intercambiables entre una metodología y otra. Cada metodología tiene sus puntos fuertes y sus flaquezas, sin embargo no es el objetivo de este estudio criticarlas por lo que no se entrará demasiado en detalle en este aspecto.

Como PILAR se basa en MAGERIT el foco de esta sección es esa metodología. No obstante también se presenta el ISO 27005 por su importancia al pertenecer a la familia ISO 27000 y las metodologías Mehari y NIST. Se busca tener una idea mejor de lo que representa la metodología MAGERIT con respecto a las otras.

3.2.1. MAGERIT

Según el Consejo Superior de Administración Electrónica (la entidad que publica este estándar) es clave en la gestión de una organización el buen gobierno [1]. Para tomar decisiones en este ámbito una adecuada gestión de riesgos es imprescindible. Sin ello establecer confianza con la Dirección es tarea ardua.

Se afirma que las organizaciones no deben solo tratar riesgos TIC; de hecho, no deben siquiera tratar riesgos TIC por separado. Por eso MAGERIT pretende ayudar a las organizaciones a tratar todo tipo de riesgos dando un marco de referencia común a las organizaciones españolas.

Si bien la metodología de gestión de riesgos reconocida internacionalmente con más importancia es el ISO 27005 esta sección se centrará en MAGERIT, por ser la metodología que se ha usado como base para desarrollar PILAR.

MAGERIT implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de las tecnologías de la información. Para conseguir eso MAGERIT persigue los siguientes objetivos:

Directos

- Concienciar a la dirección de la existencia de riesgos y de la necesidad de que sean tratados.
- Presentar un método sistemático para analizar los riesgos.
- Ayudar a planificar el tratamiento necesario para mantener los riesgos controlados.

Indirectos

- Preparar a la organización frente a procesos de evaluación, auditoría, certificación y/o acreditación

Para consiguir estos objetivos se define un modelo de valor común que facilita el establecimiento de relaciones de interdependencia entre activos. Se crea un mapa de riesgos que interrelaciona activos con los riesgos asociados a los mismos y se evalúan las salvaguardas existentes para determinar cuáles son las mejores para proteger frente a los riesgos observados. El resultado de esto es un informe del estado del riesgo residual que queda tras haber aplicado las salvaguardas. Normalmente se usa este riesgo residual para determinar mediante un informe de insuficiencias cuáles son los riesgos que deben ser tratados con mayor prioridad. Por último se combina el informe de insuficiencias con el conocimiento de la organización para elaborar un plan de seguridad destinado a tratar los riesgos [1].

3.2.1.1. Método

En el primer documento de MAGERIT se describe el método a seguir para una correcta gestión de riesgos. Este documento, siendo el más extenso de los tres, representa el núcleo de la metodología MAGERIT. Los

otros dos documento complementan este.

El método se basa en la estructura que podemos ver en la Figura 3.1. Los activos que intrínsecamente están asociados a un valor están espuestos a amenazas. Estas amenazas afectar en mayor o menor medida a los activos (generando un impacto) y tienen una cierta probabilidad de ocurrencia. La combinación de la probabilidad de ocurrencia y el impacto generado por la amenaza da lugar al riesgo.

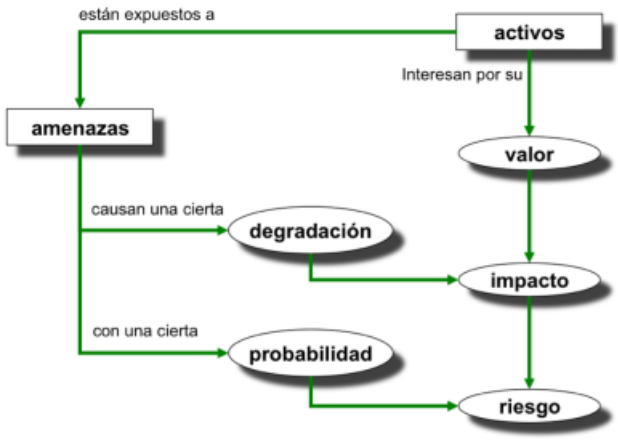

Figura 3.1: Desglose de los elementos que generan los riesgos según MAGERIT.

Este es el desglose de cómo afectan los riesgos a los activos. A esto hay que añadir qué se hace para mitigar estos riesgos. Para ello se despliegan salvaguardas destinadas a disminuir la probabilidad de materialización de las amenazas y, si esto ocurriera, disminuir el impacto generado sobre los activos. El riesgo resultante de quitar del riesgo total el riesgo mitigado por las amenazas se denomina riesgo residual. El riesgo residual representa el estado actual a nivel de riesgo del activo teniendo en cuenta sus características y salvaguardas implementadas sobre él.

Aunque MAGERIT está destinada a cualquier tipo de organización sea pública o privada, se deja entrever que la metodología está orientada hacia las administraciones públicas. Esto se hace latente por ejemplo cuando, en la fase de tratamiento de riesgos se cambia la aceptación del riesgo por algo llamado *financiación* que incluye la recomendación de guardar fondos para cuando el riesgo aceptado se materialice. Esta forma de gestionar el dinero sería difícil de concebir en una empresa privada [1].

3.2.1.2. Catálogo de elementos

En este trabajo de fin de grado se pretende facilitar el trabajo de las personas que realizan una gestión de riesgos dando elementos estándar que puedan usar durante el proceso y homogeneizar los resultados del análisis, presentando una terminología común a usar lo que facilita la coordinación entre distintos equipos.

En primer lugar se presentan las distintas categorías en las que se dividen los activos. Se definen unos grupos genéricos de los que cabe destacar los activos esenciales. Los activos esenciales representan el núcleo del análisis de riesgos, se subdividen en información que se maneja y servicios que se prestan.

A continuación se describen las dimensiones que forman los pilares de la seguridad de la información a las ya mencionadas confidencialidad, integridad y disponibilidad se añaden otras dos; autenticidad y trazabilidad. La autenticidad es una característica que indica que alguien es quien dice ser o bien que garantiza la fuente de la que proceden los datos. La trazabilidad consiste en que las actividades de una entidad pueden ser señaladas como llevadas a cabo por esa entidad.

Más tarde se establece un criterio de valoración común para que un análisis de riesgos no varíe demasiado de unos equipos de trabajo a otros y estén claros los conceptos usados. Se detallan aspectos necesarios para

la valoración como la presencia de información personal, las obligaciones legales, el histórico de incidentes de seguridad y los intereses económicos presentes entre otros.

Por último se desglosan las amenazas más comunes y las salvaguardas empleadas para combatirlas referenciándolas a las categorías de activos antes presentadas. No solo se definen estos dos aspectos de la gestión de riesgos sino que se detallan incluyendo las dimensiones afectadas por la amenaza/salvaguarda. [9]

3.2.1.3. Guía técnica

En este trabajo de fin de grado se presentan diversos métodos utilizados durante el análisis y gestión de riesgos. En primer lugar se detallan técnicas específicas para obtener resultados de interés como el uso de tabla, técnicas algorítmicas y árboles de ataque para ayudar al proceso de identificación de amenazas. A continuación se analizan técnicas más generales destinadas a la valoración de activos (con un desarrollo de la metodología Delphi y guías sobre entrevistas, reuniones y presentaciones) y a la presentación de resultados mediante técnicas gráficas [13].

3.2.2. ISO 27005

Estándar bastante diferente a MAGERIT en el sentido de que no pretende recomendar un método para la gestión de riesgos. Se centra en proporcionar un proceso continuo que consiste en realizar una serie de actividades (siendo algunas de las cuales iterativas).

Estas actividades son:

- Establecer el contexto del proceso de gestión de riesgos. Para ello se identifica el alcance, las obligaciones legales y contractuales y criterios como la tolerancia al riesgo de la organización.
- Evaluar cuantitativamente o cualitativamente información relevante sobre los riesgos. Teniendo en cuenta amenazas, información sobre los activos, y controles y vulnerabilidades existentes.
- Tratar el riesgo de forma apropiada usando métricas comunes para determinar qué riesgos hay que priorizar.
- Mantener informadas a las partes interesadas durante el proceso.
- Monitorizar y revisar el contexto, los riesgos y las obligaciones de forma continuada identificando y respondiendo apropiadamente a cambios significativos.

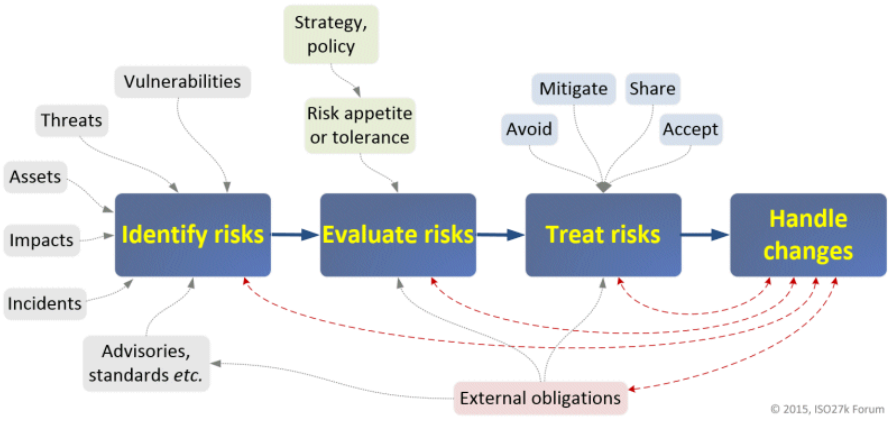

Figura 3.2: Gestión de riesgos según el ISO 27005.

Como se puede ver en la Figura 3.2, el proceso general se asimila al ISO 31000 pero difiere en que está especialmente orientado a la gestión de riesgos de la seguridad de la información. Cabe destacar la presencia del concepto de *vulnerabilidad* que se tiene en cuenta a la hora de identificar riesgos que afecten a los activos. Según MAGERIT un ordenador parcheado al día conllevaría el mismo riesgo que uno que llevase un año sin ser parcheado. El concepto de *vulnerabilidad* soluciona este aspecto [14].

3.2.3. Mehari

Mehari es una metodología de análisis y gestión de riesgos que, aunque en un principio se desarrollo por y para la empresa *CLUSIQ and CLUSIF*, pasó a ser Open Source en 2007. Incluye fórmulas listas para ser usadas en la gestión de riesgos y viene con una herramienta fácil de usar para ayudar automatizando tareas básicas.

Cabe destacar que presenta dos métodos para realizar la gestión de riesgos:

- Gestión de riesgos de forma individual y directa. Consiste en evaluar todas las situaciones de riesgo tomando decisiones específicas de acuerdo a cada una de ellas. Siendo este el método preferido por su precisión tiene la desventaja de ser algo caro.
- Gestión de riesgos de forma global e indirecta. Consiste en evaluar los riesgos desde un punto de vista genérico identificando objetivos de seguridad y certificación sin una gestión demasiado individualizada de los riesgos. Lo bueno de este método es que es rápido de efectuar y sus resultados son fáciles de comunicar. El problema es que esos resultados, a menudo, carecen de la exactitud necesaria para tomar buenas decisiones.

3.2.4. NIST SP 800-37

NIST SP 800-37 es una publicación del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) que busca dar una guía en la que se muestra como conseguir implementar un marco de referencia de la gestión del riesgo (RMF). El RMF pretende proveer de un proceso estructurado, flexible y disciplinado para gestionar riesgos de seguridad y privacidad. Curiosamente se incluye en su última revisión (Rev 2) esta gestión de riesgos de privacidad. Al parecer los legisladores americanos se están dando poco a poco cuenta de lo que ya es una idea asentada en Europa; que la privacidad y la protección del dato deben ser cuestiones de gran importancia (de ahí el desarrollo y publicación del GDPR por la Unión Europea).

Ejecutar tareas de RMF hace confluir en un solo marco de referencia procesos de gestión de riesgos a nivel de sistemas (antes referido como *bottom-up aproach*) y procesos de gestión de riesgos a nivel de organización (antes referido como *top-down aproach*) [15].

Capítulo 4

Análisis de las herramientas de Análisis y Gestión de Riesgos

A lo largo de los años surge la necesidad de gestionar riesgos cada vez más complejos en empresas cada vez más grandes. Tras la Segunda Guerra Mundial, en la década de 1950 empezó a extenderse una *nueva* forma de enfocar los riesgos; analizándolos y haciéndoles frente [16]. Desde entonces, especialmente gracias a la aparición de los ordenadores, no han hecho más que surgir herramientas de análisis y gestión de riesgos al mercado.

Para entender bien el margen de mejora que tiene PILAR por delante se van a analizar dos herramientas de análisis y gestión de riesgos con mayor madurez que PILAR. El objetivo es resaltarlas de entre las decenas de herramientas disponibles y dar sus puntos fuertes. Se pretende dar un marco de referencia con respecto a las funcionalidades de una herramienta muy similar a PILAR llamada *RMStudio* y las posibilidades de mejora para un futuro a medio y largo plazo que se pueden observar en una gran herramienta de gestión de todo tipo de riesgos (no solo en el sector de seguridad de la información) llamada *Integrum*.

Como mención honorífica cabe destacar herramientas a las que se ha destinado menos esfuerzo de desarrollo y que también están basadas en la gestión de riesgos, generalmente orientadas a dar soporte en auditorías o generar paneles con indicadores clave del estado de la organización. Entre estas herramientas se encuentran: *Auditboard* [17], *Reciprocity* [18], *Tracker networks* [19], *Netwrix Auditor* [20] y *Donesafe* [21].

4.1. RMStudio

RMStudio [22] es una herramienta principalmente dedicada a la gestión de riesgos desarrollada por *Stiki Information Security* en Islandia. La empresa consta de una decena de trabajadores, luego disponen de más recursos que los que están destinados a la herramienta PILAR. Además están certificados en ISO 27001 lo que da cierta seguridad a sus clientes de que el producto es estable y robusto frente a ataques.

La forma estándar de trabajar con RMStudio es desplegar una base de datos en un servidor a la que pueden acceder varios usuarios simultáneamente (de hecho la licencia limita el número de usuarios). Además se puede instalar un módulo que adapta la herramienta al servidor para acceder a ella mediante https (en PILAR la herramienta se tiene que instalar en cada ordenador aunque se está desarrollando una versión web).

El menú principal de la herramienta (denominado *árbol de navegación*) presente en la figura 4.1 muestra de una forma limpia y ordenada las distintas opciones presentando iconos al lado de cada una que dan una idea de la funcionalidad de cada una.

Hay cuatro categorías principales que pueden ser accedidas desde el menú principal:

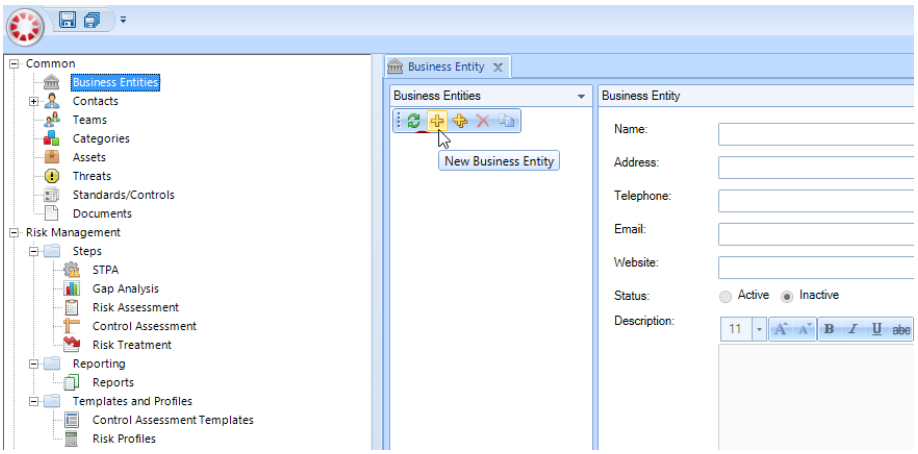

Figura 4.1: Interfaz de la herramienta RMStudio.

- Común: este apartado permite gestionar los activos, los equipos y usuarios relacionados con estos, las amenazas y las categorías que pueden ser asociadas a los activos (estas categorías indican, por ejemplo, que un activo es un servidor, asociándole los riesgos pertinentes).
- Gestión de riesgos: engloba todos los pasos de la gestión de riesgos. Primero se permite hacer un análisis de diferencias de cómo están los controles de seguridad en un momento a dónde se quiere llegar. A continuación se transiciona a la apreciación del riesgo para después dar paso a la gestión de controles de seguridad implementados para reforzar la seguridad de los activos. También se puede realizar un tratamiento de riesgos teniendo en cuenta controles actuales aplicados y futuros para ver cómo cambia el riesgo. Por último permite generar informes que se adapten a las necesidades de negocio de la organización.
- Gestión de datos: permite entender cómo funcionan los flujos de datos dentro de la organización. En este apartado se determinan qué datos existen, su relación entre ellos y quién es propietario de cada uno. En PILAR esta capa de abstracción está incluida junto con la gestión de riesgos estándar lo que, por un lado, facilita asociar datos a activos pero, por otro, complica el panorama general de activos y dependencias entre ellos.
- Gestión de la continuidad de negocio: este apartado permite analizar qué partes de la organización son vulnerables a caídas de servicio (como un corte de luz) y cómo afectan esas caídas a los sistemas permitiendo generar planes de respuesta ante incidentes. PILAR también dispone de esta funcionalidad pero no será tratada en este trabajo de fin de grado en detalle por estar centrado en el análisis y la gestión de riesgos.

Pero lo que más interesa son sus diferencias con PILAR. Destacan las siguientes ventajas:

- Categorías de activos comprensibles y fáciles de editar.
- Más estándares y normas soportados. Además pueden ser copiados, modificados de forma rápida e intuitiva.
- Permite ver y modificar su algoritmo de cálculo de riesgos.
- Interfaz sencilla e intuitiva.
- Obliga a valorar activos uno a uno. Esto puede ser considerado una ventaja o un inconveniente, dependiendo de como se analice.

- Permite colaboración simultánea en la herramienta. Además de permitir el acceso a varios usuarios a la vez a la base de datos incorpora un sistema de ticketing destinado a la separación de roles. Por ejemplo un usuario puede generar reportes de los distintos riesgos que amenazan a la organización, otro distinto generar planes de corrección de riesgos y un último aprobar estos planes.

4.2. Integrum

Integrum es una de las herramientas de gestión de riesgos más extendida del mercado [23] [24]. De acuerdo a su página web cuenta con más de un millón de usuarios con licencia distribuidos en 200 países. No solo aborda riesgos en sistemas de información, trata todo tipo de riesgos: financieros, mediambientales, laborales, etc. [25]

La herramienta, mostrada en la figura 4.2, se caracteriza por su gran modularidad. Dispone de muchos módulos independientes que interaccionan entre ellos del modo que necesite quien contrata la herramienta. Además de las funcionalidad de gestión de riesgos permite gestionar recursos humanos, formación, reuniones, etc.

Figura 4.2: Ejemplo de panel de control de Integrum.

Se aloja en la nube, lo que facilita tareas de mantenimiento, gestión de configuración y gestión de red entre otras. Además está optimizada para acceso desde dispositivos móbiles y puede ser integrada dentro del Directorio Activo de la organización (esto último permite a los usuarios identificarse con sus credenciales estándar de la organización.

Permite ser personalizada por el cliente mediante algo denominado *white label* que implica que la plataforma está tan personalizada que no tienen ningún tipo de logo de Integrum, es como si hubiese sido desarrollada sola y únicamente para el cliente.

Como se puede observar esta herramienta está destinada a multinacionales grandes en las que hay equipos destinados a la gestión de riesgos. Otras herramientas con funcionalidades similares son *Qualys* [26] y *Cura* [27].

Capítulo 5

Propuesta de mejora de PILAR

5.1. Estado actual de la herramienta PILAR

La herramienta PILAR (Procedimiento Informático-Lógico para el Análisis de Riesgos) [1] está destinada al análisis y gestión de riesgos de una organización. Al estar basada en MAGERIT, *hereda* particularidades de la metodología, como la ausencia del concepto *vulnerabilidad*. A pesar de ello, año a año se ha ido mejorando PILAR hasta ser una herramienta completa y multifuncional.

La herramienta está desarrollada y financiada parcialmente por el Centro Criptológico Nacional (CCN), siendo su principal impulsor y desarrollador el profesor José Antonio Mañas. Hasta hace poco era comercializada por la empresa A.L.H. J. Mañas S.L. [28] pero en junio de 2019 se publicó la noticia de que S2 Grupo empezará a comercializar la herramienta tras haber llegado a un acuerdo con el CCN y José A. Mañas [29].

Para aprender a usar la herramienta se puede utilizar la documentación instalada junto con la herramienta o el manual de usuario online [30]. También se ofrece un curso online a través de la página web del CCN. Y, para los usuarios más avanzados, tras salir una nueva versión importante de la herramienta,r el CCN organiza cursos de entrenamiento en las nuevas funciones.

5.1.1. Proceso de análisis y gestión de riesgos mediante PILAR

Para entender el contenido de las mejoras propuestas es esencial comprender los términos usados. Para ello a continuación se expondrá cómo funciona la herramienta de forma resumida.

En primer lugar se define el contexto del proceso de gestión de riesgos identificando activos (figura 5.1)y, si se cree conveniente, riesgos. En caso de no identificar riesgos se pueden usar los riesgos que vienen por defecto en PILAR. A continuación se clasifican los activos asignando una o varias clases de las disponibles en MAGERIT [13]. Esto permite a la herramienta asociar su biblioteca de riesgos a los activos correspondientes, pues no está expuesto a los mismos riesgos un servidor que una persona.

Una vez clasificados los activos se debe elegir cómo van a estar relacionados y valorados. Por un lado se pueden relacionar y valorar por dominios, que implica agrupar activos con elementos en común (por ejemplo agrupar según el segmento de red al que pertenezcan). Por otro lado se pueden agrupar y valorar mediante dependencias. Así se suelen situar unos activos denominados *esenciales* en la parte superior del árbol (activos intangibles como servicios ofrecidos por la organización o procesos de negocio) y se hace depender todo tipo de activos de forma que la materialización de un riesgo en un activo *hijo* afectaría al *padre* pero lo contrario no siempre es cierto. No se concreta más esta definición por lo dicho anteriormente: hay muchas formas de hacer un análisis de riesgos. Se podrían valorar todos los activos o valorar solo los superiores y dejar que ese valor se propague a través de las dependencias para lo que es aconsejable ajustar el grado de dependencia.

Una vez valorados los activos se pasa a evaluar perfiles de seguridad. Los perfiles de seguridad son

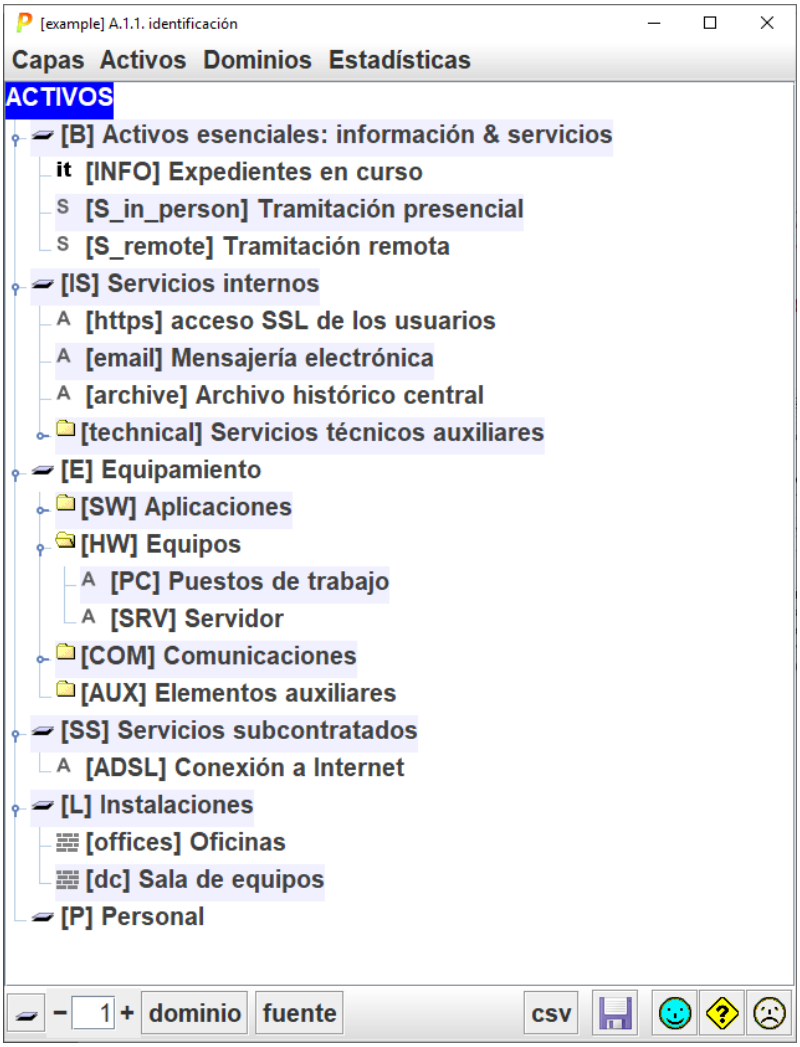

Figura 5.1: Ejemplo de pantalla de identificación de activos de PILAR.

estándares (como el ISO 27001) o leyes (como GDPR) en los que se puede fijar un grado de madurez en cada uno de los controles. Los grados de madurez empiezan en un L0, que significa que no hay nada implementado, hasta un L5 que significa que el control está implementado, monitoreado y optimizado (pasando por L1, L2, L3 y L4, que son valores intermedios entre esos extremos). PILAR consta de un conjunto de salvaguardas que aplicar a los activos, como puede ser *COM.i.1.2 Se eliminan las cuentas por defecto de las redes privadas virtuales configuradas*. Estas salvaguardas están asociadas a controles de los perfiles de seguridad. De este modo se pueden valorar las salvaguardas directamente o los controles de los perfiles de seguridad, siendo esto último bastante más rápido pues a menudo hay varias salvaguardas asociadas a un solo control.

A continuación, PILAR computa la valoración de los activos y las salvaguardas correspondientes. El riesgo que resultante de restar el riesgo original menos el riesgo eliminado por las salvaguardas se denomina riesgo residual. Este riesgo residual es la base para la toma de decisiones durante la fase posterior de tratamiento de riesgos. PILAR permite generar informes en los que se puede observar las distintas partes del proceso de forma detallada y visual.

5.1.2. Historia de las variantes de la herramienta

La primera versión de PILAR disponible para el público surgió en noviembre de 2004 con PILAR v1.2. Poca información queda de aquella primera versión, solo que se basaba en MAGERIT versión 1.0 publicada en 1997. Por aquel entonces no existía versión digital del estándar y tenía que distribuirse en papel [31].

La herramienta fue año a año adquiriendo funcionalidades y aumentando su complejidad de uso. Así, en diciembre de 2007 salió la primera versión de PILAR Basic, una variante de la herramienta más simple destinada a PYMES y a administraciones locales. PILAR Basic obliga al usuario a utilizar valoración por dominios en su análisis de riesgos simplificando el proceso. Además carece de muchas de las funcionalidades que podrían ofuscar a un usuario no iniciado (como puede ser gestión de vulnerabilidades o gestión de incidencias).

En Enero de 2009 surgió RMAT, una herramienta para personalizar PILAR para que se adapte a las necesidades de la organización. Se puede elegir comprar esta herramienta en conjunto con PILAR pero se ha de valorar previamente la necesidad de añadir más elementos al ya complejo entorno de PILAR.

Con el tiempo la herramienta PILAR siguió aumentando en complejidad. Surgió la necesidad de tener una versión más simple de la herramienta (incluso más que PILAR Basic) pues algunos usuarios la encontraban demasiado compleja para sus necesidades. Así surgió microPILAR en marzo de 2011. Para esta variante de la herramienta, se simplificó todo en extremo. Se eliminó el menú de opciones sustituyéndolo por una serie de pantallas en las que el usuario va introduciendo datos y pulsando en *siguiente*. Además se eliminó la clasificación individual de activos clasificando todos en grupo.

5.1.3. Fortalezas

Gracias a herramientas como esta se puede realizar una gestión de riesgos semi-automatizada simplificando el proceso. A continuación se detallarán los puntos fuertes tanto de las herramientas de análisis de riesgos como de ésta en particular.

Las herramientas de análisis y gestión de riesgos tienen las siguientes ventajas:

- Una vez aprende a utilizar estas herramientas el tiempo que se tarda en generar un análisis de riesgos es relativamente poco.
- Simplifican el proceso de monitorización y revisión de los riesgos pudiendo introducir cambios de forma rápida sin obligar al usuario a tener que rehacer todo el análisis de riesgos ante un cambio en el contexto.
- Contienen estadísticas de riesgos evitando a los usuarios largas sesiones de identificación y evaluación de riesgos base previo al análisis de riesgos propiamente dicho.
- Permiten actualizarse constantemente a través de internet incorporando nuevas funcionalidades y solucionando posibles problemas con la metodología o la herramienta.
- Ayudan a generar informes útiles para labores de auditoría como Declaraciones de Aplicabilidad (SoA por las siglas en inglés de *Statement of Aplicability*).
- Ayudan a generar informes útiles para presentar en juntas directivas el estado de la seguridad a personal poco familiarizado con el tema. Normalmente permiten generar gráficas que resumen visualmente cómo está la organización y qué aspectos se deben tener más en cuenta.
- Incorporan estándares que ayudan a determinar la efectividad de las salvaguardas y permiten evaluar el estado de la organización para la obtención de una certificación.

Además de esas fortalezas, PILAR también consta de las siguientes:

- Contiene estadísticas de riesgos adaptadas a la situación española. No es lo mismo la probabilidad de que haya un corte de luz o que haya un tornado en España que en un país que esté en otra geografía, como Australia.
- Incorpora el Esquema Nacional de Seguridad entre sus estándares disponibles (denominados perfiles de seguridad). A fecha de septiembre de 2019 es la única herramienta del mundo capaz de adecuar sus salvaguardas a las presentadas en ese estándar.
- Al haber sido desarrollada basándose en la metodología MAGERIT, los términos usados en castellano son conocidos por la comunidad española y no traducciones de otras lenguas.
- Permite una gestión más granular de los pilares de la seguridad añadiendo trazabilidad, autenticidad y datos personales a los conocidos confidencialidad, integridad y disponibilidad.
- Tiene el respaldo del Centro Criptológico Nacional. Una entidad de gran importancia a nivel nacional en materia de seguridad de sistemas TIC.
- Tiene un precio asequible en comparación con otras herramientas de análisis y gestión de riesgos. Además, si se contrata para un organismo de la Administración Pública está subvencionado por el Centro Criptológico Nacional.

5.2. Propuesta de mejora de PILAR

PILAR es útil y polivalente pero no es perfecta. Se han ido añadiendo buenas funciones durante los años y se han ido mejorando funcionalidades ya existentes. No obstante da la sensación que no se ha revisado el núcleo de la herramienta para hacerla más fácil para usuarios no iniciados y que no se han recogido métricas para mejorar la herramienta. Del uso de la herramienta se puede deducir que se han dedicado más esfuerzos a añadir nuevas funcionalidades que a consolidar las ya existentes

Así pues los defectos encontrados en PILAR se dividen en:

- *Bugs*: se pretende corregir fallos del código que se comporta de una forma inesperada ante una serie de acciones no tenidas en cuenta por el programador.
- Mejoras de interfaz de usuario: se pretenden corregir defectos que confunden a los usuarios de la herramienta (especialmente al principio) y tienen que ver con la interfaz gráfica.
- Mejoras de documentación: se pretenden adecuar la documentación para facilitar la compresión de conceptos.

Además de las imperfecciones ya presentes en la herramienta comentadas se han identificado otros elementos que podrían ser mejorados, son aquellos que aportarían novedad a la forma de trabajar con PILAR. Se ha dividido estos elementos en:

- Mejoras de funcionalidad: se pretende sugerir elementos que se podrían añadir o cambiar para facilitar el trabajo de los usuarios.
- Mejoras estructurales: se pretende presentar elementos que se podrían añadir o cambiar del núcleo de la herramienta para mejorar el análisis y la gestión de riesgos.

En las secciones siguientes se detallan los puntos expuestos, agrupando los tres primeros (*bugs*, mejoras de interfaz de usuario y mejoras de documentación) como una propuesta de mejoras sobre la herramienta existente, y los dos últimos (mejoras de funcionalidad y mejoras estructurales) como una propuesta de mejoras a añadir a la herramienta.

5.2.1. Propuesta de mejoras sobre la herramienta existente

Tras haber dado una visión general de que temas se va a tratar de mejorar llega el momento de señalar específicamente qué puntos han sido encontrados como problemas. No solo se pretende indicar estos puntos sino que también se buscará un remedio.

5.2.1.1. *Bugs*

Errores de código ante casos de uso que no se tuvieron en cuenta durante el desarrollo de la herramienta. Si bien es imposible predecir todas las situaciones posibles, se puede hacer pruebas para determinar algunos de estos *bugs*. De hecho, la mayoría de las actualizaciones a la herramienta consisten unicamente en correcciones de *bugs* lo que demuestra el compromiso de sus desarrolladores con tener una herramienta que funcione de acuerdo a como debería funcionar.

Salir sin guardar guarda I

Dentro de la opción del menú *Análisis de riesgos ->Actuaciones en seguridad*, después de añadir una actuación de seguridad, ésta queda guardada aunque no se presione el botón de guardar ni el botón de aceptar (saliendo de la opción del menú mediante el botón de cancelar o el botón de cerrar).

Dos posibles soluciones se pueden encontrar a este *bug*. En primer lugar se podría eliminar el botón de cancelar, pero eso haría la herramienta inconsistente luego no es la recomendada. En segundo lugar se podría guardar el estado de los elementos presentes en esa opción del menú al entrar en ella y compararlo con el estado de los elementos presentes al cancelar. Al cancelar se puede volver a cargar los elementos iniciales si hubiera alguna diferencia.

Fechas previas al segundo 0 de POSIX no aparecen reflejadas

Al igual que el *bug* anterior, este se encuentra dentro de la opción del menú *Análisis de riesgos ->Actuaciones en seguridad*. Se puede introducir fecha de inicio y fin de las actuaciones de seguridad. Lo tradicional es definir estas actuaciones como acciones correctivas tras una auditoría, puntos por mejorar del sistema identificados o respuestas a incidencias encontradas. Sin embargo hay quien puede interpretar estas actuaciones como objetivos de negocio, pudiendo ser éstos objetivos a largo plazo.

En el momento en el que se trabaja con objetivos a largo plazo hay que tener en cuenta que las fechas pueden trasladarnos varias décadas hacia atrás. Si nos trasladan más atrás del 3 de enero de 1970, será imposible tener constancia de esa fecha pues desaparece nada más ser introducida.

Ésto es debido a la forma de contar el tiempo POSIX [32], un estándar entre fabricantes de *software*. Para el tiempo POSIX se empezaron a contar los segundos desde medianoche del 1 de enero de 1970. Si no se tiene en cuenta adecuadamente las fechas, pueden ocurrir cosas extrañas: una fecha anterior a 1970 puede parecer posterior o una fecha reciente puede parecer cercana a 1970.

El problema probablemente deriva de la librería de Java utilizada. Es difícil saber exactamente cómo solucionarlo sin ver el código pero utilizar una librería moderna como java.util.Date ayudaría a zanjar el problema.

Salir sin guardar guarda II

De nuevo, el mismo problema encontrado antes se repite en otro aspecto. Esta vez, durante la modificación de un activo, si se entra en la descripción y se añade algo pero después se cancela esa modificación del activo, la descripción queda guardada como si se hubiera aceptado la modificación.

Una vez más, la solución adecuada es relativamente simple: se debe guardar la descripción al entrar en la modificación del activo y se debe comparar con la descripción existente al cancelar la operación. Si hubiera

discrepacias, se debe sustituir la descripción nueva por la anterior.

Pregunta por guardar sin haber modificado nada

Este *bug* también pertenece a la descripción de un activo. Cuando se entra a modificar un activo y se entra en la descripción del mismo sin escribir nada (y aún cancelando esa pantalla) salir de la modificación del activo cancelando pregunta si se desean guardar los cambios. Esto es extraño pues no se ha realizado ningún cambio.

La solución del *bug* anterior puede ser reutilizada para parchear este *bug* también.

5.2.1.2. Defectos de interfaz

La interfaz es lo primero que un usuario se encuentra al entrar en la herramienta. Debería ser intuitiva, agradable a la vista y fácil de manejar. En el caso de PILAR no siempre se cumplen eso. Cabe destacar que la interfaz no solo depende de quien la desarrolle; también depende del lenguaje de programación y las librerías usadas. A veces hay acciones que pueden parecer fáciles a un observador externo (como mover un botón de un sitio a otro) pero a nivel de programación pueden ser altamente difíciles o incluso imposibles porque la librería o el lenguaje no lo permiten.

Uno de los principales problemas de la herramienta es que la curva de aprendizaje es demasiado pendiente. Una mejora del interfaz ayudaría a solucionar este asunto, como se detalla a continuación.

Menú de opciones duplicado y complejo

Existen dos menús de opciones propiamente dichos en el menú Editar. Por un lado están las preferencias que ajustan el tipo y tamaño de letra usado en el programa y por otro están las opciones que ajustan todo lo demás. Además el menú de opciones es muy poco intuitivo (Figura 5.2).

Como se puede observar en la Figura 5.2 hay opciones que son una palabra, otras que son una frase, otras que son una pregunta, otras que empiezan con mayúscula, etc. Aunque la documentación es clara con respecto a estas opciones, su denominación no lo es.

Ante este problema una solución es categorizar y renombrar las distintas opciones, juntándo los dos menús en uno accesible desde un engranaje al lado de el botón de guardar en el menú principal.

Las categorías sugeridas a usar son:

- Estilo: agrupa las opciones del menú de preferencias.
- Identificación de riesgos: agrupa *probabilidad*, *consecuencias*, *amenazas* y *tiempos*.
- Análisis de riesgos: agrupa *fases*, *fases de proyecto*, *dominio de seguridad y fases de proyecto*, *transferencia de valor entre dimensiones*, *valoración*, *autenticidad* y *trazabilidad*.
- Evaluación de riesgos: agrupa *salvaguardas no evaluadas*, *madurez*, *perfil de seguridad: propagar* y *exportar salvaguardas*.
- Otros: agrupa *Xor*, *¿se guardan las amenazas al salir?*, *Riesgo en datos personales* y *riesgo residual*.

También se sugiere cambiar los nombres por otros más explicativos de acuerdo a la Tabla 5.1, así como las opciones disponibles dentro de cada opción de manera consecuente.

Además se sugiere recoger estadísticas de uso de las distintas opciones para poder identificar aquellas que no sean utilizadas apenas y puedan ser eliminadas.

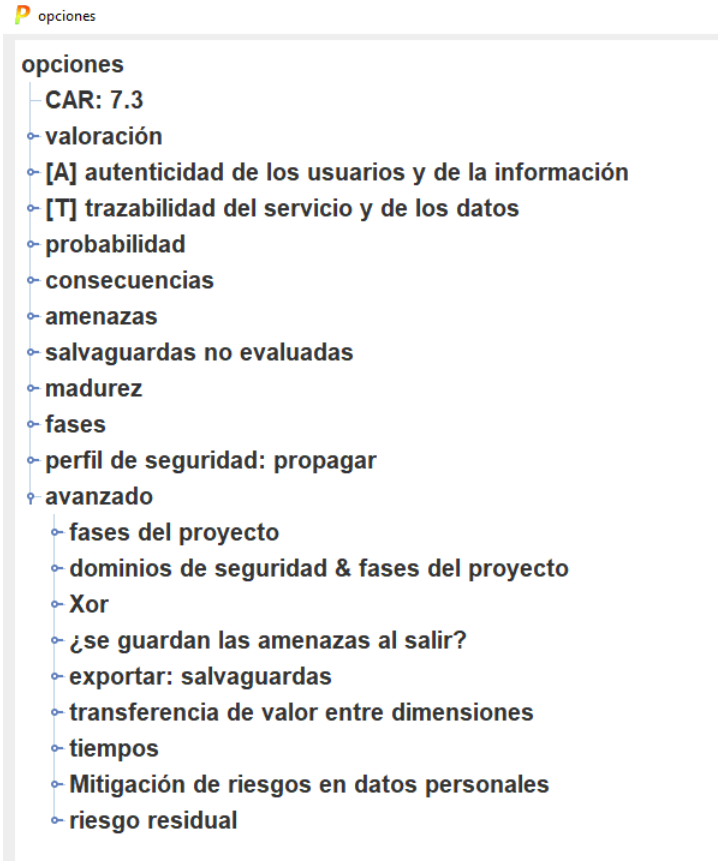

Figura 5.2: Menú de opciones de PILAR.

Menú principal complicado de navegar

De nuevo surge otra parte de PILAR con la que cuesta trabajar al principio. No es raro cuando se está empezando perderse entre los submenús y las muchas opciones disponibles. Los desarrolladores de la herramienta son conscientes de esto, por lo que incluyen la opción de poder ajustar el *nivel* de complejidad del menú (básico, medio y experto). Sin embargo, este ajuste apenas cambia el menú (aun pasando de básico a experto) por lo que el modo básico es de poca ayuda a un usuario no iniciado.

La idea es estructurar mejor el menú para que sea más sencillo navegar por él y entenderlo; y simplificar el nivel básico para que sea más útil a usuarios no iniciados, acercándolo a PILAR Basic y microPILAR.

En la Figura 5.3 se pueden observar las principales opciones del menú. Cabe destacar que hay muchas más descubribles a través de los desplegables. Al principio tal cantidad de opciones abruma lo que supone una barrera para la adopción de PILAR.

En primer lugar el submenú de proyecto es usado solo al principio y no se suele volver a tocar. Por ello es mejor que no forme parte de ese menú, estaría mejor dentro de la configuración en su propio submenú *proyecto*.

Además un usuario básico no necesita utilizar zonas lógicas ni físicas, luego se puede prescindir de esos apartados. El análisis de riesgos puede realizarse sin ellas. En cuanto al submenú amenazas realmente un usuario básico solo necesita ajustar los factores agravantes o atenuantes que afectan a los dominios del análisis. Y, con respecto a las medidas técnicas y organizativas y a las medidas de protección legal y cumplimiento. Las primeras es una gestión muy granular de las salvaguardas luego no es útil para un usuario básico. La segunda, aunque es útil, su contenido ya se encuentra en otro apartado: el de perfiles de seguridad, luego es

Opción antigua	Opción nueva
valoración	Método de valoración de activos
autenticidad de los usuarios y de la información	MAGERIT Interpolar autenticidad
trazabilidad del servicio y de los datos	MAGERIT Interpolar trazabilidad
probabilidad	Probabilidad de que se materialize una amenaza
consecuencias	Consecuencias de materialización de una amenaza
amenazas	Probabilidad e impacto de las amenazas
salvaguardas no evaluadas	Efecto de las salvaguardas no evaluadas
madurez	Escala de madurez
fases	Fases estándar usadas
perfil de seguridad: propagar	Propagación en perfiles de seguridad
fases del proyecto	Interconexión entre fases del proyecto
dominios de seguridad y fases del proyecto	Herencia de salvaguardas no evaluadas
Xor	Salvaguardas XOR
¿se guardan las amenazas al salir?	Guardado de amenazas al salir
exportar: salvaguardas	Exportar salvaguardas
transferencia de valor entre dimensiones	Transferencia de valor entre dimensiones
tiempos	Tiempo de reacción ante un ataque
Mitigación de riesgos en datos personales	Mitigaciónd de riesgos en datos personales
riesgo residual	Estimación del riesgo residual

Tabla 5.1: Sugerencia de cambio de opciones del menú por otras más explicativas

innecesario que esté ahí.

Así pues a continuación se desglosará una estructuración de los menús principales del usuario básico y el usuario experto siguiendo la estructura básica del ISO 31000. El usuario medio podría ser lo que es a día de hoy el usuario básico (adaptado a la nueva estructura).

El usuario básico estará subdividido de la siguiente manera:

- Determinación de contexto (lo que ahora se llama identificación de activos).
- Identificación de riesgos (lo que ahora se llama clases de activos).
- Análisis de riesgos.
  - Valoración de activos.
  - Dependencias entre activos (si los hubiera).
  - Valoración de dominios (si los hubiera, será el valor por defecto al crear un proyecto).
  - Factores que afecta a los dominios (lo que ahora se llama factores agravantes o atenuantes).
- Evaluación de riesgos.

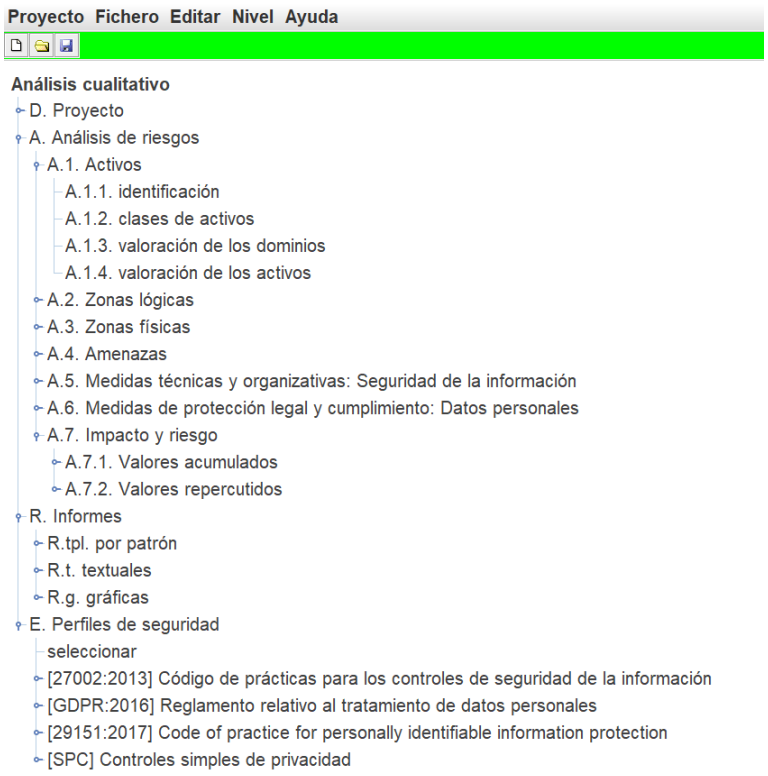

Figura 5.3: Menú principal del nivel básico de PILAR.

- Perfiles de seguridad (también podrían estar en análisis de riesgos pero se ha decidido incluirlos aquí para estructurar mejor los pasos a seguir).
- Valores acumulados.
  - Impacto.
  - Riesgo.
- Valores repercutidos.
  - Impacto.
  - Riesgo.

- Comunicación (el menú que ahora se llama Informes).

El usuario experto estará subdividido de la siguiente manera:

- Determinación de contexto.
  - Identificación de activos.
  - Nombres CPE.
  - Zonas.
    - Lógicas.
    - Físicas.
- Identificación de riesgos .
  - Clasificación de activos (lo que ahora se llama clases de activos).

    - Identificación de amenazas.
    - Valoración de amenazas.
    - Vulnerabilidades técnicas (CVEs).
    - Incidentes.
- Análisis de riesgos.
    - Valoración de activos.
    - Dependencias entre activos (si lo hubiera).
    - Valoración de dominios (si lo hubiera, será el valor por defecto al crear un proyecto).
    - Factores que afecta a los dominios (lo que ahora se llama factores agravantes o atenuantes).
- Evaluación de riesgos.
    - Perfiles de seguridad (también podrían estar en análisis de riesgos pero se ha decidido incluirlos aquí para estructurar mejor los pasos a seguir).
    - Madurez de las salvaguardas (una mezcla en una sola pantalla de lo que ahora está dentro del submenú Medidas técnicas y organizativas: Seguridad de la información y también lo que se encuentra dentro del submenú Protecciones adicionales).
    - Escenarios de riesgo.
    - Valores acumulados.
    - Valores repercutidos.
- Tratamiento de riesgos (lo que ahora se llama actuaciones en seguridad).
- Comunicación (el menú que ahora se llama Informes).

De nuevo se recomienda usar estadísticas de uso para identificar funcionalidades poco usadas que se puedan eliminar.

Eliminación de pantalla innecesaria

Nada más abrir un proyecto aparece una ventana con metadatos del proyecto que hay que cerrar. Como cambio menor se sugiere quitar esta pantalla y añadirla al menú de ayuda, ya que una vez se ha visto por primera vez ya no contiene información relevante para el análisis y gestión de riesgos.

Mejora gráfica de las dependencias

Cuando se está trabajando con dependencias entre activos a menudo se pueden encontrar situaciones complejas que conviene analizar con detalle. PILAR proporciona un método para analizar por qué un activo *hereda* un determinado valor. Para ello se muestra un esquema como el de la Figura 5.4 en el que el usuario puede mover las cajas presentadas para aclarar la dependencia. Esta visualización presenta varios problemas.

En primer lugar, cuando se están analizando activos que constan de muchas dependencias o heredan un valor desde muy arriba, en un árbol es complicado organizar el esquema para que tenga sentido. Sería más fácil si se pudiera seleccionar varios activos con el ratón y moverlos a la vez.

Además no está muy claro cuánta dependencia tiene cada línea. Se puede configurar para que sea cualquier porcentaje de 0 % a 100 % en cada una de las dimensiones. Distintos niveles de dependencia dan distintos resultados en esa dependencia, luego es clave que se haga notar. Como añadir más números al esquema que los que ya hay de por sí sería añadir otro problema (en esquemas más complejos que el mostrado) se sugiere permitir hacer clic con el ratón sobre una relación de dependencia para mostrar cómo dependen esos dos activos entre sí.

Por último, no es fácil navegar con la rueda del ratón ya que el desplazamiento es bastante lento. Sería conveniente solucionar este asunto.

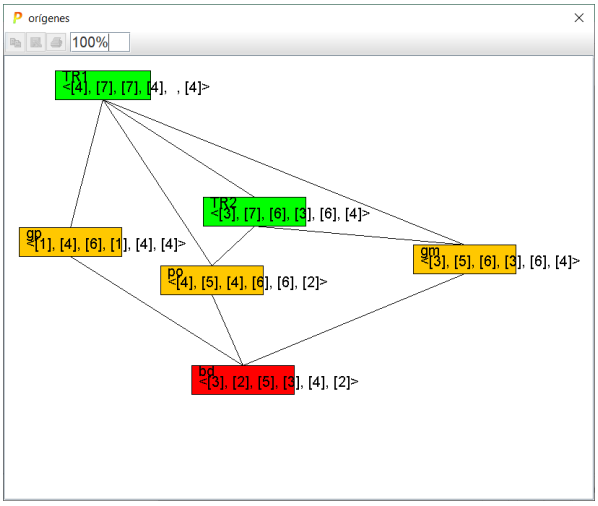

Figura 5.4: Árbol de dependencias simple de PILAR.

Pequeño ajuste de los botones

Como último punto cabe destacar algo que más que un defecto puede ser un punto a favor dependiendo de quién lo evalúe. Los botones de aceptar y cancelar son una cara sonriente y una triste respectivamente. Habrá profesionales a los que no les parecerá correcta esta caracterización.

Además se recomienda ajustar el ancho de los botones de acuerdo a la Ley de Fitts [33] y mover el botón de ayuda al lado del botón de guardar, en la parte superior de la ventana.

Permitir añadir branding de la organización que usa la herramienta

Todo organismo debe incluir su logo en documentación, página web, cartelería, puertas, etc. Como regla general cuanta más visibilidad del logo haya mejor. Así pues permitir añadir el logo al análisis y gestión de riesgos es importante para establecer corporativismo.

5.2.1.3. Defectos de documentación

Otro de los problemas que un usuario no iniciado se encuentra al empezar a utilizar la herramienta es la escasez de documentación de la misma. Existen algunas guías genéricas de cómo hacer el análisis y gestión de riesgos con PILAR pero nada excesivamente detallado. Cabe destacar que recientemente se han hecho progresos de mejora de esta documentación (la que viene instalada con PILAR) pero aún se podría mejorar algún aspecto.

Hay poca explicación de las diferencias entre las distintas variantes de PILAR

Navegar hasta la única documentación que existe sobre este tema es difícil, se puede llegar a ella a través de la página de compra de PILAR. Debería ser información más disponible; por ejemplo se podría añadir como opción del menú principal de la página web la comparación entre herramientas.

No queda claro qué hacen las zonas exactamente

Como parte de las opciones de la herramienta están las zonas. Queda claro en la documentación lo que son, pero no se entiende para qué se utilizan en el análisis de riesgos. Se debería indicar en qué elementos

influyen (añaden amenazas, ajustan el riesgo, atenúan dependencias...) para permitir un mejor uso de la herramienta.

Falta por documentar bien las clases de activos

La clasificación de activos es un proceso laborioso. Es importante asignar las clases adecuadas a los activos para que las amenazas correspondientes puedan ser añadidos a los mismos. Esto es una tarea ardua principalmente porque no hay una clara definición de lo que es cada clase. MAGERIT las explica, pero de una forma muy genérica, dejando a la imaginación completar los huecos. Sería útil tener documentado exáctamente qué quiere decir cada clase y también sería conveniente que estuvieran algo mejor estructuradas (es algo complicado navegar por ellas al principio). Esto no es un defecto de PILAR propiamente dicho pero tal vez se pueda remediar desde la herramienta.

Falta información de las amenazas

Cuando se entra en el submenú Subconjunto de amenazas y se pulsa botón derecho sobre una pulsando *más información* la página web que se abre no da información sobre la amenaza pulsada. Esto ocurre con todas las amenazas. Este defecto es un fallo documental y un *bug* al mismo tiempo.

Falta documentación de la opción Xor

Cuando se accede a la documentación que viene con PILAR 7.3.3, la información sobre la opción se encuentra a medio terminar.

5.2.2. Propuesta de mejoras añadidas a la herramienta

Se han ideado un conjunto de mejoras añadiendo funcionalidad y mejorando el proceso de análisis y gestión de riesgos. Estas propuestas, aunque están basadas en los principios de MAGERIT y PILAR, cambian procedimientos y adaptan la herramienta para darla más flexibilidad y mejor usabilidad.

5.2.2.1. Mejoras de funcionalidad

Permitir copiar dependencias

En un análisis de riesgo basado en dependencias en el que se hereda el valor de los activos según la relación de dependencia es muy importante tener estas dependencias bien modeladas. Por ello se agradecería disponer de un botón mediante el que se pudieran copiar dependencias de un activo para pegarlas en otro. Esta necesidad surge al presentarse en el análisis de riesgos dos activos con dependencias complejas y similares.

Mejorar las actuaciones de seguridad

Las actuaciones de seguridad, como se ha mencionado antes, permiten seguir lo que se ha hecho, lo que se está haciendo y lo que se va a hacer en materia de seguridad. Cuando se está trabajando con fechas límite se echan en falta notificaciones. Se agradecería la adición de notificaciones para poder llevar un seguimiento más exhaustivo de la seguridad en la organización.

Permitir la creación y borrado de activos desde el menú de dependencias

Cuando se está trabajando con las dependencias entre activos a veces surge la necesidad de modificar el inventario de activos para reflejar mejor el estado de la organización. Ya se pueden editar activos usando

el botón derecho del ratón. Faltaría poder crear y borrar activos desde ese menú para poder manejar la herramienta mejor. Incluso se podría fusionar el menú de identificación de activos y el de dependencias en uno solo aunque está bien que estén separados para esquematizar como suele funcionar cronológicamente el proceso de gestión de riesgos.

Mejorar la navegabilidad con teclado

En el siglo XXI nos importa la accesibilidad de nuestro software. La herramienta no está adaptada para gente que no pueda usar un ratón (por ejemplo por padecer la enfermedad de Párkinson). Además hay ciertas labores con el teclado que un usuario puede ver como intuitivas, que no están reflejadas en PILAR. Un ejemplo de esto se presenta durante la valoración de activos, cuando se les asignan valores que aparecen indicados al lado de cada activo. En vez de seleccionar el valor que se quiere añadir o modificar e introducirlo numéricamente se debe hacer doble clic, abrir un desplegable y darle un valor numérico de ese desplegable.

Si bien desarrollar un sistema para hacer todas las labores de la herramienta es trabajoso sí que se agradecería poder navegar algún aspecto con más facilidad. En concreto poder usar *control + z* sería una buena mejora así como permitir que se de valor a los activos y dominios mediante el teclado pudiendo navegar entre estos valores como se haría en un excel; con tabulaciones e intros.

Mover el aviso de que hay activos sin valorar

Cuando se sale de la pantalla de valoración de activos, PILAR avisa si existe algún activo que no esté valorado o no herede valor alguno. Como se indican los activos que sufren de este problema es extremadamente útil al final del proceso de valoración de activos.

Sin embargo, a menudo este proceso de valoración de activos puede llevar semanas. Así pues, ver esa pantalla cada vez que se entra a valorar activos es una inconveniencia. Si bien existe la posibilidad de ocultarla para que no vuelva a aparecer no es recomendable hacer esto pues la pantalla es útil al final de ese proceso.

La solución es introducir una nueva opción en el menú de opciones donde se pueda configurar manualmente la aparición de esa pantalla.

Permitir ocultar fases de proyecto

Disponer de distintas fases en un proyecto permite poder seguir la evolución de la seguridad a través del tiempo. Hay ocasiones en las que se requiere añadir muchas fases (por requisitos de negocio). Si, por ejemplo, todos los años se añade una fase, hay un aspecto de la herramienta que se vuelve ingestionable llegado cierto punto: los perfiles de seguridad (como se puede ver en la Figura 5.5).

control	du...	fu...	ap...	co...	current	2012	2013	2014	2015	2016	2017	2018	2019	target	PILAR
[27002:2013] Código de prácticas para los controles de seguridad de la información					L0-L5	L0-L5	L0-L5	L0-L5	L0-L5	L0-L5	L0-L5	L0-L5	L0-L5	L3-L5 (...	L2-L5
[5] Políticas de seguridad de la información					L0	L0	L0	L0	L1	L1	L3	L3	L3	L5	L2
[5.1] Directrices de gestión de la seguridad de la información					L0	L0	L0	L0	L1	L1	L3	L3	L3	L5	L2
[6] Organización de la seguridad de la información			...		L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L4-L5	L2-L4
[6.1] Organización interna					L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L4-L5	L2-L4
[6.1.1] Roles y responsabilidades en seguridad de la información					L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L0-L5 (...	L4-L5	L2-L3
[G.1.1] Comité de seguridad de la información					L0	L0	L1	L1	L1	L1	L2	L2	L2	L5	L2
[G.1.3] Se han identificado los roles y funciones requeridas					L0 (L2)	L0 (L2)	L0 (L2)	L0 (L2)	L0 (L2)	L0 (L2)	L0 (L2)	L0 (L2)	L0 (L2)	L5	L3 (L2-...
[G.1.4] Asignación de responsabilidades para la seguridad de la información					L5 (L2)	L5 (L2)	L5 (L2)	L5 (L2)	L5 (L2)	L5 (L2)	L5 (L2)	L5 (L2)	L5 (L2)	L5	L2
[G.1.2] Coordinación interna					L2	L2	L2	L2	L2	L1	L1	L1	L1	L5	L2

Figura 5.5: Ejemplo de los perfiles de seguridad cuando se introducen demasiadas fases en un proyecto de PILAR.

Aunque PILAR da la posibilidad de fusionar fases, puede darse el caso que se quiera conservar alguna para ser consultada en la posteridad, pero no se quiere mostrar durante la evaluación de los perfiles de seguridad.

Así pues, se sugiere permitir ocultar fases de proyecto desde donde son creadas.

Dejar de requerir un código por activo

Cuando se crean activos, PILAR obliga a introducir un código por activo que puede ser útil si están inventariados de una forma específica, pero puede añadir complejidad para usuarios no iniciados. Este código puede ser usado para automatizar la herramienta mediante scripts pero esa no es una funcionalidad que todo usuario esté usando por lo que obligar a introducir un código no es necesario en muchos casos.

Se propone introducir una opción de menú que permita añadir el código a los activos.

5.2.2.2. Mejoras estructurales

Por último se aborda las mejoras más importantes que se pueden añadir a PILAR: las estructurales. Estas mejoras vienen derivadas de identificar fallos en los fundamentos de la herramienta que podrían ser corregidos. Por desgracia, al tener que ver con partes esenciales de PILAR, no es fácil implementar estas mejoras, pero se considera que serían altamente beneficiosas al proceso de gestión de riesgos.

Muchas de estas mejoras se basan en el desglose de herramientas de análisis y gestión de riesgos hecho anteriormente.

Introducir el concepto de *vulnerabilidad* de una forma más directa

A lo largo de los tres libros que componen MAGERIT, el concepto de vulnerabilidad es mencionado. Pero se aborda principalmente desde el punto de vista de vulnerabilidades técnicas (CVE). No se aborda en profundidad que diversos activos tengan diversos niveles de vulnerabilidad según su contexto.

PILAR tiene en cuenta este tema desde dos enfoques:

- Salvaguardas asociadas a dominios de seguridad: cuando se divide la organización en varios dominios se pueden valorar estos dominios y establecer las salvaguardas que les afectan. En cierto modo activos de distintos dominios tienen distintos niveles de vulnerabilidad pues están protegidos de distinta manera. Cabe destacar que esto también se puede hacer con activos individualmente pero es una labor no recomendada por la gran cantidad de horas de trabajo que lleva implementar y mantener.
- Vulnerabilidades técnicas (CVE): PILAR permite asociar activos a su nombre CPE para después asociar vulnerabilidades técnicas (CVE) a esos activos a través del CPE. Esta solución es excelente si se dispone de pocos activos pero, en cuanto aumenta la complejidad de la organización, se dificulta en gran manera esta gestión tan detallada.

Como solución a este problema se sugiere implementar un sistema de gestión de vulnerabilidad más *informal*. Se sugiere añadir una opción del menú similar a la de valoración de activos visualmente, que permita dar un valor de vulnerabilidad del 1 al 10 a los activos tangibles (los que no son esenciales). Igual que con la valoración de activos, se sugerirán distintos factores para dar un valor u otro (por ejemplo: antigüedad del activo, existencia de una política de parches, experiencia de su propietario técnico en gestionar activos de esa índole, protecciones físicas/lógicas sobre el activo...)

Estas vulnerabilidades aumentarán/disminuirán la probabilidad de materialización de las amenazas teniendo efecto, eventualmente, en el riesgo residual de los activos.

Implementar perfiles de seguridad como módulos descargables

Los estándares de seguridad de la información y privacidad están continuamente cambiando. De vez en cuando sale uno nuevo y muy a menudo se actualizan los antiguos. Esto hace que haya que descargar una nueva versión de PILAR cada vez que hay algún cambio significativo. Incluso hay distintas variantes de PILAR según qué aspecto se quiera usar (y se dan casos en los que hay que instalar la herramienta dos veces para tener acceso a todas las librerías).

En primer lugar, se sugiere añadir una funcionalidad de actualización de la herramienta desde la propia herramienta. Además se sugiere implementar los diversos perfiles de seguridad como módulos descargables también desde la propia herramienta. Estas medidas darían dinamismo a la herramienta poniéndola al día con respecto a otras herramientas similares.

Valoración de perfiles de seguridad más granular

Cuando se evalúan los controles de un estándar a través de los perfiles de seguridad se pueden evaluar grupos de controles de forma genérica, lo que ahorra tiempo. Por desgracia, hay alguna salvaguarda que está relacionada con varios controles al mismo tiempo. Esto hace que al valorar controles y/o grupos de controles se solapen los resultados teniendo prioridad la última valoración que se ha hecho. Esto es grave, pues si se empieza a valorar de arriba a abajo, el resultado es distinto que si se hace a la inversa.

Se sugiere añadir una opción al menú en la que se puedan configurar los perfiles para que pregunten cada vez que hay un conflicto de este tipo. Detectar estos conflictos no es trivial por lo que se recomienda hacer un estudio de qué salvaguardas se repiten para poderlo optimizar bien.

Mejorar la visualización de madurez de los controles dentro de los perfiles de seguridad

Cuando se valora un perfil de seguridad se asigna una madurez a cada control (como se puede observar en la Figura 5.6). A las agrupaciones de controles se les denomina dominios (los cuales no hay que confundir con los dominios de PILAR; son elementos distintos).

✓ [9.2] Gestión de acceso de usuario					**L1-L5**
✓ [9.2.1] Registro y baja de usuario					**L5**
✓ [9.2.2] Provision de acceso de usuario					**L1**
✓ [9.2.3] Gestión de privilegios de acceso					**L1**
✓ [9.2.4] Gestión de la información secreta de autenticación de los usuarios					**L1**
✓ [9.2.5] Revisión de los derechos de acceso de usuario					**L1**
✓ [9.2.6] Retirada o reasignación de los derechos de acceso					**L1**

Figura 5.6: Ejemplo de madurez inexacta de los perfiles de seguridad (ISO 27002).

Un dominio presenta la madurez de sus controles de una forma aproximada. En el ejemplo se ve que hay muchos controles con una madurez inicial, poco pulida (L1) y uno que está bien implementado, definido, documentado y optimizado (L5).

De la Figura 5.6 se podría deducir de solo ver el dominio 9.2 que la madurez es aproximadamente un L3 (proceso definido) pero nada más lejos de la realidad. Por lo que esa aproximación no es útil, obligando a entrar en detalle en cada uno de los dominios del perfil de seguridad (y son muchos).

Una forma de solucionar esta carencia es introducir un gráfico de barras que indique cuántos controles se encuentran en cada nivel de madurez. Esto será muy útil especialmente cuanto más controles se agrupan en dominios (por ejemplo, evaluando todo el perfil de seguridad al completo).

En la Figura 5.6 se puede observar cómo quedaría el gráfico para este ejemplo sustituyendo el L0-L5 usado actualmente. De izquierda a derecha se representan los niveles de madurez desde el L0 hasta el L5.

Permitir acceso a la herramienta online desde dispositivos móviles

En este punto de mejora se está trabajando de forma parcial. Se está desarrollando una versión de PILAR que podrá ser instalada en un servidor web pudiendo accederse desde cualquier sitio a través de Internet.

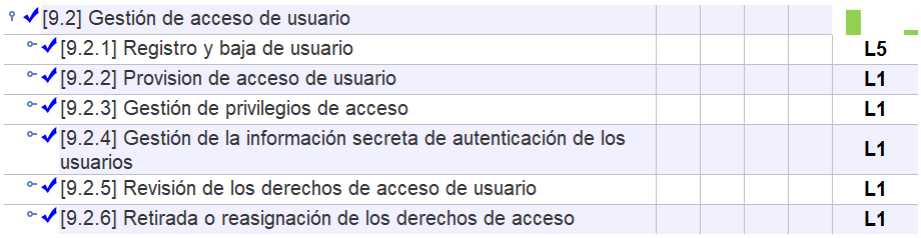

Figura 5.7: Propuesta de evaluación de madurez.

Esta propuesta de mejora va más allá de eso. Se pretende poder acceder también a la herramienta desde dispositivos móviles para facilitar el proceso de gestión de inventario de activos, valoración de activos y auditoría. Para poder trabajar desde un dispositivo móvil en estos temas es esencial rediseñar el menú principal (por ejemplo con la propuesta hecha anteriormente).

Además esto incluye un requisito adicional: sería adecuado poder acceder a la herramienta incluso con conexiones de Internet intermitentes mediante sincronización offline.

Permitir crear un panel personalizable con datos importantes de la gestión de riesgos

Cuando se trabaja gestionando riesgos a veces se pierde objetividad. Disponer de un panel con distintos indicadores del negocio ayuda a mantener los datos presentes a la vez que facilita la comunicación del estado del análisis y gestión de riesgos al personal ejecutivo no versado en el tema que tomará decisiones basándose en los resultados. Es esencial permitir la personalización de este panel para adecuarse a las necesidades de negocio de cada organización.

Si bien no se darán detalles de como debe hacerse esta mejora (pues es tan compleja que podría llevar otro trabajo de fin de grado entero desglosarla) se recomienda seguir el ejemplo de otras herramientas como *Integrum*.

Facilitar la creación de flujos de trabajo

Hoy en día se puede automatizar PILAR mediante *scripts* que interaccionan con la herramienta. El problema de este acercamiento es que es complicado de abordar por un usuario no familiarizado con programación.

Así pues se sugiere facilitar el proceso de automatización mediante una interfaz de usuario intuitiva. Esta automatización por ejemplo puede abordar temas como la actualización automática de valores de los activos (por medio de emails que derivan a encuestas) y la gestión de vulnerabilidades (permitiendo agregar datos desde una herramienta como *Nessus* [34]). Además se debería permitir enviar emails automáticos cuando se cumplen ciertas características para casos en los que haya que supervisar manualmente la herramienta (por ejemplo cuando el valor de un activo cambia muy bruscamente)

Certificar de ISO 27001 y/o ENS la entidad que desarrolla y provee PILAR

Si bien es complicado alcanzar una certificación de ISO 27001 o ENS en una organización tan pequeña es totalmente posible. La empresa encargada de PILAR, *A.L.H. J. Mañas S.L.*, puede subcontratar lo necesario para certificarse de estos estándares si así lo desea.

Disponer de al menos una certificación ayudará a dar confianza a los usuarios de PILAR en la herramienta. Es posible incluso que los fondos necesarios para hacer una adecuación al ENS pudieran ser proporcionados por el CCN debido a que está promoviendo el estándar con esa subvención.

Permitir acceder y modificar el algoritmo de análisis de riesgos de la herramienta

Trabajar con PILAR al principio puede resultar complicado porque no se entiende cómo funionan todas las partes de PILAR. Disponer de el algoritmo simplificaría el proceso de prueba y error necesario para acostumbrarse a la herramienta. Además poder modificar el algoritmo daría flexibilidad a cada análisis de riesgos permitiendo adecuar PILAR a las distintas organizaciones que la usan. Esta práctica es llevada a cabo por otra herramienta similar: *RMStudio*.

Capítulo 6

Evaluación de resultados

A continuación se evalúan los resultados obtenidos realizando una encuesta a tres usuarios de la herramienta y entrevistando al principal desarrollador e impulsor de la herramienta, José A. Mañas.

En la tabla 6.1 se pueden ver los resultados de la encuesta realizada. El usuario 1 es un usuario avanzado de la herramienta, con amplia experiencia en análisis y gestión de riesgos. El usuario 2 también es un usuario avanzado de la herramienta y ostenta un cargo de ejecutivo, luego valora las propuestas hechas desde otra perspectiva. Por último, el usuario 3 es un usuario *junior*, que ha trabajado con la herramienta pero tampoco la domina como los otros dos.

Se ha pedido a los usuarios que valoren cada propuesta asignando uno de los siguientes valores:

- Excelente: La idea es muy buena, debería ser implementada pues, o bien presenta una mejora sobre un aspecto que es considerado un problema actualmente, o bien es una idea novedosa que ayudaría en gran manera al proceso de análisis y gestión de riesgos.
- Buena: la idea es buena, debería ser considerada seriamente su implantación.
- Media: la idea no es ni especialmente buena ni especialmente mala. El término adecuado sería *regular*. Sin embargo, las connotaciones negativas de esa palabra impiden su uso en la encuesta.
- Mala: la idea no está encaminada adecuadamente.
- Muy Mala: la idea es muy mala. Su implementación iría en contra de la usabilidad de la herramienta o empeoraría el proceso de análisis y gestión de riesgos.
- N/A: no aplica. El usuario no conoce la funcionalidad a evaluar por lo que decide no opinar del tema.

Es importante recalcar que se les ha pedido expresamente que se expresen con libertad en la encuesta y que no tengan problemas en expresar valoraciones negativas ante cualquier aspecto del trabajo de fin de grado.

Aquello que más llama la atención de la encuesta es la valoración del apartado *permitir acceder y modificar el algoritmo de análisis de riesgos de PILAR*. Ahí se muestra una valoración excelente, una buena y una muy mala. Esta heterogeneidad se debe, a que un usuario respeta la decisión de los creadores de la herramienta y cree que se deben adaptar los usuarios a la herramienta pues no hay problema con el algoritmo. Esto choca con la visión de los otros dos que, encuentran la idea novedosa y les parece atractiva su implementación para poder ajustar el análisis de riesgos según las necesidades de cada organización.

Destacan como buenas ideas: *mejorar gráfica de las dependencias*, *permitir copiar dependencias*, *mejorar la navegabilidad con teclado*, *implementar los perfiles de seguridad como módulos descargables*, *eliminar interferencia entre la valoración de perfiles de seguridad* y *facilitar la creación de flujos de trabajo*.

Las propuestas de mejora que peor acogida han tenido han sido: *dejar de requerir un código por activo*, *introducir el concepto de vulnerabilidad* y *mejorar la visualización de madurez de los controles*. De estas tres mejoras cabe destacar el razonamiento usado para valorar negativamente a *introducir el concepto de vulnerabilidad*: al estar ausente en la metodología MAGERIT, se considera una decisón de diseño excluir este concepto de la metodología, por lo que introducirlo sería ir en contra de las directivas de MAGERIT.

Por último se ha consultado la opinión de José A. Mañas, el principal desarrollador e impulsor de la herramienta. Sin él no hubiera sido posible PILAR como es conocida.

La parte que más le ha gustado ha sido el rediseño de los menús, está de acuerdo con el trabajo de fin de grado en que no son muy funcionales. Además considera que se le han añadido demasiadas funcionalidades experimentales que se han acabado quedando en la herramienta porque algunos usuarios dependieran de ellas (como por ejemplo las llamadas zonas que asocian amenazas a ciertos activos que actuan de frontera como pueden ser los routers).

Aparte de eso, comenta que hay partes de la herramienta que, desde un punto de vista de código, son difíciles de arreglar. Por ejemplo, los problemas de guardado mencionados radican de cómo están estructuradas las pantallas dentro de la herramienta, en su momento se tomó la decisión de no reestructurar eso luego no va a ser cambiado.

Por último ha prometido revisar con su equipo los puntos presentados para incorporar algunas de estas propuestas en siguientes versiones de la herramienta. En concreto lo que más le interesan son las propuestas visuales presentadas.

	Usuario 1	**Usuario 2**	**Usuario 3**
Mejorar el menú de opciones	Buena	Media	Media
Mejorar el menú de navegación	Buena	Media	Buena
Eliminar de pantalla innecesaria	Media	Media	Buena
Mejorar gráfica de dependencias	Buena	Excelente	Excelente
Ajuste menor de los botones	Media	Media	Media
Permitir añadir branding de la organización que usa PILAR	Media	Excelente	Media
Documentar mejor las zonas	Buena	Buena	N/A
Documentar mejora las clases de activos	Buena	Media	Media
Permitir copiar dependencias	Excelente	Excelente	Buena
Mejorar las actuaciones de seguridad	Media	Media	N/A
Permitir la modificación de activos y dependencias desde un mismo menú	Excelente	Media	Media
Mejorar la navegabilidad con teclado	Excelente	Excelente	Excelente
Mover el aviso de activo sin valorar	Media	Media	Media
Permitir ocultar fases del proyecto	Media	Buena	Buena
Dejar de requerir un código por activo	Mala	Muy Mala	Media
Introducir el concepto de vulnerabilidad	Mala	Muy Mala	Mala
Implementar los perfiles de seguridad como módulos descargables	Buena	Excelente	Buena
Eliminar interferencia entre la valoración de perfiles de seguridad	Excelente	Excelente	Excelente
Mejorar la visualización de madurez de los controles	Muy Mala	Mala	Media
Permitir el acceso desde dispositivos móviles	Media	Media	Media
Permitir crear un panel personalizable con datos de la gestión de riesgos	Buena	Buena	Buena
Facilitar la creación de flujos de trabajo	Buena	Excelente	Buena
Certificar de ISO 27001 o del ENS la empresa que desarrolla y provee de PILAR	Buena	Media	Buena
Permitir acceder y modificar el algoritmo de análisis de riesgos de PILAR	Buena	Muy mala	Excelente

Tabla 6.1: Encuesta a usuarios de PILAR.

Capítulo 7

Conclusión y líneas futuras

Como el objetivo final de este trabajo de fin de grado es proponer una mejora de la herramienta PILAR, aquí se resumirán los puntos importantes de lo sugerido anteriormente.

En primer lugar, el problema de usabilidad de la herramienta se considera el más importante de acuerdo a las opiniones de sus usuarios recogidas. Muchas de las sugerencias van destinadas a solucionar eso. En concreto cabe destacar la necesidad de mejorar la gráfica de dependencias entre activos y permitir copiar estas dependencias. También es importante mejorar la documentación de PILAR para que sea más fácil usar la herramienta sin necesitar formación previa. Además, se recomienda adaptar o trasladar la herramienta a otro lenguaje de programación, de modo que tenga una interfaz más moderna y versátil. Por último, se debe remarcar la importancia de recoger estadísticas de uso de las distintas funcionalidades de la herramienta, para poder eliminar algunas que no sean demasiado usadas.

En cuanto al problema de falta de funcionalidad en algunos aspectos hay varios puntos que se recomiendan tratar. En primer lugar, se recomienda solucionar el problema de interferencia entre la valoración de los perfiles de seguridad. También se sugiere implementar los perfiles de seguridad como módulos descargables de un repositorio. Por último, se recomienda facilitar la creación de flujos de trabajo para automatizar aspectos de la herramienta sin necesidad de *scripts*. Este último punto no ha sido profundizado demasiado, pero se recomienda hacer encuestas para determinar las funcionalidades más comunes necesitadas por los usuarios.

De cara a investigaciones futuras se podría estructurar estas encuestas y datos recogidos por la herramienta para dirigir la investigación a lo más usado. Además, se podría coorrelar esto con un desarrollo de aplicación móvil adaptada a las necesidades de los usuarios. También se puede desarrollar más el concepto del panel personalizablecon datos de la gestión de riesgos. Lo bueno de esta iniciativa es que también podrá servir para añadir más puntos de mejora a la herramienta, al dar visibilidad a indicadores clave que de otro modo estuvieran ocultos (como por ejemplo un histórico de madurez de salvaguardas individuales).

Bibliografía

[1] Ministerio de Hacienda y Administraciones Públicas. *MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información v3*, octubre 2012. Libro I.

[2] Jose A. Mañas. PILAR y RMAT versiones. `https://www.pilar-tools.com/download/stable_es.html`, 2019.

[3] CN-CERT. EAR/PILAR. `https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html`, 2019.

[4] International Electrotechnical Commission. ISO/IEC 31000:2018, Risk management, 2018.

[5] Real Academia de la Lengua Española. *Diccionario de la lengua española*. S.L.U. ESPASA LIBROS, 23 edition, 2014. ISBN 9788467041897.

[6] Ramón Abella Rubio. Coso ii y la gestión integral de riesgos del negocio. *Estrategia Financiera*, 225, febrero 2006.

[7] International Electrotechnical Commission. ISO/IEC 31010:2009, Risk Management - Risk assessment techniques, 2009.

[8] Product Quality Research Institute. Hazard and Operability Analysis (HAZOP), 2009.

[9] Ministerio de Hacienda y Administraciones Públicas. *MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información v3*, octubre 2012. Libro II.

[10] Michael E. Whitman and Herbert J. Mattord. *Principles of Information Security*. Course Technology CENGAGE Learning, 2011.

[11] Asociación Española de Normalización y Certificación. Metodología de análisis y gestión de riesgos para los sistemas de información, 2008.

[12] Ministerio de la Presidencia. 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. `https://www.boe.es/eli/es/rd/2010/01/08/3`, 2010.

[13] Ministerio de Hacienda y Administraciones Públicas. *MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información v3*, octubre 2012. Libro III.

[14] International Organization for Standarization. *ISO 27005, Information Security Risk Management*, julio 2018.

[15] Secretary Wilbur L. Ross, Jr. Nist special publication 800-37 revision 2. Technical report, National Institute of Standards and Technology, diciembre 2018.

[16] Vincent T. Covello and Jeryl Mumpower. Risk Analysis and Risk Management: An Historical Perspective. *Society for Risk Analysis*, 5(2):103–118, 1984.

[17] AuditBoard Inc. AuditBoard. `https://www.auditboard.com/`, 2019.

[18] Reciprocity Inc. Reciprocity. https://reciprocitylabs.com/, 2019.

[19] Tracker Networks Inc. Tracker Networks. https://trackernetworks.com/, 2019.

[20] Netwrix Corporation. Netwrix Auditor. https://www.netwrix.com/auditor.html, 2019.

[21] Donesafe Pty Ltd. Donesafe. https://donesafe.com/, 2019.

[22] Stiki Information Security. RMStudio. https://www.riskmanagementstudio.com/, 2019.

[23] Nash Riggins. Top providers of compliance services. https://www.financialdirector.co.uk/2018/07/10/top-providers-of-compliance-services/, 2018.

[24] Swatee Chand. Project Risk Management: Know How To Mitigate Risks. https://dzone.com/articles/project-risk-management-know-how-to-mitigate-risks, 2019.

[25] Integrum Systems. Integrum. https://www.integrumsystems.com/, 2019.

[26] Qualys Inc. Qualys. https://www.qualys.com/, 2019.

[27] CURA Software Solutions. CURA. https://www.curasoftware.com/, 2019.

[28] José A. Mañas. Herramientas de Análisis y Gestión de Riesgos. http://shop.ar-tools.com/, 2019.

[29] Anónimo. S2 grupo comercializará la herramienta de análisis y gestión de riesgos del ccn. *CSO Edición Digital*, junio 2019.

[30] José A. Mañas. Entorno de análisis de riesgos. http://pilar-tools.com/, 2019.

[31] Ministerio de Hacienda y Administraciones Públicas. *MAGERIT versión 1.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Boletín Oficial del Estado, 1997. ISBN 9788434009608.

[32] Andrew M. W.Richard Stevens, Bill Fenner. *UNIX Network Programming: The sockets networking API, Volumen 1, pag. 606*. Pearson Education, Inc., 1 edition, 2004. ISBN 0131411551.

[33] Paul M. Fitts. The information capacity of the human motor system in controlling the amplitude of movement. *Journal of Experimental Psychology*, 121(3):262–269, junio 1954.

[34] Inc Tenable. Nessus. http://pilar-tools.com/, 2019.