Proyecto Fin de Máster
Máster Universitario en Ingeniería de Telecomunicación

Análisis de riesgo de la infraestructura que da soporte a un servicio de Teleasistencia domiciliaria

Autor: Ezequiel Montero Ramírez
Tutor: Fernando Cárdenas Fernández

Dpto. Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2013

Proyecto Fin de Máster
Máster Universitario en Ingeniería de Telecomunicación

Análisis de riesgo de la infraestructura que da soporte a un servicio de Teleasistencia domiciliaria

Autor:
Ezequiel Montero Ramírez

Tutor:
Fernando Cárdenas Fernández
Profesor a tiempo parcial

Dpto. de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2022

Proyecto Fin de Máster: Análisis de riesgo de la infraestructura que da soporte a un servicio de Teleasistencia domiciliaria

Autor: Ezequiel Montero Ramírez

Tutor: Fernando Cárdenas Fernández

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2022

El Secretario del Tribunal

Agradecimientos

El presente trabajo de fin de grado ha sido realizado bajo la tutela y supervisión de D. Fernando Cárdenas Fernández, a quien me gustaría expresar mayor y más profundo agradecimiento no solo por hacer posible la realización de este trabajo sino por toda la ayuda y oportunidades que siempre me ha ofrecido desde que nos conocimos.

A mis padres, por traerme a este mundo y guiarme día a día hasta donde hoy mis propios pasos me han llevado.

A mi padre, por animarme a estudiar ciencias, por convencerme de llegar más lejos que nadie y realizar este máster viéndome siempre capaz de lograr cualquier cosa.

A mi madre, por ver donde nadie más ve, por hacerte cargo de tantas responsabilidades para que yo pueda estar completamente centrado en la consecución de mis muchos objetivos, la finalización de este trabajo uno de ellos.

A mis abuelos Andrés, Araceli, Ezequiel y Teresa, por ser ejemplos de valores de vida y moldearme como persona.

Al resto de mi familia por siempre mostrar interés por mis avances en el que sabían, duro y complejo proceso de convertirme en ingeniero.

A todos mis profesores que han dejado huella en mí en forma de recuerdos, conocimientos y enseñanzas imprescindibles para haber llegado a donde hoy estoy.

A mis amigos de la carrera, por el enorme significado que le han dado a la palabra compañerismo durante los momentos difíciles y por la enorme amistad forjada durante los momentos buenos que mantenemos y mantendremos más allá de cualquier estudio o formación académica. A Pepelu, David, Manu, Sebas, Fabio, Rafa, Javi, Miguel Ángel, Joseca y Ramsés.

A todas las personas que me ha dado el mundo del baloncesto, en especial a mis compañeros de equipo, los cuales han convertido mis pocos ratos libres en tiempo de disfrute pleno forjando así las mejores amistades que hoy en día tengo.

Por último, a todas esas amistades y personas especiales, que no entran en ninguna categoría por su forma de ser única, esas que nunca sobran y su valor es incalculable.

Ezequiel Montero Ramírez

Estudiante de Máster Universitario en Ingeniería de Telecomunicación

Sevilla, 2022

Resumen

Cuando comencé a plantearme sobre qué y cómo llevar a cabo mi Trabajo Fin de Máster había una serie de aspectos de los cuales jamás dudé: quería que estuviese centrado en la ciberseguridad, rama en la que me encontraba especializándome, y quería que tuviese un alcance más allá de lo académico, a la altura del mundo laboral real. Bajo este contexto, siendo alumno de D. Fernando Cárdenas Fernández en la asignatura de Gestión de la Ciberseguridad, surgió la oportunidad de realizar unas prácticas en la empresa UNEI y trabajar en un proyecto centrado en torno al Análisis de riesgo de la infraestructura que da soporte a un servicio de Teleasistencia domiciliaria. Acepté sin dudarlo dos veces y cargado de ilusión ya que la oportunidad casaba a la perfección con los objetivos que previamente me había marcado para mi mismo. Una vez llevado a cabo este trabajo, puedo concluir que será de gran utilidad de cara a la adopción por parte de la empresa del Esquema Nacional de Seguridad, certificación cada vez más demandada en el entorno laboral español.

Abstract

When I started to think about what and how to carry out my MSc's Thesis there were a number of aspects that I never doubted: I wanted it to be focused on cybersecurity, a field in which I was specializing, and I wanted it to have a scope beyond the academic, at the height of the real working world. In this context, being a student of Mr. Fernando Cárdenas Fernández in the subject of Cybersecurity Management, the opportunity arose to do an internship in the company UNEI and work on a project focused on the risk analysis of the infrastructure that supports a home telecare service. I accepted without hesitation and full of enthusiasm because the opportunity matched perfectly with the objectives that I had previously set for myself. Once this work has been carried out, I can conclude that it will be very useful for the adoption by the company of the National Security Scheme, a certification increasingly demanded in the Spanish work environment.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN Y OBJETIVO

No hay segunda oportunidad para una primera impresión.

Oscar Wilde

Unei es una empresa sin ánimo de lucro cuyo objeto social desde su fundación hace más de 30 años siempre ha sido la inserción laboral de personas con enfermedades mentales o discapacidad, siendo prueba de ello que de sus más de 1.000 trabajadores, el 80% de la plantilla son personas con discapacidad y más de 500 presentan alguna enfermedad mental no impidiendo esto que el 80% de los contratos de esta tengan carácter indefinido.

Estos valores unidos a la búsqueda continua de la excelencia son los causantes de que la empresa se encuentre en continuo crecimiento, y dentro de este crecimiento destaca especialmente la línea de instalación y mantenimiento del servicio de Teleasistencia Avanzada que ha sufrido un incremento de plantilla del 30.8% en el último año.

Con este incremento UNEI se ha situado como la primera empresa en España de operaciones de instalación y mantenimiento de equipos e infraestructura de teleasistencia, tieniendo cómo clientes a la Junta de Andalucía o a Cruz Roja, entre otras entidades [1].

En la época de la digitalización y dada esta relación con instituciones públicas y/o amparadas por el Estado, UNEI como empresa que presta un servicio a entidades públicas, se ve obligada a cumplir con los requisitos del Esquema Nacional de Seguridad, de ahora en adelante, ENS [2].

El objetivo del ENS es establecer la política de seguridad en la utilización de medios electrónicos a través de unos principios básicos y requisitos mínimos que permitan una adecuada protección de la información. Por tanto, su finalidad es mediante medidas que garantizen la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos generar las condiciones necesarias de confianza para permitir a ciudadanos y administraciones públicas el ejercicio de derechos y cumplimiento de deberes en el uso de medios electrónicos. Esto tiene como consecuencia implícita la aparición de elementos y metodologías comunes que guíen la actuación de las administraciones públicas en materia de seguridad de las tecnologías de la información a la par que un lenguaje común para facilitar la interacción entre estas y las entidades privadas [2].

La adopción del ENS consta de dos pasos inciales fundamentales: establecer una Política de seguridad e identificar la información y servicios de la entidad. El primero requiere de establecer roles, funciones y procedimientos de designación y el segundo consiste en valorar la información y los servicios, identificar a los responsables de estos, realizar un análisis de riesgo y desarrollar un plan a partir de este anterior para alcanzar el pleno cumplimiento del ENS [2].

Esto se alinea a la perfección con la premisa en que coinciden todos los modelos y referentes de seguridad tanto nacionales como internacionales de que la confianza en seguridad se construye en torno al Análisis y a la gestión de Riesgos [2].

Todo lo comentado hasta este momento es lo que motiva y justifica el objetivo de la realización de este proyecto: adecuar el tan exitoso servicio de teleasistencia de UNEI al ENS. Esto sin duda requiere de realizar sobre su infraestructura un análisis de riesgo bajo las pautas de una metodología ya consolidada y posiblemente, mediante una herramienta que aporte comodidad a la tarea.

Esto conlleva la necesidad de un estudio del estado del arte alrededor de las metodologías existentes y sus posibles ligaduras intrínsecas a una o un conjunto de tecnologías que faciliten el realizar el análisis de riesgo aplicando estas. Dicho estudio se comenta a continuación en el siguiente apartado.

2 ESTADO DEL ARTE Y TECNOLOGÍAS

La tecnología por si sola no basta. También tenemos que poner el corazón.

Jane Goodall

En este capítulo se procede a analizar tanto el estado del arte en cuanto a metodologías de análisis y gestión de riesgo como las tecnologías que dan soporte a la realización de dichos análisis, teniendo en cuenta que en ocasiones existe una ligadura implícita entre unas y otras.

Una vez analizadas las opciones se procederá a justificar las elecciones de metodología y herramientas a utilizar para este proyecto

2.1. Estado del arte

A la hora de elegir una metodología de análisis de riesgo es de común acuerdo que el hecho más importante es que esta metodología conste de un reconocimiento previo extendido y permita tener un mecanismo de gestión reproducible.

Como esto último es algo que cumplen todas las metodologías, quizás en la práctica el factor más determinante a la hora de elegir una metodología frente a otras sea la mejor adaptación de una de estas a la realidad de la organización [3].

Una vez dicho esto, se procede a analizar las diferentes metodologías que fueron consideradas como opción para llevar a cabo este proyecto:

2.1.1 NIST SP 800-30: Guide for Conducting Risk Assessments

2.1.1.1 Introducción

Esta metodología para gestión de riesgos en proyectos de tecnologías de la información, de ahora en adelante TI, nació en el seno de la agencia que le da nombre, el National Institute of Standard Technology y sus objetivos de partida fueron [4]:

- El aseguramiento de los sistemas de Información
- El análisis de riesgos
- Optimizar la gestión de estos a partir del resultado del análisis

- Proteger el conjunto de habilidades de una organización para alcanzar su misión, no limitándose al área de TI

Su principal característica es que se organiza en torno a un proceso de tres pasos: estructura y evaluación del riesgo, responder al riesgo (mitigación) y seguimiento del riesgo (reevaluación) y hoy en día cuenta con un alto reconocimiento en la comunidad por alcanzar niveles satisfactorios en hardware, software, bases de datos, redes y telecomunicaciones [3].

2.1.1.2 Ventajas y desventajas

La principal ventaja de esta metodología es que la guía para evaluación de riesgos que proporciona revierte en un bajo costo en el análisis de riesgo que hace más atractivo el enfoque de la mejora de la administración de riesgos a través de los resultados obtenidos.

Por contra, su mayor desventaja es que no contempla elementos tan asentados en la industria a día de hoy como procesos, activos o dependencias [3].

2.1.2 CRAMM: CCTA Risk Analysis and Management Method

2.1.2.1 Introducción

CRAMM es la metodología de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico y debido a esto tiene un gran calado tanto en la administración pública británica como en empresas e instituciones de gran tamaño.

Esta metodología consta de tres etapas para su puesta en práctica [5]:

- Primera etapa: definición de objetivos y alcance, evaluación de los activos (físicos, software, datos…) y del impacto sobre el negocio
- Segunda etapa: Identificación de las amenazas y vulnerabilidades como preámbulo para la realización del análisis de riesgo
- Tercera etapa: Identificación y selección de las medidas de seguridad a aplicar junto a los riesgos residuales tras la aplicación de estas.

El citado análisis de riesgo se caracteriza a su vez por emplear una metodología mixta, es decir, abarca valores tanto cuantitativos como cualitativos.

2.1.2.2 Ventajas y desventajas

Como consecuencia de emplear la metodología mixta CRAMM es aplicable a todo tipo de sistemas de información siendo esta su principal ventaja junto a la posibilidad de poder aplicar la metodología a lo largo de todo el ciclo de vida del Sistema de información.

Por el contrario, su mayor desventaja, de manera muy similar a la de NIST SP 800-30, es que no contempla elementos como los procesos y los recursos [3].

2.1.3 ISO/IEC 27005:2008 Information Security Risk Management

2.1.3.1 Introducción

Esta norma proporciona una serie de directrices para la gestión de riesgos de seguridad de la información basándose en los conceptos especificados en la norma ISO/IEC 27001 que pretenden ayudar a la hora de poner en práctica de manera satisfactoria la gestión y el análisis de riesgo. Esta metodología es aplicable a todo tipo de organizaciones siendo el único requisito para estas el tener la intención de manejar los riesgos que podría comprometer la seguridad de la información de la organización [6].

2.1.3.2 Ventajas y desventajas

Una de las principals características que facilitan que se mantenga su alto reconocimiento es el caracter

internacional de la norma y su compatibilidad con otras normas ISO/IEC como la 27002 y la ya citada 27001. A esto tambien ayuda lo reciente de la publicación de última version.

A demás en el plano functional permite realizar un análisis cuantitativo complete tanto en el análisis como en la gestion de riesgos para la cual establece una causula complete orientada a la monitorización y revision de estos.

Por otro lado sus mayores impedimentos son el no ser una norma certificable y la inexistencia de técnicas, comparativas ni herramientas para la implementación de la metodología.

2.1.4 Octave v2.0: Operationally Critical Threat, Asset and Vulnerability Evaluation

2.1.4.1 Introducción

La metodología Octave fue desarrollada en la Universidad Carnegie Mellon de Pensilvania y esta orientada hacia la coordinación y cooperación de personas y/o entidades de sectores operativos distintos permitiendo que estos trabajen de manera conjunta.

Dicho propósito hace que inevitablemente su foco este puesto en las necesidades de las partes que colaboran y el propósito es que se alcancen manteniendo un equilibrio entre tecnología, riesgos operativos y prácticas de seguridad [7].

2.1.4.2 Ventajas y desventajas

La principal ventaja de esta metodología es que permite al desarrollador conocer los requisitos de usuarios y/o clients, lo que hace sencillo la modificación de los sistemas de información además de menos costoso debido a que los cambios en el desarrollo de proyectos son mas baratos de realizar en las etapas iniciales de este.

Por otra parte, su inconveniente es que no es válido para grandes empresas, sólo para pequeñas y medianas; y además su implementación require de un gran conocimiento técnico [3].

2.1.5 MAGERIT v3.0: Metodología de análisis y gestion de Riesgos

2.1.5.1 Introducción

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España cuya función consiste en investigar los riesgos soportados por los Sistemas de Información y recomendar medidas de recomendada adopción para el control de dichos riesgos.

Además, más allá de su función, tiene los siguientes objetivos [8]:

- Concienciar a los responsables de las organizaciones de la existencia de riesgos en las organizaciones de información y la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados de las tecnologías de la información y Comunicaciones, de ahora en Adelante TIC.
- Ayudar a planificar y descubrir el tratamiento oportuno de los riesgos
- Preparar la organización para procesos de evaluación, auditoria y certificación o acreditación segun corresponda.

2.1.5.2 Ventajas y desventajas

La principal ventaja es que ofrece un método sistematizado para determiner los riesgos en los sistemas de información a la par que ayuda a identificar y pkanificar las medidas necesarias para reducer las vulnerabilidades.

Su desventaja es que la metodología es de dificil implementación por el hecho de que los activos se convierten en puros valores económicos [3].

2.1.6 Comparativa de tecnologías

Como se puede observer a simple vista al ser metodologías que comparting, a grosso modo, un mismo objetivo, tienen una serie de características ccomunes que se repiten y es en pequeños detalles del ámbito de aplicación de cada una en lo que se diferencian.

Bajo el objetivo de tener una visión final de conjunto, se establecen los siguientes criterios conforme a los que se realizará una comparación el la posterior table [3]:

1. Mide el nivel de seguridad del Sistema de infromación
2. Identifica amenazas y vulnerabilidades en los sistemas de información
3. Evalua los riesgos y optimiza los costes de las tecnologías de información
4. Posee un plan de contingencia en caso de vulnerabilidades

Tabla 2.1 - Comparativa de Metodologías

	CRAMM	NIST SP 800-30	OCTAVE	MAGERIT
Crieterio 1	Cumple	No Cumple	No cumple	No cumple
Crieterio 2	Cumple	Cumple	Cumple	Cumple
Crieterio 3	Cumple	No cumple	Cumple	Cumple
Crieterio 4	Cumple	Cumple	Cumple	Cumple

Por motivos obvios explicados en su correspondiente sección de “Ventajas y Desventajas” la metodología definida en la norma ISO/IEC 27005:2008 no ha sido incluida en la comparación.

2.2 Tecnologías

Una vez analizadas las principales metodologías para el análisis de riesgo, es momento de realizar una parte del estudio sobre la otra parte de la ecuación, las tecnologías y/o herramientas que dan soporte a una realización más cómoda de estos análisis.

Resulta evidente que una herramienta o tecnología diseñada específicamente para la la puesta en práctica de una de las citadas metodologías facilitará mucho más el esfuerzo a invertir en el análisis de riesgo que la utilización de una herramienta genérica de análisis de riesgo donde el esfuerzo de cumplir la metodología escogida recae sobre el usuario de la aplicación.

Esto será completamente determinante en el enfoque utilizado para el análisis del estado de las tecnologías disponibles ya que nos centraremos en herramientas específicamente diseñadas para seguir alguna de las metodologías estudiadas en el apartado anterior.

2.2.1 Herramientas para NIST SP 800-30

Archer NIST-Aligned Privacy Framework App es una aplicación que permite de manera sencilla y visual para evaluar el nivel de implementación actual de las protecciones de seguridad de la metodología NIST SP 800-30 en comparación con el nivel de implementación objetivo. En esta comparación la herramienta muestra las

deficiencias y permite, en función de estas, priorizar e implementar planes de acción para mejorar la protección de las organizaciones [9].

Esta herramienta se basa a la vez en NIST Privacy Framework, un marco de trabajo desarrollado de forma abierta y colaborativa junto a las partes interesadas (stakeholders) de la industria en el que se recogen beunas prácticas y los aspectos más interesantes obtenidos de la experiencia en la aplicación de la metodología NIST SP 800-30 [10].

Mientras que para el uso de esta aplicación se debe pagar una licencia, existe una alternativa de uso libre desarrollada por el propio NIST llamada SCAP Composer, la cual permite crear protocolos automáticos de seguridad de manera sencilla e integrable [11].

2.2.2 Herramientas para CRAMM

En este caso la misma Agencia Central de Comunicación y Telecomunicación del gobierno británico que creó la metodología desarrolla su propio producto software para el análisis y gestion de riesgos, incluyendo más de 3000 contramedidas de salvaguarda [12].

El lanzamiento más reciente de esta aplicación consta de un periodo de prueba de 30 días y posteriormente hay que adquirir una de las dos versions: Express o Expert. La version express tiene un precio de 1500 libras por la adquisición y una licencia annual de 250 libras esterlinas. Por otro lado la version Expert tiene un precio de adquisición de 2950 libras esterlinas y un coste de licencia annual de 875 [13].

2.2.3 Herramientas para ISO/IEC 27005:2008

Como ya se ha comentado en repetidas ocaciones no existe herramienta ni product software para la implementación de esta metodología.

2.2.4 Herramientas para Octave v2.0

Como comentabamos en el apartado de análisis del estado del arte, esta norma es de dificil aplicación por requerir de un gran conocimiento técnico y en parte esto se debe a la inexistencia de aplicaciones que faciliten la puesta en práctica de la metodología a la hora de realizar un análisis de riesgo.

2.2.5 Herramientas para MAGERIT v3.0

PILAR es una herramienta desarrollada y financiada parcialmente por el Centro Criptográfico Nacional, de ahora en adelante CCN, que permite realizar el análisis y la gestión de riesgos siguiendo la metodología MAGERIT.

Esta aplicación consta de distintas variantes que van actualizándose periodicamente estando dirigidas a todas aquellas organizaciones y/o organismos que cuentan con infraestructura de TIC y que necestan gestionar sus activos mediante la realización de análisis de impacto y continuidad de operaciones tanto de carácter cuantitativo como de carácter cualitativo.

La licencia para cualquiera de las versions de PILAR es gratuita para todos los organismos de la administración pública, sin embargo, para las entidades privadas es de pago adaptándose el precio al tamaño de la entidad, la versión del programa que se requiera y el número de usuarios [14].

2.3 Elección y justificación

Como ya se ha comentado anteriormente, la realización de este proyecto de análisis de riesgo se enmarca en el plan de aplicación y adaptación de UNEI al ENS debido a la estrecha colaboración que mantiene a través del servicio de teleasistencia con las entidades públicas.

Esto es el factor determinante que justifica elegir como metodología MAGERIT por ser la empleada por las

administraciones públicas. Esto implicitamente conlleva la elección de alguna de las versiones de PILAR como herramienta para la realización del análisis de riesgo, lo cual es ventajoso también debido al hecho de que uno de los proveedores de UNEI posee un gran *expertise* con esta herramienta.

2.4 Uso de la herramienta

A continuación, se procede a explicar el funcionamiento de la herramienta PILAR y las diferentes opciones que contiene como forma de ilustrar porqué la información anteriormente recabada es necesaria y como los diferentes detalles al respecto de esta son requeridos por la aplicación para la realización del análisis de riesgo. La descripción del uso del programa se va a realizar conforme a la guía de uso publicada por el CCN [15] y la propia documentación de PILAR [16].

2.4.1 Configuración del proyecto

Si iniciamos la aplicación veremos dos pantallas, una de log que nos va a acompañar a lo largo de la ejecución de todo el programa y otra que nos proporcionará un botón para comenzar el análisis de riesgo; tal y como se muestra en la siguiente imagen (los datos de licencia han sido pixelados por cuestiones de privacidad).

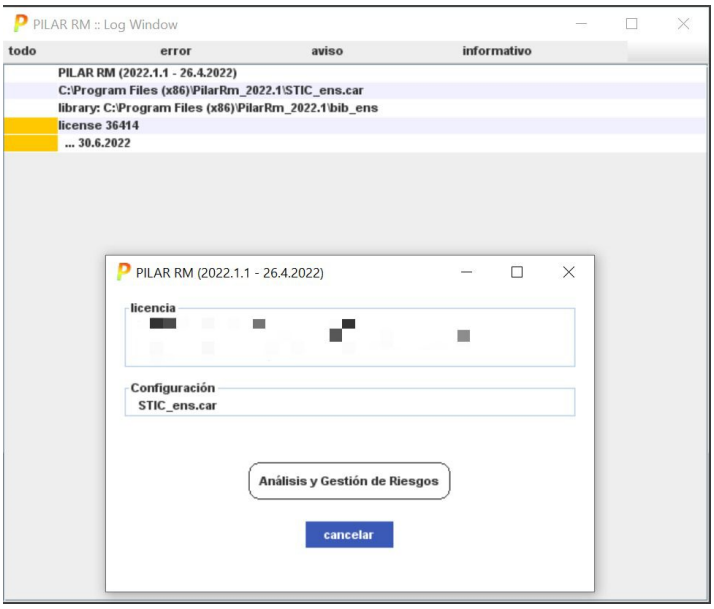

Figura 2.1 - Pantallas de inicio de la aplicación PILAR

Una vez pulsemos el botón de Análisis y Gestión de Riesgos se nos abrirá el programa donde lo primero que debemos hacer es crear un nuevo proyecto haciendo clic en Proyecto > Nuevo y rellenar la información que nos solicita (la interfaz del programa tiene la particularidad de hacer equivalente la cara sonriente al tick verde y la cara triste a la cruz roja):

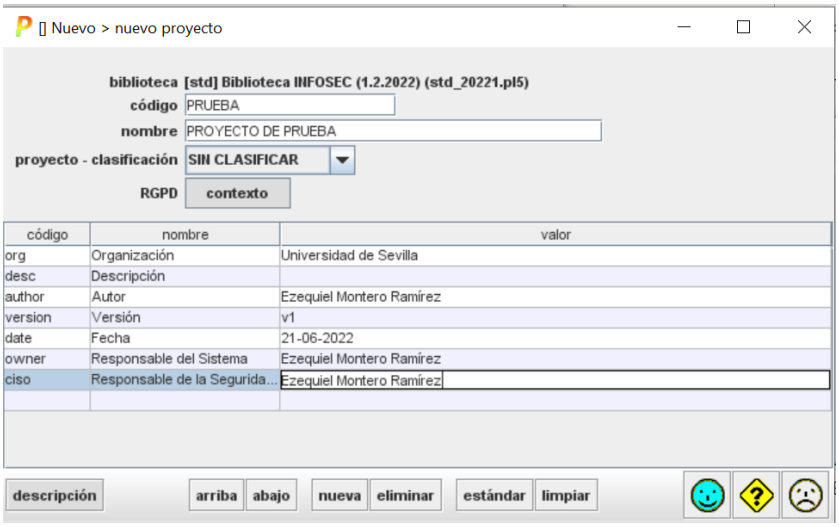

Figura 2.2 - Creación del Proyecto

Tras esto nos pedirá que escojamos las pautas a seguir en el tratamiento de riesgos. Como se puede observar además de las medidas del Esquema Nacional de Seguridad, que son las que nos interesan, se pueden escoger entre otras salvaguardas propias de pilar, del Reglamento General de Protección de Datos (de ahora en adelante RGPD) o de organizaciones como el NIST, de la cual una de sus metodologías fue tenida en cuenta en el análisis del capitulo anterior.

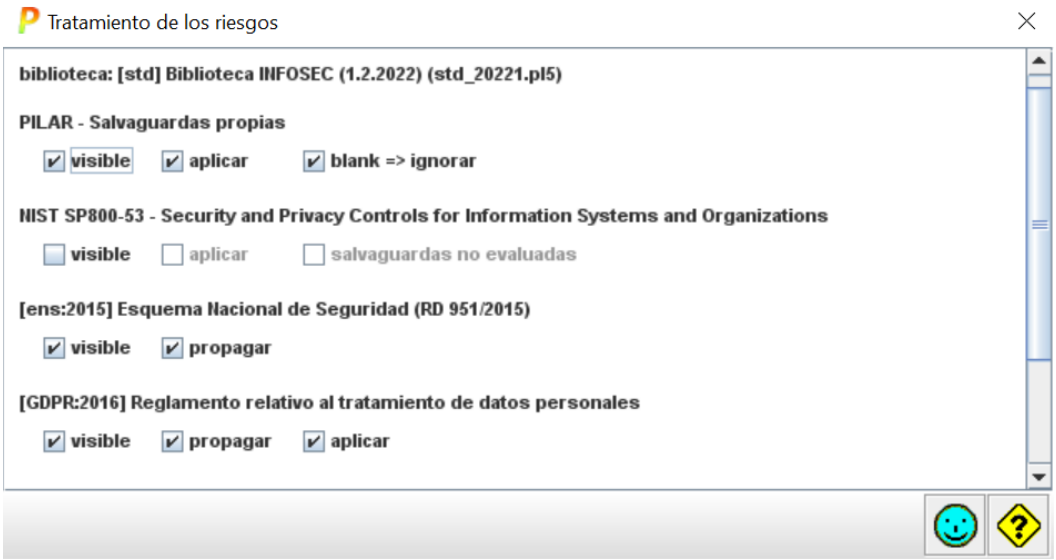

Figura 2.3 - Selección de Tratamientos de Riesgos

Tras esto se nos mostrará la pantalla principal del proyecto y hemos de saber que la herramienta PILAR permite realizar un análisis de riesgos en tres niveles distintos: básico (color de interfaz verde), medio (color de interfaz amarillo) y experto (color de interfaz amarillo).

Esto condicionará los aspectos del proyecto que podremos definir y los que se nos mostrarán, por lo tanto, para poder alcanzar una capacidad de detalle máxima, este proyecto ha sido realizado en el nivel experto de la aplicación.

Para cambiar de un nivel a otro tan solo tendremos que seleccionar el que deseemos tras hacer clic en la barra superior de la imagen que se muestra a continuación.

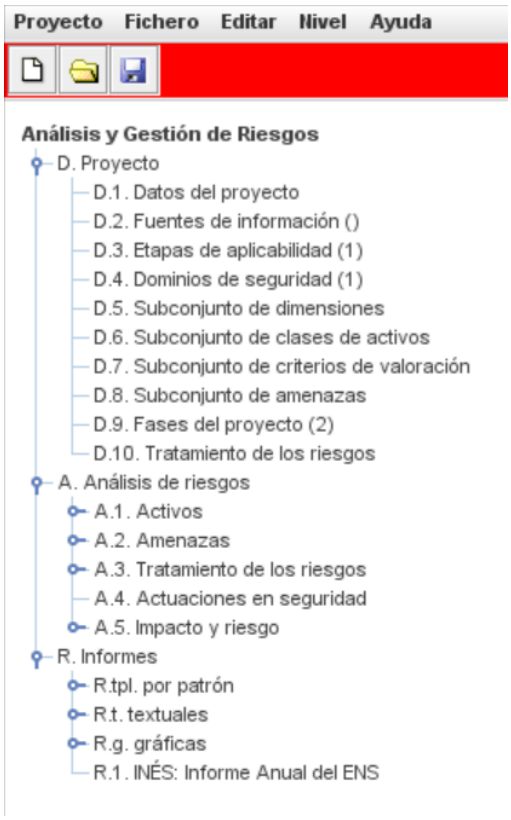

Figura 2.4 - Organización del Proyecto

Como se puede observar PILAR estructura el proyecto en tres partes:

- D. Proyecto: Contiene la información y los parámetros de configuración de tratamiento de riesgo que hemos configurado en la creación del proyecto.
- A. Análisis de Riesgo: Es la sección donde introduciendo la información anteriormente recogida la aplicación realizará el análisis de riesgo.
- R. Informes: Sección donde se encuentra la información resultante del procesamiento automático de la información realizado por la aplicación.

Dado que el nivel experto contiene un profundo nivel de detalle, se procede a describir las secciones más interesantes en los siguientes subapartados dedicados a cada una de las partes en las que la propia aplicación divide el proyecto.

2.4.2 Sección (D) Proyecto

Con la información que introducimos el programa automáticamente rellena las subsecciones D.1 Datos del proyecto y D.10 Tratamiento de los riesgos, pero si queremos profundizar en detalle debemos emplear las siguientes subsecciones [17]:

- D.2 Fuentes de Información: sección donde identificar a las personas implicadas en el proyecto que proporcionarán información al análisis de riesgo. En nuestro caso consideraremos al equipo de Tecnología como fuente única de la información.
- D.4 Dominios de seguridad: Permite que se apliquen distintas salvaguardas de forma conjunta sobre aplicaciones diferentes según el grado de madurez de esta y el grado de cumplimiento que se le exija. Esto es especialmente interesante a la hora de analizar más de un servicio core de una misma empresa, pero en nuestro caso como nos centramos solo en el servicio de teleasistencia utilizaremos un solo dominio, el dominio base que crea por defecto el programa.

- D.5 Subconjunto de dimensiones: Permite seleccionar las dimensiones que se van a tener en cuenta para el análisis de riesgos. Las opciones disponibles son las siguientes:

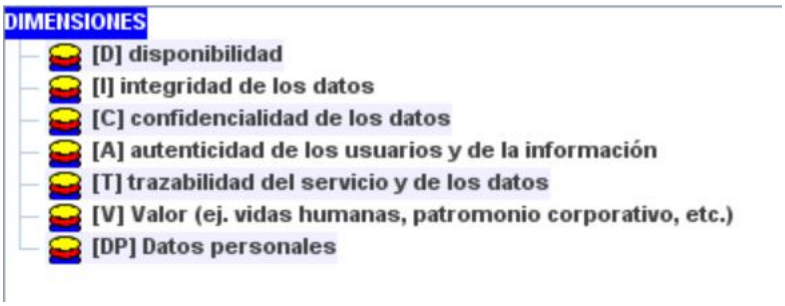

Figura 2.5 – Dimensiones disponibles para el Análisis de Riesgos

- D.6 Subconjunto de clases de activos: PILAR por defecto define una serie de tipos de activos, según una clasificación que ofrece, y a ellos asocia una serie de amenazas para cada una de las dimensiones y salvaguardas. Dentro de esta clasificación que se muestra a continuación existe una gran cantidad de etiquetas que aplicadas en conjunto sobre un activo permiten definirlo con gran nivel de detalle. Se muestra a continuación la rama principal del árbol de etiquetas:

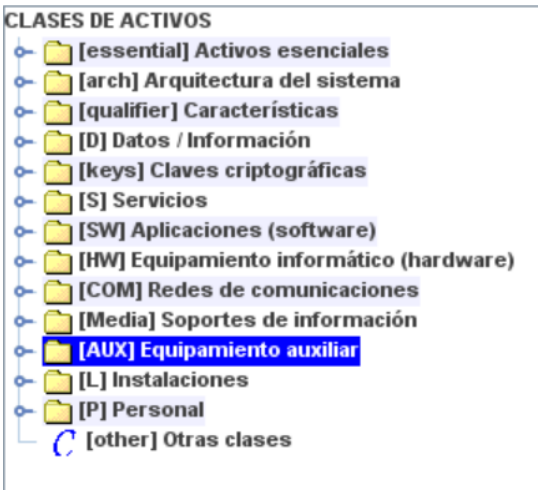

Figura 2.6 - Subconjuntos de Clases de Activos

- D.7 Subconjunto de criterios de valoración: Dado que estamos empleando la versión destina a aplicar el ENS define los criterios de valoración de los activos como Bajo, Medio y Alto para las siguientes dimensiones:

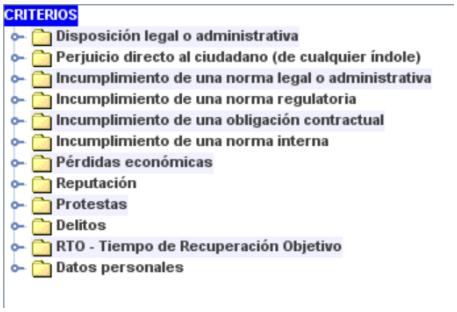

Figura 2.7 - Criterios de Valoración de Activos

- D.8 Subconjunto de amenazas: en esta sección se eligen con cuales de las amenazas definidas en

MAGERIT se desean trabajar. Por defecto se encuentran todas con su código de identificación definido en MAGERIT y activada por defecto para que se tenga en cuenta en el análisis de riesgo. Se muestran algunas de ellas a continuación como forma de ilustrar al lector lo comentado.

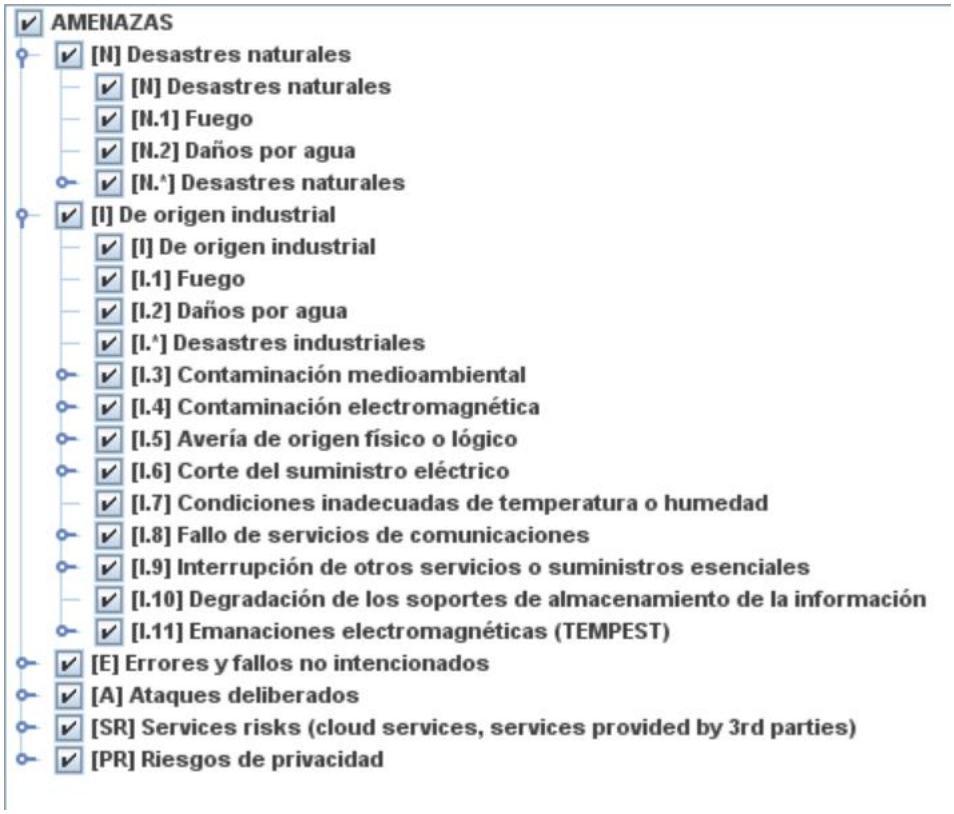

Figura 2.8 - Subconjunto de Amenazas

- D.9 Fases del proyecto: Se suelen definir la fase actual y la fase target.

2.4.3 Sección (A) Análisis de Riesgos

Esta sección es la más importante ya que en ella es donde se realiza el análisis de riesgo como tal y donde se obtienen los resultados. Por ello se encuentra a su vez divida en 5 subsecciones que se explican en detalle en los siguientes subapartados:

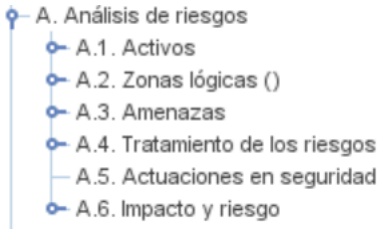

Figura 2.9 - Subsecciones del Análisis de Riesgos

2.4.3.1 A.1 Activos

Esta sección es la de mayor importancia en el análisis de riesgo ya que será el fundamento para llevarlo a cabo

utilizando la información recabada anteriormente, la cual ha sido descrita en el subapartado de tareas previas.

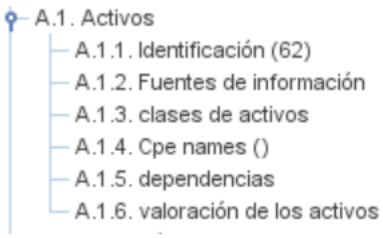

Figura 2.10 - Sección de Activos

Se procede a continuación a detallar los diferentes subapartados y como realizar a través de ellos el análisis de riesgo:

- A.1.1. Identificación: Como primer paso para definir los activos, se les asignará una categoría dentro de la siguiente clasificación:

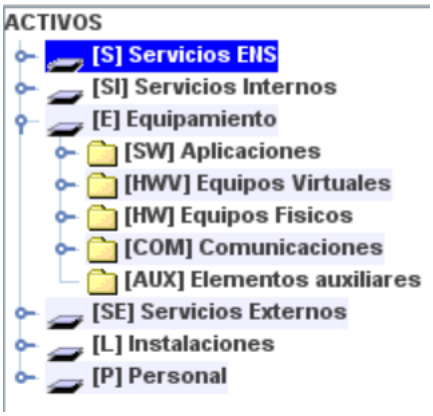

Figura 2.11 - Clasificación de Activos

Para completar dicha definición habrá que asignar al activo un código, un nombre (que profundice en la descripción del código) y aplicar sobre este las etiquetas que correspondan. Se muestra un ejemplo real de nuestro análisis de riesgo final:

Figura 2.12 - Identificación de un Activo

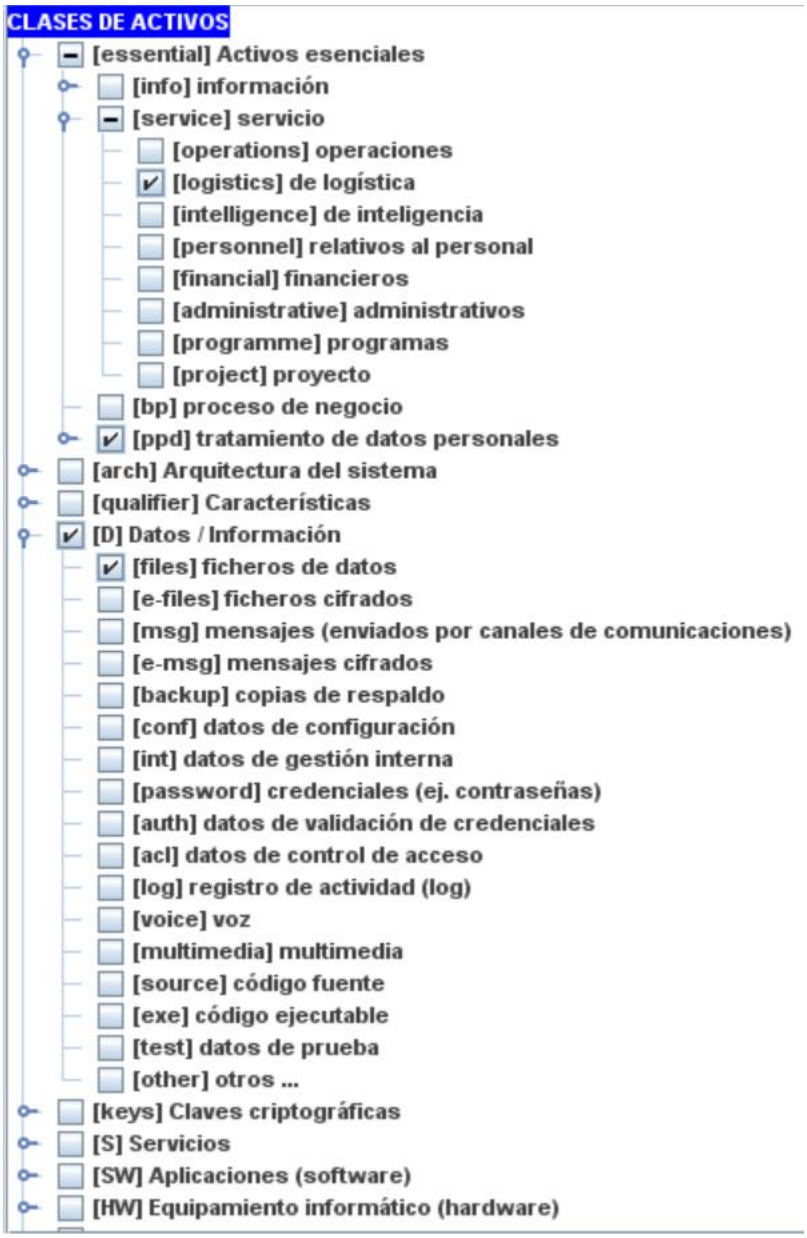

Figura 2.13 - Clasificación del Activo de ejemplo

Si se observa detenidamente, con los menús mostrados en las dos últimas capturas de pantalla anteriores se puede cumplimentar los subapartados A.1.2 y A.1.3 de Fuentes de información y Clases de Activos, respectivamente.

- A.1.4 CPE (Common Platform Enumeration) names: Permite mediante un fichero importar un sistema de nombrado.
- A.1.5 Dependencias: Los activos rara vez se encuentran aislados, sino que de forma más que habitual se relacionan entre sí haciendo que el valor y el riesgo existente en estos varíe a consecuencia tanto en términos acumulados como repercutidos.

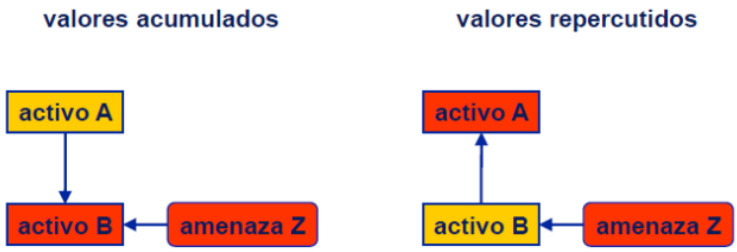

Figura 2.14 - Valores Acumulados y Repercutidos

La forma de reflejar esto que tiene PILAR es mediante el establecimiento de dependencias entre los siguientes activos. La forma recomendada por el CCN en su guía de uso de PILAR es en primera instancia establecer los servicios que dependen de otros servicios y en segundo lugar definir las dependencias de estos servicios con otros activos que no sean servicios, tal y como se muestra en la siguiente imagen [15].

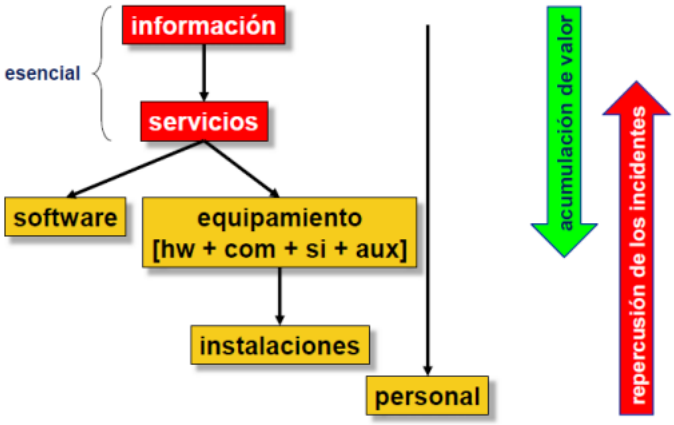

Figura 2.15 - Establecimiento de Dependencias

- A.1.6 Valoración de Activos: En esta sección de la interfaz se valorarán los activos en los niveles Bajo, Medio y Alto en las diferentes dimensiones que se han decidido tener en cuenta.

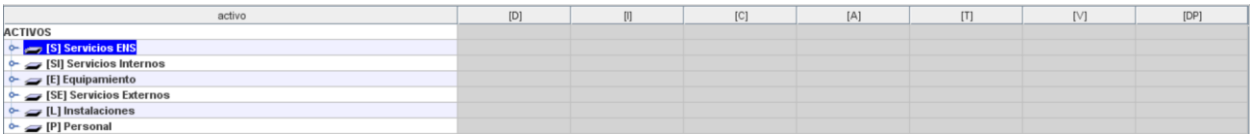

Figura 2.16 - Matriz de Valoración de Activos

2.4.3.2 A.2 Zonas lógicas

Las zonas son un conjunto de activos protegidos por un mismo perímetro y se utilizan en PILAR para detallar las arquitecturas de defensa en profundidad. Estas se emplean para determinar la posición del ataque de manera que este se origina en una zona y puede progresar a otras zonas a través de los elementos de frontera.

Como consecuencias, un activo que pertenezca a una o más zonas, será objeto directo de los ataques desde la zona a la que pertenece y objeto indirecto de ataques originados en otra zona, a través de los activos de frontera.

En concreto, las zonas lógicas son aquellas que se emplean para separar la red interna del exterior mediante dispositivos y servicios de frontera tales como cortafuegos y zonas desmilitarizadas, de ahora en adelante DMZ.

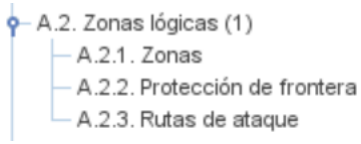

Figura 2.17 - Configuración de Zonas Lógicas

Para su uso en pilar debemos definir en A.2.1 las zonas que deseamos considerar, en A2.2 las protecciones que separan las diferentes zonas y en A.2.3 las posibles rutas de ataque.

2.4.3.3 A.3 Amenazas

En esta sección trabajaremos con las amenazas que se tendrán en cuenta en el análisis de riesgos. PILAR aplica por defecto un perfil típico de ataque a los activos según como los hayamos caracterizado incluyendo valores de posibilidad de ocurrencia y de posibles consecuencias a través de un fichero Excel o xml denominado, de ahora en adelante TSV, Threat Standard Values [17].

Si se desea variar estos valores se puede modificar directamente el fichero buscando en la carpeta de configuración de la aplicación PILAR o mediante la propia interfaz seleccionando Editar > Opciones > Amenazas y cambiando la opción (por defecto) de automático a manual o mix, tal y como se puede ver a continuación.

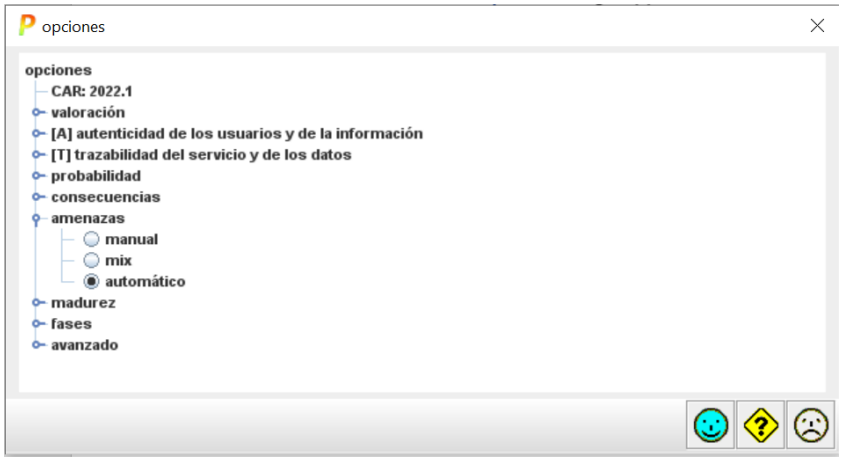

Figura 2.18 - Modificación de la Configuración de Amenazas

Si nos centramos en las diferentes subsecciones encontraremos lo siguiente:

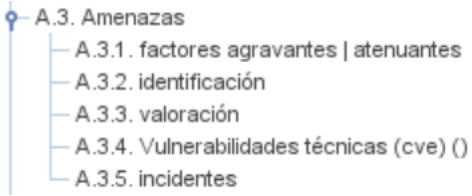

Figura 2.19 - Subsección de Amenazas

- A.3.1 Factores agravantes | atenuantes: Sección donde podremos hacer variar la probabilidad de ocurrencia y el perjuicio de las amenazas en cada uno de los dominios de seguridad.

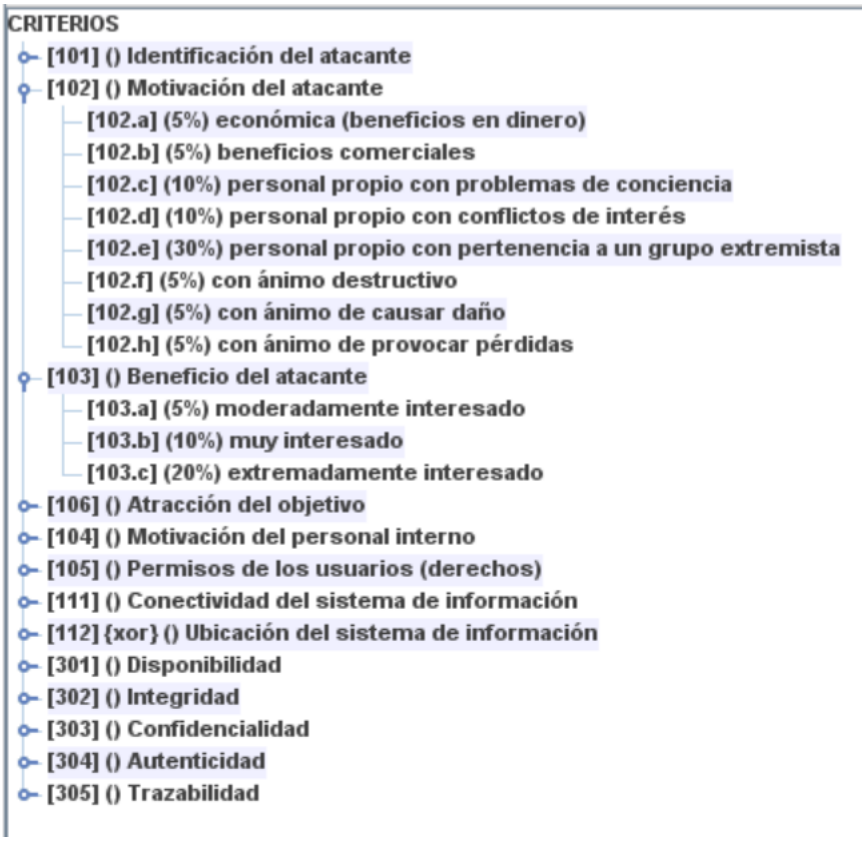

Figura 2.20 - Criterios de ocurrencia de Amenazas

- A.3.2 Identificación: Si hacemos clic sobre este menú veremos las amenazas que PILAR ha detectado para cada uno de los activos por la descripción que hemos hecho de ellos, y en caso de estar en modo manual o mix, asignar a los activos amenazas de entre las contempladas.

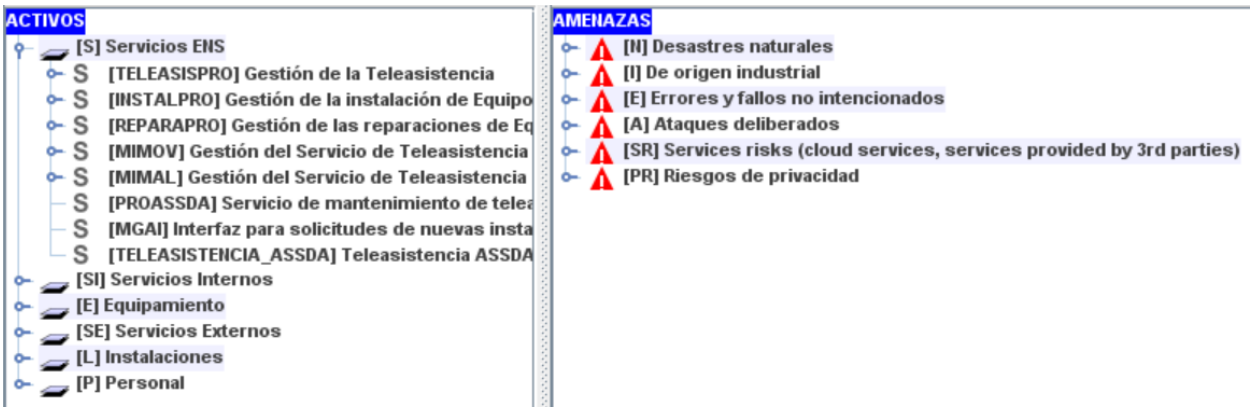

Figura 2.21 – Identificación y Asignación de Amenazas

- A.3.3 Valoración: Aquí se observan los valores TSV de frecuencia y riesgo en cada una de las dimensiones elegidas para cada uno de los activos.

ACTIVOS						
[S] Servicios ENS						
[TELEASISPRO] Gestión de la Teleasistencia			1%	10%	50%	100%
[E.15] Alteración de la información		1		1%		
[E.18] Destrucción de la información		1	1%			
[E.19] Fugas de información		1			10%	
[A.5] Suplantación de la identidad		10		10%	50%	100%
[A.6] Abuso de privilegios de acceso		10	1%	10%	50%	
[A.11] Acceso no autorizado		100		10%	50%	

Figura 2.22 - Ejemplo de Valoración de Amenazas

- A.3.4. Vulnerabilidades técnicas: Permite añadir vulnerabilidades conocidas mediante su código CVE (Common Vulnerabilities and Exposure)
- A.3.5. Incidentes: Registro de incidentes

2.4.3.4 A.4 Tratamiento de los riesgos

En esta sección se encuentran los valores de las medidas de seguridad escogidas durante la configuración del proyecto. Teniendo en cuenta las escogidas para nuestro caso, se mostrará de la siguiente manera:

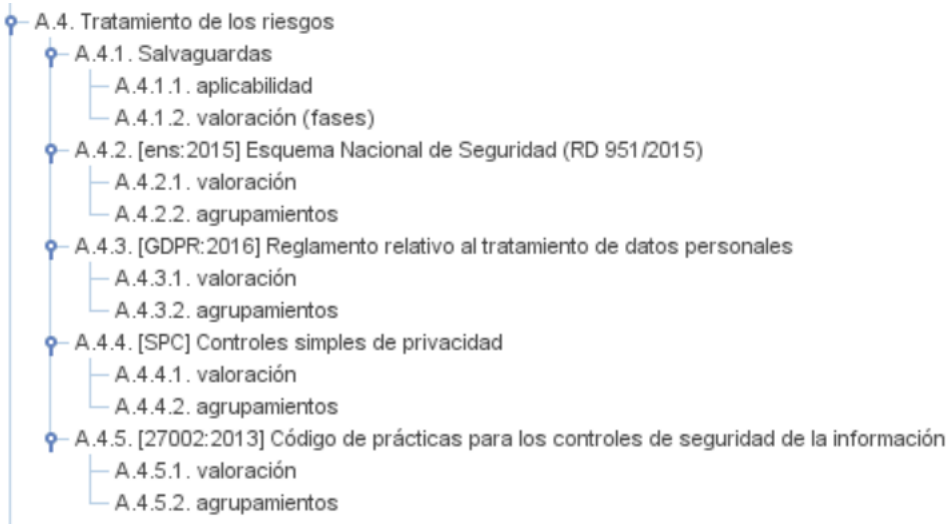

Figura 2.23 - Sección de Tratamiento de Riesgos

Por ejemplo, si hacemos clic en la valoración de las salvaguardas del ENS (las que nos interesan) podremos ver las salvaguardas concretas que debremos implementar y que impacto tendrán estas en reducir el riesgo:

recomendación		nivel	control	dudas	fuente	ens	base	com...
			[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)					
6		B	[org] Marco organizativo					
6		B	[org.1] Política de Seguridad			M		
6		B	[org.2] Normativa de seguridad			M		
6		B	[org.3] Procedimientos de seguridad			M		
3		B	[org.4] Proceso de autorización			M		
8		B	[op] Marco operacional					
6		B	[op.pl] Planificación					
8		B	[op.acc] Control de acceso					
3		B	[op.acc.1] Identificación			M		
			La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:					
			Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que:					

Figura 2.24 - Ejemplo de Salvaguardas ENS recomendadas por PILAR

2.4.3.5 A.5 Actuaciones en seguridad

Registro de las actuaciones llevadas a cabo como forma de avanzar desde la fase current a la fase target.

2.4.3.6 A.6 Impacto y riesgo

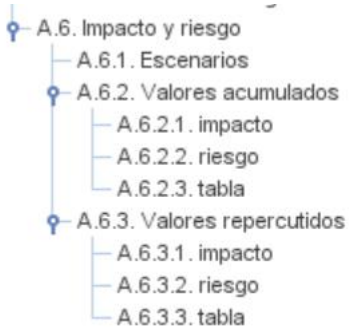

Figura 2.25 - Sección de Impacto y Riesgo

En esta sección podremos hallar los valores acumulados y repercutidos de riesgos e impactos, conceptos que se proceden a definir para su mejor comprensión [18]:

- Impacto/Riesgo acumulado: Tiene en cuenta el hecho de que los activos dependen unos de otros y por tanto la materialización de amenazas en los activos inferiores causa un daño directo sobre éstos y un daño indirecto sobre los activos superiores.
- Impacto/Riesgo repercutido: Tiene en cuenta únicamente los activos superiores, sin entrar a tener en consideración el efecto que tienen sobre aquellos activos que tienen dependencia de estos.

Mientras que los valores acumulados se emplean para definir las salvaguardas de las que hay que dotar el sistema, los repercutidos se utilizan para decidir qué niveles de riesgo aceptar.

Para los valores de impacto emplea la escala [B]ajo, [M]edio y [A]lto y utiliza la siguiente escala para los riesgos [16]:

Figura 2.26 - Escala de Riesgos

Los resultados de esta sección se incluirán junto a los demás en el apartado de realización de Análisis de Riesgos.

2.4.4 Sección (R) Informes

Esta sección, tal y como su nombre indica se pueden obtener tanto informes (con extensión .rtf o .html) de los aspectos que nos interesen como gráficas. Se muestra a continuación la interfaz que ofrece PILAR, en la que solo habrá que hacer doble clic sobre la subsección que nos interese y seguir el menú contextual que se abrirá para escoger los datos a utilizar en la generación del informe y/o g´rafica que deseemos.

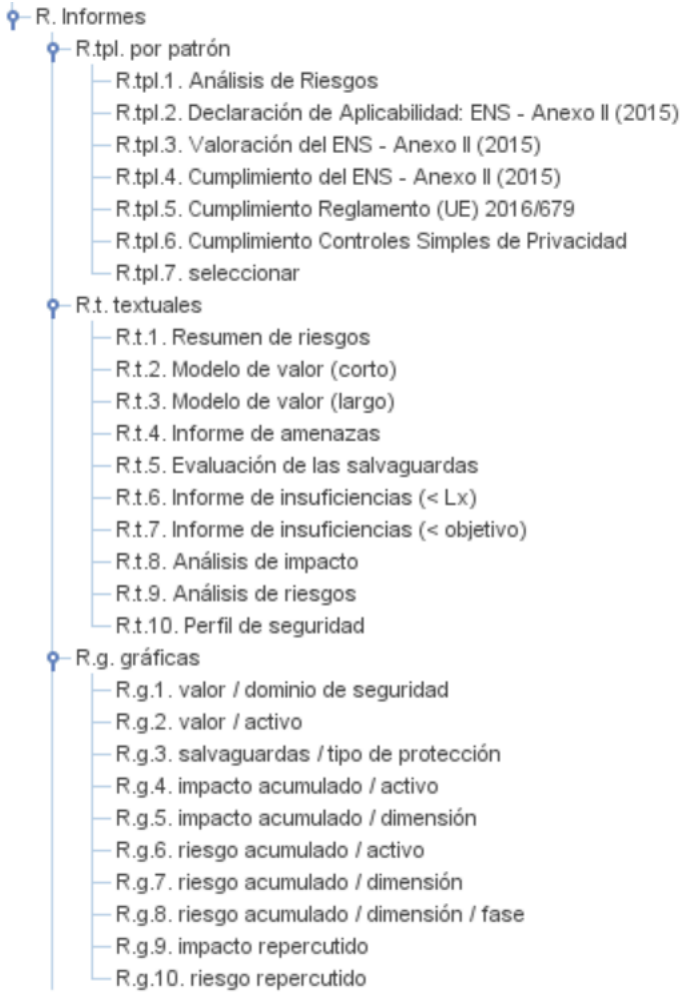

Figura 2.27 - Interfaz de Generación de Informes

3 IMPLEMENTACIÓN

La tecnología es importante, pero lo único realmente relevante es lo que hacemos con ella.

Muhammad Yunus

A lo largo de este capítulo se pretende describir el proceso completo de la realización de este proyecto, para lo cual tomaremos como punto de partida la ya justificada decisión de utilizar la aplicación PILAR como herramienta para aplicar la metodología MAGERIT en la realización del análisis de riesgo.

Para una mejor comprensión de como se ha llevado a cabo del proceso, dividiremos este en las tareas realizadas para obtener la información necesaria para realizar el análisis de riesgo, el aprendizaje del uso de la herramienta, la realización del análisis en sí, los resultados arrojados por este y las acciones realizadas por mi persona como respuesta a los resultados obtenidos. Cada una de las fases nombradas se corresponde con uno de los siguientes subapartados.

3.1 Tareas Previas

A continuación, se procede a describir las principales tareas realizadas en pos de obtener la información necesaria para realizar un análisis de riesgo lo más preciso posible. La calidad y profundidad de detalle con que se realicen estas tareas repercutirá en un mayor control del estado real de riesgo de los activos y permitirá diseñar planes de mitigación óptimos.

3.1.1 Inventariado de Máquinas Virtuales

Uno de los mayores retos a la hora de realizar un análisis de riesgo consiste en adquirir el conocimiento suficiente para entender, no sólo como funciona la red de la empresa o entidad sino, como esta es empleada por los usuarios y cómo a través de ella se ofrecen los servicios que constituyen los activos para la empresa o entidad.

A este respecto, como primera toma de contacto con la empresa se realizó un inventariado de todas las máquinas virtuales con direcciones IPs expuestas al exterior de la red de la empresa. Esta información fue recabada de los siguientes sistemas de información, control y monitorización:

- vCenter: herramienta de gestión y administración de VMWare para máquinas virtuales situadas en una única localización geográfica.
- GestioIP IPAM (Internet Protocol Address Management): Software automatizado de código abierto para la gestión de redes y direcciones IPs.
- Consola de gestión Kaspersky: Consola que reúne información de equipos Windows en los que se ha instalado el software de antivirus Kaspersky y los incidentes que se detecten en estos.
- Nominalia: Herramienta web para la gestión del servicio DNS contratado a un tercero externo.
- GLPI: Sistema de gestión de servicios y seguimiento de incidentes.
- Zabbix: Sistema de gestión de monitorización de redes utilizado principalmente para la detección de caídas de servidores críticos.

- Listado de servidores del directorio activo Windows.

Tras recoger la información de los diferentes sistemas esta fue cruzada y se procedió allí donde fuese necesario para lograr que esta fuese consistente a lo largo de todos los sistemas de información mencionados. Esto fue llevado a cabo a través de la herramienta Microsoft Excel y concretamiente haciendo uso de la función BUSCARV().

3.1.2 Construcción de la Matriz de Aplicaciones y Servicios

La tarea que a continuación va a ser descrita parte del inventariado anteriormente descrito y su realización supone el pilar fundamental del análisis de riesgo. El objetivo de esta no era otro que, dentro del marco de el servicio de teleasistencia, obtener un mapa de los activos que permiten que este se ofrezca y las dependencias existentes en estos activos (ya sea de fostware, hardware, personal, servicios externalizados…).

Dada la tan amplia extensión de esta tarea y del interés ya constatado en realizarla con un nivel de detalle lo más profundo posible se decidió realizarla en distintas fases, que se explicarán a continuación, e ir almacenando toda la información en un archivo de Microsoft Excel.

En la primera fase se identificaron los diferentes servicios TI que componen en conjunto el servicio de teleasistencia y una vez identificados cada uno de estos servicios se procedió en una segunda fase a, para cada uno de ellos, identificar los componentes con los cuales tenían dependencias clasificando estos por nivel de criticidad, por el tipo de activo e indicar el host en que se encuentran.

Los tipos de activos contemplados son claves criptográficas, componentes, datos, hardware, software y servicio. De esta manera una fila del documento Excel resultante tendría la estructura siguiente:

Tabla 3.1 - Ejemplo de entrada a la Matriz de Aplicaciones y Servicios

Servicio Esencial	Tipo de Activo	Criticidad	Dependencia	Host
InstalPRO	Datos	Crítico	BBDD Filemaker TeleasisPRO	unvmwfmak04

3.2 Realización del Análisis de Riesgo

En este apartado se procede a describir la realización del análisis de riesgo a partir de la información recogida anteriormente y siguiendo el uso de la herramienta visto en el capítulo anterior. Para una mejor comprensión por parte del lector a continuación se realiza, de forma previa al análisis, la descripción pormenorizada del servicio de teleasistencia.

3.2.1 Descripción del servicio

Para comenzar a describir es de especial interés entender quienes son el cliente y el usuario final del servicio de Teleasistencias ASSDA. El cliente de UNEI es ASSDA, Agencia de Servicios Sociales y Dependencias de Andalucía (organismo público de la Junta de Andalucía) mientras que el usuario final es la persona que solicita que se le instale un dispositivo de teleasistencia.

El proceso comienza con dicha solicitud, la cual ASSDA envía a UNEI a través del servicio externo de Cuestionario MGAI y UNEI la recibe en su servicio propio MGAI.

Los datos de estas solicitudes son recogidos por el servicio TeleasisPRO encargado de coordinar y asegurar las citas para la instalación de los dispositivos. Este servicio hace uso de Vodafone Call Recording para grabar la llamada con el usuario final como prueba de que la cita ha sido concertada. Además, con la información de las distintas citas organiza rutas de instalación.

De esta información de citas y rutas bebe el servicio InstalPRO encargado de realizar y dejar registradas las instalaciones. Para la correcta instalación es necesario identificar cual es el operador que da servicio a dicha vivienda para así poder realizar la instalación de manera adecuada. Esto se realiza mediante el servicio externo de PeopleCall.

El modelo de intercambio de datos entre InstalPRO y TeleasisPRO (su fuente de datos) es similar al modelo cliente-servidor, y con la experiencia se ha comprobado que funciona con una extrema lentitud cuando existe una distancia considerable entre estos. Para compensar esta situación se hace uso del servicio INUVIKA, un VDI/RDP que permite eliminar estos problemas de lentitud.

Llegados a este punto ya tendríamos el dispositivo instalado y bajo este contexto podrían ocurrir dos hechos:

- Recibir una solicitud de mantenimiento del dispositivo ya sea a petición del cliente, por que salte una alarma o porque haya transcurrido un tiempo; la cual será atendida por ProASSDA sin implicar esta necesidad obligada de reparación.
- Recibir una solicitud de reparación en laboratorio del dispositivo, la cual será atendida por ReparaPRO.

Por último, el dispositivo que se entrega se denomina MIMOV y contene una aplicación de igual nombre que a través del servicio propio de UNEI GeoposPRO hace peticiones al servicio externo de GoogleMaps para transmitir su posición. En ocasiones esta información no es del todo precisa y se emplea el servicio interno MGAI DEYDE para hacer uso del servicio externo DEYDE que mediante un sistema de direcciones postales resuelve estas imprecisiones.

También se ha de dejar constancia de que existe otro dispositivo similar a MIMOV denominado MIMAL, de igual funcionamiento, exclusivo para la empresa Tunstall.

Como forma de resumir lo descrito se muestra a continuación el siguiente diagrama:

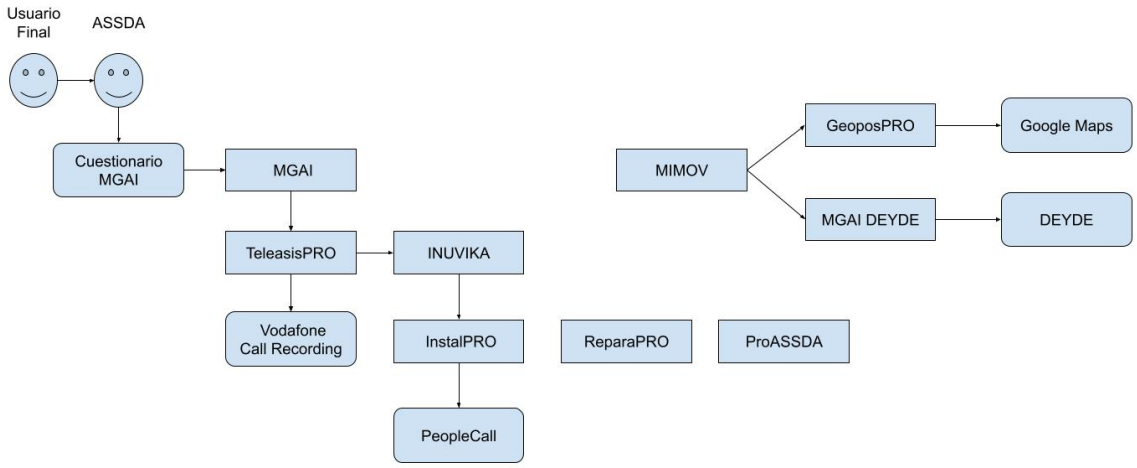

Figura 3.1 - Esquema de la estructura del servicio de Teleasistencia

3.2.2 Traslado de la información a la herramienta

A continuación, se va a mostrar como la información reunida en las tareas previas junto a la descripción del servicio es trasladada a la herramienta PILAR siguiendo el orden indicado en el apartado dedicado a la explicación del uso de la herramienta. Dado que dicho apartado fue explicado en detalle para una comprensión lo más profunda posible del funcionamiento de la herramienta, en este apartado se mostrarán solo las secciones de interés entendiéndose que aquellas que no se muestren mantendrán sus valores de configuración por defecto. Este será el caso de la sección (D) Proyecto al completo.

El primer aspecto relevante será la identificación de los activos, comenzaremos guiándonos por la Figura 3.1 para extraer de ella los activos esenciales destinados al usuario final (denominados Servicios ENS). Estos se muestran a continuación:

Figura 3.2 - Identificación de Servicios ENS

La caracterización de cada uno de estos servicios se considera innecesaria de añadir a esta memoria ya que solo aportaría peculiaridades alargando excesivamente la extensión. En lugar de eso se opta por mostrar la caracterización de uno de ellos, la cual resulta ser bastante representativa y similar a las de los demás. Esta será una pauta que se repetirá con los diferentes tipos de activos.

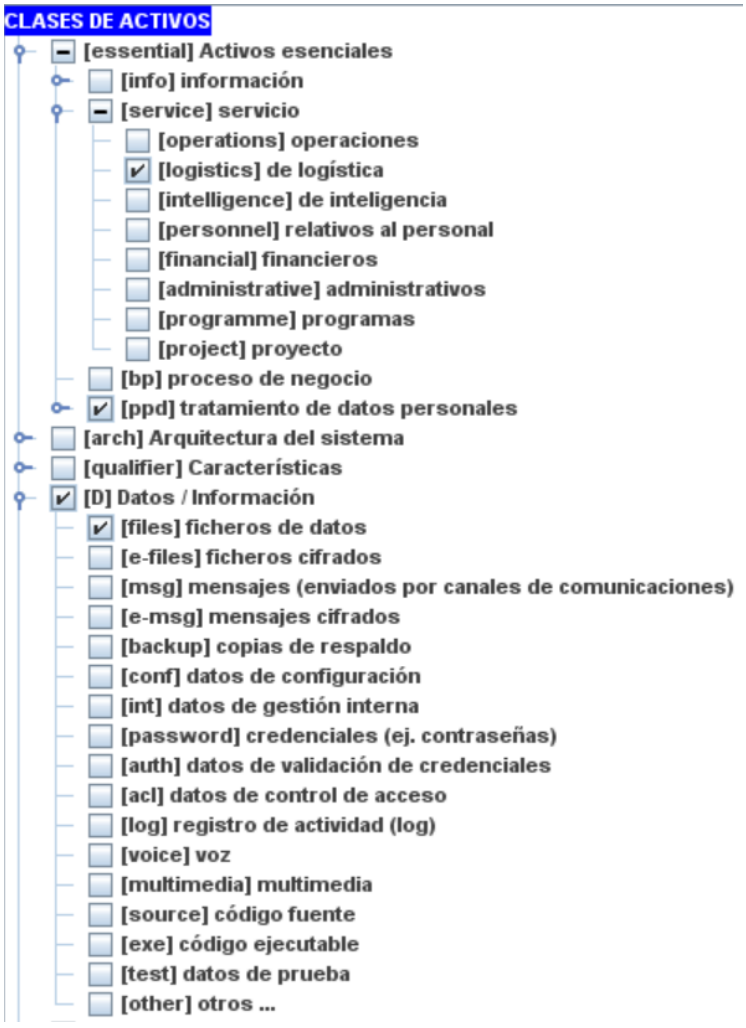

Figura 3.3 - Caracterización de TeleasisPRO

Una vez realizado esto procederemos con los servicios internos, estos son aquellos que no son empleados por los usuarios finales, sino que dan soporte a aquellos que si lo son; es decir, los denominados Servicios ENS. Se pueden observar a continuación:

Figura 3.4 – Identificación de Servicios Internos

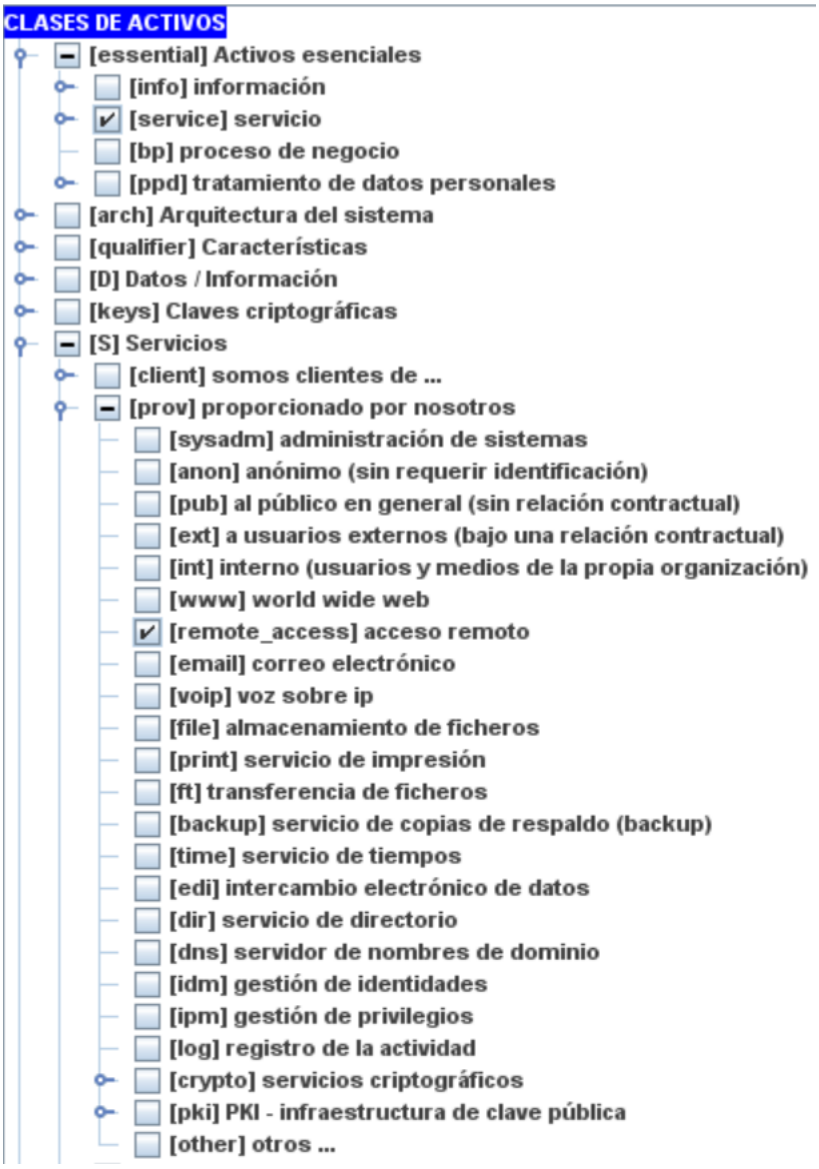

Figura 3.5 - Caracterización de INUVIKA

Una vez definido tanto los servicios finales (Servicios ENS) como los que les dan soporte, es buen momento para identificar los Servicios Externos que se emplean:

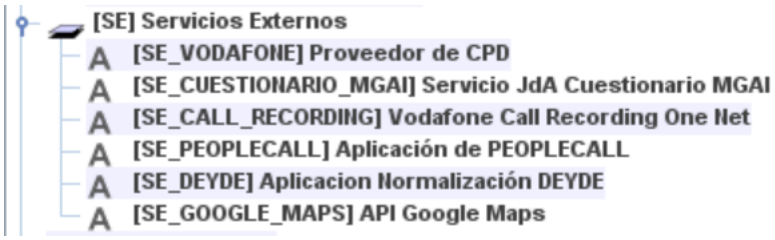

Figura 3.6 - Identificación de Servicios Externos

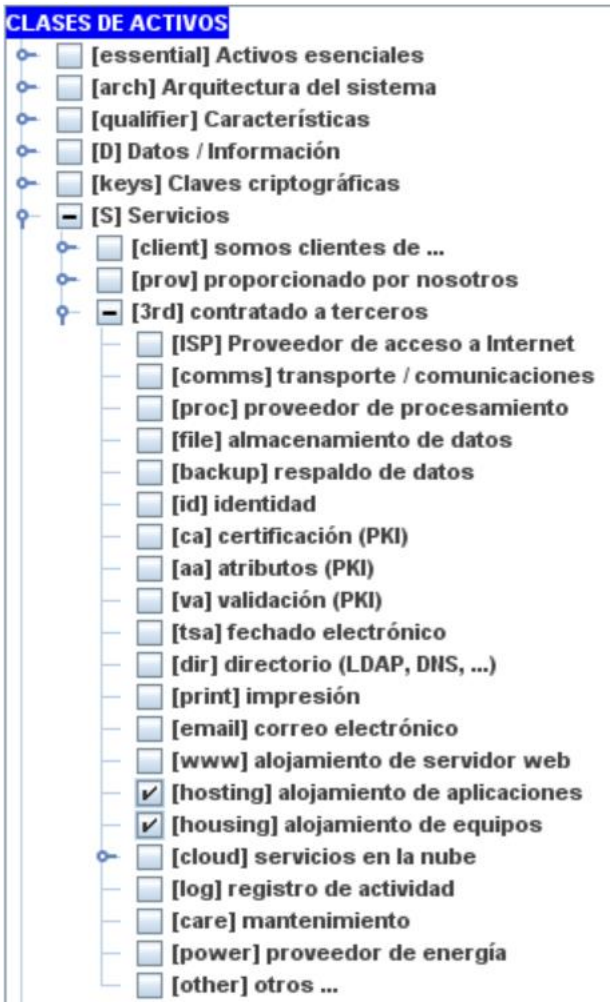

Figura 3.7 - Caracterización Proveedor de CPD

Tras definir todos los tipos de servicios es momento de comenzar a detallar el equipamiento que da soporte a estos. Comenzaremos por las aplicaciones Software:

Figura 3.8 - Identificación del Equipamiento Software

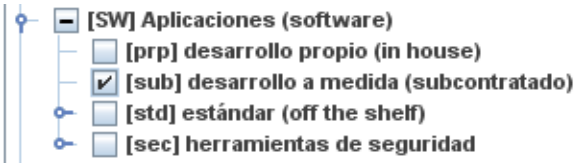

Figura 3.9 - Caracterización de la Aplicación Movil MIMOV

Siguiendo un orden lógico definiremos ahora los equipos, en este caso virtuales, en los que se hospedaran estos softwares.

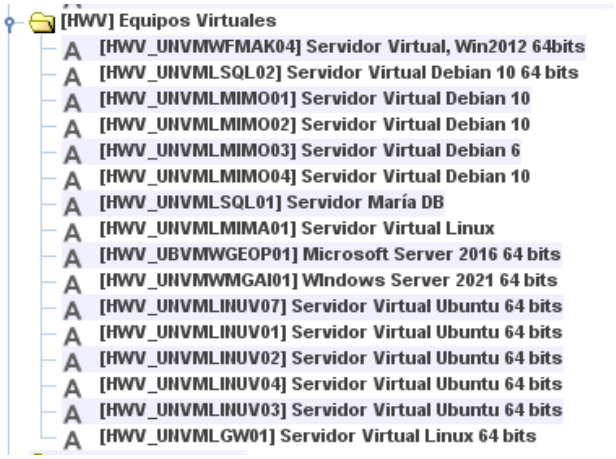

Figura 3.10 - Identificación de Hardware Virtual

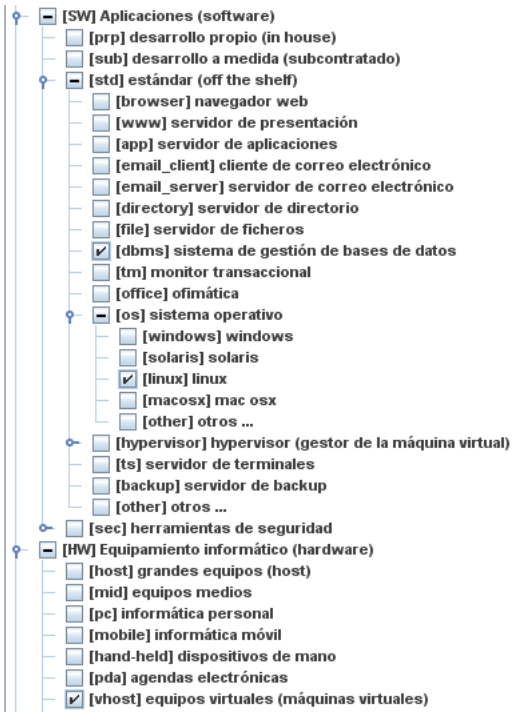

Figura 3.11 - Caracterización de un Servidor Virtual Linux

Por último, tocará definir los equipos físicos sobre los que se encuentran estas instancias virtuales, en nuestro caso se tratará de un único Cluster.

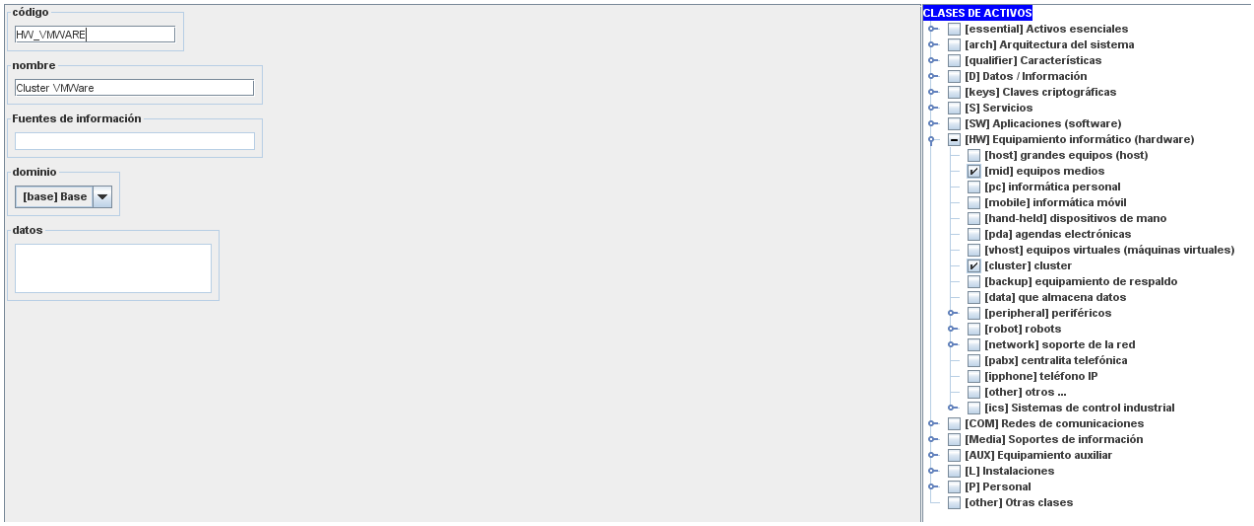

Figura 3.12 - Identificación y Caracterización del Clúster VMWare

En lo respectivo a [L] Instalaciones físicas solo tendremos una que se caracterizará de la siguiente forma:

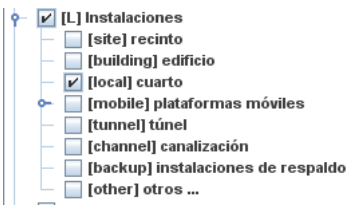

Figura 3.13 - Caracterización de la Sede de Automoción 30

Por último, el [P] Personal se dividirá en tres tipos: administradores (los dos primeros), desarrolladores y usuarios internos (último caso):

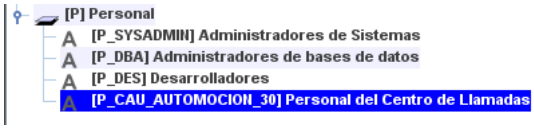

Figura 3.14 - Identificación del tipo de Personal involucrado

Con esto concluimos la identificación de activos, siendo el siguiente paso por realizar el establecimiento de las dependencias entre servicios definidas en la Figura 3.1:

Figura 3.15 - Identificación de Dependencias de Servicios

A continuación, habría que identificar las dependencias de los activos software con el equipamiento de hardware virtual:

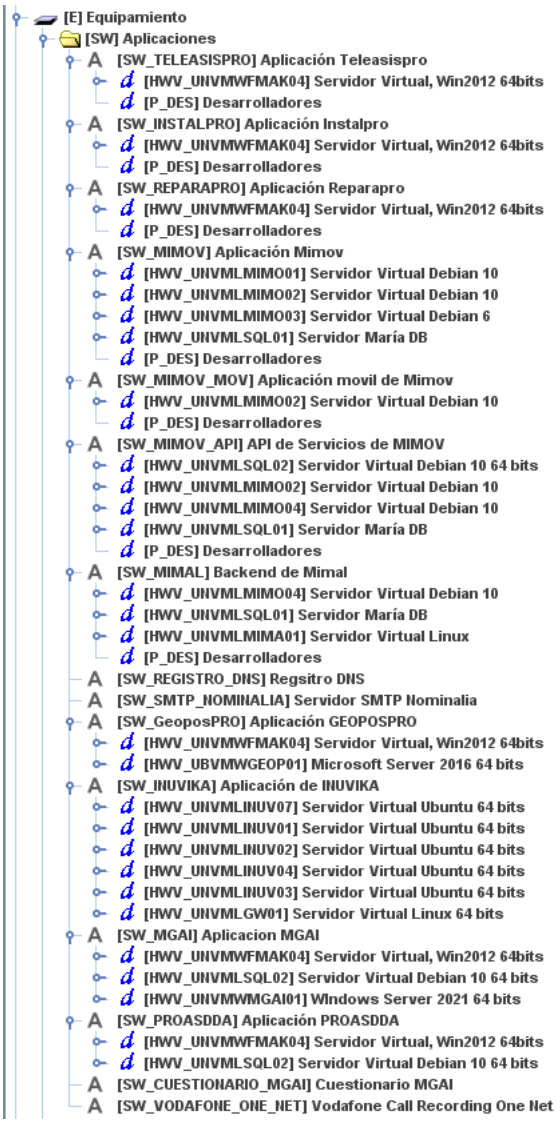

Figura 3.16 - Identificación de Dependencias de Software

Finalmente, estableceremos respecto al equipamiento virtual los hosts físicos donde se encuentran (aunque ya sabemos que están todos en el clúster VMWare) y que perfiles de usuarios tienen acceso a estos:

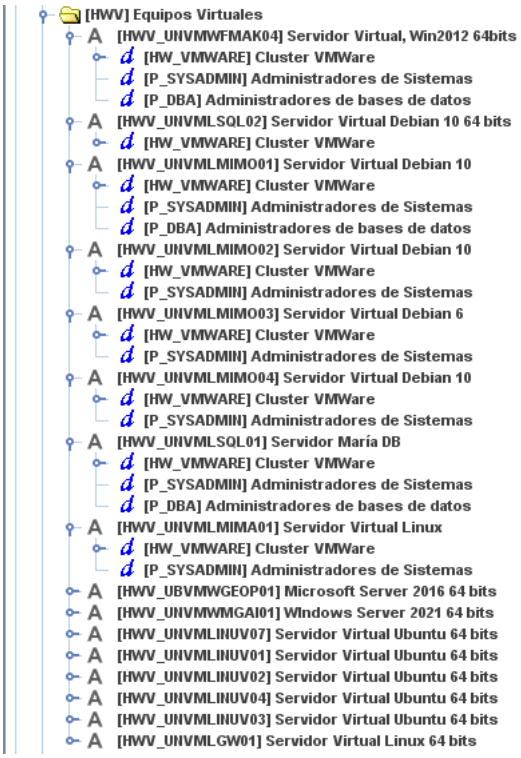

Figura 3.17 - Identificación de Dependencias de Equipos Virtuales

De esta forma, el último paso restante antes de poder obtener los resultados del análisis será la valoración de los activos esenciales, denominados Servicios ENS, en cada una de las dimensiones de seguridad tenidas en cuenta (en este caso disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad):

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[S] Servicios ENS					
[TELEASISPRO] Gestión de la Teleasistencia	[M]	[B]	[M]	[B]	[M]
[INSTALPRO] Gestión de la instalación de Equipos	[B]	[B]	[M]	[B]	[M]
[REPARAPRO] Gestión de las reparaciones de Equ	[B]	[B]	[B]	[B]	[B]
[MIMOV] Gestión del Servicio de Teleasistencia M	[M]	[M]	[M]	[M]	[M]
[MIMAL] Gestión del Servicio de Teleasistencia M	[M]	[M]	[M]	[M]	[M]
[PROASSDA] Servicio de mantenimiento de teleas	[B]	[B]	[B]	[B]	[M]
[MGAI] Interfaz para solicitudes de nuevas instal	[M]	[M]	[B]	[B]	[M]
[TELEASISTENCIA_ASSDA] Teleasistencia ASSDA	[M]	[M]	[B]	[B]	[M]

Figura 3.18 - Valoración de Activos Esenciales

Llegados a este punto ya podríamos ver la enorme lista de salvaguardas a aplicar para lograr cumplir con el ENS. Dado que la implementación completa de estas queda fuera del alcance del proyecto estas no se mostrarán a continuación ya que carecen de especial interés, sino que las salvaguardas que si se han implementado se comentarán en uno de los siguientes apartados.

3.3 Resultados

Con toda la información que se requiere para realizar el análisis de riesgo ya introducida en la herramienta PILAR, ahora podremos acceder a la sección (R) Informes para extraer los resultados que nos interesen en formato html o de texto.

Quizás el más interesante de ellos, dado el enfoque de este trabajo, sea la extracción en texto de un informe que refleje el propio análisis de riesgo. Para ello seleccionamos en la interfaz lo siguiente:

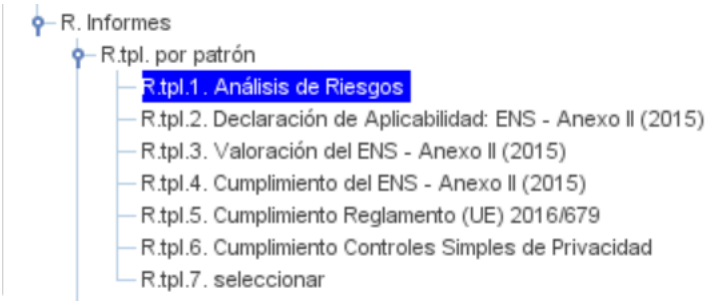

Figura 3.19 - Extracción del Informe de Análisis de Riesgo

Tras esto nos pedirá un nombre para el archivo de texto que contendrá el informe. Se muestran a continuación los resultados más interesantes de dicho documento.

3.3.1 Riesgo acumulado

En esta sección se presentan los principales riesgos en cada dominio de seguridad del sistema tanto en la situación actual como en la situación o fase Target que se desea alcanzar.

La leyenda para las tablas de esta sección será la siguiente:

- Amenaza: presenta la amenaza dentro del catálogo de PILAR. Una amenaza aparece cuando algún activo del sistema está expuesto a ella
- D – dimensión: se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza
- I – impacto: se muestra el máximo impacto causado por esta amenaza en algún activo del sistema
- R – riesgo: se muestra el máximo riesgo al que está expuesto el sistema por causa de esta amenaza

Tabla 3.2 – Riesgo acumulado potencial máximo de amenazas

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[M-]	{4,5}
[A.5] Suplantación de la identidad	C, A	[M]	{4,2}
[A.13] Repudio (negación de actuaciones)	T	[M]	{3,9}
[E.24] Caída del sistema por agotamiento de recursos	D	[M-]	{3,7}
[A.15] Modificación de la información	I	[M-]	{3,7}
[A.24] Denegación de servicio	D	[M-]	{3,7}

Tabla 3.3 - Riesgos acumulado Fase Target

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[B]	{3,0}
[A.5] Suplantación de la identidad	C, A	[B+]	{2,6}
[A.6] Abuso de privilegios de acceso	C	[B]	{2,2}
[E.24] Caída del sistema por agotamiento de recursos	D	[B]	{2,2}
[A.13] Repudio (negación de actuaciones)	T	[B+]	{2,1}
[A.24] Denegación de servicio	D	[B]	{2,1}

3.3.2 Riesgo repercutido

En esta sección se presentan los máximos riesgos a los que están expuestos los activos esenciales del sistema tanto en el estado actual como en la fase Target. Para esta sección la leyenda de las tablas será igual a la empleada en la sección anterior.

Tabla 3.4 – Exposición actual de los activos esenciales a los principales riesgos

activo	amenaza	D	I	R
[TELEASISPRO] Gestión de la Teleasistencia	[A.11] Acceso no autorizado	C	[M-]	{4,5}
[INSTALPRO] Gestión de la instalación de Equipos de Teleasistencia	[A.11] Acceso no autorizado	C	[M-]	{4,5}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[A.11] Acceso no autorizado	C	[M-]	{4,5}
[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[A.11] Acceso no autorizado	C	[M-]	{4,5}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[A.5] Suplantación de la identidad	C, A	[M]	{4,2}
[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[A.5] Suplantación de la identidad	C, A	[M]	{4,2}
[TELEASISPRO] Gestión de la Teleasistencia	[A.13] Repudio (negación de actuaciones)	T	[M]	{3,9}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[A.13] Repudio (negación de actuaciones)	T	[M]	{3,9}
[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[A.13] Repudio (negación de actuaciones)	T	[M]	{3,9}
[PROASSDA] Servicio de mantenimiento de	[A.13] Repudio (negación de	T	[M]	{3,9}

teleasistencia con ASSDA	actuaciones)			
[MGAI] Interfaz para solicitudes de nuevas instalaciones ASSDA	[A.13] Repudio (negación de actuaciones)	T	[M]	{3,9}
[TELEASISTENCIA_ASSDA] Teleasistencia ASSDA	[A.13] Repudio (negación de actuaciones)	T	[M]	{3,9}
[TELEASISPRO] Gestión de la Teleasistencia	[E.24] Caída del sistema por agotamiento de recursos	D	[M-]	{3,7}
[TELEASISPRO] Gestión de la Teleasistencia	[A.24] Denegación de servicio	D	[M]	{3,7}
[TELEASISPRO] Gestión de la Teleasistencia	[A.6] Abuso de privilegios de acceso	C	[M-]	{3,7}
[TELEASISPRO] Gestión de la Teleasistencia	[A.19] Revelación de información	C	[M-]	{3,7}
[TELEASISPRO] Gestión de la Teleasistencia	[A.5] Suplantación de la identidad	C	[M-]	{3,7}
[INSTALPRO] Gestión de la instalación de Equipos de Teleasistencia	[A.5] Suplantación de la identidad	C	[M-]	{3,7}
[INSTALPRO] Gestión de la instalación de Equipos de Teleasistencia	[A.19] Revelación de información	C	[M-]	{3,7}
[INSTALPRO] Gestión de la instalación de Equipos de Teleasistencia	[A.6] Abuso de privilegios de acceso	C	[M-]	{3,7}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[E.24] Caída del sistema por agotamiento de recursos	D	[M-]	{3,7}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[A.24] Denegación de servicio	D	[M]	{3,7}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[A.15] Modificación de la información	I	[M-]	{3,7}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[A.6] Abuso de privilegios de acceso	C	[M-]	{3,7}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[A.19] Revelación de información	C	[M-]	{3,7}
[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[E.24] Caída del sistema por agotamiento de recursos	D	[M-]	{3,7}
[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[A.24] Denegación de servicio	D	[M]	{3,7}
[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[A.15] Modificación de la información	I	[M-]	{3,7}

[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[A.19] Revelación de información	C	[M-]	{3,7}
[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[A.6] Abuso de privilegios de acceso	C	[M-]	{3,7}
[MGAI] Interfaz para solicitudes de nuevas instalaciones ASSDA	[E.24] Caída del sistema por agotamiento de recursos	D	[M-]	{3,7}
[MGAI] Interfaz para solicitudes de nuevas instalaciones ASSDA	[A.24] Denegación de servicio	D	[M-]	{3,7}
[MGAI] Interfaz para solicitudes de nuevas instalaciones ASSDA	[A.15] Modificación de la información	I	[M-]	{3,7}
[TELEASISTENCIA_ASSDA] Teleasistencia ASSDA	[E.24] Caída del sistema por agotamiento de recursos	D	[M-]	{3,7}
[TELEASISTENCIA_ASSDA] Teleasistencia ASSDA	[A.24] Denegación de servicio	D	[M]	{3,7}
[TELEASISTENCIA_ASSDA] Teleasistencia ASSDA	[A.15] Modificación de la información	I	[M-]	{3,7}

Tabla 3.5 - Exposición de los activos esenciales a los principales riesgos en la fase Target

activo	amenaza	D	I	R
[TELEASISPRO] Gestión de la Teleasistencia	[A.11] Acceso no autorizado	C	[0]	{1,2}
[INSTALPRO] Gestión de la instalación de Equipos de Teleasistencia	[A.11] Acceso no autorizado	C	[0]	{1,2}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[A.11] Acceso no autorizado	C	[0]	{1,2}
[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[A.11] Acceso no autorizado	C	[0]	{1,2}
[MIMOV] Gestión del Servicio de Teleasistencia Movil	[A.5] Suplantación de la identidad	A	[0]	{0,96}
[MIMAL] Gestión del Servicio de Teleasistencia Movil para Tunstall	[A.5] Suplantación de la identidad	A	[0]	{0,96}

3.4 Aplicación de salvaguardas

Una vez obtenidos y analizados los resultados del análisis de riesgo se procede a documentar las salvaguardas aplicadas como forma de avanzar hacia el cumplimiento del ENS y algunas actuaciones que han sido necesarias realizar para mantener garantizada la seguridad de los activos. Las salvaguardas serán identificadas por su código establecido en la metodología MAGERIT [19].

3.4.1 Salvaguarda [op.exp.1.control]

La salvaguarda [op.exp.1.control] especifica que se debe mantener un inventario actualizado de todos los elementos del sistema, identificando su propietario y naturaleza, ya sean estos activos de información, servicios, aplicaciones software o equipo hardware.

Si se observa, esta salvaguarda fue implementada incluso antes de realizarse el análisis de riesgo, ya que para realizar este fue necesario hacer un inventariado de máquinas virtuales y rellenar los datos de la Matriz de Aplicaciones y Servicios que contiene toda la información que se especifica en la salvaguarda.

3.4.2 Salvaguarda [op.exp.3.d] [tools.V7]

Las salvaguardas que nacen de la rama [op.exp.3.d] establecen todos los requisitos a cumplir a la hora de reaccionar a las vunerabilidades reportadas y más concretamente la salvaguarda [tolos.V7] trata de la reparación de dichas vulnerabilidades.

A lo largo de la realización de este proyecto se han detectado 4 incidentes asociados a vulnerabilidades, de los cuales 3 se resolvieron en colaboración con Nunsys, una empresa que proporciona a UNEI soporte con temas de ciberseguridad, y el incidente restante fue resuelto de forma interna. De todos ellos se documentó el proceso de resolución de los respectivos incidentes.

De los incidentes resueltos de manera conjunta a Nunsys dos de ellos se trataban de servidores en los que se había detectado la coexistencia de manera simultanea de varios virus y amenazas activas y un tercero en el cual por error de configuración desde hace demasiado tiempo no se había realizado un análisis de antivirus.

3.4.2.1 Incidentes resueltos junto a Nunsys

- Servidor UNVMWTEMP01: llevar a cabo un análisis de vulnerabilidades mediante Kaspersky para subsanar la no realización reciente y una vez se arrojen los resultados parchear todas las vulnerabilidades detectadas categorizadas como de importancia alta y crítica.
- Servidor PERSONALSRV2: se identificó como necesario actualizar el sistema operativo completo dada la gran cantidad de actualizaciones parciales de nivel de importancia alta y crítica. Tras esto se procedió a eliminar los virus detectados mediante la herramienta Kaspersky y se hizo un estudio de ciertas acciones tales como escaneos de la red que eran detectados como incidentes críticos para identificar si eran de origen operativo o malicioso y en consecuencia a esto aceptar dichas acciones provocando que dejasen de aparecer como incidentes o que se siguiesen detectando de la misma manera respectivamente.
- Servidor ULTEO-APSW2: Tanto el número de vulnerabilidades activas como de amenazas activas detectadas era tan alto que requirió

3.4.2.2 Vulnerabilidad Log4j

Este incidente se trató del descubrimiento de una vulnerabilidad zero-day relacionada con todos aquellos programas desarrollados en Java que empleasen Log4j para la escritura de registros. Este fue notificado por el CCN [21].

En concreto, la vulnerabilidad estaba presente en aquellas aplicaciones web donde la configuración tuviese habilitada la escritura pudiéndose añadir la opción JMSAppender. Esta opción permitía a un atacante malicioso inyectar en la petición hhtp una petición hacia un servidor externo LDAP (del atacante) con el cual llevar a cabo una elevación de permisos que permitiese ejecutar código en la máquina atacada [22].

Dentro del proceso para subsanar este incidente, lo primero era identificar qué servidores de la red de la organización presentaban esta vulnerabilidad, por tanto, necesitábamos de un *scanner*. Para escoger cual utilizar había principalmente dos opciones: un scanner web desarrollado por RedHat o alguna de las múltiples opciones de código abierto en Github.

La principal desventaja de cada opción respectivamente es que el scanner web no podía automatizarse mediante un script dado que la web contenía un captcha (para evitar un uso malicioso del mismo) y en el caso de las opciones de Github, pese a sí permitir su automatización mediante script, había que revisar a fondo el

código para que no contuviese nada de carácter malicioso. Dada la urgencia del incidente se decidió emplear el scanner web de RedHat [23].

Una vez escaneadas todas las máquinas que alojaban servidores web se detectó un único positivo, lo cual a priori iba a facilitar la resolución del incidente. En el momento en que se atendió esta incidencia existían dos soluciones posibles para nuestro caso concreto, la de los desarrolladores de Log4j [24] y la del fabricante del producto concreto que presentaba la vulnerabilidad, Qlik [22].

El problema es que al acceder al servidor afectado no se encontró ninguno de los archivos de extensión .jar sobre los cuales se debían aplicar las acciones de mitigación, tan solo un archivo log4j.js (node) que según la comunidad se encontraba libre de la vulnerabilidad [25]. Además, profundizando en como funcionaba el ataque descubrimos que las reglas del firewall de acceso a la máquina lo bloqueaban por lo que se interpretó el resultado del scanner como un falso positivo.

Para cuando se obtuvo esta conclusión, de manera paralela a nivel organizativo se decidió pasar a ser clientes del servicio Qlik bajo el modelo SaaS y con una versión del programa que ya incluía el parcheo de la vulnerabilidad.

3.4.3 Salvaguarda [op.acc.1] [IA.4.2.5.1]

Las salvaguardas enmarcadas dentro del código [op.acc.1] pertenecen al marco operacional, concretamente al control de acceso, siendo en ese contexto donde la salvaguarda [IA.4.2.5.1] indica que las cuentas que ya no son necesarias deben ser eliminadas.

Si trasladamos esta medida a la red de UNEI esto se traduce en la realización de un estudio de las cuentas del directorio activo de Windows para determinar qué cuentas ya no eran necesarias y proceder a su desactivación y eliminación. Ambas tareas fueron realizadas exitosamente.

3.4.4 Salvaguarda [op.acc.4.a]

Aprovechando la necesidad de realizar el estudio comentado en la sección anterior, se decidió que este abarcara algo más e incluyó también un análisis de aquellas cuentas que en un momento determinado habían requerido de unos permisos superiores a los que hoy en día necesitan.

Una vez determinados estos usuarios se ajustaron los permisos para cumplir así con la salvaguarda [op.acc.4.a] que establece que los privilegios de usuario deben reducirse al mínimo estrictamente neesario para cumplir sus obligaciones de forma que se acoten los daños que pueda causar un usuario de manera accidental o intencionada.

Para llevar a cabo este *downgrade* en los privilegios se utilizó la herramienta de gestión de directorio activo de Windows aprovechando además para eliminar algunas prácticas poco recomendables, tal y como el hecho de que las contraseñas de usuario no caduquen periódicamente.

3.4.5 Salvaguarda [op.exp.7.d]

La salvaguarda [op.exp.7.d] determina que debe existir un procedimiento de gestión de incidentes para informar a las partes interesadas, tanto internas como externas.

Llevado al entorno de UNEI, parte de implementar esta salvaguarda requería que la consola de antivirus Kaspersky, que reúne todos los incidentes ocurridos en los dispositivos en los que se encuentra instalado este software de antivirus, enviase notificaciones automáticas.

Se decidió que estas notificaciones se enviasen por correo y para no saturar las bandejas de correo de los destinatarios estas solo se emitiesen cuando Kaspersky identificase como de nivel crítico. Se adjunta a continuación una imagen de como se configuró lo citado a través de la herramienta Kaspersky Security Center.

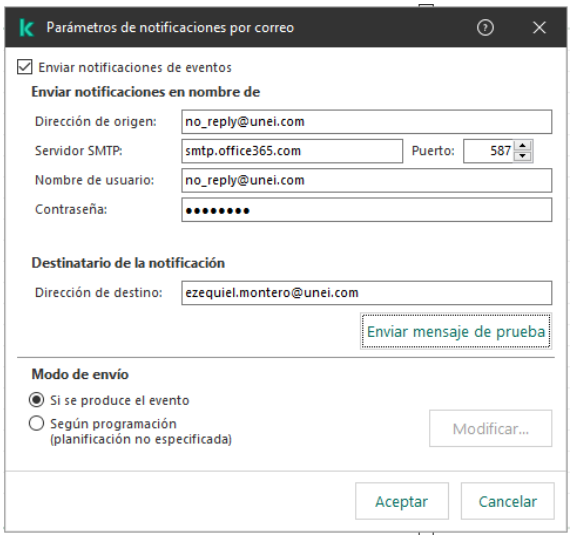

Figura 3.20 - Configuración de las Notificaciones de Incidentes

Tras realizar esta implementación nos dimos cuenta de que a la hora de configurar las tablets Lenovo para los empleados Kaspersky detectaba un programa que viene instalado por defecto en ellas como potencialmente peligroso generando una notificación de alerta crítica.

Ante esto se contactó con la ya mencionada Nunsys para que analizasen el software y dieran veredicto sobre la peligrosidad o no de este. Cuando determinaron que no existía riesgo asociado a esa aplicación se trabajó de manera conjunta para definir una excepción a las reglas de notificaciones anteriormente configuradas.

3.4.6 Salvaguarda [op.exp.4.c]

La salvaguarda [op.exp.4.c] indica que debe de existir un procedimiento para aplicar las actualizaciones de seguridad, parches y nuevas versiones de software que tenga en cuenta cuándo es mejor llevarlas a cabo y que las priorice según la variación del riesgo que supongan.

Para implementar esta salvaguarda de nuevo se cooperó con la empresa Nunsys con el objetivo de instalar un Windows Server Update Services, WSUS de ahora en adelante. Esta herramienta permite manejar de forma centralizada y sencilla la distribución de parches a través de todos los equipos de la red corporativa mediante actualizaciones automáticas [20].

4 CONCLUSIONES

La vida es el arte de sacar conclusiones suficientes a partir de datos insuficientes.

Samuel Butler

Como forma de concluir esta memoria, se procede a la realización de un análisis general de los objetivos a cumplir como medida para obtener conclusiones al respecto de este trabajo. Se podría decir que, una vez realizado este proyecto, este se estructuraba sobre tres cimientos principales: adquirir el conocimiento necesario sobre el estado del arte y las tecnologías, llegar a conocer como UNEI a través de su red ofrece a los clientes su servicio de teleasistencia y en ultimo lugar, plasmar la información obtenida sobre una herramienta que facilite el análisis de riesgo.

En lo relativo al estado del arte y las tecnologías, en este proyecto se ha profundizado en la comparativa de tecnologías ya introducida por D. Fernando Cárdenas Fernández en la asignatura de Gestión de la Ciberseguridad. La principal conclusión en este aspecto es que, de entre las metodologías de análisis de riesgos más prestigiosas, no existe una mejor que otra, sino que cada una de ellas ofrece sus propias características y pequeñas diferencias. Es esto último lo que debe guiar en la decisión de escoger una metodología ya que lo más determinante es como de bien se adapte esta a la empresa o entidad en la cua se desea realizar el análisis de riesgo. En el caso de este proyecto la elección de la metodología MAGERIT y la herramienta PILAR fue sencilla dado el contexto de colaboración con las entidades públicas.

Con respecto a llegar a conocer como funciona la infraestructura de UNEI para ofrecer su servicio de teleasistencia he de decir que ha sido todo un reto cuyo éxito no podría haber alcanzado sin la colaboración de los diferentes compañeros de UNEI implicados en cada uno de los activos necesarios en este servicio. La principal ayuda a la hora de realizar esta ardua tarea siempre fue el saber que, a cada nivel extra de detalle alcanzado en la identificación de activos y dependencias, más cerca nos encontraríamos de realizar un análisis de riesgos óptimo.

Por último, en lo referente al análisis de riesgos, más allá de los resultados particulares arrojados por el mismo y ya anteriormente comentados en esta memoria, la principal conclusión es que su realización supone un paso muy importante en el proceso de aplicación y adaptación al ENS por parte de UNEI.

REFERENCIAS

[1] (Octbre 25, 221). "La empresa social UNEI, referente en integración laboral de personas con problemas de salud mental, supera el millar de empleados". Diario de Sevilla. https://www.diariodesevilla.es/empresas-al-dia/UNEI-referente-integracion-problemas-empleados_0_1623138420.html

[2] Centro Criptológico Nacional (2022). Esquema Nacional de Seguridad - Preguntas frecuentes. Recuperado de https://www.ccn-cert.cni.es/publico/dmpublidocuments/ENS-FAQ.pdf

[3] Cárdenas Fernández, Fernando (2021). Transparencias de la asignatura Gestión de la Ciberseguridad. Recuperado de https://ev.us.es/webapps/portal/execute/tabs/tabAction?tab_tab_group_id=_29_1

[4] Elite-formacion (2018). Método de Análisis de Riesgos NIST SP 800-30. Recuperado el 26 de junio de 2022, de http://elite-formacion.blogspot.com/2018/04/metodo-de-analisis-de-risgos-nist-sp.html

[5] SecurityArtwork (2012). Introducción al Análisis de Riesgos. Metodologías (I). Recuperado el 26 de junio de 2022, de https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

[6] Seguinfo (2008). ISO 27005:2008: Gestión de Riesgos. Recuperado el 26 de junio de 2022, de https://seguinfo.wordpress.com/2008/06/18/iso-270052008-gestion-de-riesgos/

[7] SecurityArtwork (2012). Introducción al Análisis de Riesgos. Metodologías (II). Recuperado el 26 de junio de 2022, de https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-ii/

[8] UCE-DTIC (2021). Metodología MAGERIT, análisis y gestión de riesgos. Recuperado el 26 de junio de 2022, de https://uce-dtic.blogspot.com/2021/02/metodologia-magerit-analisis-y-gestion.html

[9] Archer Community (2020). Archer NIST-Aligned Privacy Framework App-Pack. Recuperado el 26 de junio de 2022, de https://www.archerirm.community/t5/exchange-overviews/archer-nist-aligned-privacy-framework-app-pack/ta-p/558459

[10] NIST (2022). Privacy Framework. Recuperado el 26 de junio de 2022, de https://www.nist.gov/privacy-framework

[11] NIST (2020). SCAP Composer. Recuperado el 26 de junio de 2022, de https://www.nist.gov/services-resources/software/scap-composer

[12] ITSMSolutions (2006). 10 Steps To Do It Yourself CRAMM. Recuperado el 26 de junio de 2022, de https://www.itsmsolutions.com/newsletters/DITYvol2iss8.htm

[13] ENISA (2022). Cramm. Recuperado el 26 de junio de 2022, de https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

[14] EAR (2022). EAR herramientas. Recuperado el 26 de junio de 2022, de https://www.ar-tools.com/es/tools/blanca/index.html

[15] Centro Criptológico Nacional (2018). Guía de Seguridad de las TIC CCN-STIC 470. PI LAR – Manual de Usuario v7.1. Recuperado el 26 de junio de 2022, de https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2841-ccn-stic-470i1-pilar-manual-de-usuario-v7-1/file.html

[16] EAR (2021). PILAR Basic. Análisis y Gestión de Riesgos. Ayuda. Recuperado el 26 de junio de 2022, de https://www.ar-tools.com/doc/help_basic_es_e_20212.pdf

[17] Security Artwork (2012). Análisis de riesgos con PILAR. Recuperado el 26 de junio de 2022, de https://www.securityartwork.es/2012/11/02/analisis-de-riesgos-con-pilar/

[18] Universidad Católica de Colombia (2021). Diseño de Recomendaciones de Seguridad Informática sobre los Activos de Información Críticos. Recuperado el 26 de junio de 2022, de https://repository.ucatolica.edu.co/bitstream/10983/2425/3/2%20Anexos.pdf

[19] Centro Criptológico Nacional (2012). MAGERIT – versión 3.0. Libro II - Catálogo de Elementos.

Recuperado el 26 de junio de 2022, de https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file

[20] Wikipedia (2022). Windows Server Update Services. Recuperado el 26 de junio de 2022, de https://es.wikipedia.org/wiki/Windows_Server_Update_Services

[21] Centro Criptológico Nacional (2021). CCN-CERT AL 09/21 Vulnerabilidad en Apache Log4j 2. Recuperado el 26 de junio de 2022, de https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/11435-ccn-cert-al-09-21-vulnerabilidad-en-apache-log4j-2.html

[22] Red Hat Custom Portal (2021). CVE-2021-4104. Recuperado el 26 de junio de 2022, de https://access.redhat.com/security/cve/CVE-2021-4104

[23] Red Hat (2021). Log4j Vulnerability Scanner. Recuperado el 26 de junio de 2022, de https://scanner.checklog4j.com/

[24] QLIK (2021). CVE-2021-45105/CVE-2021-44832 - Update to log4j 2.17.1 for Qlik Replicate and Qlik Enterprise Manager. Recuperado el 26 de junio de 2022, de https://community.qlik.com/t5/Knowledge/CVE-2021-45105-CVE-2021-44832-Update-to-log4j-2-17-1-for-Qlik/ta-p/1876190

[25] GitHub Community (2021). Is log4js-node affected by the log4s vulnerability? Recuperado e 26 de junio de 2022, de https://github.com/log4js-node/log4js-node/issues/1105

GLOSARIO

ENS: Esquema Nacional de Seguridad 1

TI: Tecnologías de la Información 3

TIC: Tecnologías de la información y comunicaciones 5

CCN: Centro criptográfico nacional 7

RGPD: Reglamento General de Protección de Datos 11

DMZ: Zona Desmilitarizada 12