Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013

Nombre Estudiante: Raúl Prieto Pozo

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio José Segovia Henares
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha entrega: 6 de junio de 2016

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013*
Nombre del autor:	*Raúl Prieto Pozo*
Nombre del consultor/a:	*Antonio José Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	06/2016
Titulación::	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave	*SGSI, ISO 27001:2013, ANÁLISIS DE RIEGOS*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El presente trabajo describe la hoja de ruta que se ha de llevar a cabo para realizar la implantación de la norma ISO/IEC 27001:2013 en una organización.

El objetivo principal es evaluar el estado inicial de la organización en materia de seguridad de la información y definir un conjunto de proyectos dirigidos a reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables.

El desarrollo del trabajo está apoyado sobre la norma ISO/IEC 27001:2013. Se trata de un estándar internacional que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.

Con el objeto de realizar todo el proceso de implantación, el trabajo se ha estructurado en seis etapas: contextualización del proyecto y situación actual de la organización, sistema de gestión documental, análisis de riesgos, propuestas de proyectos, auditoría de cumplimiento y presentación de resultados.

A la luz de resultados obtenidos durante el trabajo, se puede afirmar que el proceso de implantación del SGSI en la organización ficticia propuesta, ha sido todo un éxito. Puesto que los niveles de riesgo a los que se encontraba expuesta la compañía inicialmente han disminuido considerablemente y ha aumentado el nivel de madurez de la empresa en materia de seguridad de la información.

Abstract (in English, 250 words or less):

The following essay describes the roadmap which must be followed for implementing the ISO/IEC 27001:2013 norm in an organization.

The main aim is to evaluate the initial state of the company in terms of the security of the information and to device a set of projects addressed to reducing to an adequate level the risks to which the organization is exposed to.

The development of this essay is based on the ISO/IEC 27001:2013 norm. This is an international standard which specifies the necessary requirements to establish, implement, maintain and improve the system of security management of the information.

With the purpose of conducting the whole process of implementation, this project has been structured in six stages: contextualization of the project and current position of the company, documentary management system, risk analysis, project proposals, compliance audits and result presentation.

In the light of the results obtained during the analysis, it can be affirmed that the process of implementation of the ISMS in the proposed fictitious organization, has been a success. Given that the risk levels to which the company was initially exposed to have significantly decreased and the level of matureness of the business has increased in terms of information security.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

La necesidad a cubrir en este proyecto es la importancia de que una organización disponga de un Sistema de Gestión en Seguridad de la Información.

El Plan de Implementación de la ISO/IEC 27001:2013 es un aspecto clave en cualquier organización que desea alinear sus objetivos y principios de seguridad a la normativa Internacional de Referencia.

El principal objetivo es sentar las bases del proceso de mejora continua en materia de seguridad de la Información, permitiendo a las organizaciones conocer el estado de la misma y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales.

Se trata de un tema que frecuentemente no preocupa a las altos comités de dirección de las organizaciones pero en el momento que descubren que en su empresa ha habido una fuga de información o han sufrido una denegación de servicio de sus aplicaciones corporativas y por ello una pérdida de dinero o reputación, comienzan a valorar la importancia de disponer de un SGSI.

Para que no se trate de acciones reactivas y puntuales, es decir, a posterior de la incidencia ocurrida, se debe de implantar un SGSI que permita reducir los riesgos a los que está expuesta una organización y dedicar los recursos necesarios a prevenir los posibles ataques o incidencias que puede sufrir una entidad.

1.2 Objetivos del Trabajo

El presente Trabajo Final de Máster tiene como objetivos:

- Familiarizarse con la norma ISO/IEC 27001:2013 y su anexo A.
- Conocer las diferentes etapas necesarias para llevar a cabo la implantación de un Sistema de Gestión de Seguridad de la Información.
- Conocer el concepto de política de seguridad y desarrollarla.
- Conocer la estructura de un procedimiento del sistema de gestión documental y desarrollarlo.
- Conocer las diferentes metodologías para desarrollar un análisis de riesgos y llevarlo a cabo.
- Estudiar los posibles proyectos que se pueden llevar a cabo para reducir las amenazas a las que está expuesta una organización.

- Conocer cómo se realiza una auditoría de cumplimiento y el concepto de no conformidad y acción correctiva.
- Diferenciar al público al que te diriges a la hora de presentar las conclusiones y resultados de la implantación del SGSI.

1.3 Enfoque y método seguido

La norma ISO/IEC 27001:2013 es un estándar reconocido a nivel internacional y sobre el que se apoyan las organizaciones certificadoras para determinar si una organización cumple con los requisitos necesarios que debe tener un Sistema de Gestión de Seguridad de la Información.

Por ello, la norma ha servido como guía para realizar el proyecto. No obstante, el estándar citado no especifica que metodología se ha de seguir para desarrollar el análisis de riesgos.

Para elaborar el análisis de riesgos se ha escogido la metodología MAGERIT por su reconocimiento a nivel nacional y por ser una de las guías más aceptadas y utilizadas en el ámbito del análisis de riesgos.

1.4 Planificación del Trabajo

El trabajo se ha estructurado en seis fases, las cuales están establecidas en un margen de tiempo. En la siguiente tabla se puede observar las tareas a realizar en cada fase y el tiempo necesario que se debe dedicar.

Los días necesarios indicados son a tiempo completo, es decir, 8 horas por día establecido.

Fase 1: Situación actual: Contextualización, objetivos y análisis diferencial
Días necesarios: **5 días** Introducción al Proyecto. Enfoque y selección de la empresa que será objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa con respecto la ISO/IEC 27001+ISO/IEC 27002

Fase 2: Sistema de Gestión Documental
Días necesarios: **10 días** Elaboración de la Política de Seguridad. Documentación del SGSI

Fase 3: Análisis de riesgos
Días necesarios: **16 días** Elaboración de una metodología de análisis de riesgos: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.

Fase 4: Propuesta de Proyectos
Días necesarios: **11 días** Evaluación de proyectos que debe llevar a cabo la Organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de los mismos.

Fase 5: Auditoría de Cumplimiento de la ISO/IEC 27002:2013
Días necesarios: **7 días** Evaluación de controles, madurez y nivel de cumplimiento.

Fase 6: Presentación de Resultados y entrega de Informes
Días necesarios: **6 días** Consolidación de los resultados obtenidos durante el proceso de análisis. Realización de los informes y presentación ejecutiva a la Dirección. Entrega del proyecto final.

Con el fin de que se puedan cumplir los plazos definidos en este apartado y el proyecto salga adelante, se ha realizado el siguiente Diagrama de Gantt, en el cual se puede visualizar la planificación a seguir:

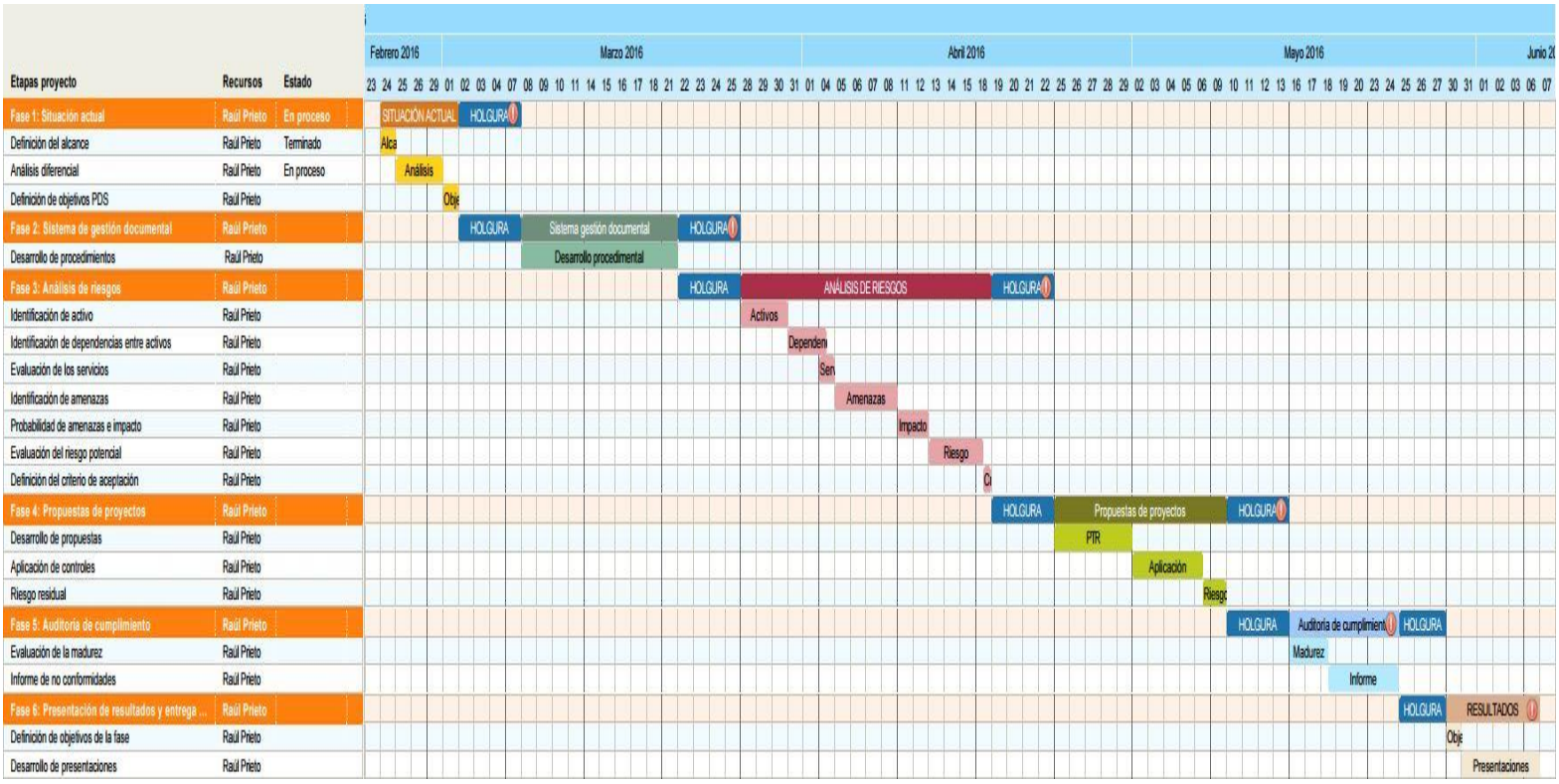


Ilustración 1 Diagrama de Gantt - Planificación TFM

1.5 Breve sumario de productos obtenidos

Se puede afirmar que la implantación de la ISO/IEC 27001:2013 ha sido todo un éxito ya que la compañía ya dispone de un Sistema de Gestión de Seguridad de la Información y además ha logrado disminuir los riesgos a los que estaba expuesta inicialmente.

En la fase 6 se han reflejado los resultados en diferentes presentaciones en PowerPoint: resumen ejecutivo, presentación a la compañía, presentación del estado de cumplimiento de los controles y presentación a la dirección.

1.6 Breve descripción de los otros capítulos de la memoria

- Fase 1: Situación actual.
  - En la primera fase se introduce el trabajo a desarrollar y se explica el contenido de la ISO 27001:2013. Se selecciona la empresa ficticia sobre la que se va a realizar el proyecto. Esta fase finaliza con el análisis diferencial y la descripción de los objetivos del Plan Director de seguridad.

- Fase 2: Sistema de gestión documental.
  - En la segunda fase se introduce la importancia de disponer de un sistema de gestión documental y se desarrollan los procedimientos necesarios.

- Fase 3: Análisis de riesgos.
    - En la tercera etapa del proyecto se elabora el análisis de riesgos para conocer cuáles son las amenazas a las que está expuesta la organización y se establece el criterio de aceptación de riesgos.

- Fase 4: Propuestas de proyectos.
    - En la cuarta fase se describen los proyectos a realizar para disminuir los riesgos identificados en la fase anterior. Estos proyectos se acotan en un límite de tiempo.

- Fase 5: Auditoría de cumplimiento.
    - En la quinta fase se realiza una auditoría de cumplimiento para detectar posibles incidencias o no conformidades tras la implantación del SGSI.

- Fase 6: Presentación de resultados y entrega de informes
    - En la última fase se presentan los resultados obtenidos a lo largo del proyecto en cuatro presentaciones en PowerPoint.

2. Fase 1: Situación actual

2.1 Introducción

El incremento exponencial del uso de las nuevas tecnologías en las organizaciones, y la cada vez mayor dependencia de los sistemas de información, hacen que los procesos de negocio de una empresa dependan en gran medida de la disponibilidad de sus sistemas de información, y de la integridad y confidencialidad de los datos que éstos gestionan. Así, se definen los tres pilares sobre los que se basa la seguridad de los sistemas de información:

- **Disponibilidad**: debemos tener garantías de que la información va a estar disponible en el momento en que se necesita.
- **Integridad**: debemos tener garantías de que la información es exacta, y de que está protegida frente a alteraciones o pérdidas.
- **Confidencialidad**: debemos tener garantías de que sólo las personas autorizadas disponen de acceso a la información.

Con idea de incrementar la eficacia de la seguridad, las organizaciones deben valorar la seguridad de sus sistemas de información desde un enfoque global, que tenga en cuenta no sólo aspectos técnicos, sino también físicos, organizativos e incluso legales. El conocimiento del estado de la seguridad de la información bajo este prisma global como paso previo a iniciativas específicas, permite a las organizaciones conocer su estado inicial en materia de seguridad, paso imprescindible para ordenar, con conocimiento de causa, las acciones futuras en relación a esta materia. Es en este contexto donde entra en juego el Plan Director de Seguridad (PDS).

Este PDS permite conocer el estado inicial en materia de seguridad de una organización referenciado a estándares internacionales que servirán de baremo a lo largo de todo el proceso.

Permite, dado este estado inicial, planificar de manera ordenada y alineada con la estrategia corporativa, las iniciativas adecuadas para llevar el estado de esta seguridad global a niveles objetivo, siendo éstos conocidos y aceptados por la organización. Permite en definitiva saber dónde estamos, dónde queremos ir y cómo lo haremos de la manera más eficaz posible. Además, la organización habrá pensado en los problemas y sus soluciones antes de que estos se materialicen, hecho crucial de cara al tipo de reacción inmediata que suelen requerir los incidentes de seguridad.

Una vez alcanzados los niveles objetivo en seguridad de la información, hay que tener presente que la seguridad es un proceso continuo, no un proyecto o un producto, un proceso continuado en el tiempo que como tal, necesita de una gestión.

En este sentido, un Sistema de Gestión de la Seguridad de la Información (SGSI) introduce el concepto de mejora continua (entre otros), garantizando tanto el mantenimiento en el tiempo de los niveles de seguridad establecidos en una organización determinada como el incremento paulatino de los mismos.

Un SGSI se puede definir como el sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información; este sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad corporativos. Es importante enfatizar de nuevo la definición de la seguridad de la información que se hace dentro del sistema de gestión, ya que se considera la misma como un proceso continuo, no como un producto o servicio concretos, introduciendo además en la seguridad el ciclo de mejora continua habitual en los sistemas de gestión.

Actualmente, es posible la implantación de un SGSI basado en diferentes normas y estándares, tanto nacionales como internacionales. En este sentido, destaca por encima de las demás la ISO/IEC 27001:2013 [0], basada en el estándar británico BS-7799-2. Entre los múltiples beneficios obtenidos al implantar un sistema de gestión basado en esta norma, encontramos la certificación del sistema por parte de entidades acreditadas, así como su apoyo en la norma ISO/IEC 27002:2013 (anterior ISO 27002:2005), un código de buenas prácticas para la gestión de la seguridad de la información.

2.2 Origen de la ISO 27001 e ISO 27002

La ISO 27001 [1] es la norma ISO que establece los requisitos para implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

La ISO 27001 como la conocemos hoy en día, ha sido resultado de la evolución de otros estándares relacionados con la seguridad de la información. Se trata de los siguientes:

- 1901 – Normas “BS”: La British Standards Institution publica normas con el prefijo “BS” con carácter internacional. Estas son el origen de normas actuales como ISO 9001, ISO 14001 u OHSAS 18001.

- 1995- BS 7799-1:1995: Mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Eran recomendaciones que no permitían la certificación ni establecía la forma de conseguirla.

- 1998 – BS 7799-2:1999: Revisión de la anterior norma. Establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.

- 1999 – BS 7799-1:1999: Se revisa.

- 2000 – ISO/IEC 17799:2000: La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios.

- 2002 – BS 7799-2:2002: Se publicó una nueva versión que permitió la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.

- 2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.

- 2007 – ISO 17799: Se renombra y pasa a ser la ISO 27002:2005

- 2007 – ISO/IEC 27001:2007: Se publica la nueva versión.

- 2009 – Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M:2009

- 2013 – Actualización a la ISO 27001:2013 y 27002:2013

La estructura de la norma ISO 27001:2013 está basada en los siguientes puntos: introducción, alcance, referencias normativas, términos y definiciones, contexto de la organización, liderazgo, planeación, soporte, operación, evaluación del desempeño y mejora. Sobre esta norma se aplica el círculo PDCA [2] (del inglés plan-do-check-act, es decir, planificar-hacer-verficar-actuar) basado en la mejora continua de la calidad.

En la siguiente imagen se puede observar la estructura de la norma a implementar:

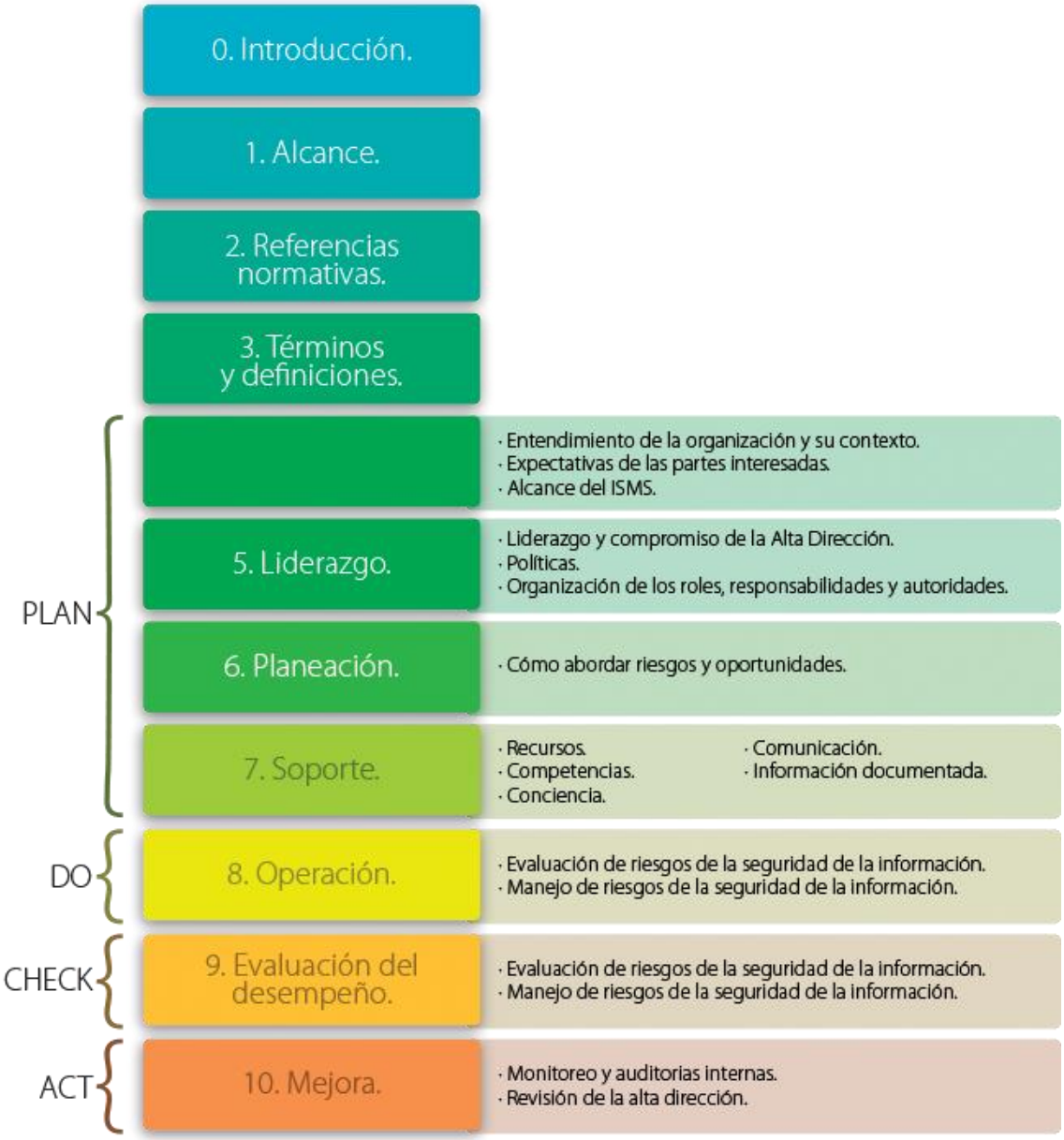


Ilustración 2 Estructura ISO 27001 Fuente: http://www.magazcitum.com.mx

Además la ISO 27001 incorpora un anexo A de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Se trata de la ISO 27002 y su alcance está orientado a la seguridad de la información en las empresas u organizaciones.

Este anexo está compuesto por 114 controles distribuidos en 14 dominios de seguridad siendo los siguientes:

Ilustración 3 Dominios 27002. Fuente: isaca.org

Los cambios más significativos en la nueva ISO 27001:2013 e ISO 27002:2013 respecto a la anterior versión, ISO 27001:2005 e ISO 27002:2005, son los siguientes:

1. Reestructuración del estándar con la estructura de ISO Anexo SL
2. Ya no se habla directamente de PDCA, sino de Mejora Continua.
3. Mayor conocimiento del contexto de la organización y de las necesidades de las partes interesadas
4. Proceso de análisis de riesgos más general y alineado a ISO 31000
5. Ya no se habla de la relación:
    a. Riesgos → Activos → Amenazas → Vulnerabilidades

6. Se habla de propietario del riesgo.
7. Mayor importancia al liderazgo y compromiso de la Dirección
8. Mayor relevancia a la definición de Objetivos d Seguridad
9. Mayor relevancia a la medición y monitorización.
10. Se elimina la lista de documentos obligatorios y no se distinguen documentos y registros. Se generaliza como “información documentada”
11. Revisión por la Dirección no tan exhaustiva
12. Se eliminan las acciones preventivas y solo existen acciones correctivas.

Si se realiza una comparación o “matching” entre la ISO 27001:2013 y 27001:2005 se obtiene la siguiente tabla:

ISO 27001:2013	ISO 27001:2005
0. Introducción.	0. Introducción.
1. Alcance.	1. Objeto y campo de aplicación.
2. Referencias normativas.	2. Normas para consulta.
3. Términos y definiciones.	3. Términos y definiciones.
4. CONTEXTO DE LA ORGANIZACIÓN.	
4.1 Entendimiento de la organización y su contexto.	8.3 Acción preventiva.
4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Nuevo requisito. 5.2.1 Provisión de recursos. 7.3 Resultados de la revisión.
4.3 Determinación del campo de aplicación del sistema de gestión de seguridad de la información.	4.2.1 Creación del SGSI. 4.2.3 Supervisión y revisión del SGSI. Nuevo requisito. 4.3.1 General. 4.3.2 Control de documentos.
4.4 Sistema de Gestión de Seguridad de la Información.	4. Requisitos generales. 5.2.1 Provisión de los recursos.
5. LIDERAZGO	
5.1 Liderazgo y compromiso.	4.2.1 Creación del SGSI. 5.1 Compromiso de la dirección. Nuevo requisito.
5.2 Política.	4.2.1 Creación del SGSI. 5.1 Compromiso de la dirección. 4.3.3 Control de registros. 4.3.1 Requisitos de la documentación. 4.3.2 Control de documentos.
5.3 Funciones, responsabilidades y autoridad en la organización.	5.1 Compromiso de la dirección. 6 Auditorías internas del SGSI. 4.3.3 Control de registros.
6. PLANIFICACIÓN	

6.1 Acciones para tratar los riegos y oportunidades.	4.2.1 Creación del SGSI. 8.3 Acción preventiva. Nuevo requisito. 4.2.2 Implementación y operación del SGSI.
6.1.2 Apreciación de Riesgos de Seguridad de la Información.	4.2.1 Creación del SGSI. Nuevo requisito. 5.1 Compromiso de la dirección.
6.1.2 Evaluación de Riesgos de Seguridad de la Información.	4.3.1 Requisitos de la documentación.
6.1.3 Tratamiento del Riesgo de Seguridad de la Información.	4.2.1 Creación del SGSI. Nuevo requisito. 4.3.1 Requisitos de la documentación. 4.2.2 Implementación y operación del SGSI.
6.2 Objetivos de seguridad de la información y planificación para su consecución.	5.1 Compromiso de la Dirección. Nuevo requisito. 4.2.3 Supervisión y revisión del SGSI. 4.3.1 Requisitos de la documentación. Nuevo requisito.
7. SOPORTE	
7.1 Recursos.	4.2.2 Implementación y operación del SGSI. 5.2.1 Provisión de recursos.
7.2 Competencia.	5.2.2 Concienciación, formación y capacitación.
7.3 Concienciación.	Nuevo requisito. 4.2.2 Implementación y operación del SGSI. 5.2.2 Concienciación, formación y capacitación.
7.4 Comunicación.	4.2.4 Mantenimiento y mejora del SGSI 5.1 Compromiso de la Dirección. Nuevo requisito.
7.5 Información documentada. 7.5.1 Generalidades	4.3.1 Requisitos de la documentación. Nuevo requisito.
7.5.2 Creación y actualización.	4.3.2 Control de documentos. Nuevo requisito.
7.5.3 Control de información documentada.	4.3.2 Control de documentos 4.3.3 Control de registros.
8. OPERACIÓN	
8.1 Planificación y control operacional.	Nuevo requisito 4.2.2 Implementación y operación del SGSI. 4.3.3 Control de registros.

	Nuevo requisito. 8.3 Acción preventiva.
8.2 Apreciación de los riesgos de seguridad de la información.	4.2.3 Supervisión y revisión del SGSI. 4.3.1 Requisitos de la documentación.
8.3 Tratamiento de los riesgos de seguridad de la información.	4.2.2 Implementación y operación del SGSI. 4.3.3 Control de registros.
9. EVALUACIÓN DEL DESEMPEÑO	
9.1 Seguimiento, medición, análisis y evaluación.	4.2.3 Supervisión y revisión del SGSI. 6. Auditorías internas del SGSI. 4.2.2 Implementación y operación del SGSI Nuevo requisito. 4.3.3 Control de registros.
9.2 Auditoría interna.	4.2.3 Supervisión y revisión del SGSI. 6 Auditorías internas del SGSI. 4.3.1 Requisitos de la documentación. 4.3.3 Control de registros.
9.3 Revisión por la dirección.	4.2.3 Supervisión y revisión del SGSI. 5.1 Compromiso de la dirección. 7.2 Datos iniciales de la revisión. Nuevo requisito. 4.3.3 Control de registros. 7.1 Generalidades.
10. MEJORA	
10.1 No conformidad y acciones correctivas.	8.2 Acción correctiva. 8.3 Acción preventiva. 4.2.4 Mantenimiento y mejora del SGSI. Nuevo requisito.
10.2 Mejora continua.	4.2.4 Mantenimiento y mejora del SGSI 5.2.1 Provisión de recursos 8.1 Mejora continua

Tabla 1 Comparación entre ISO 27001:2013 y 27001:2005

Si realizamos la misma tarea respecto a la ISO 27001:2013 y 27001:2005 se obtiene la siguiente tabla:

ANEXO A. ISO 27001:2013	ANEXO A. ISO 27001:2005
5. Políticas de seguridad de la información	5. Políticas de seguridad de la información
5.1 Dirección de gestión de seguridad de la información	5.1 Política de seguridad de la información
5.1.1 Políticas para la seguridad de la información	5.1.1 Documento de política de seguridad de la información
5.1.2 Revisión de las políticas de seguridad de la información	5.1.2. Revisión de la política de seguridad de la información
6. Organización de la seguridad de la información	6. Aspectos organizativos de la seguridad de la información
6.1 Organización interna	6.1 Organización interna
6.1.1 Roles y responsabilidades en seguridad de la información	6.1.3 Asignación de responsabilidades relativas a la seguridad de la información 8.1.1 Funciones y responsailidades
6.1.2 Segregación de tareas	10.1.3 Segregación de tareas
6.1.3 Contacto con las autoridades	6.1.6 Acuerdos de confidencialidad
6.1.4 Contacto con grupos de especial interés	6.1.7 Contacto con grupos de especial interés
6.1.5 Seguridad de la información en la gestión de proyectos	Nuevo control en ANEXO A. ISO 27001:2013
6.2 Teletrabajo y dispositivos móviles	11.7 Ordenadores portátiles y teletrabajo
6.2.1 Política de dispositivos móviles	11.7.1 Ordenadores portátiles y comunicaciones
6.2.2 Teletrabajo	11.7.2 Teletrabajo
7 Seguridad en recursos humanos	8 Seguridad en recursos humanos
7.1 Previo al empleo	8.1 Previo al empleo
7.1.1 Investigación de antecedentes	8.1.2 Investigación de antecedentes
7.1.2 Términos y condiciones del empleo	8.1.3 Términos y condiciones del empleo
7.2 Durante el empleo	8.2 Durante el empleo
7.2.1 Responsabilidades de gestión	8.2.1 Responsabilidades de la Dirección
7.2.2 Concienciación, educación y capacitación en seguridad de la información	8.2.2 Concienciación, formación y capacitación
7.2.3 Proceso disciplinario	8.2.3 Proceso disciplinario
7.3 Cambio y fin del empleo	8.3 Cese del empleo o cambio de puesto
7.3.1 Responsabilidades ante la finalización o cambio	8.3.1 Responsabilidad del cese o cambio
8. Gestión de activos	7. Gestión de activos
8.1 Responsabilidad sobre activos	7.1 Responsabilidad sobre activos

8.1.1 Inventario de activos	7.1.1 Inventario de activos
8.1.2 Propiedad de los activos	7.1.2 Propiedad de los activos
8.1.3 Uso aceptable de los activos	7.1.3 Uso aceptable de los activos
8.1.4 Devolución de los activos	7.1.4 Devolución de los activos
8.2 Clasificación de la información	7.2 Clasificación de la información
8.2.1 Clasificación de la información	7.2.1 Directrices de clasificación
8.2.2 Etiquetado de la información	7.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de la información	10.7.3 Procedimiento de manipulación de la información
8.3 Manipulación de soportes	10.7 Manipulación de soportes
8.3.1 Gestión de soportes extraíbles	10.7.1 Gestión de soportes extraíbles
8.3.2 Eliminación de soportes	10.7.2 Retirada de soportes
8.3.3 Soportes físicos en tránsito	10.8.3 Soportes físicos en tránsito
9. Control de acceso	11. Control de acceso
9.1 Requisitos de negocio para el control de acceso	11.1 Requisitos de negocio para el control de acceso
9.1.1 Política de control de acceso	11.1.1 Política de control de acceso
9.1.2 Acceso a las redes y a los servicios de red	11.4.1 Acceso a las redes y a los servicios de red
9.2 Gestión del acceso de usuarios	11.2 Gestión del acceso de usuarios
9.2.1 Registro y baja de usuario	11.2.1 Registro de usuario 11.5.2 Identificación y autenticación de usuario
9.2.2 Provisión de acceso de usuario	11.2.1 Registro de usuario
9.2.3 Gestión de privilegios de acceso	11.2.2 Gestión de privilegios
9.2.4 Gestión de la información secreta de autenticación de los usuarios	11.2.3 Gestión de contraseñas de usuario
9.2.5 Revisión de los derechos de acceso de usuario	11.2.4 Revisión de los derechos de acceso de usuario
9.2.6 Retirada o reasignación de los derechos de acceso	8.3.3 Retirada de los derecho de acceso
9.3 Responsabilidades del usuario	11.3 Responsabilidades de usuario
9.3.1 Uso de la información secreta de autenticación	11.3.1 Uso de contraseña
9.4 Control de acceso a sistemas y aplicaciones	11.6 Control de acceso a las aplicaciones y a la información
9.4.1 Restricción del acceso a la información	11.6.1 Restricción del acceso a la información
9.4.2 Procedimientos seguros de inicio de sesión	11.5.1 Procedimientos seguros de inicio de sesión

	11.5.5 Desconexión automática 11.5.6 Limitación del tiempo de conexión
9.4.3 Sistema de gestión de contraseñas	11.5.3 Sistemas de gestión de contraseñas
9.4.4 Uso de utilidades con privilegios del sistema	11.5.4 Uso de los recursos del sistema
9.4.5 Control de acceso al código fuente de programas	12.4.3 Control de acceso al código fuente de los programas
10. Criptografía	Nuevo dominio (parte de A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información)
10.1 Controles criptográficos	12.3 Controles criptográficos
10.1.1 Política de uso de los controles criptográficos	12.3.1 Política de uso de los controles criptográficos
10.1.2 Gestión de claves	12.3.2 Gestión de claves
11. Seguridad física y ambiental	9. Seguridad física y del entorno
11.1 Áreas seguras	9.1 Áreas seguras
11.1.1 Perímetro de seguridad física	9.1.1 Perímetro de seguridad física
11.1.2 Controles físicos de entrada	9.1.2 Controles físicos de entrada
11.1.3 Seguridad de oficinas, despachos y recursos	9.1.3 Seguridad de oficinas, despachos y recursos
11.1.4 Protección contra las amenazas externas y ambientales	9.1.4 Protección contra las amenazas externas y ambientales
11.1.5 El trabajo en áreas seguras	9.1.5 El trabajo en áreas seguras
11.1.6 Áreas de carga y descarga	9.1.6 Áreas de acceso público y de carga y descarga
11.2 Equipamiento	11.2 Seguridad de los equipos
11.2.1 Emplazamiento y protección de equipos	9.2.1 Emplazamiento y protección de equipos
11.2.2 Instalaciones de suministro	9.2.2 Instalaciones de suministro
11.2.3 Seguridad del cableado	9.2.3 Seguridad del cableado
11.2.4 Mantenimiento de los equipos	9.2.4 Mantenimiento de los equipos
11.2.5 Retirada de materiales propiedad de la empresa	9.2.7 Retirada de materiales propiedad de la empresa
11.2.6 Seguridad de los equipos fuera de las instalaciones	9.2.5 Seguridad de los equipos fuera de las instalaciones
11.2.7 Reutilización o eliminación de equipos	9.2.6 Reutilización o eliminación de equipos
11.2.8 Equipo de usuario desatendido	11.3.2 Equipo de usuario desatendido
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	11.3.3 Política de puesto de trabajo despejado y pantalla limpia

12. Seguridad en operaciones	Nuevo dominio (parte de A.10 Gestión de comunicaciones y operaciones)
12.1 Responsabilidades y procedimientos de operación	10.1 Responsabilidades y procedimientos de operación
12.1.1 Documentación de los procedimientos de operación	10.1.1 Documentación de los procedimientos de operación
12.1.2 Gestión de cambios	10.1.2 Gestión de cambios
12.1.3 Gestión de capacidades	10.3.1 Gestión de capacidades
12.1.4 Separación de los entornos de desarrollo, prueba y operación	10.1.4 Separación de los recursos de desarrollo, prueba y operación
12.2 Protección frente a malware	10.4 Protección contra código malicioso y descargable
12.2.1 Controles contra el código malicioso	10.4.1 Controles contra el código malicioso 10.4.2 Controles contra el código descargado
12.3 Copias de seguridad	10.5 Copias de seguridad
12.3.1 Copias de seguridad de la información	10.5.1 Copias de seguridad de la información
12.4 Registro y monitorización	10.10 Supervisión
12.4.1 Registro de eventos	10.10.1 Registro de auditorías 10.10.2 Supervisión del uso del sistema 10.10.5 Registro de fallos
12.4.2 Protección de la información de registro	10.10.3 Protección de la información de los registros
12.4.3 Registro de administración y operación	10.10.3 Protección de la información de los registros 10.10.4 Registros de administración y operación
12.4.4 Sincronización del reloj	10.10.6 Sincronización del reloj
12.5 Control del software en operación	Nuevo objetivo de control (parte de A.12.4 Seguridad de los archivos del sistema)
12.5.1 Instalación de software en explotación	12.4.1 Control del software en explotación
12.6 Gestión de vulnerabilidades técnicas	12.5 Seguridad en los procesos de desarrollo y soporte
12.6.1 Gestión de vulnerabilidades técnicas	12.6.1 Control de las vulnerabilidades técnicas
12.6.2 Restricciones en la instalación de software	Nuevo control en ANEXO A. ISO 27001:2013
12.7 Consideraciones sobre auditoría de los sistemas de información	15.3 Consideraciones sobre auditoría de los sistemas de información
12.7.1 Controles de auditoría de sistemas de información	15.3.1 Controles de auditoría de sistemas de información

13. Seguridad de las comunicaciones	Nuevo dominio (parte de A.10 Gestión de comunicaciones y operaciones)
13.1 Gestión de la seguridad de la red	10.6 Gestión de la seguridad de redes
13.1.1 Controles de red	10.6.1 Controles de red
13.1.2 Seguridad de los servicios de red	10.6.2 Seguridad de los servicios de red
13.1.3 Segregación en redes	11.4.2 Segregación de las redes
13.2 Transferencia de información	10.8 Intercambio de información
13.2.1 Políticas y procedimientos de transferencia de información	10.8.1 Políticas y procedimientos de transferencia de información
13.2.2 Acuerdos de intercambio de información	10.8.2 Acuerdos de intercambio de información
13.2.3 Mensajería electrónica	10.8.4 Mensajería electrónica
13.2.4 Acuerdos de confidencialidad o no revelación	6.1.5 Acuerdos de confidencialidad
14. Adquisición, desarrollo y mantenimiento de sistemas	12. Adquisición, desarrollo y mantenimiento de sistemas
14.1 Requisitos de seguridad en los sistemas de información	12.1 Requisitos de seguridad en los sistemas de información
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	12.1.1 Análisis de requisitos y especificaciones de seguridad de la información
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	10.9.1 Comercio electrónico 10.9.3 Información puesta a disposición pública
14.1.3 Protección de las transacciones de servicios de aplicaciones	10.9.2 Transacciones en línea
14.2 Seguridad en los procesos de desarrollo y soporte	12.6 Seguridad en desarrollo y proceso de soporte
14.2.1 Política de desarrollo seguro	Nuevo control en ANEXO A. ISO 27001:2013
14.2.2 Procedimientos de control de cambios en sistemas	12.5.1 Procedimientos de control de cambios en sistemas
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
14.2.4 Restricciones a los cambios en los paquetes de software	12.5.3 Restricciones a los cambios en los paquetes de software
14.2.5 Principios de ingeniería de sistemas seguros	Nuevo control en ANEXO A. ISO 27001:2013
14.2.6 Entornos de desarrollo seguro	Nuevo control en ANEXO A. ISO 27001:2013
14.2.7 Externalización del desarrollo de software	12.5.5 Externalización del desarrollo de software
14.2.8 Pruebas funcionales de seguridad de sistemas	Nuevo control en ANEXO A. ISO 27001:2013

14.2.9 Pruebas de aceptación de sistemas	10.3.2 Aceptación del sistema
14.3 Datos de prueba	Nuevo objetivo de control (parte 12.4 Seguridad de los archivos del sistema)
14.3.1 Protección de los datos de prueba	12.4.2 Protección de los datos de prueba
15. Relaciones con proveedores	Nuevo dominio (parte de 6.2 Terceros)
15.1 Seguridad de la información en las relaciones con proveedores	Nuevo objetivo de control
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Nuevo control en ANEXO A. ISO 27001:2013
15.1.2 Requisitos de seguridad en contratos con terceros	6.2.3 Tratamiento de la seguridad en contratos con terceros
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	Nuevo control en ANEXO A. ISO 27001:2013
15.2 Gestión de la entrega de los servicios prestados por proveedores	10.2 Gestión de la entrega de los servicios prestados por proveedores
15.2.1 Control y revisión de la provisión de servicios del proveedor	10.2.2 Control y revisión de la provisión de servicios del proveedor
15.2.2 Gestión de cambios en la provisión del servicio del proveedor	10.2.3 Gestión de cambios en la provisión del servicio del proveedor
16. Gestión de incidentes de seguridad de la información	13. Gestión de incidentes de seguridad de la información
16.1 Gestión de incidentes de seguridad de la información y mejoras	13.2 Gestión de incidentes de seguridad de la información y mejoras
16.1.1 Responsabilidades y procedimientos	13.2.1 Responsabilidades y procedimientos
16.1.2 Notificación de los eventos de seguridad de la información	13.1.1 Notificación de los eventos de seguridad de la información
16.1.3 Notificación de puntos débiles de la seguridad	13.1.2 Notificación de puntos débiles de la seguridad
16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	Nuevo control en ANEXO A. ISO 27001:2013
16.1.5 Respuesta a incidentes de seguridad de la información	Nuevo control en ANEXO A. ISO 27001:2013
16.1.6 Aprendizaje de los incidentes de seguridad de la información	13.2.2 Aprendizaje de los incidentes de seguridad de la información
16.1.7 Recopilación de evidencias	13.2.3 Recopilación de evidencias

17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio	14. Gestión de la continuidad de negocio
17.1 Continuidad en la seguridad de la información	14.1 Aspectos de la SI en la gestión de la continuidad del negocio
17.1.1 Planificación de la continuidad en seguridad de la información	14.1.2 Continuidad del negocio y evaluación de riesgos
17.1.2 Implementar la continuidad de la seguridad de la información	14.1.1 Inclusión de la SI en el proceso de gestión de la continuidad de negocio. 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la SI 14.1.4 Marco de referencia para la planificación de la continuidad de negocio
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad de negocio
17.1 Redundancias	Nuevo objetivo de control (parte de A14.1.2 Continuidad de negocio y evaluación de riesgos)
17.2.1 Disponibilidad de los recursos de tratamiento de la información	Nuevo control en ANEXO A. ISO 27001:2013
18. Cumplimiento	15 Cumplimiento
18.1 Cumplimiento con los requisitos legales y contractuales	15.1 Cumplimiento con los requisitos legales y contractuales
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	15.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
18.1.2 Derechos de propiedad intelectual (DPI)	15.1.2 Derechos de propiedad intelectual (DPI)
18.1.3 Protección de los registros de la organización	15.1.3 Protección de los documentos de la organización
18.1.4 Protección y privacidad de la información de carácter personal	15.1.4 Protección y privacidad de la información de carácter personal
18.1.5 Regulación de los controles criptográficos	15.1.6 Regulación de los controles criptográficos
18.2 Revisiones de seguridad de la información	15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico
18.2.1 Revisión independiente de la seguridad de la información	6.1.8 Revisión independiente de seguridad de la información
18.2.2 Cumplimiento de las políticas y normas de seguridad	15.2.1 Cumplimiento de las políticas y normas de seguridad

18.2.3 Revisión del cumplimiento técnico	15.2.2 Comprobación del cumplimiento técnico

Tabla 2 Comparación entre ISO 27002:2013 y 27002:2005

2.3 Selección de empresa

La implementación de la norma ISO 27001:2013 se realizará en la empresa Fictional S.L. Se trata de una PYME dedicada a la logística de mercancías de ámbito provincial con una única sede central.

Los principales servicios ofrecidos por Fictional son los siguientes: envío de mercancía convencional, envío de mensajería urgente 24 horas y el envío de mercancías peligrosas. Por volumen de facturación el servicio más importante es el de mercancías peligrosas. El servicio de 24 horas dispone de recargo en caso de pasar esta hora.

Fictional tiene 40 empleados de los cuales únicamente tienen relevancia en los sistemas de información las siguientes personas:

- Andrés, cuyo puesto es Gerente.
- Adrián, responsable de sistemas.
- Ana, responsable de RRHH.
- Aurelio, responsable de desarrollo.

Solo existe una persona que tenga la misma importancia que el gerente, su hijo Antonio pero en este caso es porque es el único chofer que dispone de carnet para transportar mercancías peligrosas y suele tener frecuentes bajas.

En cuanto al sistema de información, está ubicado en un “CPD” el cual tiene un climatizador y una cabina de discos para copias. En él se encuentran 4 servidores, uno que hace de AD y dominio, un servidor de correo, un servidor de aplicaciones (que se utiliza principalmente para el CRM) y un servidor web que se emplea para la plataforma B2C.

En cuanto a comunicaciones únicamente disponen de un router conectado por cable a los servidores, que a su vez es WiFi y da soporte al área de administración y gerencia que es la única que dispone de equipos.

En el lado de las aplicaciones, existen dos aplicaciones corporativas que dan soporte al negocio, un paquete CRM ubicado en el servidor de aplicaciones para obtener datos sobre los clientes, una aplicación B2C que se emplea para el servicio de mercancía peligrosa, los servicios 24h y convencional, éste corre sobre una base de datos mysql y un apache que están en el servidor de aplicaciones web. Se emplea Exchange en el servidor de correo.

A nivel de servicios internos se dispone del servicio de correo, servicio de AD y servicio de backup. Para el suministro eléctrico el proveedor es Iberdrola, en cuanto a telefonía y ADSL el proveedor es Telefónica y existe una empresa que ofrece soporte al desarrollo de la herramienta de B2C, por otra parte existe una sala de archivo en el que se guardan datos de clientes.

A nivel de datos todo se vertebra con datos de clientes que se emplean para todos los servicios, datos del CRM, datos de la herramienta B2C que se emplean para el servicio de mercancías peligrosas, datos de entregas y pedidos.

2.4 Alcance del SGSI

En el ámbito de un plan de Implementación de la ISO 27001:2013 es necesario indicar que partes de la organización estarán involucradas en el mismo. La determinación del alcance [3] del Sistema de Gestión de la Seguridad de la Información permitirá obtener una visión más detallada sobre los límites de la implantación.

El alcance de un SGSI puede variar en función del tamaño de la organización, volumen de la información tratada, número de clientes, volúmenes de activos físicos y lógicos, número de sedes u oficinas… Con el fin de discernir qué elementos formarán parte del alcance, se considerarán aquellas que por sus funciones y responsabilidades ayuden en primera instancia a dar cumplimiento a la misión institucional.

Respecto al caso del proyecto actual, el alcance del SGSI en Fictional S.L. estará determinado por los sistemas de información que dan soporte a los servicios de envío de mercancías, según la declaración de aplicabilidad vigente.

2.5 Análisis diferencial

Uno de los pasos más importantes antes de iniciar la implementación de la ISO 27001:2013 en una organización, es conocer el estado inicial de la misma según los requerimientos de la norma y el anexo A.

El análisis diferencial permite obtener el nivel en el que se encuentra una organización en torno a la seguridad de la información. Para valorar los requisitos de la norma se ha seguido el Modelo de Madurez de la Capacidad [4]. Se trata de un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al software. Este modelo establece un conjunto de prácticas o procesos clave agrupados en Áreas Clave de Proceso (KPA – Key Process Area).
Para cada área de proceso se definen un conjunto de buenas prácticas que se deben de seguir:

- Definidas en un procedimiento documentado.
- Provistas de los medios y formación necesarios.
- Ejecutadas de un modo sistemático, universal y uniforme.
- Medidas
- Verificadas

Estas áreas de proceso se agrupan en cinco niveles de madurez, de tal modo que si una organización consigue obtener institucionalizadas todas las prácticas en un nivel, se considera que ha alcanzado ese nivel de madurez.

Los niveles en los que se pueden clasificar estos procesos o en este caso, los requerimientos de la norma ISO 27001 son los siguientes:

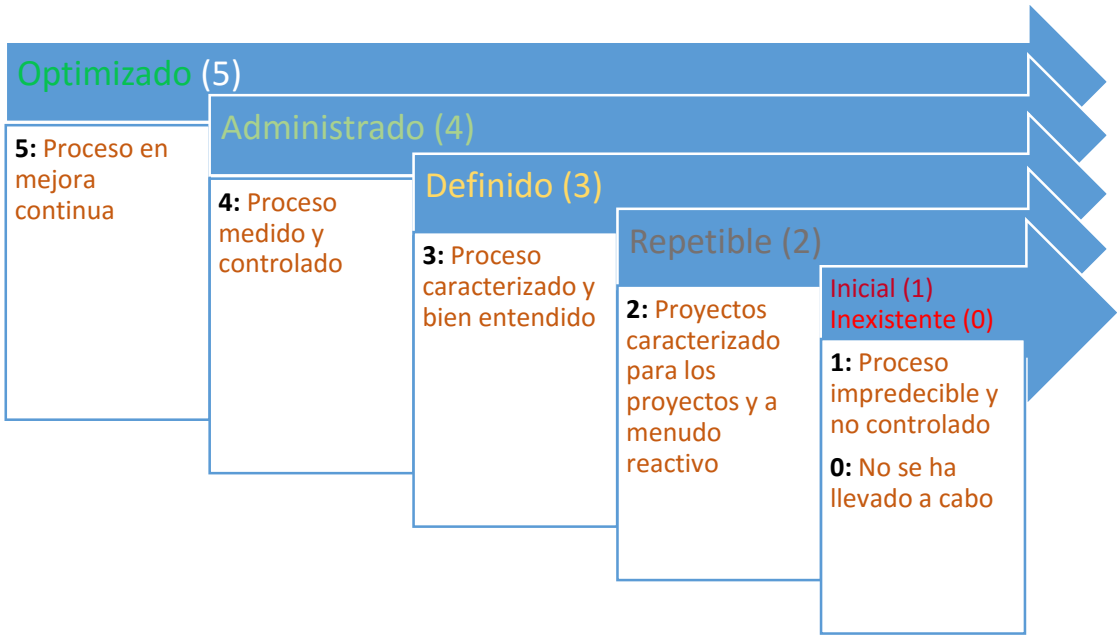


Ilustración 4 CMM (elaboración propia)

En primer lugar se ha realizado el análisis diferencial sobre la ISO 27001:2013 y en segundo lugar sobre el anexo A de la misma o ISO 27002:2013.

La valoración realizada sobre Fictional S.L. se basa en los apartados de la norma ISO 27001:2013 del 4 al 10.

4) Contexto de la organización: se encuentra documentado las partes relevantes en el ámbito de la seguridad de la información pero no los requisitos ni el alcance del sistema de gestión de seguridad.

- Valor actual: 1.

5) Liderazgo: la alta dirección de Fictional ha demostrado un cierto nivel de compromiso respecto al sistema de gestión de seguridad de la información ya que ha decidido invertir en ella. No obstante no existe una política de seguridad de la información ni están documentados los roles, responsabilidades y autoridades de la empresa.

- Valor actual: 1.

6) Planificación: no se ha llevado a cabo anteriormente ningún análisis de riesgos y por tanto no existe un tratamiento de los mismos.

- Valor actual: 0.

7) Soporte: la organización no ha determinado ni proporcionado los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora 0continúa del sistema de gestión de seguridad de la información.

- Valor actual: 0.

8) Operación: la compañía Fictional ha analizado a muy alto nivel algunos riesgos de seguridad de la información pero sin que se propongan o produzcan modificaciones sobre ellos y sin tener en cuenta el punto 6) Planificación.

- Valor actual: 1.

9) Evaluación del desempeño: actualmente no se está evaluando el desempeño de la seguridad de la información ni la eficacia del sistema de gestión de seguridad de la información al no existir dicho SGSI.

- Valor actual: 0.

10) Mejora: la compañía Fictional no dispone de un Plan de Acciones Correctivas al no existir no conformidades en auditorías anteriores. Por tanto no se está llevando a cabo una mejora continua en la empresa.

- Valor actual: 0.

Estos valores se desea que aumenten a medio plazo y a largo plazo, para ello se ha realizado la siguiente tabla y gráfico radial con el que se puede discernir a simple vista cual es el estado actual respecto a la ISO 27001:2013 y donde se desea llegar.

Requisitos	CMM Actual	CMM Objetivo medio plazo	CMM Objetivo largo plazo
Contexto de la organización	1	4	5
Liderazgo	1	3	4
Planificación	0	4	5
Soporte	0	4	5
Operación	1	4	5
Evaluación del desempeño	0	3	4
Mejora	0	4	5

Tabla 3 Análisis diferencial ISO 27001:2013 – Fictional S.L.

Ilustración 5 Análisis diferencial ISO 27001:2013 – Fictional S.L.

Respecto al análisis diferencial de la ISO 27002:2013, los resultados son los siguientes:

No.	Control	CMM actual	CMM objetivo MP	CMM objetivo LP
MARCO DE CONTROLES				
5	5. Políticas de seguridad de la información	0	3	5
5.1	Dirección de gestión de seguridad de la información	0	3	5
5.1.1	Políticas para la seguridad de la información	0	3	5
5.1.2	Revisión de las políticas de seguridad de la información	0	3	5
6	6. Organización de la seguridad de la información	1	2	3
6.1	Organización interna	1	3	5
6.1.1	Roles y responsabilidades en seguridad de la información	0	3	5
6.1.2	Segregación de tareas	0	3	5
6.1.3	Contacto con las autoridades	1	3	5

6.1.4	Contacto con grupos de especial interés	0	3	5
6.1.5	Seguridad de la información en la gestión de proyectos	0	3	5
6.2	Teletrabajo y dispositivos móviles	0	0	0
6.2.1	Política de dispositivos móviles	0	0	0
6.2.2	Teletrabajo	0	0	0
7	7. Seguridad en recursos humanos	1	3	5
7.1	Previo al empleo	2	3	5
7.1.1	Investigación de antecedentes	2	3	5
7.1.2	Términos y condiciones del empleo	2	3	5
7.2	Durante el empleo	1	3	5
7.2.1	Responsabilidades de gestión	1	3	5
7.2.2	Concienciación, educación y capacitación en seguridad de la información	0	3	5
7.2.3	Proceso disciplinario	0	3	5
7.3	Cambio y fin del empleo	1	3	5
7.3.1	Responsabilidades ante la finalización o cambio	1	3	5
8	8. Gestión de activos	1	3	5
8.1	Responsabilidad sobre activos	1	3	5
8.1.1	Inventario de activos	1	3	5
8.1.2	Propiedad de los activos	0	3	5
8.1.3	Uso aceptable de los activos	1	3	5
8.1.4	Devolución de los activos	0	3	5
8.2	Clasificación de la información	0	3	5
8.2.1	Clasificación de la información	0	3	5
8.2.2	Etiquetado de la información	0	3	5
8.2.3	Manipulación de la información	0	3	5
8.3	Manipulación de soportes	1	3	5
8.3.1	Gestión de soportes extraíbles	1	3	5
8.3.2.	Eliminación de soportes	1	3	5

8.3.3	Soportes físicos en tránsito	1	3	5
9	9. Control de acceso	1	3	5
9.1	Requisitos de negocio para el control de acceso	1	3	5
9.1.1	Política de control de acceso	1	3	5
9.1.2	Acceso a las redes y a los servicios de red	1	3	5
9.2	Gestión del acceso de usuarios	1	3	5
9.2.1	Registro y baja de usuario	1	3	5
9.2.2	Provisión de acceso de usuario	1	3	5
9.2.3	Gestión de privilegios de acceso	1	3	5
9.2.4	Gestión de la información secreta de autenticación de los usuarios	1	3	5
9.2.5	Revisión de los derechos de acceso de usuario	1	3	5
9.2.6	Retirada o reasignación de los derechos de acceso	1	3	5
9.3	Responsabilidades del usuario	1	3	5
9.3.1	Uso de la información secreta de autenticación	1	3	5
9.4	Control de acceso a sistemas y aplicaciones	1	3	5
9.4.1	Restricción del acceso a la información	1	3	5
9.4.2	Procedimientos seguros de inicio de sesión	1	3	5
9.4.3	Sistema de gestión de contraseñas	1	3	5
9.4.4	Uso de utilidades con privilegios del sistema	1	3	5
9.4.5	Control de acceso al código fuente de programas	1	3	5
10	10. Criptografía	0	0	0
10.1	Controles criptográficos	0	0	0
10.1.1	Política de uso de los controles criptográficos	0	0	0
10.1.2	Gestión de claves	0	0	0
11	11. Seguridad física y ambiental	2	4	5

11.1	Áreas seguras	2	3	5
11.1.1	Perímetro de seguridad física	2	3	5
11.1.2	Controles físicos de entrada	2	3	5
11.1.3	Seguridad de oficinas, despachos y recursos	2	3	5
11.1.4	Protección contra las amenazas externas y ambientales	2	3	5
11.1.5	El trabajo en áreas seguras	2	3	5
11.1.6	Áreas de carga y descarga	2	3	5
11.2	Equipamiento	2	4	5
11.2.1	Emplazamiento y protección de equipos	2	3	5
11.2.2	Instalaciones de suministro	2	3	5
11.2.3	Seguridad del cableado	2	3	5
11.2.4	Mantenimiento de los equipos	2	3	5
11.2.5	Retirada de materiales propiedad de la empresa	2	5	5
11.2.6	Seguridad de los equipos fuera de las instalaciones	2	3	5
11.2.7	Reutilización o eliminación segura de equipos	2	3	5
11.2.8	Equipo de usuario desatendido	1	3	5
11.2.9	Política de puesto de trabajo despejado y pantalla limpia	1	3	5
12	12. Seguridad en operaciones	1	3	5
12.1	Responsabilidades y procedimientos de operación	1	3	5
12.1.1	Documentación de los procedimientos de operación	1	3	5
12.1.2	Gestión de cambios	0	3	5
12.1.3	Gestión de capacidades	0	3	5
12.1.4	Separación de los entornos de desarrollo, prueba y operación	1	3	5
12.2	Protección frente a malware	1	3	5
12.2.1	Controles contra el código malicioso	1	3	5

12.3	Copias de seguridad	2	3	5
12.3.1	Copias de seguridad de la información	2	3	5
12.4	Registro y monitorización	0	3	5
12.4.1	Registro de eventos	0	3	5
12.4.2	Protección de la información de registro	0	3	5
12.4.3	Registro de administración y operación	0	3	5
12.4.4	Sincronización del reloj	2	3	5
12.5	Control del software en operación	0	3	4
12.5.1	Instalación de software en explotación	0	3	4
12.6	Gestión de vulnerabilidades técnicas	1	3	5
12.6.1	Gestión de vulnerabilidades técnicas	1	3	5
12.6.2	Restricciones en la instalación de software	1	3	5
12.7	Consideraciones sobre auditoría de los sistemas de información	0	3	5
12.7.1	Controles de auditoría de sistemas de información	0	3	5
13	13. Seguridad de las comunicaciones	1	3	5
13.1	Gestión de la seguridad de la red	1	3	5
13.1.1	Controles de red	1	3	5
13.1.2	Seguridad de los servicios de red	1	3	5
13.1.3	Segregación en redes	1	3	5
13.2	Transferencia de información	1	3	5
13.2.1	Políticas y procedimientos de transferencia de información	0	3	5
13.2.2	Acuerdos de intercambio de información	1	3	5
13.2.3	Mensajería electrónica	1	3	5
13.2.4	Acuerdos de confidencialidad o no revelación	1	3	5
14	14. Adquisición, desarrollo y mantenimiento de sistemas	1	3	5

14.1	Requisitos de seguridad en los sistemas de información	1	3	5
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	1	3	5
14.1.2	Asegurar los servicios de aplicaciones en redes públicas	0	3	5
14.1.3	Protección de las transacciones de servicios de aplicaciones	0	3	5
14.2	Seguridad en los procesos de desarrollo y soporte	1	3	5
14.2.1	Política de desarrollo seguro	1	3	5
14.2.2	Procedimientos de control de cambios en sistemas	1	3	5
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	0	3	5
14.2.4	Restricciones a los cambios en los paquetes de software	0	3	5
14.2.5	Principios de ingeniería de sistemas seguros	0	3	5
14.2.6	Entornos de desarrollo seguro	1	3	5
14.2.7	Externalización del desarrollo de software	0	3	5
14.2.8	Pruebas funcionales de seguridad de sistemas	0	3	5
14.2.9	Pruebas de aceptación de sistemas	0	3	5
14.3	Datos de prueba	0	3	5
14.3.1	Protección de los datos de prueba	0	3	5
15	15. Relaciones con proveedores	1	3	5
15.1	Seguridad de la información en las relaciones con proveedores	1	3	5
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	1	3	5

15.1.2	Requisitos de seguridad en contratos con terceros	1	3	5
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	1	3	5
15.2	Gestión de la entrega de los servicios prestados por proveedores	1	3	5
15.2.1	Control y revisión de la provisión de servicios del proveedor	1	3	5
15.2.2	Gestión de cambios en la provisión del servicio del proveedor	1	3	5
16	16. Gestión de incidentes de seguridad de la información	0	3	5
16.1	Gestión de incidentes de seguridad de la información y mejoras	0	3	5
16.1.1	Responsabilidades y procedimientos	0	3	5
16.1.2	Notificación de los eventos de seguridad de la información	0	3	5
16.1.3	Notificación de puntos débiles de la seguridad	0	3	5
16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	0	3	5
16.1.5	Respuesta a incidentes de seguridad de la información	0	3	5
16.1.6	Aprendizaje de los incidentes de seguridad de la información	0	3	5
16.1.7	Recopilación de evidencias	0	3	5
17	17. Aspectos de seguridad de la información en la gestión de la continuidad de negocio	1	3	5
17.1	Continuidad en la seguridad de la información	0	3	5
17.1.1	Planificación de la continuidad en seguridad de la información	0	3	5

17.1.2	Implementar la continuidad de la seguridad de la información	0	3	5
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	0	3	5
17.1	Redundancias	1	3	5
17.2.1	Disponibilidad de los recursos de tratamiento de la información	1	3	5
18	18. Cumplimiento	2	3	5
18.1	Cumplimiento con los requisitos legales y contractuales	2	3	4
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	2	3	5
18.1.2	Derechos de propiedad intelectual (DPI)	2	3	5
18.1.3	Protección de los registros de la organización	2	3	5
18.1.4	Protección y privacidad de la información de carácter personal	2	3	5
18.1.5	Regulación de los controles criptográficos	0	0	0
18.2	Revisiones de seguridad de la información	1	3	5
18.2.1	Revisión independiente de la seguridad de la información	1	3	5
18.2.2	Cumplimiento de las políticas y normas de seguridad	0	3	5
18.2.3	Revisión del cumplimiento técnico	1	3	5

Tabla 4 Análisis diferencial ISO 27002:2013 – Fictional S.L.

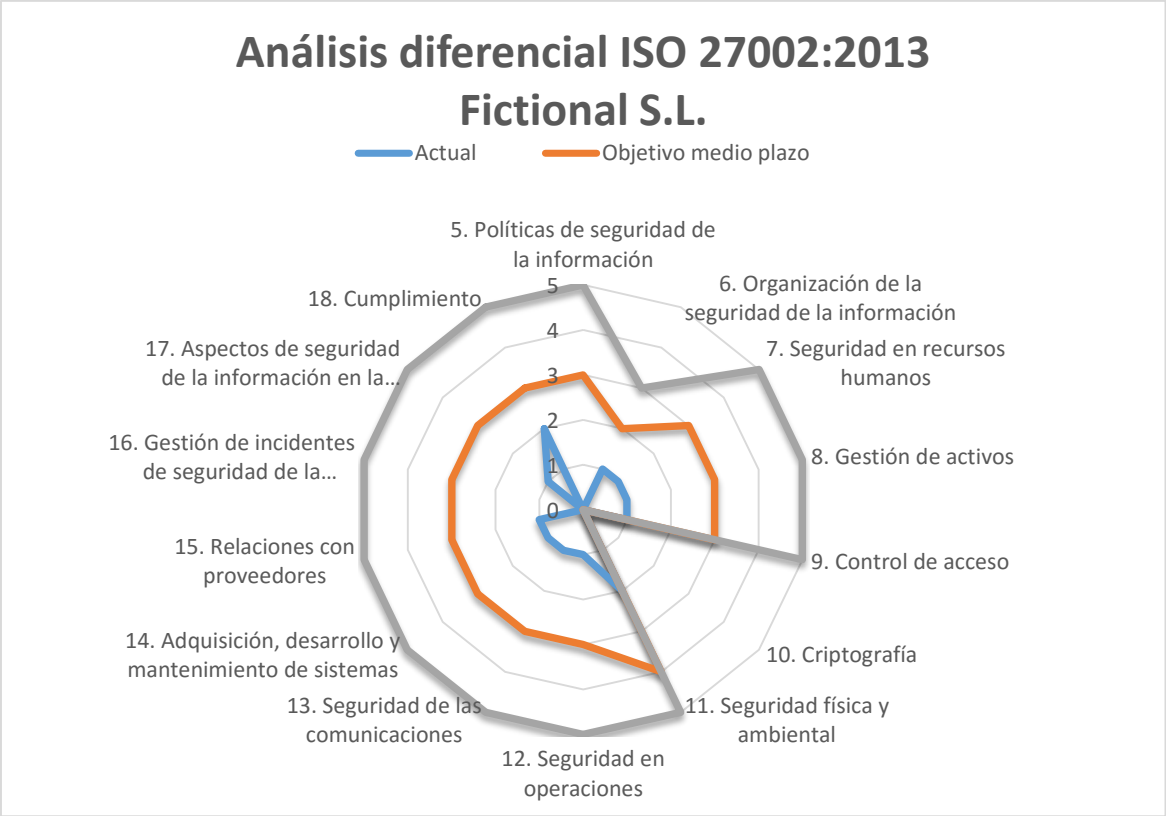


Ilustración 6 Análisis diferencial ISO 27002:2013 – Fictional S.L.

Una vez realizado el análisis diferencial de la ISO 27001:2013 y el anexo de buenas prácticas, se obtiene una visión del estado de seguridad de la organización Fictional. Esta visión se puede valorar actualmente como inmadura.

Se deberá realizar un esfuerzo por parte del Comité de Dirección para que la situación mejore considerablemente. Para ello se establecerán una serie de objetivos a partir de los cuales mediante le implantación de la ISO 27001:2013, la compañía Fictional logrará una mayor madurez de sus sistemas de información.

2.6 Objetivos Plan Director de Seguridad

Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información dirigido a reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.

Es fundamental para la realización de un buen Plan Director de Seguridad o PDS que recoja los objetivos estratégicos de la empresa, la definición del alcance y las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización así como terceros que colaboran con ésta.

Para llevar a cabo el PDS se van a realizar las siguientes fases o etapas:

1. Situación actual: Contextualización, objetivos y análisis diferencial.
2. Sistema de Gestión Documental
3. Análisis de riesgos
4. Propuesta de Proyectos
5. Auditoría de Cumplimiento de la ISO 27002:2013
6. Presentación de resultados y entrega de Informes.

Durante las diferentes fases del PDS se pretenderá que se cumplan una serie de objetivos. Tal y como indica la ISO 27001, estos objetivos de seguridad de la información se deberán establecer en las funciones y niveles que la organización desee. Dichos objetivos de seguridad deben de ser coherentes con la política de seguridad de la información, medibles (si es posible), comunicados y actualizados.

En primer lugar se establecerán una serie de objetivos de alto nivel, los cuales se consideran para la organización Fictional S.L. los más relevantes a corto plazo. Estos objetivos han sido aprobados por el Comité de Dirección y han conllevado a una serie de objetivos específicos que se deberán de tratar a partir de un listado de acciones expuesto a continuación. Para ello se ha seguido la siguiente estructura:

- [OAN_XX] Objetivo de Alto Nivel
    - [OBN_XX] Objetivo de Bajo Nivel
        - Acción:
        - Medible:

- **[OAN_01]** Conocer el grado de los riesgos a los que está expuesta la organización.
    - **[OBN_01]** Reducir el nivel de vulnerabilidades sobre los activos IT más sensibles para la organización.
        - Acción: se realizará un análisis de riesgos a partir de la metodología MAGERIT.
        - Medible: comparación de resultados de una prueba de ‘pentest’ previa y posterior al análisis de riesgos y la implantación de salvaguardas.

- **[OAN_02]** Mejorar el nivel de formación y concienciación de los empleados de la organización.

    - **[OBN_02]** Aumentar el número de horas de formación en seguridad de la información
        - Acción: impartir sesiones a los empleados en concienciación de seguridad de la información.
        - Medible: comparación de resultados al realizar un test de concienciación en seguridad de la información antes y después de los cursos.

- **[OAN_03]** Garantizar la continuidad de los servicios que presta la organización ante una posible catástrofe.

    - **[OBN_03]** Reducir el tiempo de restauración de las funciones críticas de la organización.
        - Acción: realizar un plan de Continuidad de Negocio IT.
        - Medible: tiempo medio de restauración < X horas.

- **[OAN_04]** Aumentar la confianza en los clientes ofreciendo a su vez una imagen más seria de cara a la competencia.

    - **[OBN_04]** Obtener la certificación ISO 27001:2013 por una entidad certificadora.
        - Acción: reducción de no conformidades de la auditoría interna a realizar.
        - Medible: ¿Se obtiene certificación? Sí o no.

    - **[OBN_04.1]** Reducir el número de incidentes de seguridad no tratados.
        - Acción: Implantar una herramienta de ‘ticketing’ para la gestión de incidencias.
        - Medible: (número de incidentes no tratos / número de incidentes de seguridad) < X

- **[OAN_05]** Aumentar la disponibilidad de los procesos de negocio de la organización.

    - **[OBN_05]** Aumentar disponibilidad de la aplicación B2C
        - Acción: Implantar un servidor web de respaldo en un CPD alternativo del que dispone la organización.
        - Medible: nº de caídas de la aplicación < X

3. Fase 2: Sistema de gestión documental

3.1 Introducción

Durante la implantación de la ISO 27001:2013 en una organización, se requiere de una serie de acciones o tareas que conllevan a su vez la necesidad de documentar información sobre ellas. Por ejemplo, cómo se van a realizar, quien las va a realizar, que recursos se van a necesitar, la periodicidad de las mismas, etc.

Si nos situamos sobre la ISO 27001:2013, podemos observar como en la mayoría de apartados a implementar en una organización se requiere de una documentación asociada y se indica de la siguiente forma:

"La organización debe conservar información documentada sobre el proceso de […]"

Podemos afirmar que los sistemas de gestión tienen como base un sistema de gestión documental, el cual debe de cumplir una serie de requisitos según indica la norma:

"La información documentada requerida por el sistema de gestión de seguridad de la información y por esta norma internacional se debe controlar para asegurarse de que:

a) *Esté disponible y preparada para su uso, dónde y cuándo se necesite;*
b) *Esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).*

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

c) *Distribución, acceso, recuperación y uso;*
d) *Almacenamiento y preservación, incluida la preservación de la legibilidad;*
e) *Control de cambios (por ejemplo, control de la versión);*
f) *Retención y disposición.*

La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión de seguridad de la información se debe identificar y controlar, según sea adecuado."

Con el fin de abordar los requisitos como disponibilidad, confidencialidad e integridad de la documentación del Sistema de Gestión de Seguridad de la Información, la organización Fictional S.L. dispondrá de un repositorio documental en el cual se almacenarán todos los procedimientos, normativas y documentos asociados con el SGSI.

3.2 Esquema documental

El esquema documental [5] de un SGSI está compuesto por una serie de políticas, manuales, normativas y procedimientos. Este esquema documental debe de ir creándose y actualizándose en función de las necesidades de cada organización. Tal y como indica la norma ISO 27001:2013:

"Cuando se crea y se actualiza la información documentada, la organización debe asegurarse, en la manera que corresponda, de lo siguiente:

a) *La identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);*
b) *El formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);*
c) *La revisión y aprobación con respecto a la idoneidad y adecuación."*

Para lo que este proyecto requiere, en el caso de Fictional S.L., se desarrollará el cuerpo básico documental del SGSI. Dicho cuerpo estará compuesto por los siguientes documentos:

Nomenclatura: SGSI - Procedimiento o Política de Seguridad - Apartado al que referencia o Apartado al que referencia del Anexo – Numeración _ Nombre del procedimiento

SGSI-PS-Política de seguridad.

SGSI-P-09-01_Gestión de indicadores.

SGSI-P-10-02_Procedimiento de acciones correctivas y no conformidades.

SGSI-P-A.06-01_Asignación de responsabilidades.

SGSI-P-A.08-01_Clasificación y tratamiento de la información.

SGSI-P-A.18-01_Procedimiento de Auditorías Internas.

3.2.1 SGSI-PS-Política de seguridad

Las organizaciones deben definir una "política de seguridad de la información" al máximo nivel que sea aprobado por la Dirección y establezca el enfoque de la organización para gestionar sus objetivos de seguridad de la información. [6]

La política de seguridad se encuentra en el documento "SGSI-PS-Política de seguridad".

Fictional S.L.	MANUAL DE PROCEDIMIENTOS CONFIDENCIAL	SGSI-PS Revisión: 01 Fecha: 20/03/2016 Página: 1 de 5
SGSI-PS-Política de seguridad		

Ilustración 7 Índice "SGSI-PS-Política de seguridad"

3.2.2 SGSI-P-09-01_Gestión de indicadores

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información. Para ello debe establecer indicadores que puedan llegar a medir la eficacia, formación y concienciación de la entidad en el ámbito de la seguridad de la información.

Estos indicadores pueden ir asociados tanto a los controles como a los objetivos de seguridad. En este procedimiento se determinarán indicadores asociados a los objetivos de seguridad indicados en la fase anterior ya que actualmente se desconocen los controles que justifican y los que no para Fictional S.L.

La gestión de indicadores se encuentra en el documento “SGSI-P-09-01_Gestión de indicadores”.

Fictional S.L.	MANUAL DE PROCEDIMIENTOS CONFIDENCIAL	SGSI-P-09-01 Revisión: 01 Fecha: 20/03/2016 Página: 1 de 4
SGSI-P-09-01_Gestión de indicadores		

Ilustración 8 Índice “SGSI-P-09-01_Gestión de indicadores”

3.2.3 SGSI-P-10-01_Procedimiento de acciones correctivas y no conformidades

Todo sistema implantado requiere de un mantenimiento que permita la prevención y corrección de anomalías detectadas, la norma ISO 27001 así lo contempla dentro del establecimiento y gestión del Sistema de Gestión de Seguridad de la Información.

El procedimiento de acciones correctivas y no conformidades se encuentra en el documento “SGSI-P10-01_Procedimiento de acciones correctivas y no conformidades”.

Fictional S.L.	MANUAL DE PROCEDIMIENTOS CONFIDENCIAL	SGSI-PS Revisión: 01 Fecha: 21/03/2016 Página: 1 de 6
SGSI-P-10-01_Procedimiento de acciones correctivas y no conformidades		

Ilustración 9 Índice “SGSI-P-10-01_Procedimiento de acciones correctivas y no conformidades.

3.2.4 SGSI-P-A.06-01_Asignación de responsabilidades

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización.

El procedimiento de asignación de responsabilidades se encuentra en el documento “SGSI-P-06-01_Asignación de responsabilidades”

Ilustración 10 Índice "SGSI-P-A.06-01_Asignación de responsabilidades.

3.2.5 SGSI-P-A.08-01_Clasificación y tratamiento de la información

La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizada.

El procedimiento de clasificación y tratamiento de la información se encuentra en el documento "SGSI-P-A.08-01_Clasificación y tratamiento de la información"

Ilustración 11 Índice "SGSI-P-A.08-01_Clasifiación y tratamiento de la información"

3.2.6 SGSI-P-A.18-01_Procedimiento de Auditorías Internas

La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de seguridad de la información cumple con los requisitos propios de la organización para su sistema de gestión de seguridad de la información y los requisitos de esta norma internacional.

El procedimiento de auditorías internas se encuentra en el documento "SGSI-P-A.18-01_Procedimiento de Auditorías Internas"

Ilustración 12 Índice "SGSI-P-A.18-01_Procedimiento de Auditorías internas"

4. Fase 3: Análisis de riesgos

4.1 Introducción

Previo a introducir el concepto de análisis de riesgos y su importancia en la implantación de un Sistema de Gestión de Seguridad de la Información, es necesario entender los conceptos básicos como riesgos, amenazas y vulnerabilidades.

Se considera riesgo a la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él causando daños a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegen de forma adecuada.

Los eventos que pueden desencadenar un incidente, produciendo daños materiales o inmateriales en los activos se denominan amenazas. Estas amenazas pueden llevarse a cabo si los grupos de activos no están protegidos al igual que sus vulnerabilidades.

Por ello, cuando se habla de vulnerabilidades, se refiere a las debilidades que tienen los activos y que pueden ser aprovechadas por una amenaza. Además de estos tres conceptos básicos, existen una serie de términos que facilitarán la comprensión del por qué es necesario llevar a cabo un análisis de riesgos.

- **Impacto**: es la consecuencia de la materialización de una amenaza sobre un activo.

- **Riesgo intrínseco**: es la posibilidad de que se produzca un impacto determinado en un activo.

- **Salvaguarda**: es la práctica, procedimiento o mecanismo que reduce el riesgo. Pueden actuar disminuyendo el impacto o la probabilidad.

- **Riesgo residual**: se trata del riesgo que queda tras la aplicación de la salvaguarda. Eliminar el riesgo al 100% es imposible, por tanto siempre habrá un riesgo residual.

Una vez se han definido los conceptos necesarios para desarrollar un análisis de riesgos, se podría decir que se trata de un proceso que consiste en identificar los riesgos a los que está expuesta una organización, con el objetivo de determinar su magnitud e identificar las áreas que requieren implantar salvaguardas.

A través del análisis de riesgos, una organización podrá conocer el impacto económico de un fallo de seguridad y la probabilidad de que ocurra dicho fallo. Además, se podrá cubrir las necesidades de seguridad de la organización teniendo en cuenta los recursos con los que cuenta.

El análisis de riesgos por tanto aporta objetividad a los criterios en los que se apoya la seguridad de la organización, ya que su objetivo es proteger los activos con mayor criticidad. Esto permite a la organización gestionar los riesgos por sí misma y ayuda a la toma de decisiones en función de los riegos propios.

Con el fin de evitar la subjetividad durante el análisis de riesgos, es importante que se cuente con la colaboración de diferentes áreas de la compañía y no únicamente con el área propietaria del activo. De esta forma se evitará la subjetividad que pueda tener el responsable de dicho activo.

Por otro lado, el análisis de riesgos debe utilizar unos criterios definidos con claridad que se puedan reproducir sucesivamente. Esto es necesario para que se pueda ir comparando el nivel de riesgo en una organización conforme se va mejorando el Sistema de Gestión de Seguridad de la Información.

El proceso del análisis de riesgos debe estar documentado para poder justificar las acciones que se van a desarrollar y conseguir el nivel de seguridad que la organización desea alcanzar.

Para ello, existen diferentes metodologías que pueden facilitar la realización de un análisis de riesgos. Estas metodologías indican los pasos a seguir para su correcta ejecución, ya que puede conllevar una gran multitud de variables.

Entre las diferentes metodologías para elaborar un análisis de riesgos, se encuentran: MAGERIT, OCTAVE, NIST SP 800-30, CRAMM, MEHARI… Para el presente proyecto, se utilizará la metodología MAGERIT, puesto que se encuentra extendida en las organizaciones como una de las metodologías más recomendables.

4.2 Metodología MAGERIT

MAGERIT [7] hace referencia a las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones. Esta metodología cubre la fase de Análisis y Gestión de Riesgos.

Esta metodología ha sido elaborada por el Consejo Superior de Administración Electrónica (CSAE), Ministerio De Hacienda Y Administración Pública – Gobierno de España, como respuesta a la percepción de que la Administración y en general toda la sociedad, dependen de forma creciente de las tecnologías de información para el cumplimiento de su misión.

MAGERIT tiene una visión estratégica global de la Seguridad de los Sistema de Información. Esta visión comienza en un modelo de análisis y gestión de riesgos que comprende tres modelos: entidades, eventos y procesos.

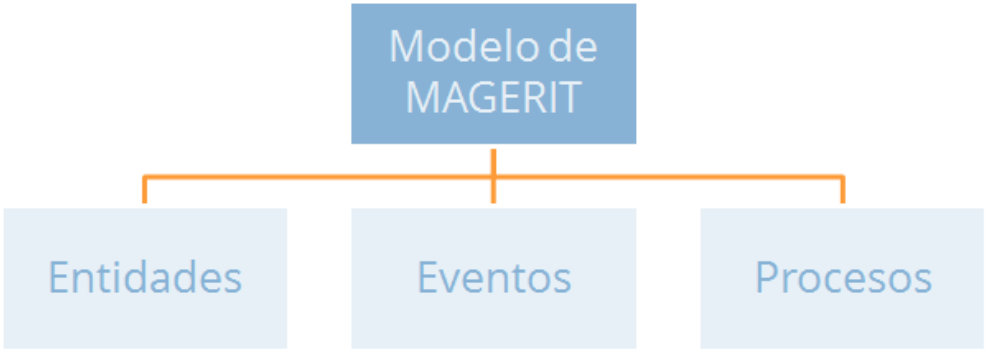


Ilustración 13 Modelo MAGERIT Fuente: http://www.pmg-ssi.com/

Este modelo está conformado por siete fases, las cuales se seguirán en el presente proyecto, excepto pequeñas modificaciones que puedan ser realizadas por las particularidades de la empresa Fictional.

Las fases recomendadas por la metodología MAGERIT para realizar el análisis de riesgo, son las siguientes ocho:

1. Identificación y agrupación de activos

En esta fase se identifican los activos relacionados con los procesos de negocio y que deben por tanto que protegerse. Estos activos se agrupan en función de sus características y tipo:

- Capa de negocio
  - Servicios
  - Datos
- Servicios internos
- Equipamiento
  - Aplicaciones
  - Equipos
    - Servidores
  - Comunicaciones
    - Router, IPS, FW
    - Switch
    - Terminadores de túneles
  - Elementos auxiliares
- Servicios subcontratados
- Instalaciones
- Personal
  - Departamentos críticos
  - Personal crítico

2. Establecimiento de las dependencias entre activos

En la segunda fase se establecen las dependencias entre los distintos activos de un modo jerarquizado y de acuerdo con lo establecido en la metodología MAGERIT, evaluando el grado de vinculación expresado en tanto por ciento y en función de los siguientes parámetros:

- **Disponibilidad**, es decir, en qué grado nos afecta el hecho de que el servicio o los datos estimados no se encuentren disponibles durante un periodo de tiempo significativo.

- **Integridad** de los datos, o hasta qué punto podemos asumir y afecta la corrupción o pérdida de los mismos.

- **Confidencialidad** de los datos, es decir, las implicaciones que suponen la pérdida de confidencialidad mediante el acceso a éstos por personas no autorizadas.

- **Autenticidad** de los usuarios del servicio y de quien accede a los datos, es decir, hasta qué punto es de necesidad disponer de las garantías suficientes para conocer la autoría o propiedad de la información.

- **Trazabilidad** del servicio y de los datos, o la garantía de poder realizar un seguimiento de quien y que información ha sido accedido, modificada o eliminada en todo momento.

Establecer la dependencia entre los activos es necesario para poder categorizar el riesgo acumulado en los servicios ofrecidos por Fictional.

3. Evaluación de los servicios

En la tercera fase se realiza una valoración de los servicios ofrecidos por Fictional así como la información empleada en dicha gestión, dentro del alcance del SGSI. La valoración se realiza en función de los distintos aspectos que comprende la seguridad:

- **Disponibilidad**: propiedad de la información por la que se garantiza que ésta se encuentra accesible únicamente en el momento que es requerida.

- **Integridad**: propiedad de la información por la que se garantiza que ésta no ha sido modificada o alterada de forma no autorizada durante el tratamiento.

- **Confidencialidad**: propiedad de la información por la que se garantiza que ésta se encuentra accesible únicamente a personal autorizado para su acceso.

- **Autenticidad**: propiedad de la información por la que se garantiza la autoría y la propiedad de la información.

- **Trazabilidad**: propiedad de la información por la que se garantiza poder realizar un seguimiento de quien y que información ha sido accedido, modificada o eliminada en todo momento.

Destacar que no todas estas variables afectan a servicios o información, siendo las variables aplicables las siguientes:

Dimensión	Servicio final	Información
Disponibilidad	Aplica	No aplica
Integridad	No aplica	Aplica
Confidencialidad	No aplica	Aplica
Autenticidad	Aplica	No aplica
Trazabilidad	Aplica	No aplica

Tabla 5 Servicio – Dimensiones – Servicio - Información

Los criterios que se han seguido para realizar la valoración son los propuestos en la guía CCN 803 STIC *Valoración de los sistemas.* En esta guía se concreta la forma en la que se evalúan los servicios de acuerdo con los criterios del Esquema Nacional de Seguridad y que son aplicables a la ISO 27001.

Bajo
Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
1. La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.
2. El sufrimiento de un daño menor por los activos de la organización.
3. El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4. Causar un perjuicio menor a algún individuo, que aun siendo molesto pueda ser fácilmente reparable.
5. RTO 1 día – 5 días
6. Otros de naturaleza análoga.

Tabla 6 Criterio valoración de servicios "Bajo" en MAGERIT

Medio
Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
1. La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.
2. El sufrimiento de un daño significativo por los activos de la organización.
3. El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4. Causar un perjuicio significativo a algún individuo, de difícil reparación.
5. RTO 4 horas – 1 día
6. Otros de naturaleza análoga.

Tabla 7 Criterio valoración de servicios "Medio" en MAGERIT

Alto
Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
1. La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
2. El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
3. El incumplimiento grave de alguna ley o regulación.
4. Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5. RTO <4 horas
6. Otros de naturaleza análoga.

Tabla 8 Criterio valoración de servicios "Alto" en MAGERIT

4. Identificación de las amenazas

En la cuarta fase, una vez se han identificado los activos y se han valorado, se procede a identificar las posibles amenazas a las que estos están expuestos. Es recomendable no relacionar más de 5 amenazas por activo, ya que de lo contrario la complejidad y envergadura del proyecto crece de manera difícilmente controlable.

5. Probabilidad de amenazas y estimación de impacto

En la quinta fase se determina la probabilidad de suceso, o frecuencia potencial, de una amenaza de acuerdo con el tiempo aproximado para que se materialice. Se define la frecuencia potencial de ocurrencia pudiendo ser “Baja”, “Medio”, “Alta”, “Muy Alta”, de acuerdo a la escala siguiente:

Valor	Frecuencia real
	N/A
Bajo	1 en 10 años
Medio	1 en 1 años
Alto	10 en 1 año
Muy alto	100 en 1 año

Tabla 9 Valor - Frecuencia de amenazas en MAGERIT

Además en esta fase también se especifica en qué grado afecta a las dimensiones de seguridad DICAT (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad) el impacto al materializarse la amenaza. El grado se va a determinar cuantitativamente en función de si el impacto es “N/A”, “Bajo”, “Medio”, “Alto” y “Muy Alto”.

- **N/A**: La amenaza no tiene implicaciones relevantes sobre la dimensión DICAT considerada.

- **Bajo**: Las implicaciones de la amenaza sobre la dimensión DICAT considerada generan un problema menor y limitado que implica un plan de acciones ya definido previamente, y no tiene repercusiones de mayor nivel.

- **Medio**: Las implicaciones de la amenaza sobre la dimensión DICAT considerada generan un problema menor aunque evidente a nivel financiero, operacional o reputacional, ante el que no hay definido un plan de acciones.

- **Alto**: Las implicaciones de la amenaza sobre la dimensión DICAT considerada afecta significativamente al funcionamiento de la universidad pero no influye en su continuidad ni en la consecución de sus objetivos de negocio, aunque requiere un esfuerzo de gestión y coordinación para su mitigación.

- **Muy Alto**: Las implicaciones de la amenaza sobre la dimensión DICAT considerada afecta de manera grave al funcionamiento de la universidad y pone en peligro la consecución de objetivos de negocio, e incluso su continuidad a corto/medio plazo.

La siguiente tabla muestra el porcentaje de afectación de la amenaza al materializarse en función del valor:

Valor	Porcentaje de afectación
N/A	0
Bajo	1
Medio	10
Alto	50
Muy alto	90
Total	100

Tabla 10 Valor- Impacto de la amenaza en MAGERIT

6. Evaluación del riesgo potencial

En la sexta fase se extrae el riesgo potencial al que están expuestos los servicios de la organización. Para cada uno de los servicios se evalúan las cinco dimensiones de la seguridad DICAT, y para cada una de ellas se consideran las amenazas que le pueden afectar, obteniendo de este modo un valor numérico agregado, resultado de valorar el impacto y la probabilidad de cada uno de los pares servicio / amenaza en esa dimensión en concreto.

Los valores que obtenidos están comprendidos entre 0 y 10, y se consideran significativos los valores iguales o superiores a 0,80, si bien este baremo es orientativo y se pueden variar en función del riesgo que se pretende asumir.

7. Aplicación de controles

Una vez se han evaluado los riesgos potenciales se analizan las salvaguardas implantadas o a implantar en la organización para eliminar o minimizar los riesgos mediante el documento de selección de controles, obteniendo así los riesgos efectivos sobre los activos según la tabla resultante de la fase anterior.

Para reflejar el actual estado del riesgo en el ámbito de la seguridad de la información, a la hora de realizar el análisis de riesgos deben contemplarse las medidas de seguridad implantadas en la entidad.

En este sentido la manera de aplicar los controles al análisis de riesgos, se realiza en base al CMM (grado de madurez) de los controles implantados en la organización. El CMM se corresponde con el siguiente esquema.

- **L0-No existente**: no se lleva a cabo el control
- **L1-Inicial**: el control se realiza sin frecuencia predefinida de un modo totalmente informal, ni existe un procedimiento claramente definido
- **L2-Repetible**: el control se realiza de un modo periódico, pero sin estar claramente definido a nivel documental

- **L3-Definido**: el control se implementa periódicamente, de un modo formal y se encuentra documentado.
- **L4-Gestionado**: el control se implementa periódicamente, de un modo formal, se encuentra documentado y se mide su eficiencia periódicamente mediante métricas
- **L5-Optimizado**: el control se implementa periódicamente, de un modo formal, se encuentra documentado, se mide su eficiencia periódicamente mediante métricas y se aborda un proceso de la mejora continua e innovación del control.

Cabe destacar que la aplicación engloba un conjunto de salvaguardas bajo los controles y existen ciertos solapes de controles, lo que implica que al seleccionar determinado nivel de madurez en un control existe la posibilidad de que modifique los valores anteriormente introducidos. Es por eso que cuando en el campo referente al dominio de control aparece un rango quiere que decir que dentro del dominio existen controles con valores comprendidos en dicho rango.

8. Evaluación del riesgo residual

Tras la obtención del riesgo potencial y la determinación del grado de madurez alcanzado en la implantación de los controles aplicables por la ISO 27002, se determina el riesgo al que se encontraría sometido la entidad tras la aplicación de los controles.

Una vez se han identificado las fases que se desarrollarán en el análisis de riesgos a partir de la metodología MAGERIT, para el desarrollo del mismo se utilizará la herramienta PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos).

Se trata de un software desarrollado en Java por el Centro Nacional de Inteligencia – Centro Criptológico Nacional y con colaboración del MAP. Esta herramienta permite realizar un enfoque tanto cualitativo como cuantitativo para el análisis de riesgos. En el presente proyecto se realizará un análisis de riesgos cualitativo.

Se trata de una herramienta con un alto grado de aceptación por parte de las Administraciones Públicas.

4.3 Identificación y agrupación de activos

Los activos [8] con mayor relevancia en los procesos de negocio de Fictional son los siguientes:

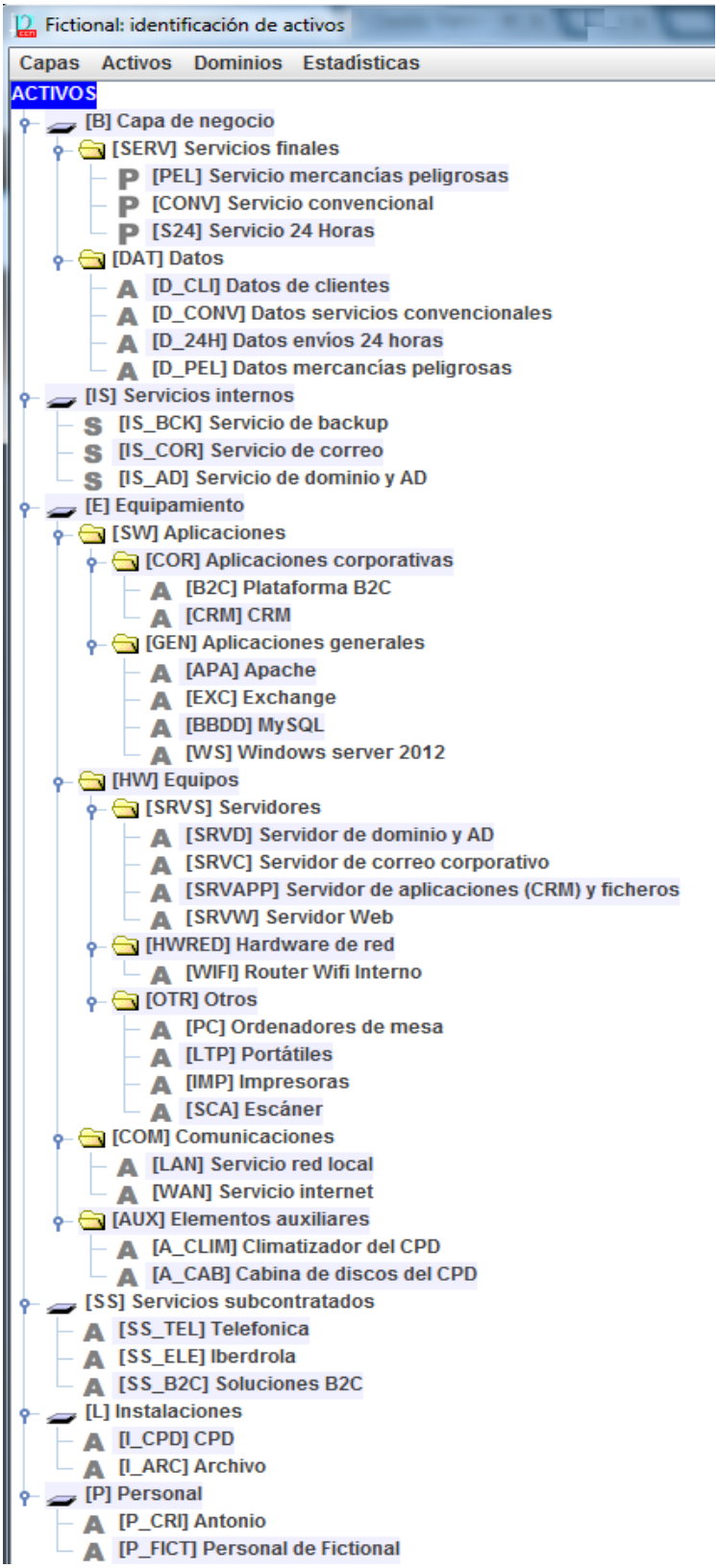


Ilustración 14 Activos identificados

4.4 Dependencias entre activos

Se valoran los servicios ofrecidos por Fictional así como la información empleada en dicha gestión:

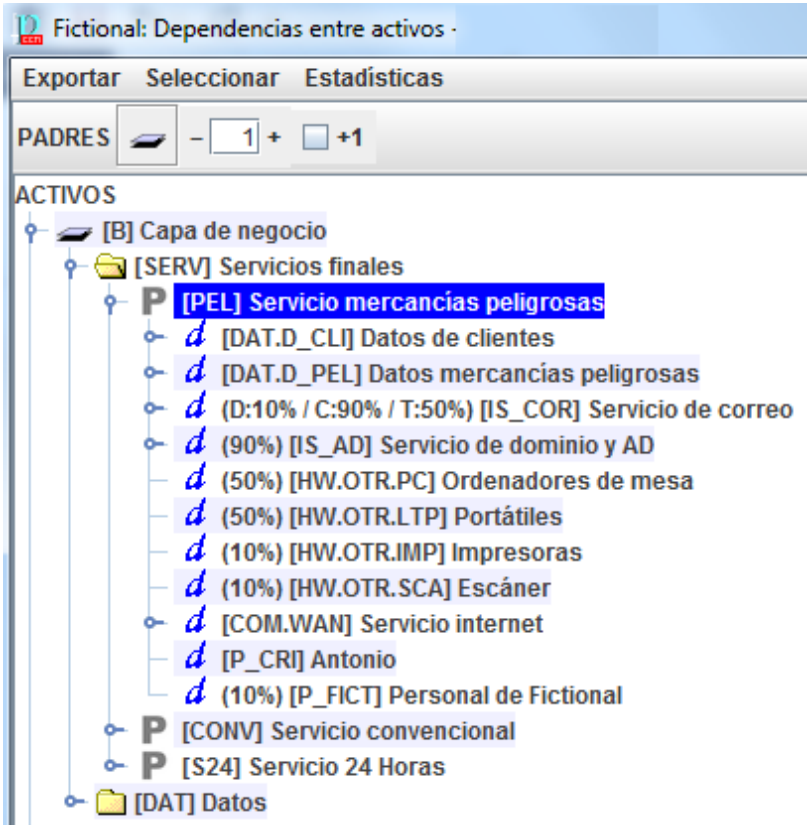


Ilustración 15 Dependencias agrupadas en Servicio mercancías peligrosas

Ilustración 16 Dependencias desplegadas en Servicio mercancías peligrosas

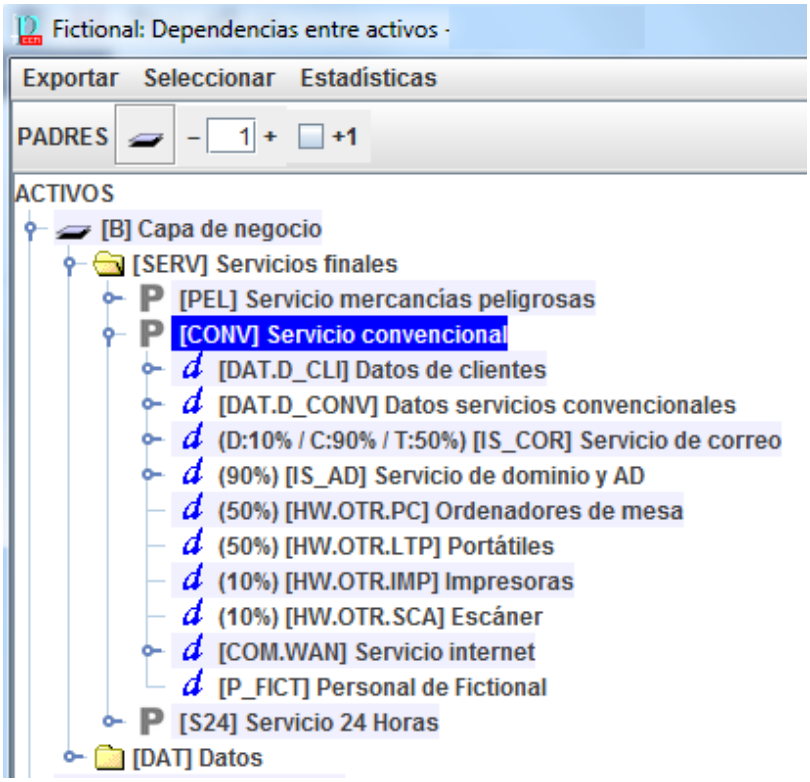


Ilustración 17 Dependencias agrupadas en Servicio convencional

Ilustración 18 Dependencias desplegadas en Servicio convencional

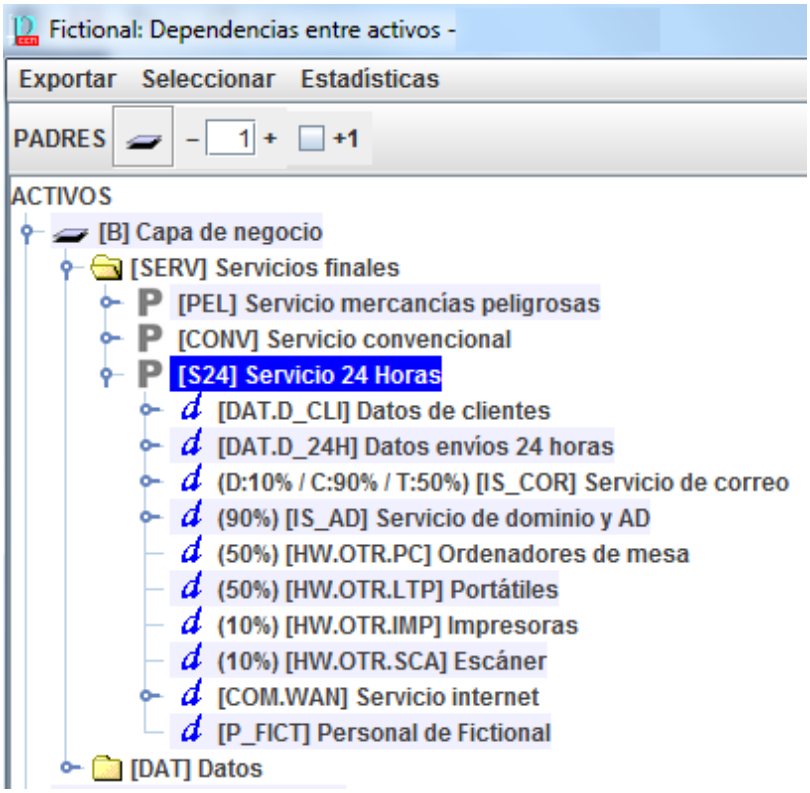


Ilustración 19 Dependencias agrupadas en Servicio 24 horas

Ilustración 20 Dependencias desplegadas en Servicio 24 horas

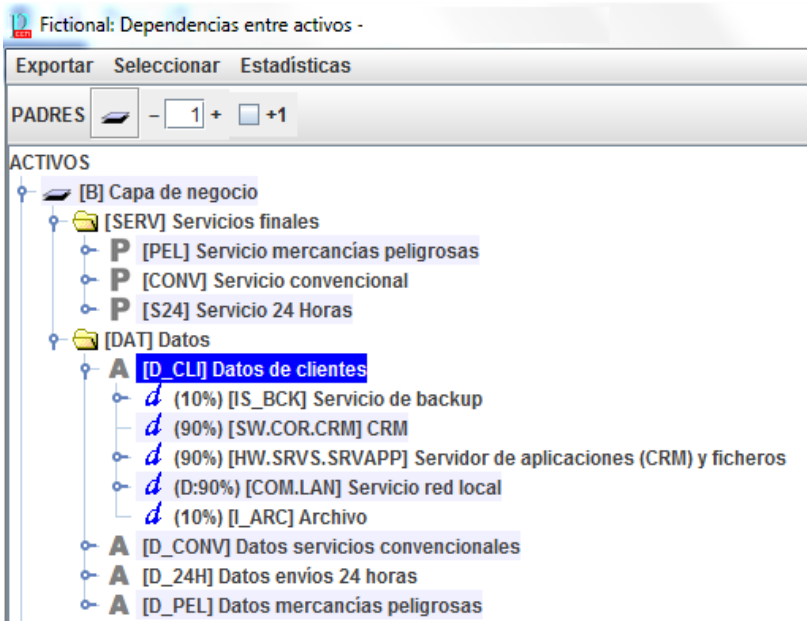


Ilustración 21 Dependencias agrupadas Datos de clientes

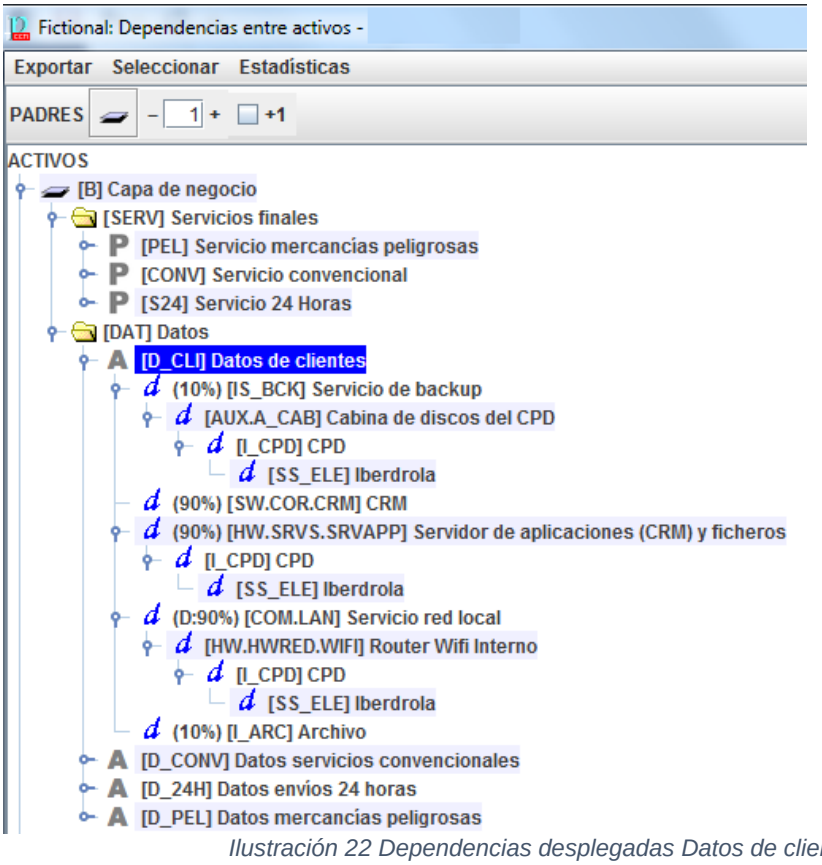


Ilustración 22 Dependencias desplegadas Datos de clientes

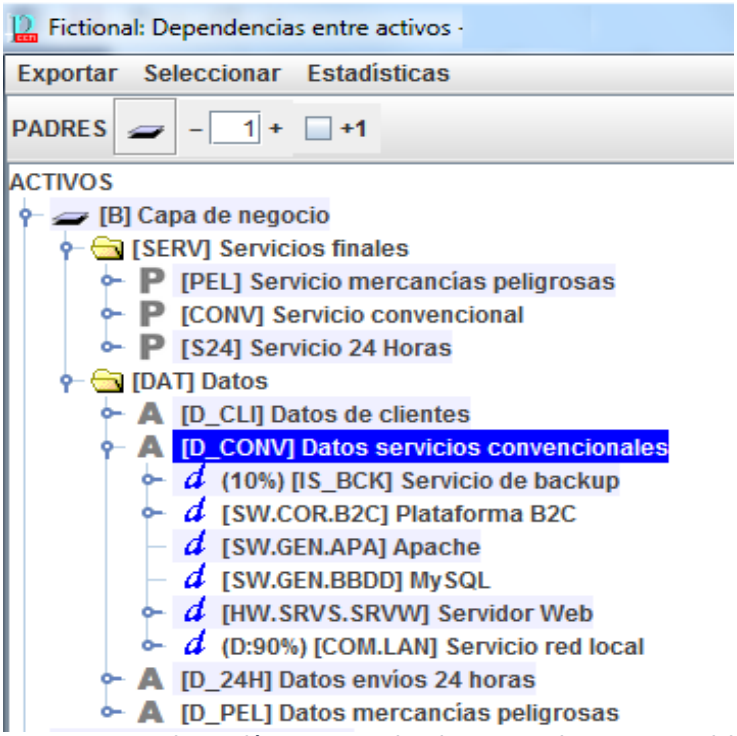


Ilustración 23 Dependencias agrupadas Datos servicios convencionales

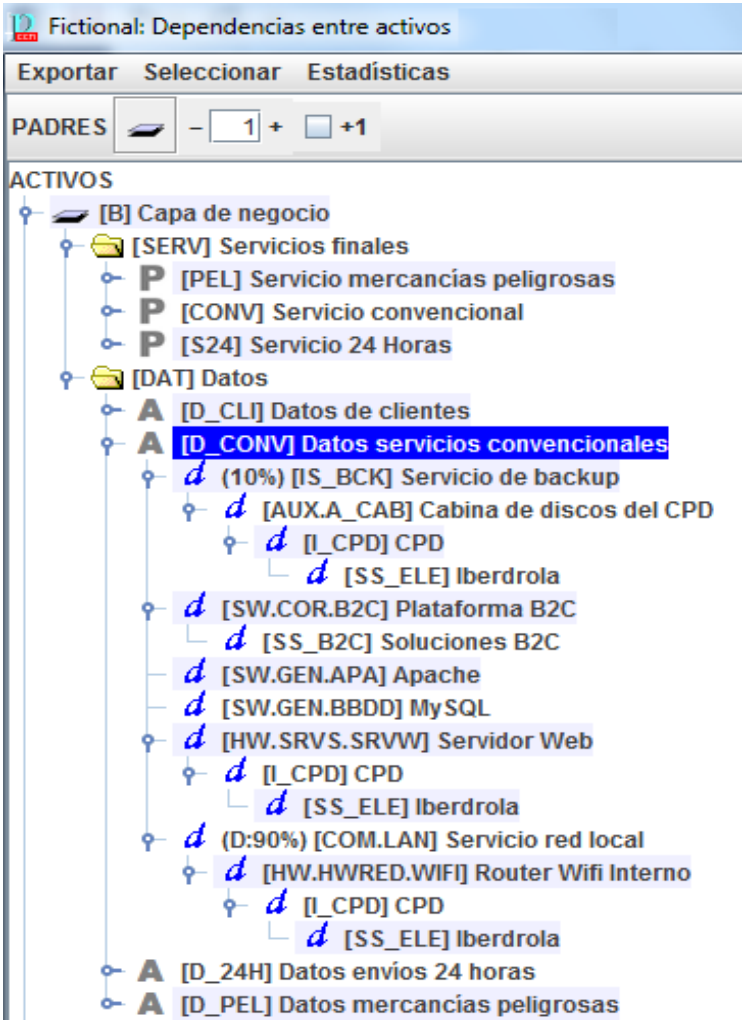


Ilustración 24 Dependencias desplegadas Datos servicios convencionales

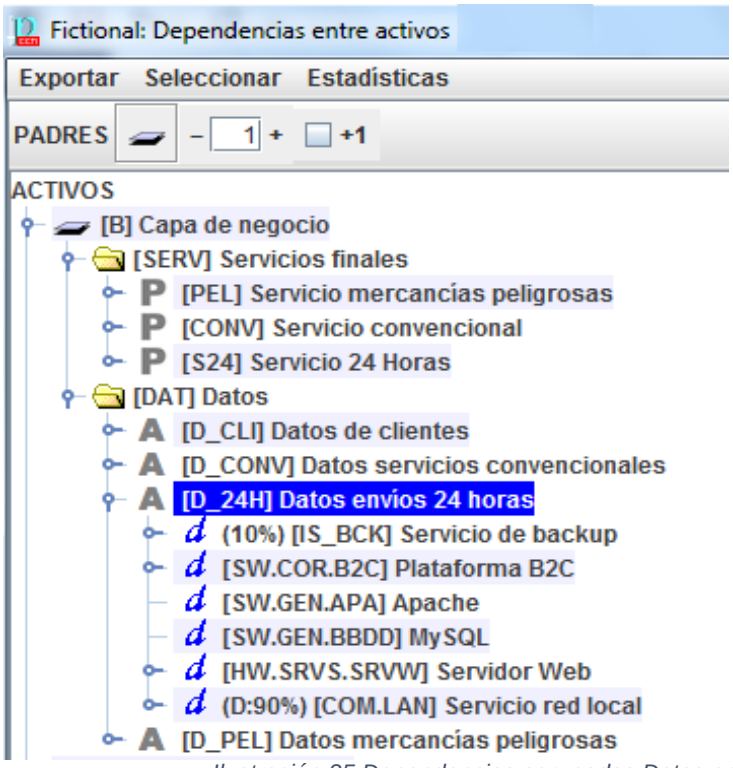


Ilustración 25 Dependencias agrupadas Datos envíos 24 horas

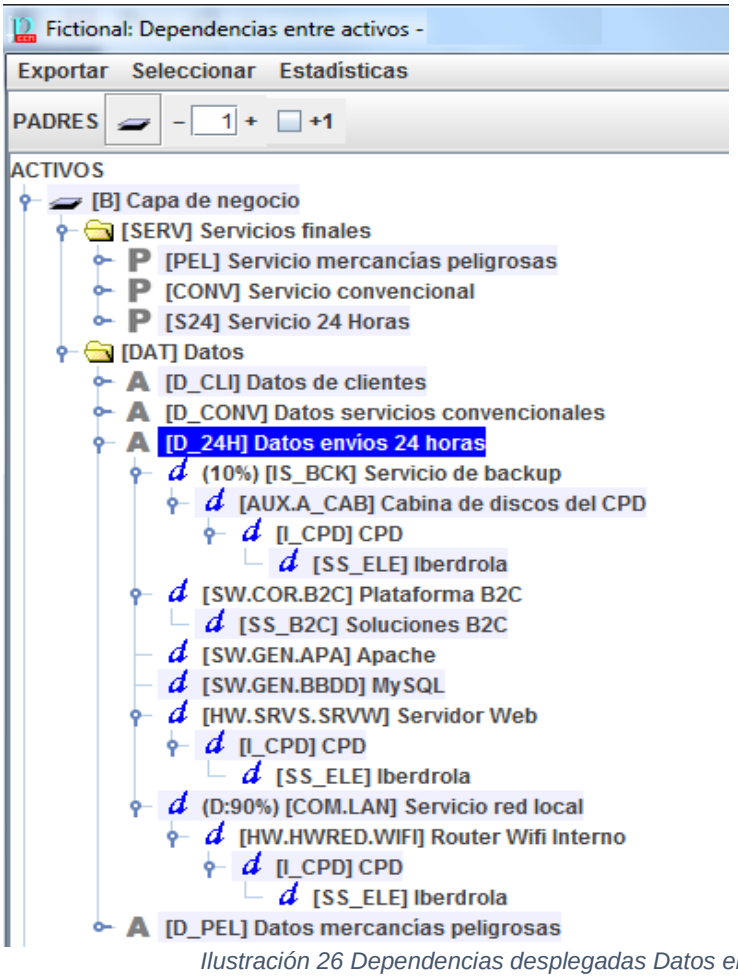


Ilustración 26 Dependencias desplegadas Datos envíos 24 horas

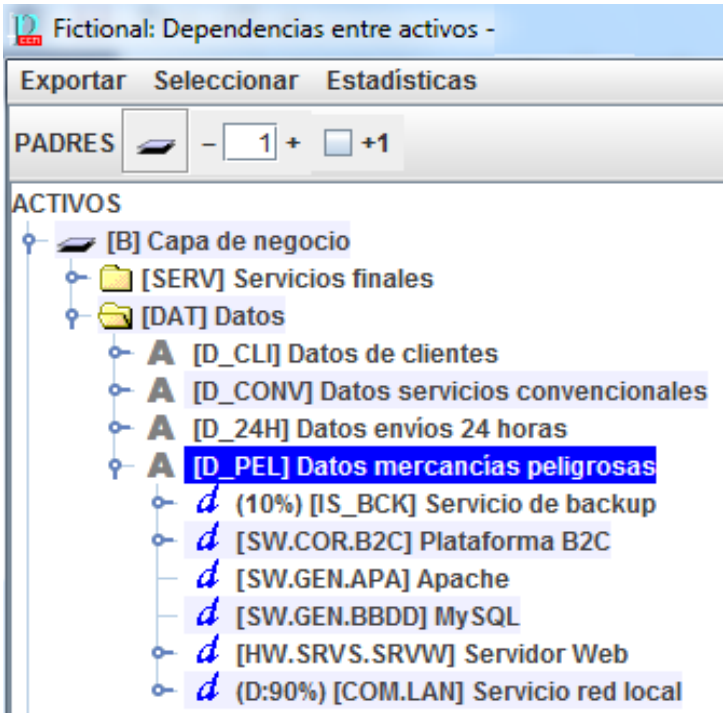


Ilustración 27 Dependencias agrupadas Datos mercancías peligrosas

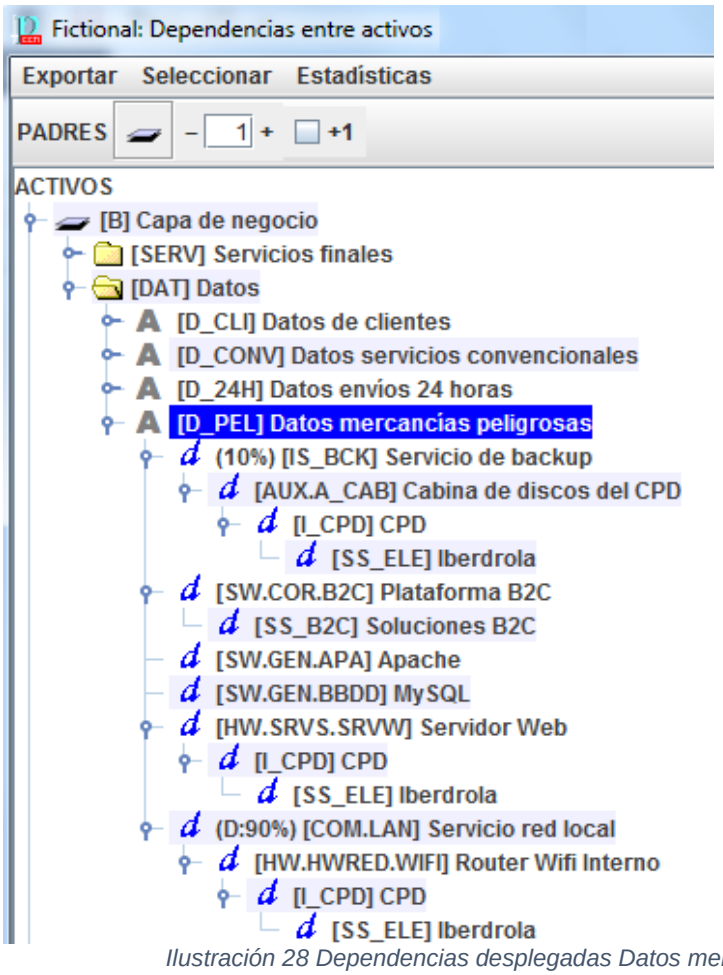


Ilustración 28 Dependencias desplegadas Datos mercancías peligrosas

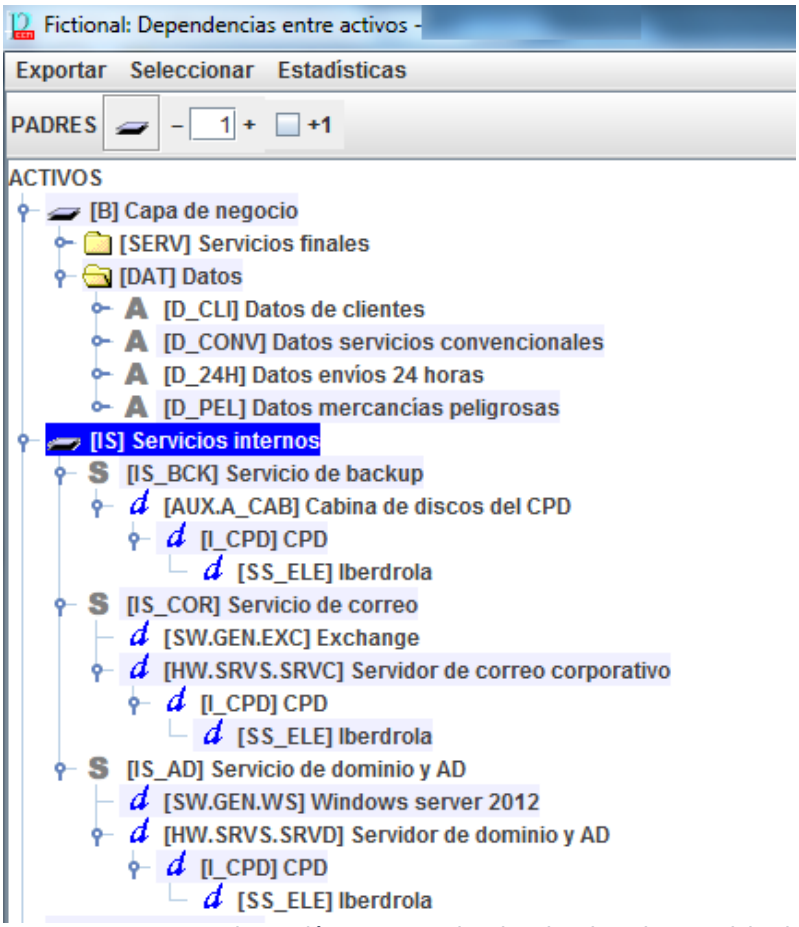


Ilustración 29 Dependencias desplegadas Servicios internos

Ilustración 30 Dependencias desplegadas Equipamiento

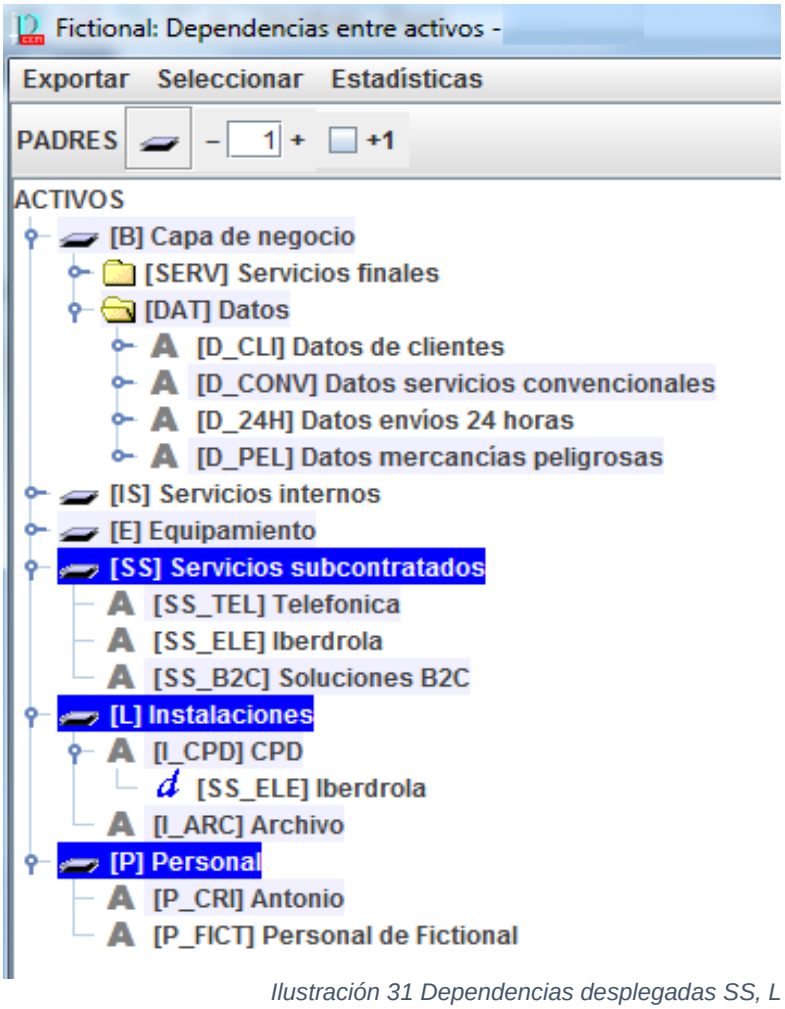
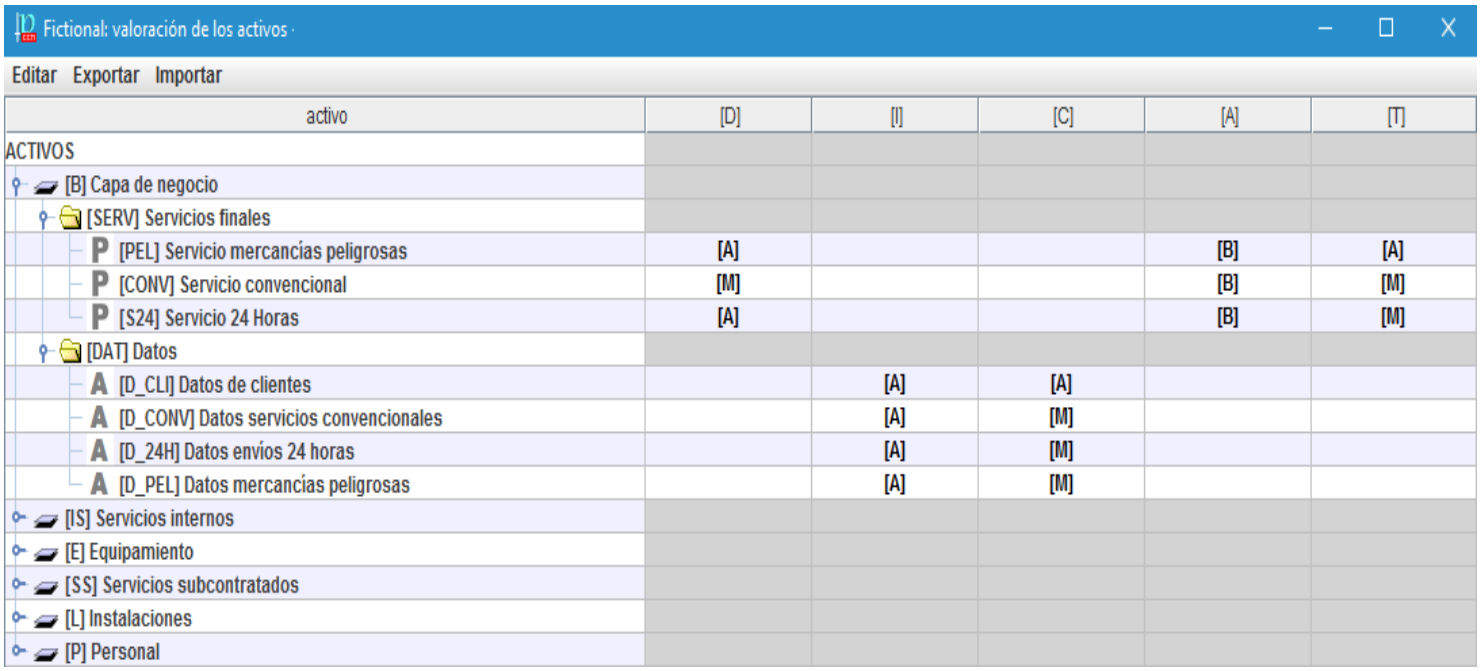


Ilustración 31 Dependencias desplegadas SS, L y P

4.5 Evaluación de los servicios

En esta fase se ha realizado la valoración de los servicios ofrecidos por la organización Fictional así como la información empleada en dichos servicios. Se ha seguido la tabla indicada en la metodología del análisis de riesgos.

Para los servicios se valora la disponibilidad, la autenticidad y la trazabilidad. En cambio, en los datos empleados para que se lleven a cabo los servicios, se valora la integridad y la confidencialidad de los mismos.



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Capa de negocio					
[SERV] Servicios finales					
P [PEL] Servicio mercancías peligrosas	[A]			[B]	[A]
P [CONV] Servicio convencional	[M]			[B]	[M]
P [S24] Servicio 24 Horas	[A]			[B]	[M]
[DAT] Datos					
A [D_CLI] Datos de clientes		[A]	[A]		
A [D_CONV] Datos servicios convencionales		[A]	[M]		
A [D_24H] Datos envíos 24 horas		[A]	[M]		
A [D_PEL] Datos mercancías peligrosas		[A]	[M]		
[IS] Servicios internos					
[E] Equipamiento					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Ilustración 32 Valoración de los servicios y datos

4.6 Identificación de las amenazas

En la cuarta fase, una vez se han identificado los activos y se han valorado, se identifican las posibles amenazas a los que estos están expuestos.

En el caso de estudio de este proyecto, se han identificado las siguientes amenazas:

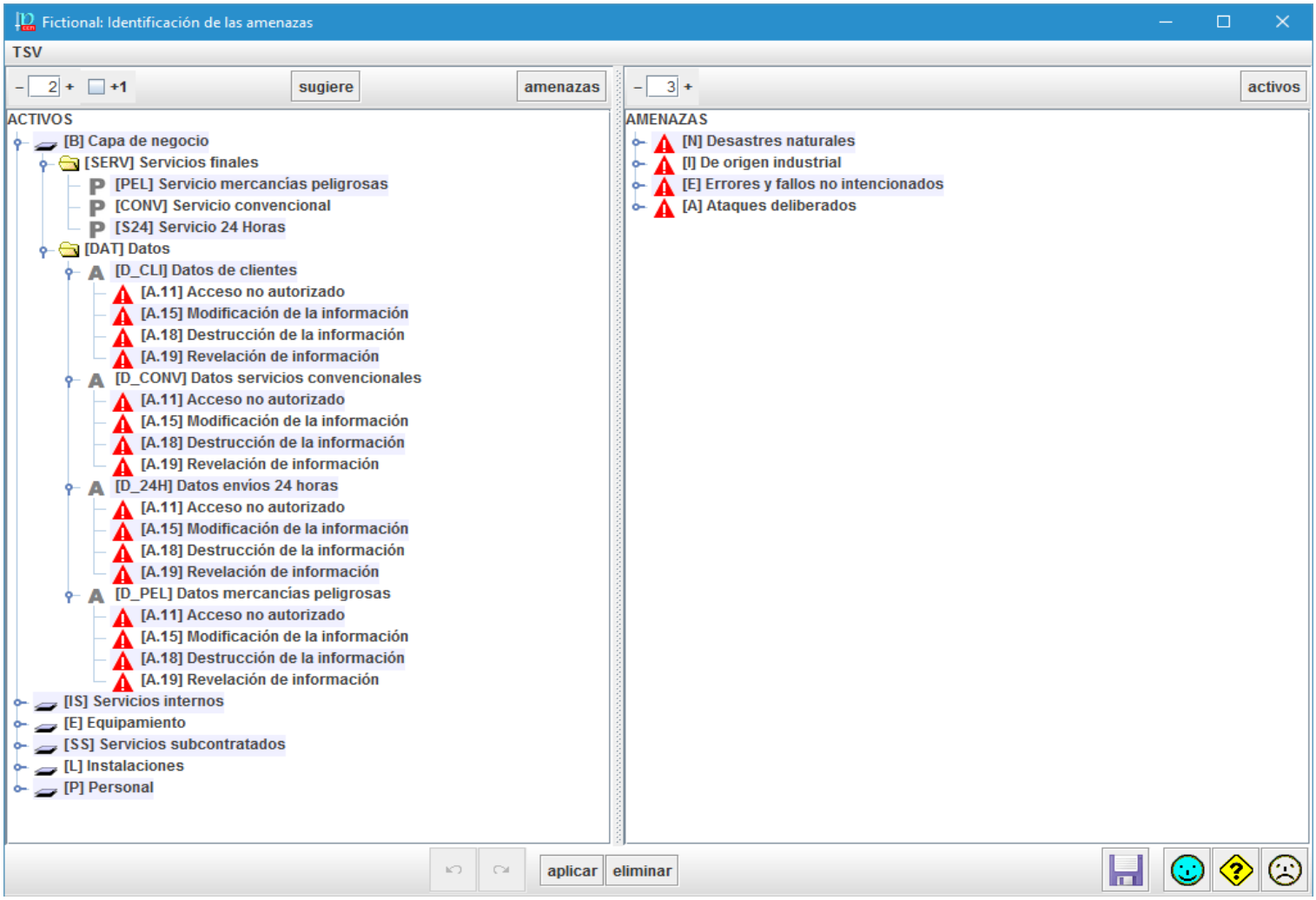


Ilustración 33 Amenazas en datos

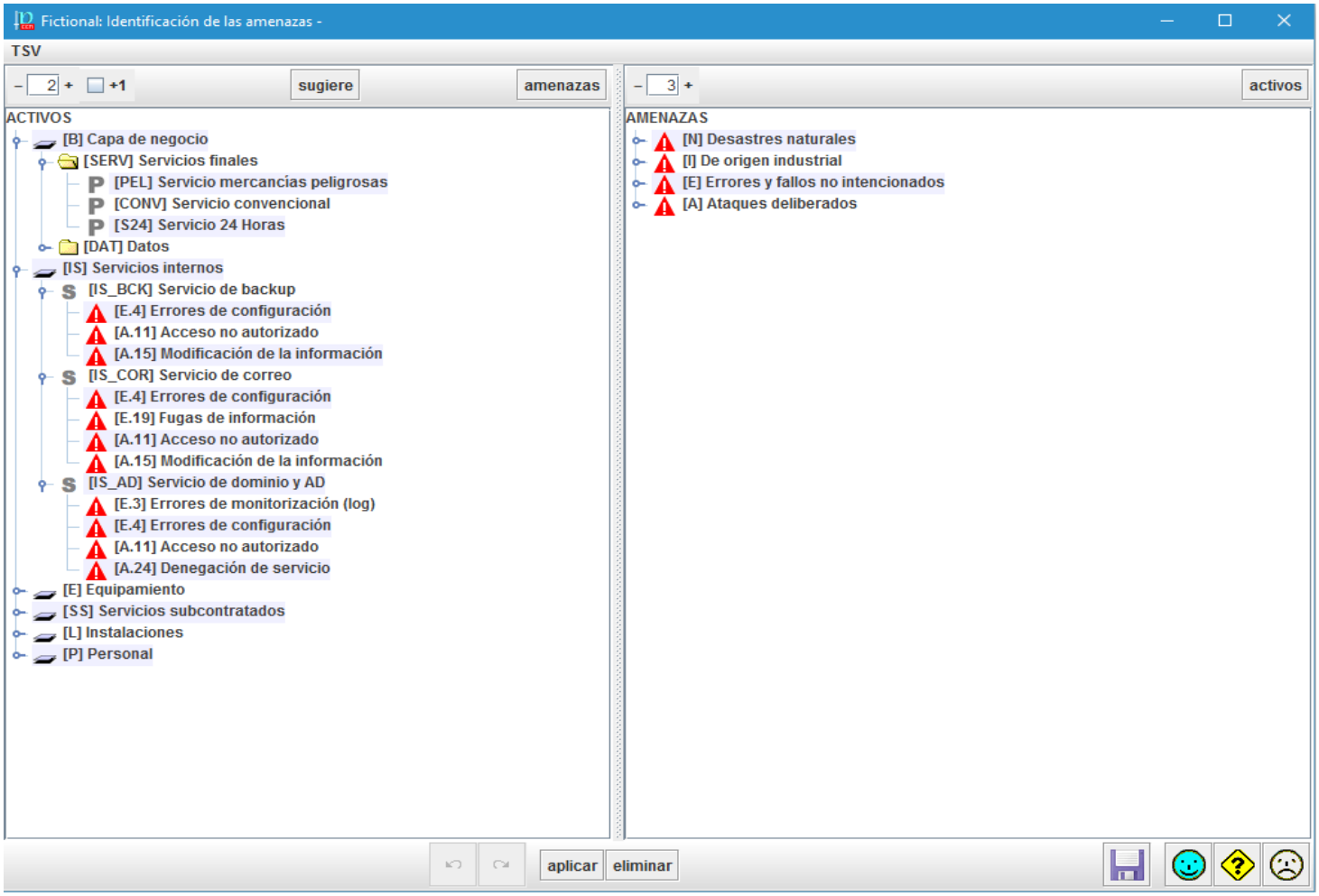


Ilustración 34 Amenazas en Servicios internos

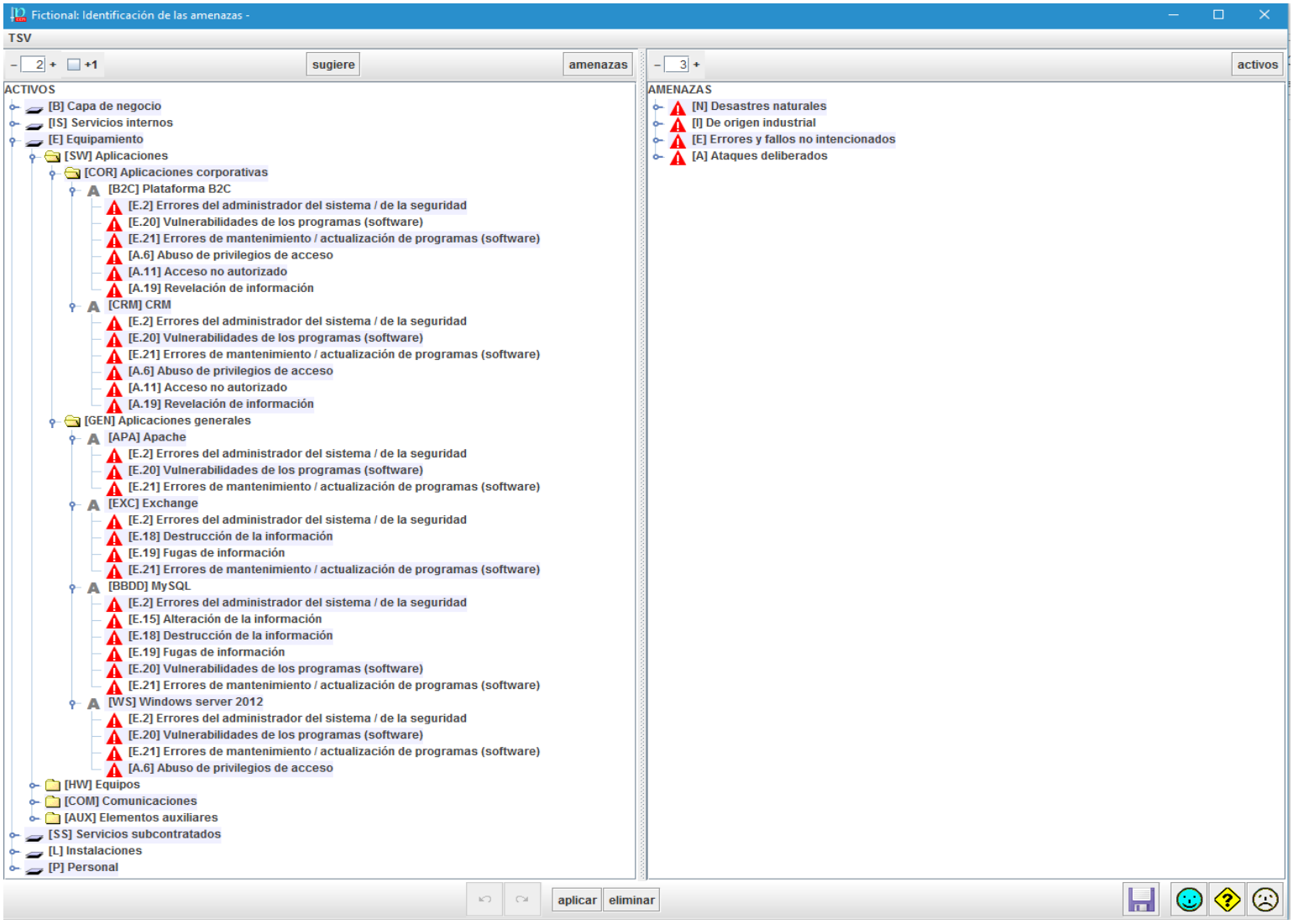


Ilustración 35 Amenazas en Equipamiento – Aplicaciones – Aplicaciones corporativas y aplicaciones generales

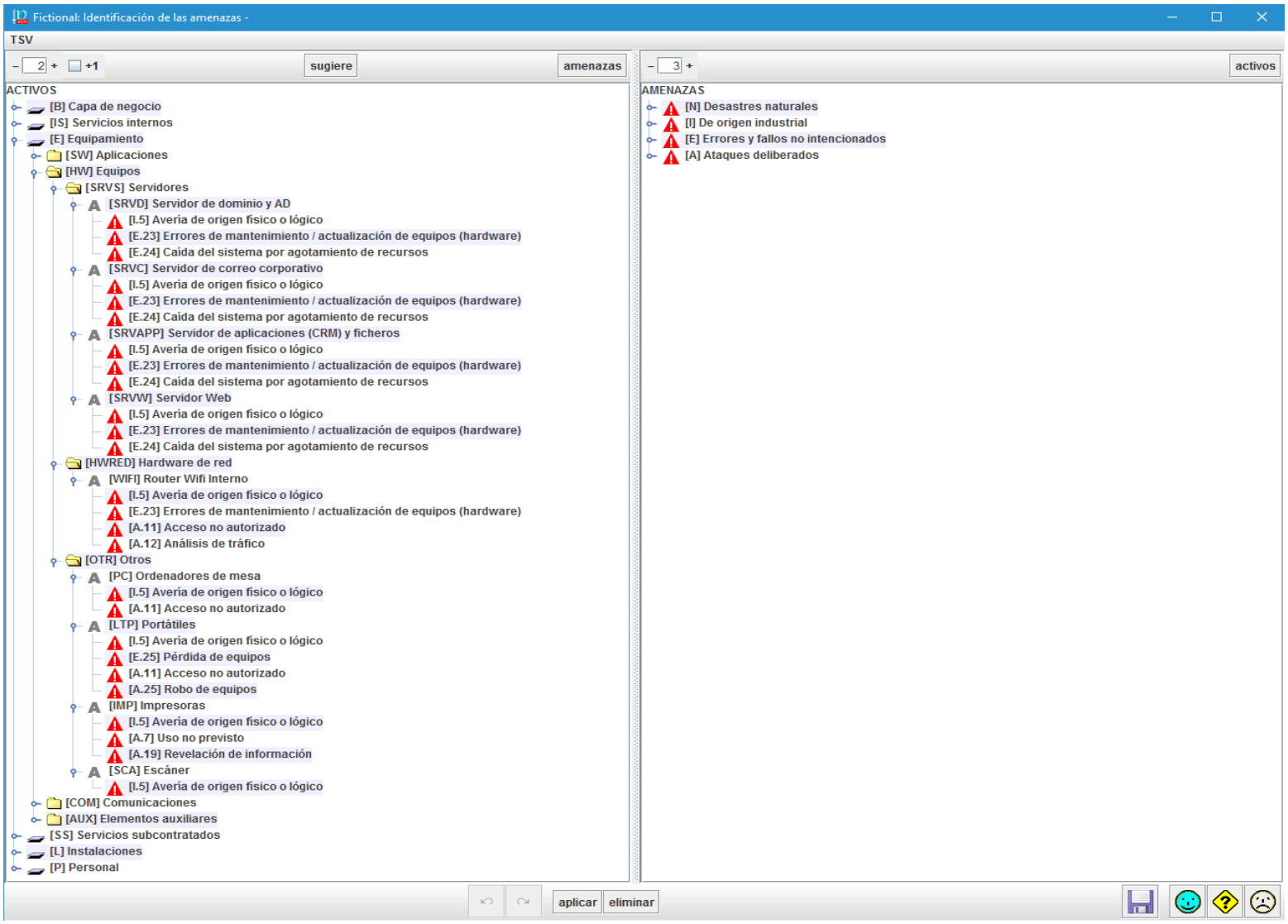


Ilustración 36 Amenazas en Equipamiento - Equipos - Servidores, hardware de red y otros

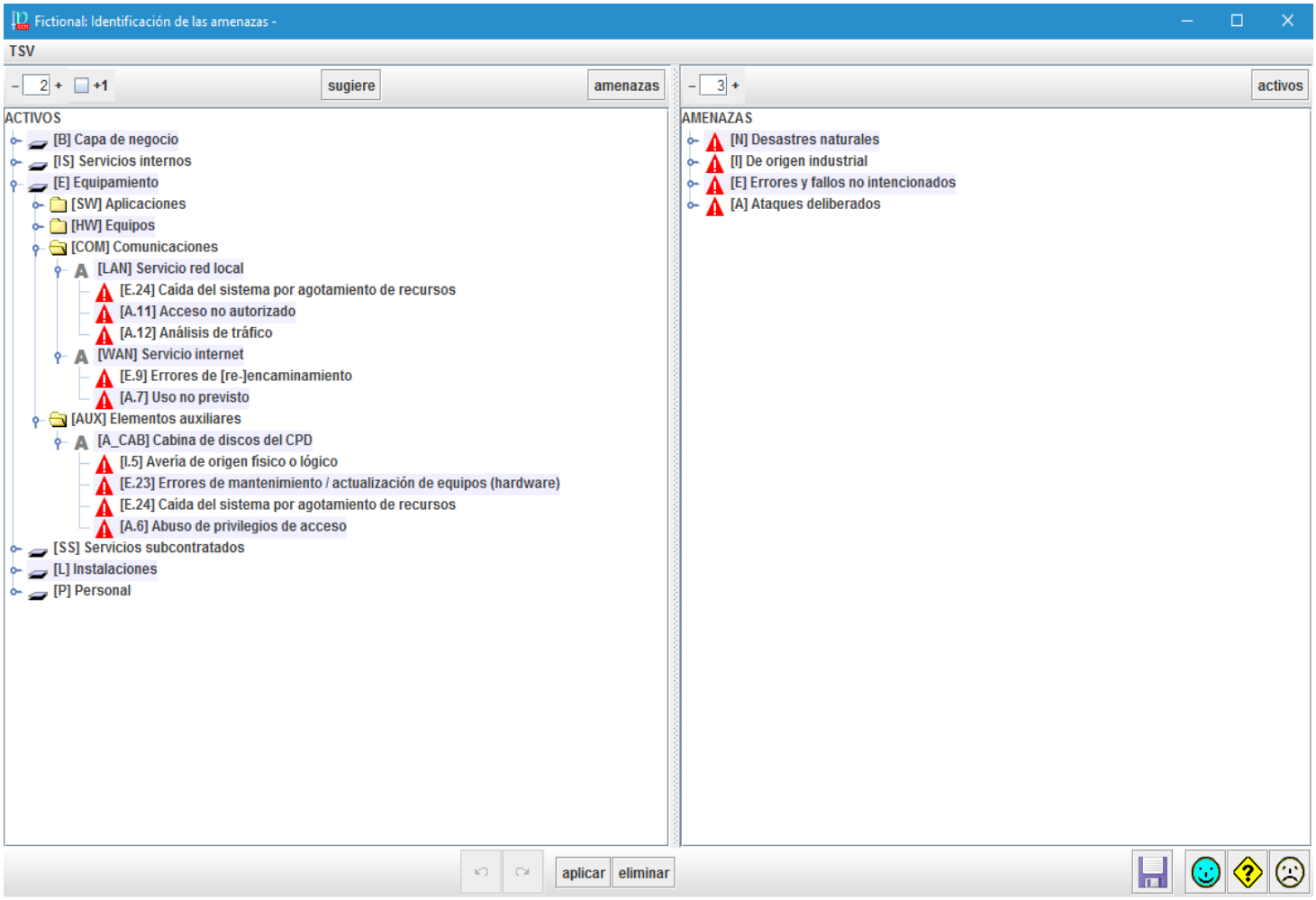


Ilustración 37 Amenazas en Equipamiento - Comunicaciones y Elementos auxiliares

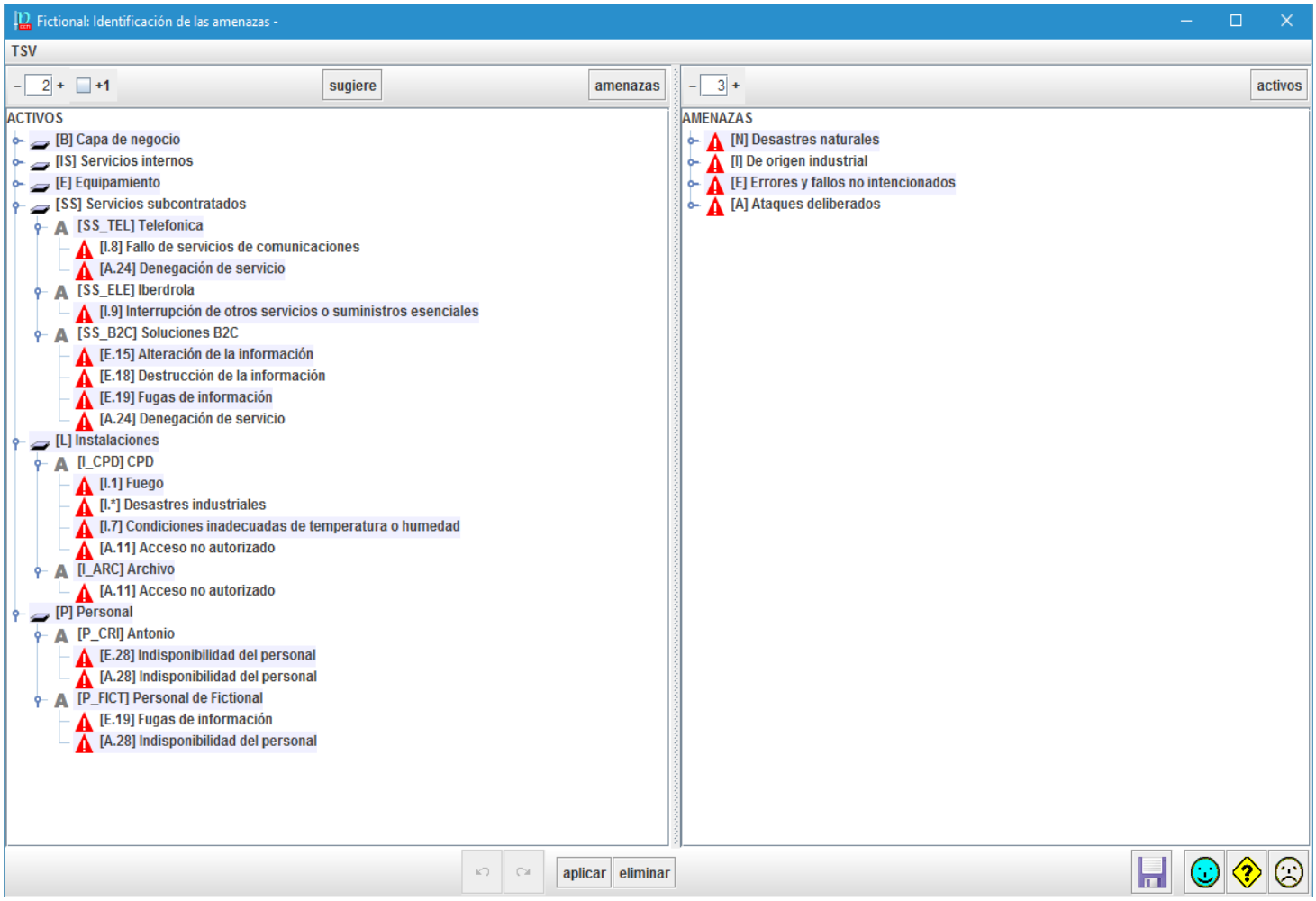


Ilustración 38 Amenazas en Servicio subcontratados, Instalaciones y Personal

4.7 Probabilidad de amenazas e impacto

En esta fase se ha determinado la probabilidad de suceso, o frecuencia potencial, de una amenaza de acuerdo con el tiempo aproximado para que se materialice.

Por otro lado se ha especificado en qué grado afecta a las dimensiones DICAT el impacto al materializarse la amenaza.

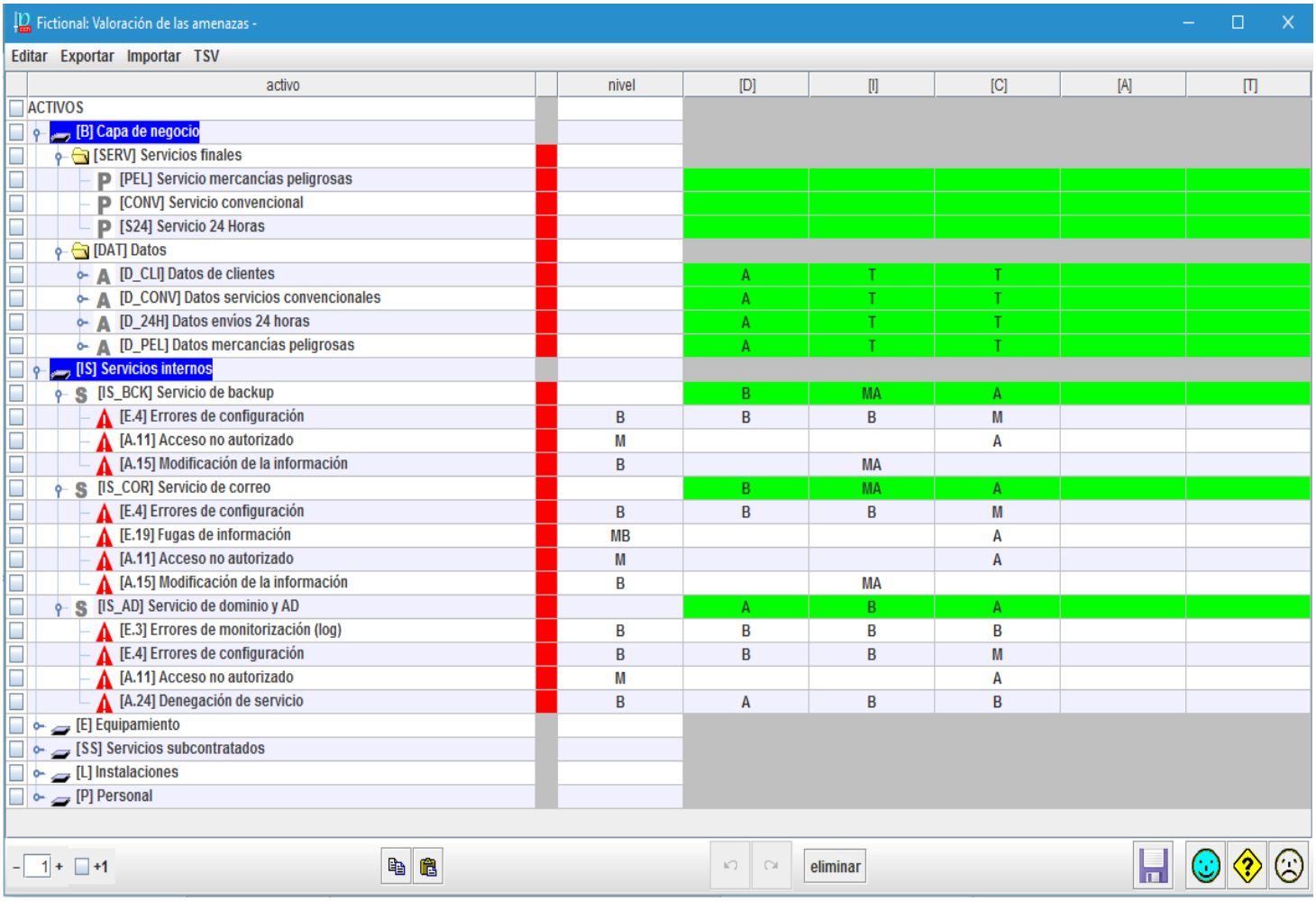


Ilustración 39 Valoración de amenazas - Capa de negocio y Servicios internos

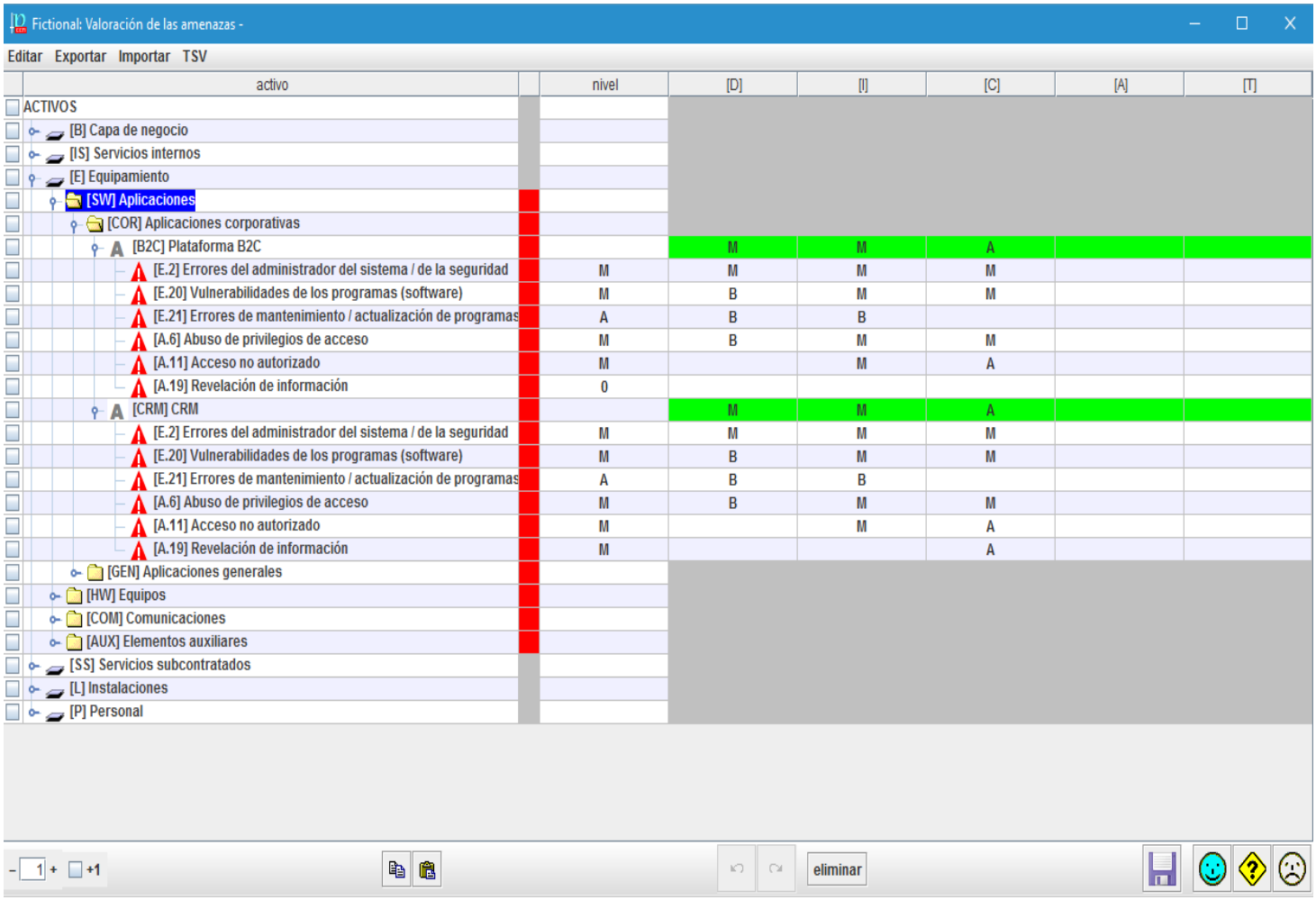


Ilustración 40 Valoración de amenazas en Aplicaciones - Aplicaciones corporativas

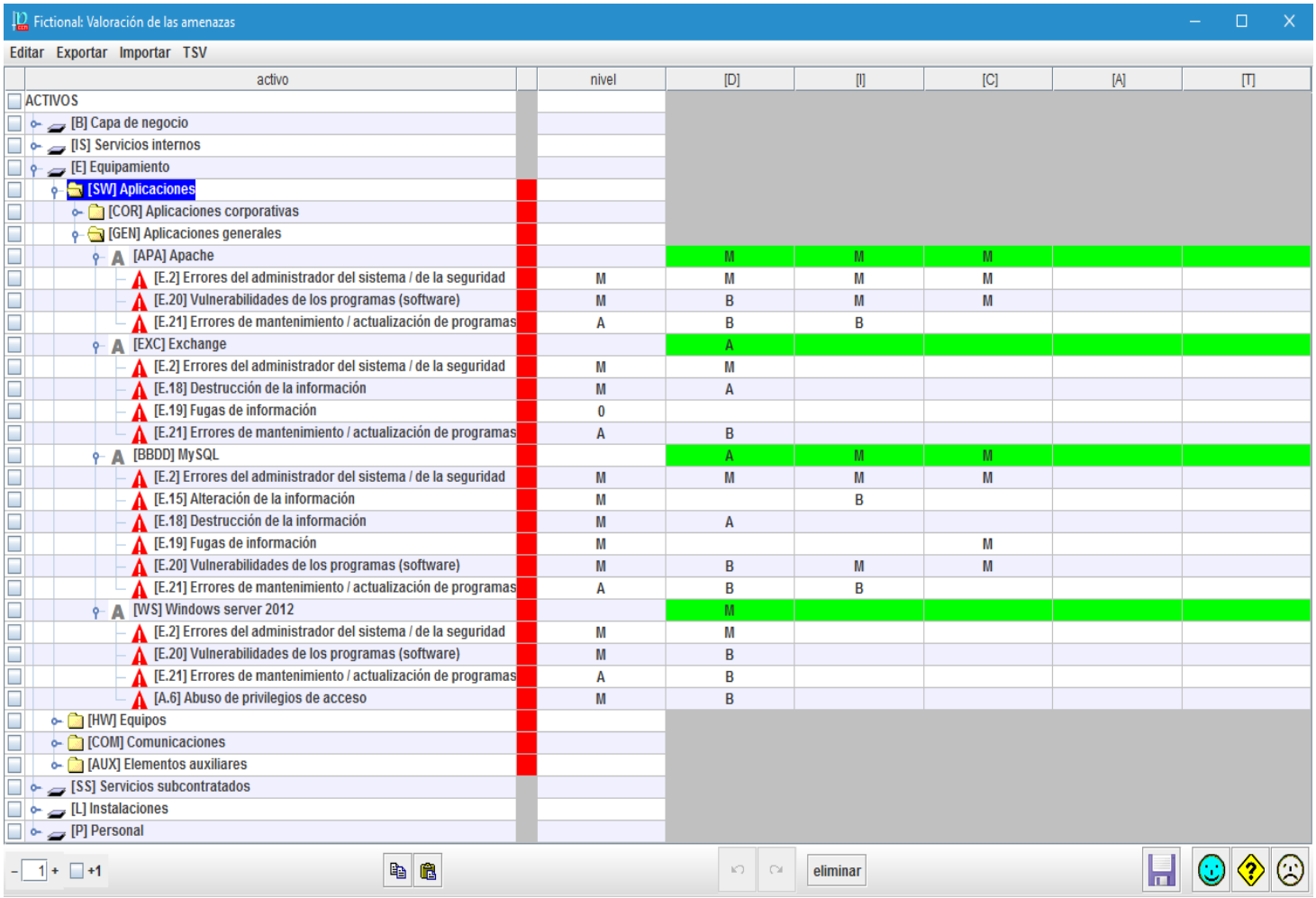


Ilustración 41 Valoración de amenazas en Equipamiento - Aplicaciones - Aplicaciones generales

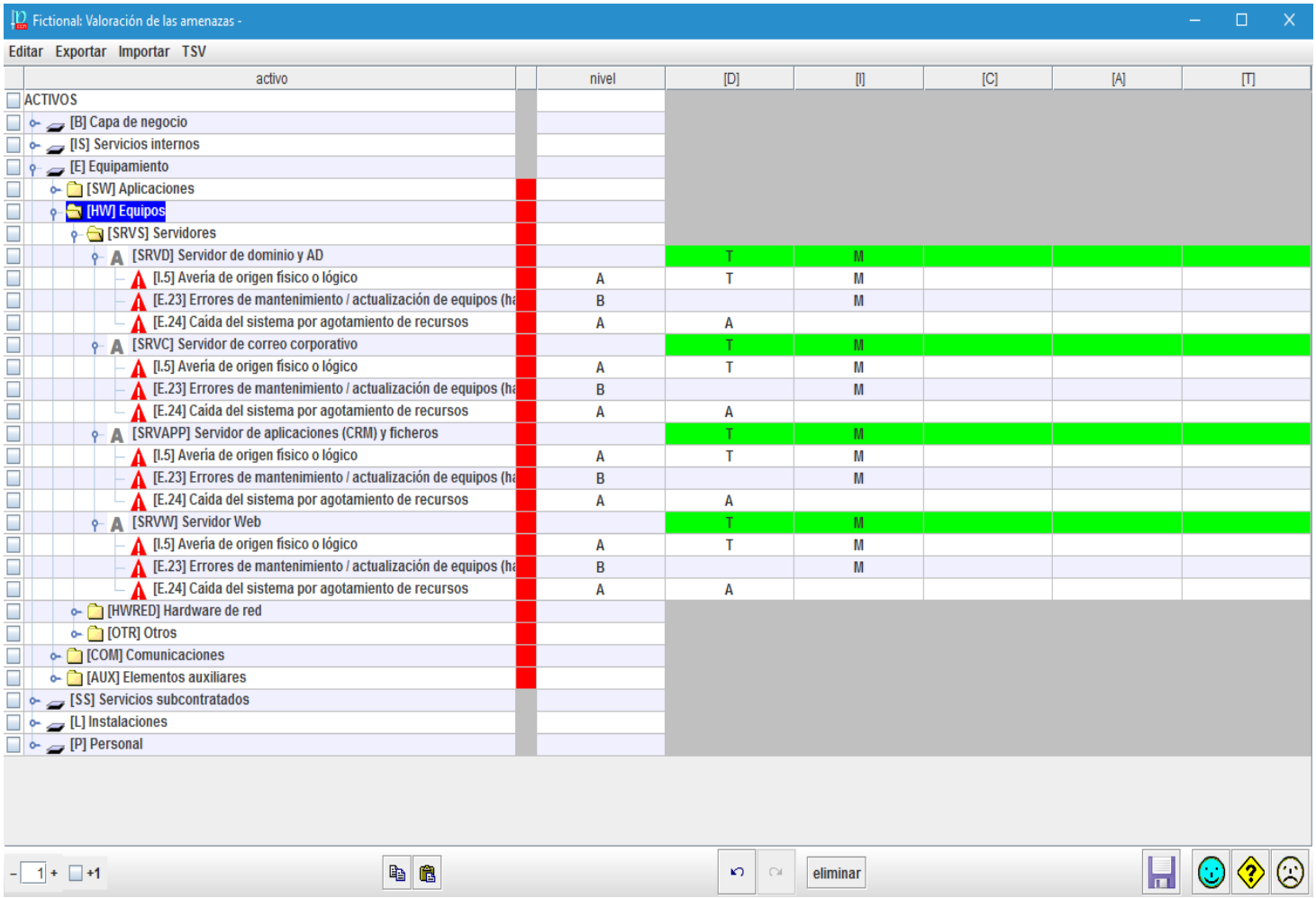


Ilustración 42 Valoración de amenazas en Equipamiento - Equipos - Servidores

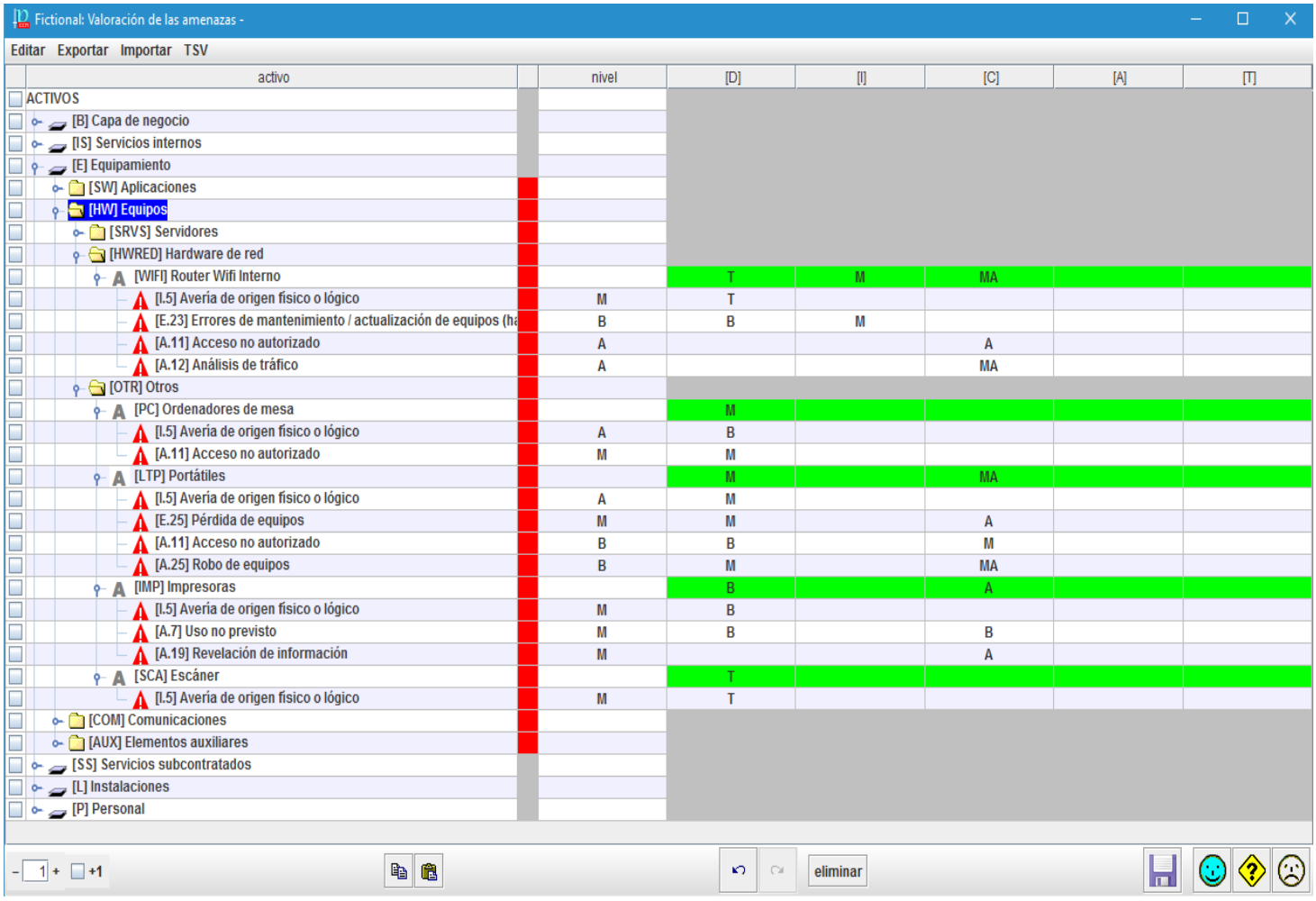


Ilustración 43 Valoración de amenazas en Equipamiento - Equipos - Hardware de red y otros

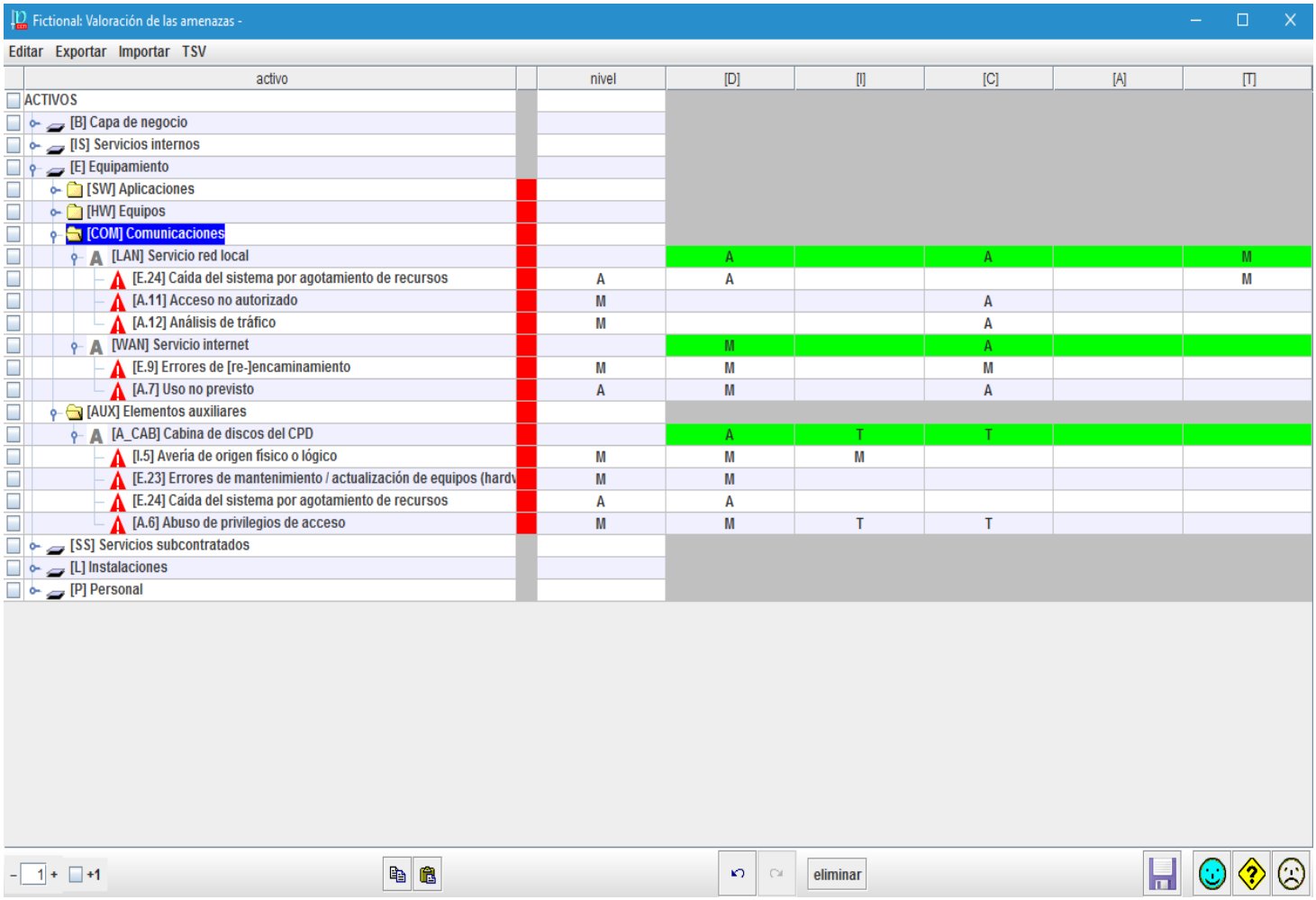


Ilustración 44 Valoración de amenazas en Equipamiento - Comunicaciones y elementos auxiliares

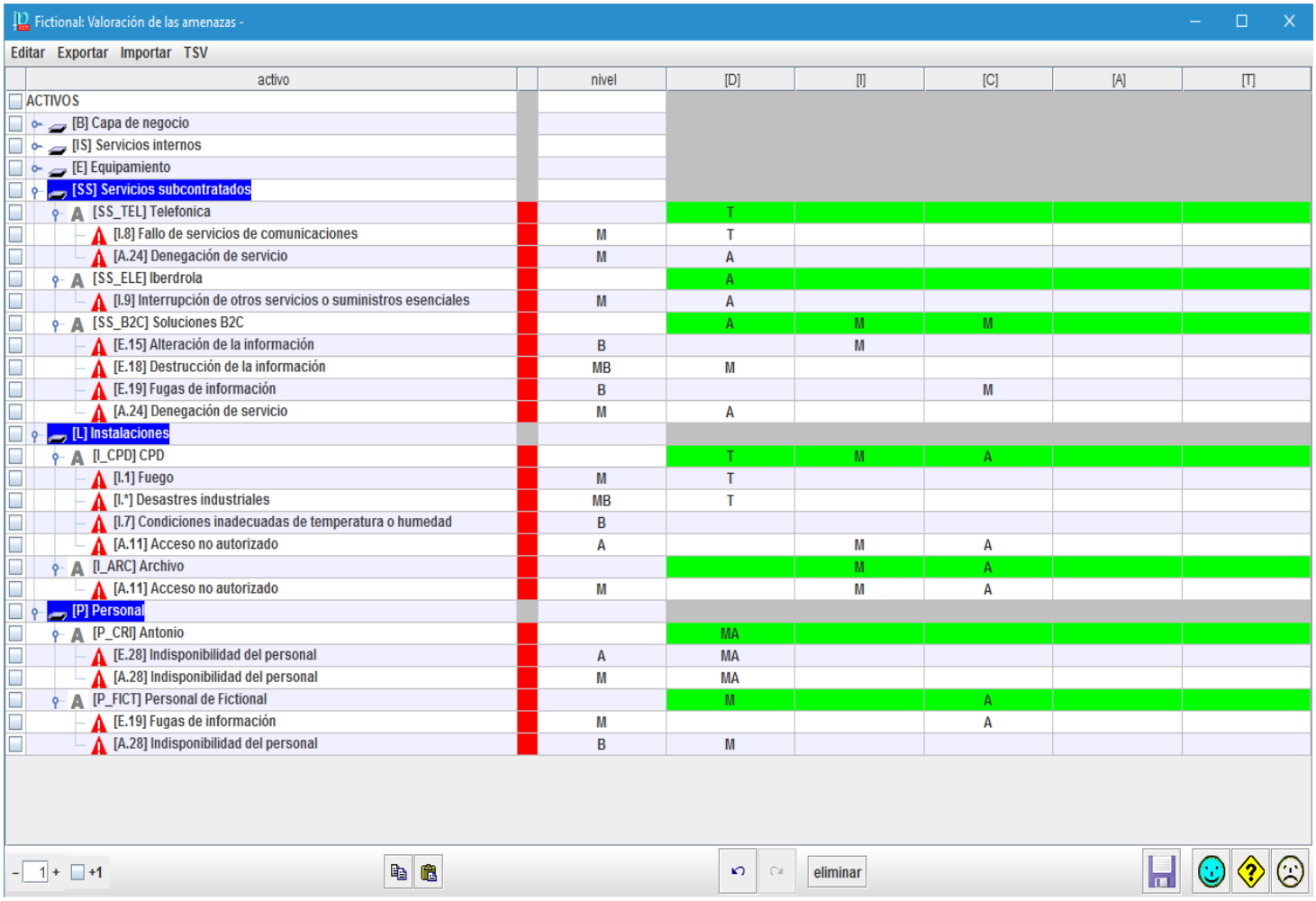
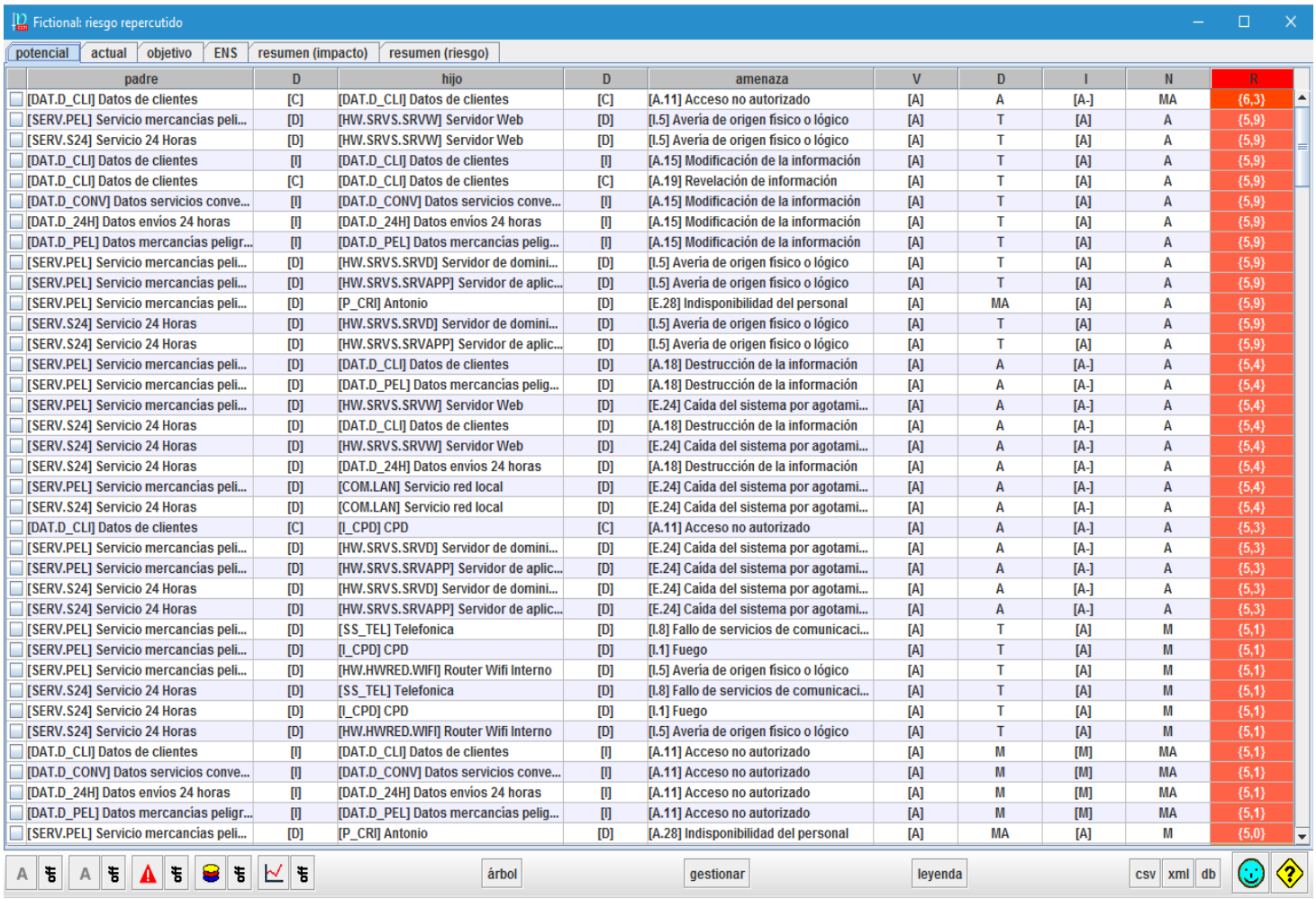


Ilustración 45 Valoración de amenazas en Servicios subcontratados, Instalaciones y Personal

4.8 Evaluación del riesgo potencial

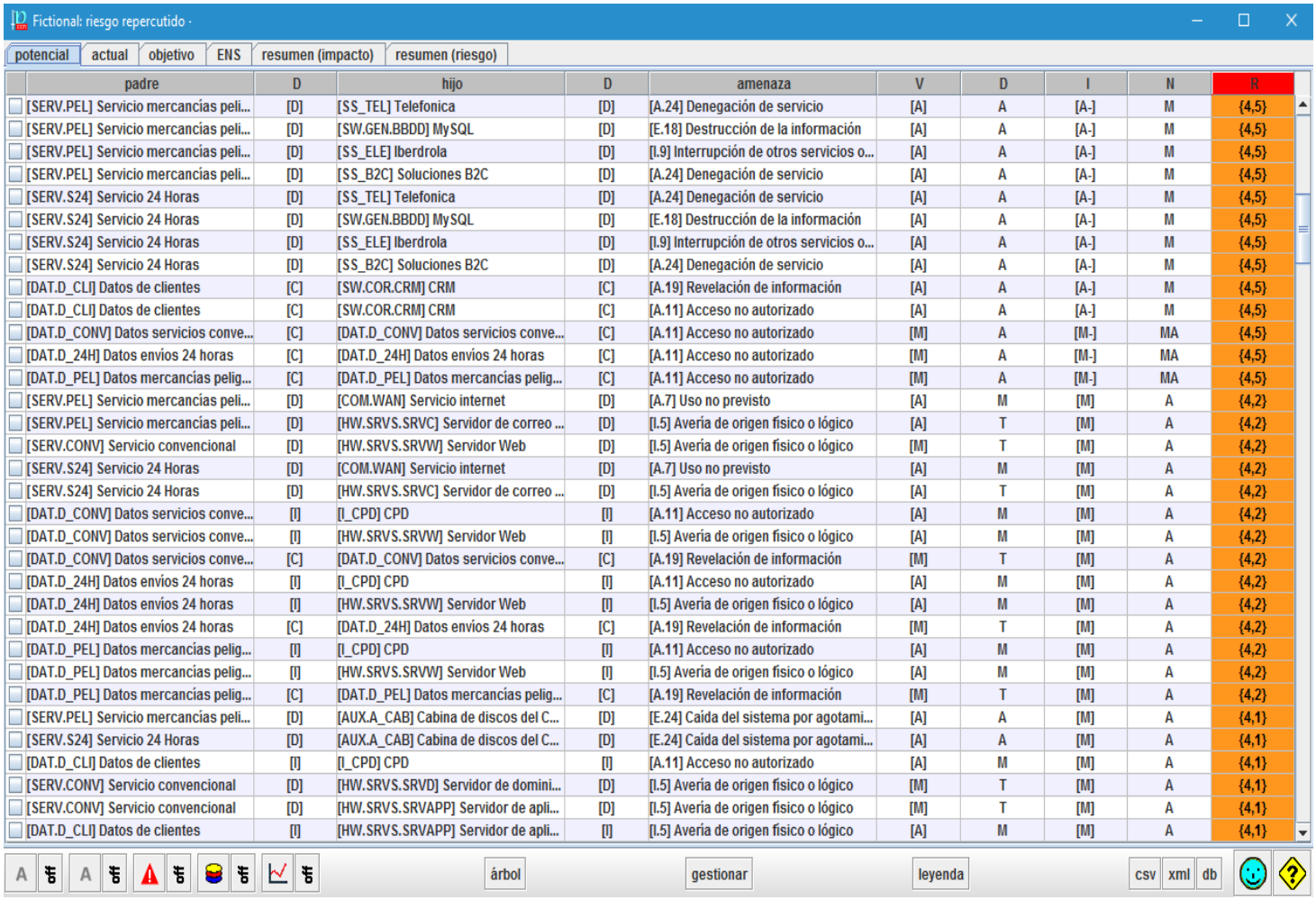
Llegamos a la última fase, en la cual se extrae el riesgo potencial al que están expuestos los servicios de Fictional.

Se trata del riesgo al que está expuesto cada activo sin que se hayan aplicado medidas ni salvaguardas en la compañía.



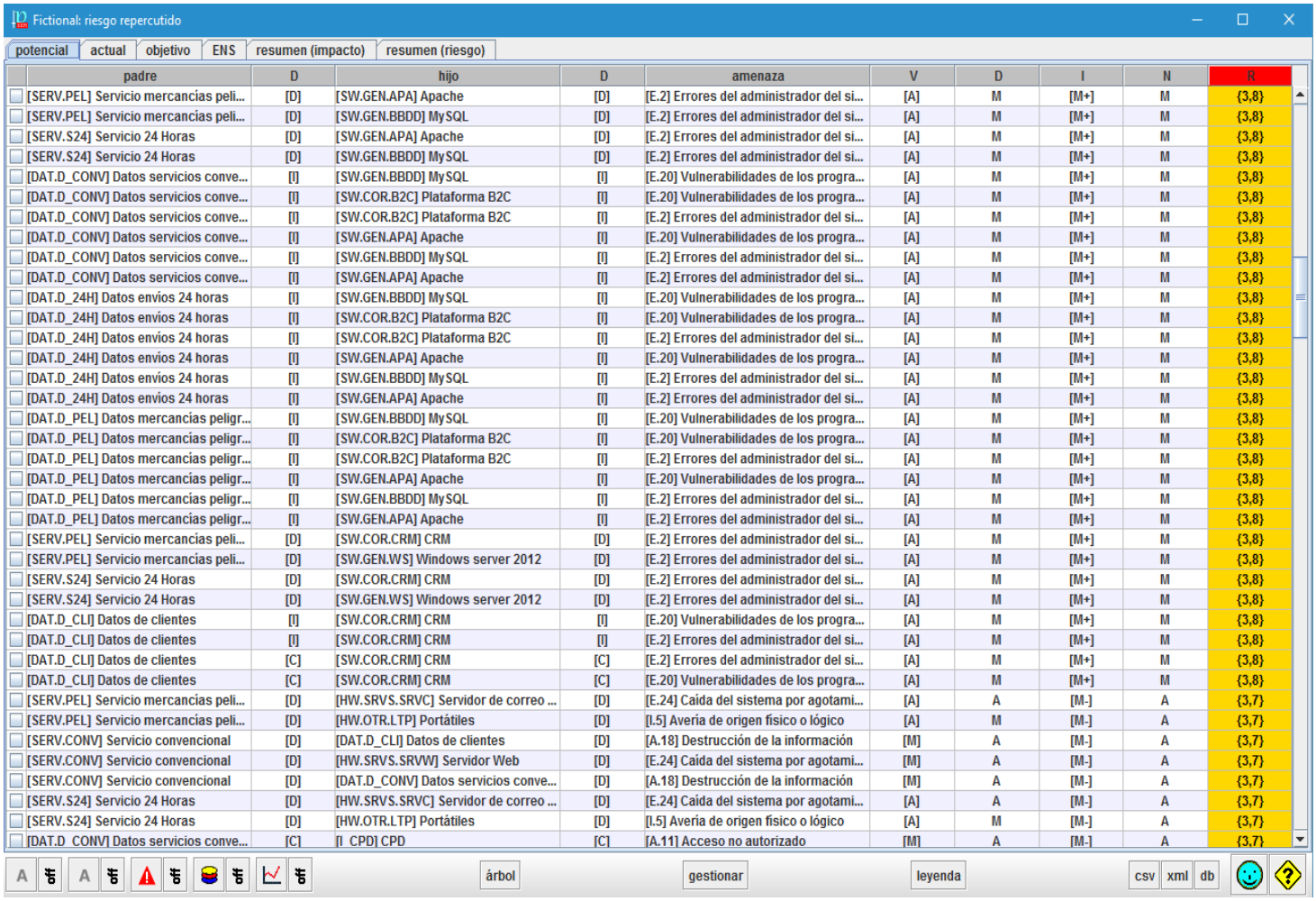
padre	D	hijo	D	amenaza	V	D	I	N	R
[DAT.D_CLI] Datos de clientes	[C]	[DAT.D_CLI] Datos de clientes	[C]	[A.11] Acceso no autorizado	[A]	A	[A-]	MA	{6,3}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[A]	A	{5,9}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[A]	A	{5,9}
[DAT.D_CLI] Datos de clientes	[I]	[DAT.D_CLI] Datos de clientes	[I]	[A.15] Modificación de la información	[A]	T	[A]	A	{5,9}
[DAT.D_CLI] Datos de clientes	[C]	[DAT.D_CLI] Datos de clientes	[C]	[A.19] Revelación de información	[A]	T	[A]	A	{5,9}
[DAT.D_CONV] Datos servicios conve...	[I]	[DAT.D_CONV] Datos servicios conve...	[I]	[A.15] Modificación de la información	[A]	T	[A]	A	{5,9}
[DAT.D_24H] Datos envíos 24 horas	[I]	[DAT.D_24H] Datos envíos 24 horas	[I]	[A.15] Modificación de la información	[A]	T	[A]	A	{5,9}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[DAT.D_PEL] Datos mercancías peligr...	[I]	[A.15] Modificación de la información	[A]	T	[A]	A	{5,9}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.SRVS.SRVD] Servidor de domini...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[A]	A	{5,9}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.SRVS.SRVAPP] Servidor de aplic...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[A]	A	{5,9}
[SERV.PEL] Servicio mercancías peli...	[D]	[P_CRI] Antonio	[D]	[E.28] Indisponibilidad del personal	[A]	MA	[A]	A	{5,9}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVD] Servidor de domini...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[A]	A	{5,9}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVAPP] Servidor de aplic...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[A]	A	{5,9}
[SERV.PEL] Servicio mercancías peli...	[D]	[DAT.D_CLI] Datos de clientes	[D]	[A.18] Destrucción de la información	[A]	A	[A-]	A	{5,4}
[SERV.PEL] Servicio mercancías peli...	[D]	[DAT.D_PEL] Datos mercancías peligr...	[D]	[A.18] Destrucción de la información	[A]	A	[A-]	A	{5,4}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[A-]	A	{5,4}
[SERV.S24] Servicio 24 Horas	[D]	[DAT.D_CLI] Datos de clientes	[D]	[A.18] Destrucción de la información	[A]	A	[A-]	A	{5,4}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[A-]	A	{5,4}
[SERV.S24] Servicio 24 Horas	[D]	[DAT.D_24H] Datos envíos 24 horas	[D]	[A.18] Destrucción de la información	[A]	A	[A-]	A	{5,4}
[SERV.PEL] Servicio mercancías peli...	[D]	[COM.LAN] Servicio red local	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[A-]	A	{5,4}
[SERV.S24] Servicio 24 Horas	[D]	[COM.LAN] Servicio red local	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[A-]	A	{5,4}
[DAT.D_CLI] Datos de clientes	[C]	[I_CPD] CPD	[C]	[A.11] Acceso no autorizado	[A]	A	[A-]	A	{5,3}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.SRVS.SRVD] Servidor de domini...	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[A-]	A	{5,3}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.SRVS.SRVAPP] Servidor de aplic...	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[A-]	A	{5,3}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVD] Servidor de domini...	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[A-]	A	{5,3}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVAPP] Servidor de aplic...	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[A-]	A	{5,3}
[SERV.PEL] Servicio mercancías peli...	[D]	[SS_TEL] Telefonica	[D]	[I.8] Fallo de servicios de comunicaci...	[A]	T	[A]	M	{5,1}
[SERV.PEL] Servicio mercancías peli...	[D]	[I_CPD] CPD	[D]	[I.1] Fuego	[A]	T	[A]	M	{5,1}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[A]	M	{5,1}
[SERV.S24] Servicio 24 Horas	[D]	[SS_TEL] Telefonica	[D]	[I.8] Fallo de servicios de comunicaci...	[A]	T	[A]	M	{5,1}
[SERV.S24] Servicio 24 Horas	[D]	[I_CPD] CPD	[D]	[I.1] Fuego	[A]	T	[A]	M	{5,1}
[SERV.S24] Servicio 24 Horas	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[A]	M	{5,1}
[DAT.D_CLI] Datos de clientes	[I]	[DAT.D_CLI] Datos de clientes	[I]	[A.11] Acceso no autorizado	[A]	M	[M]	MA	{5,1}
[DAT.D_CONV] Datos servicios conve...	[I]	[DAT.D_CONV] Datos servicios conve...	[I]	[A.11] Acceso no autorizado	[A]	M	[M]	MA	{5,1}
[DAT.D_24H] Datos envíos 24 horas	[I]	[DAT.D_24H] Datos envíos 24 horas	[I]	[A.11] Acceso no autorizado	[A]	M	[M]	MA	{5,1}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[DAT.D_PEL] Datos mercancías peligr...	[I]	[A.11] Acceso no autorizado	[A]	M	[M]	MA	{5,1}
[SERV.PEL] Servicio mercancías peli...	[D]	[P_CRI] Antonio	[D]	[A.28] Indisponibilidad del personal	[A]	MA	[A]	M	{5,0}

Ilustración 47 Riesgo potencial



padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.PEL] Servicio mercancías peli...	[D]	[SS_TEL] Telefonica	[D]	[A.24] Denegación de servicio	[A]	A	[A-]	M	{4,5}
[SERV.PEL] Servicio mercancías peli...	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.18] Destrucción de la información	[A]	A	[A-]	M	{4,5}
[SERV.PEL] Servicio mercancías peli...	[D]	[SS_ELE] Iberdrola	[D]	[I.9] Interrupción de otros servicios o...	[A]	A	[A-]	M	{4,5}
[SERV.PEL] Servicio mercancías peli...	[D]	[SS_B2C] Soluciones B2C	[D]	[A.24] Denegación de servicio	[A]	A	[A-]	M	{4,5}
[SERV.S24] Servicio 24 Horas	[D]	[SS_TEL] Telefonica	[D]	[A.24] Denegación de servicio	[A]	A	[A-]	M	{4,5}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.18] Destrucción de la información	[A]	A	[A-]	M	{4,5}
[SERV.S24] Servicio 24 Horas	[D]	[SS_ELE] Iberdrola	[D]	[I.9] Interrupción de otros servicios o...	[A]	A	[A-]	M	{4,5}
[SERV.S24] Servicio 24 Horas	[D]	[SS_B2C] Soluciones B2C	[D]	[A.24] Denegación de servicio	[A]	A	[A-]	M	{4,5}
[DAT.D_CLI] Datos de clientes	[C]	[SW.COR.CRM] CRM	[C]	[A.19] Revelación de información	[A]	A	[A-]	M	{4,5}
[DAT.D_CLI] Datos de clientes	[C]	[SW.COR.CRM] CRM	[C]	[A.11] Acceso no autorizado	[A]	A	[A-]	M	{4,5}
[DAT.D_CONV] Datos servicios conve...	[C]	[DAT.D_CONV] Datos servicios conve...	[C]	[A.11] Acceso no autorizado	[M]	A	[M-]	MA	{4,5}
[DAT.D_24H] Datos envíos 24 horas	[C]	[DAT.D_24H] Datos envíos 24 horas	[C]	[A.11] Acceso no autorizado	[M]	A	[M-]	MA	{4,5}
[DAT.D_PEL] Datos mercancías pelig...	[C]	[DAT.D_PEL] Datos mercancías pelig...	[C]	[A.11] Acceso no autorizado	[M]	A	[M-]	MA	{4,5}
[SERV.PEL] Servicio mercancías peli...	[D]	[COM.WAN] Servicio internet	[D]	[A.7] Uso no previsto	[A]	M	[M]	A	{4,2}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.SRVS.SRVC] Servidor de correo ...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M]	A	{4,2}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[M]	A	{4,2}
[SERV.S24] Servicio 24 Horas	[D]	[COM.WAN] Servicio internet	[D]	[A.7] Uso no previsto	[A]	M	[M]	A	{4,2}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVC] Servidor de correo ...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M]	A	{4,2}
[DAT.D_CONV] Datos servicios conve...	[I]	[I_CPD] CPD	[I]	[A.11] Acceso no autorizado	[A]	M	[M]	A	{4,2}
[DAT.D_CONV] Datos servicios conve...	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[M]	A	{4,2}
[DAT.D_CONV] Datos servicios conve...	[C]	[DAT.D_CONV] Datos servicios conve...	[C]	[A.19] Revelación de información	[M]	T	[M]	A	{4,2}
[DAT.D_24H] Datos envíos 24 horas	[I]	[I_CPD] CPD	[I]	[A.11] Acceso no autorizado	[A]	M	[M]	A	{4,2}
[DAT.D_24H] Datos envíos 24 horas	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[M]	A	{4,2}
[DAT.D_24H] Datos envíos 24 horas	[C]	[DAT.D_24H] Datos envíos 24 horas	[C]	[A.19] Revelación de información	[M]	T	[M]	A	{4,2}
[DAT.D_PEL] Datos mercancías pelig...	[I]	[I_CPD] CPD	[I]	[A.11] Acceso no autorizado	[A]	M	[M]	A	{4,2}
[DAT.D_PEL] Datos mercancías pelig...	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[M]	A	{4,2}
[DAT.D_PEL] Datos mercancías pelig...	[C]	[DAT.D_PEL] Datos mercancías pelig...	[C]	[A.19] Revelación de información	[M]	T	[M]	A	{4,2}
[SERV.PEL] Servicio mercancías peli...	[D]	[AUX.A_CAB] Cabina de discos del C...	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[M]	A	{4,1}
[SERV.S24] Servicio 24 Horas	[D]	[AUX.A_CAB] Cabina de discos del C...	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[M]	A	{4,1}
[DAT.D_CLI] Datos de clientes	[I]	[I_CPD] CPD	[I]	[A.11] Acceso no autorizado	[A]	M	[M]	A	{4,1}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVD] Servidor de domini...	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[M]	A	{4,1}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVAPP] Servidor de apli...	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[M]	A	{4,1}
[DAT.D_CLI] Datos de clientes	[I]	[HW.SRVS.SRVAPP] Servidor de apli...	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[M]	A	{4,1}

Ilustración 48 Riesgo potencial



padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.PEL] Servicio mercancías peli...	[D]	[SW.GEN.APA] Apache	[D]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[SERV.PEL] Servicio mercancías peli...	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.APA] Apache	[D]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.GEN.APA] Apache	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.GEN.APA] Apache	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.APA] Apache	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.APA] Apache	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.GEN.APA] Apache	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.GEN.APA] Apache	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[SERV.PEL] Servicio mercancías peli...	[D]	[SW.COR.CRM] CRM	[D]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[SERV.PEL] Servicio mercancías peli...	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.CRM] CRM	[D]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_CLI] Datos de clientes	[I]	[SW.COR.CRM] CRM	[I]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[DAT.D_CLI] Datos de clientes	[I]	[SW.COR.CRM] CRM	[I]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_CLI] Datos de clientes	[C]	[SW.COR.CRM] CRM	[C]	[E.2] Errores del administrador del si...	[A]	M	[M+]	M	{3,8}
[DAT.D_CLI] Datos de clientes	[C]	[SW.COR.CRM] CRM	[C]	[E.20] Vulnerabilidades de los progra...	[A]	M	[M+]	M	{3,8}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.SRVS.SRVC] Servidor de correo ...	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[M-]	A	{3,7}
[SERV.PEL] Servicio mercancías peli...	[D]	[HW.OTR.LTP] Portátiles	[D]	[I.5] Avería de origen físico o lógico	[A]	M	[M-]	A	{3,7}
[SERV.CONV] Servicio convencional	[D]	[DAT.D_CLI] Datos de clientes	[D]	[A.18] Destrucción de la información	[M]	A	[M-]	A	{3,7}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[E.24] Caída del sistema por agotami...	[M]	A	[M-]	A	{3,7}
[SERV.CONV] Servicio convencional	[D]	[DAT.D_CONV] Datos servicios conve...	[D]	[A.18] Destrucción de la información	[M]	A	[M-]	A	{3,7}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVC] Servidor de correo ...	[D]	[E.24] Caída del sistema por agotami...	[A]	A	[M-]	A	{3,7}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.LTP] Portátiles	[D]	[I.5] Avería de origen físico o lógico	[A]	M	[M-]	A	{3,7}
[DAT.D_CONV] Datos servicios conve...	[C]	[I_CPD] CPD	[C]	[A.11] Acceso no autorizado	[M]	A	[M-]	A	{3,7}

Ilustración 49 Riesgo potencial

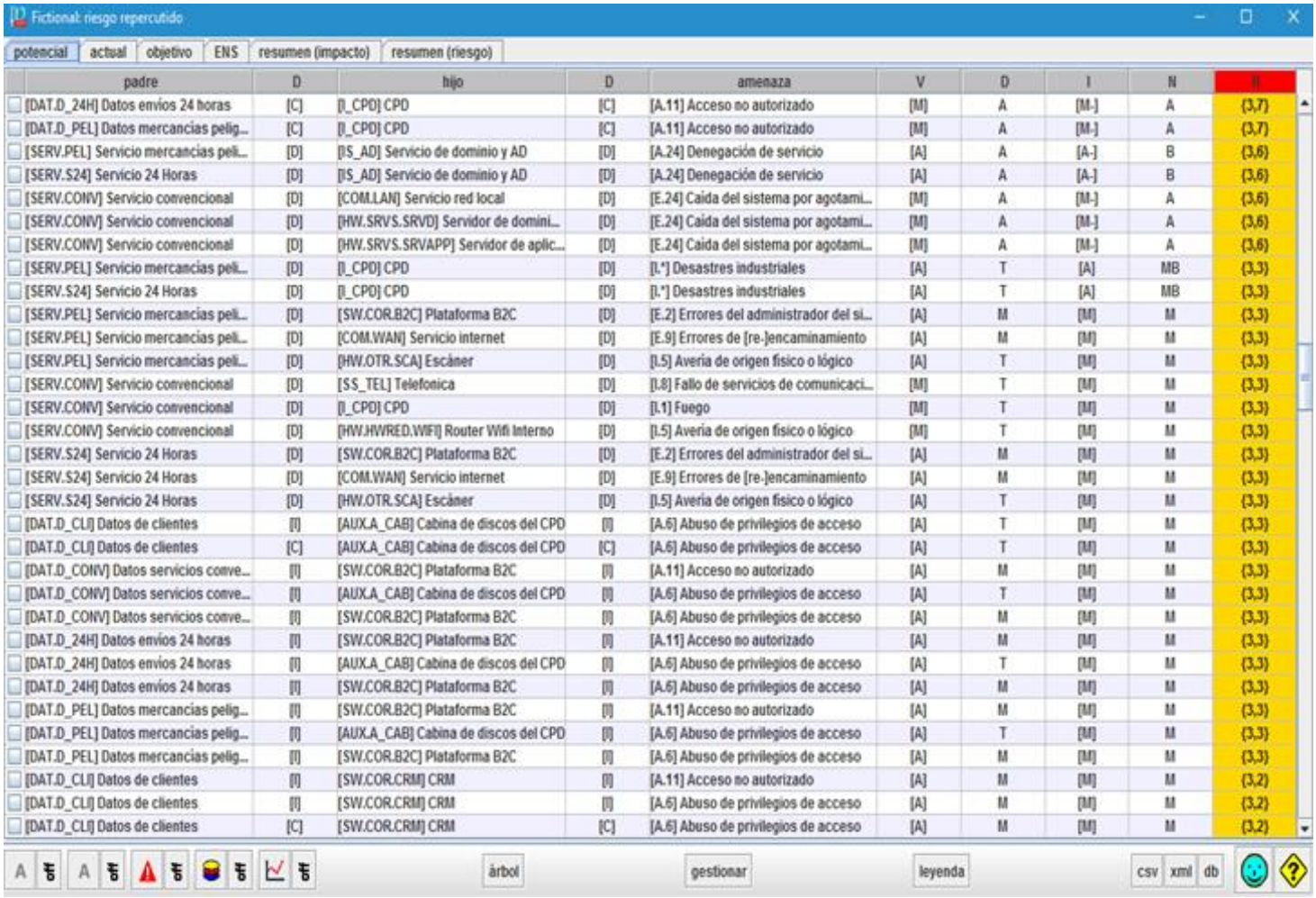
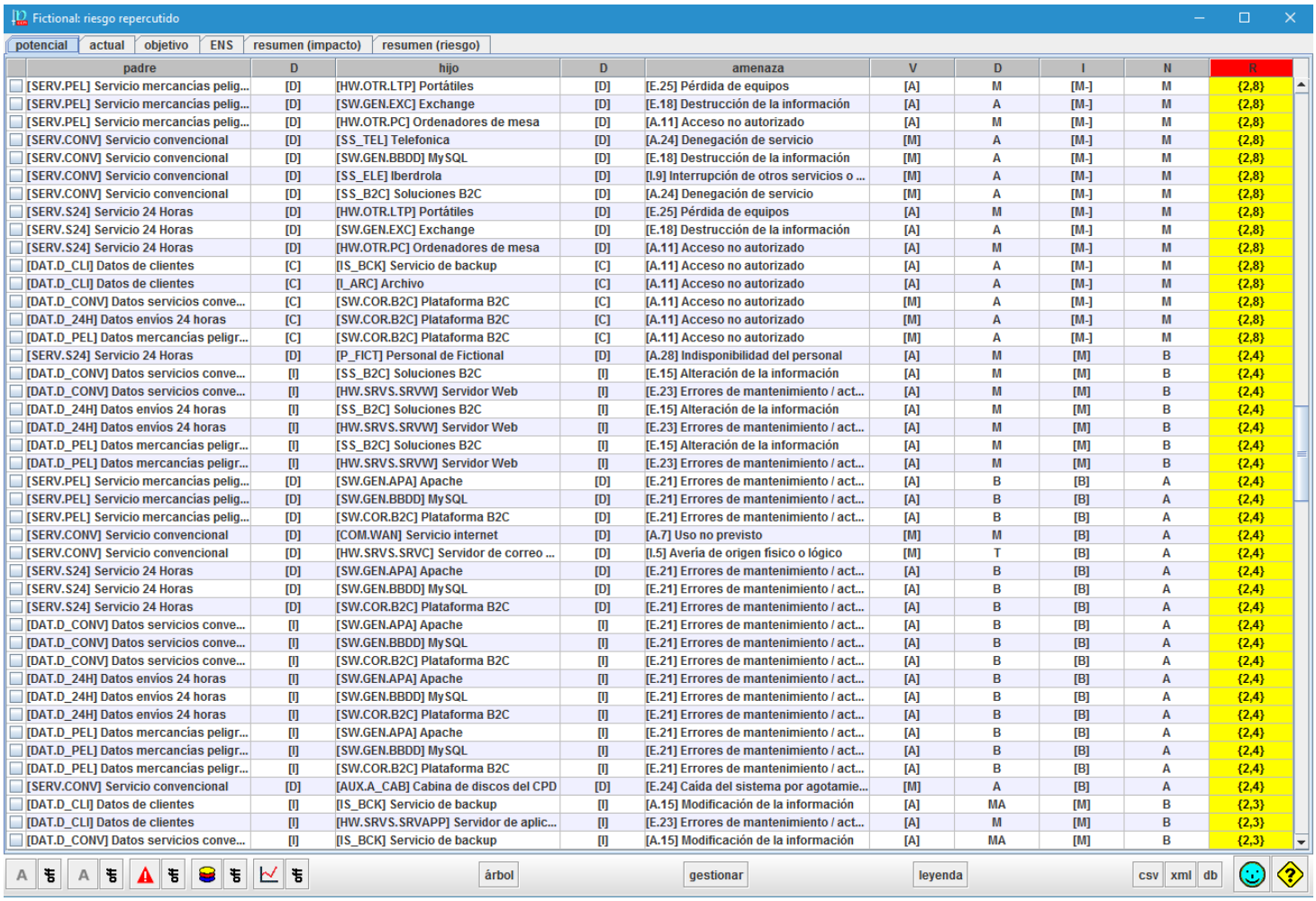
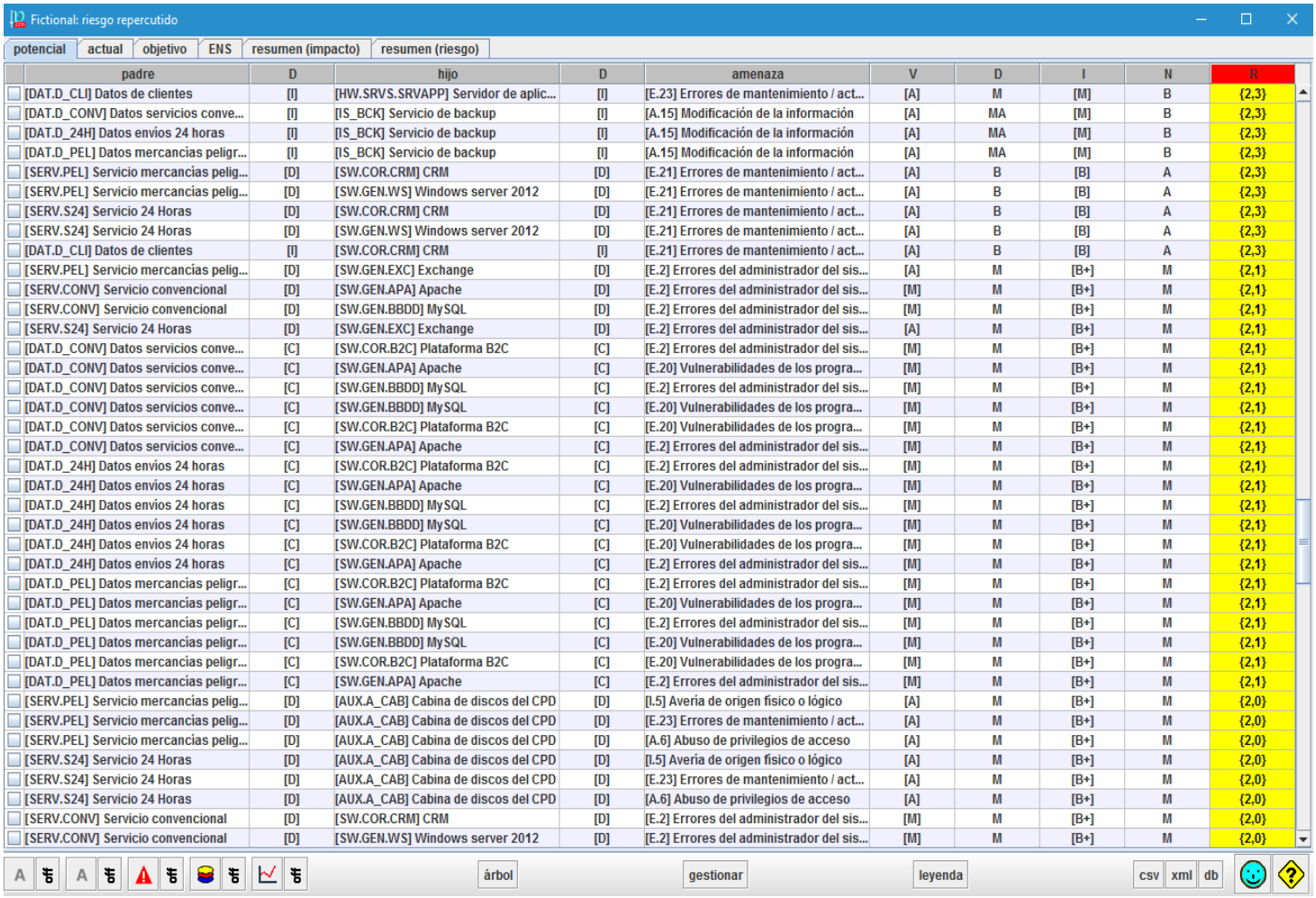


Ilustración 50 Riesgo potencial



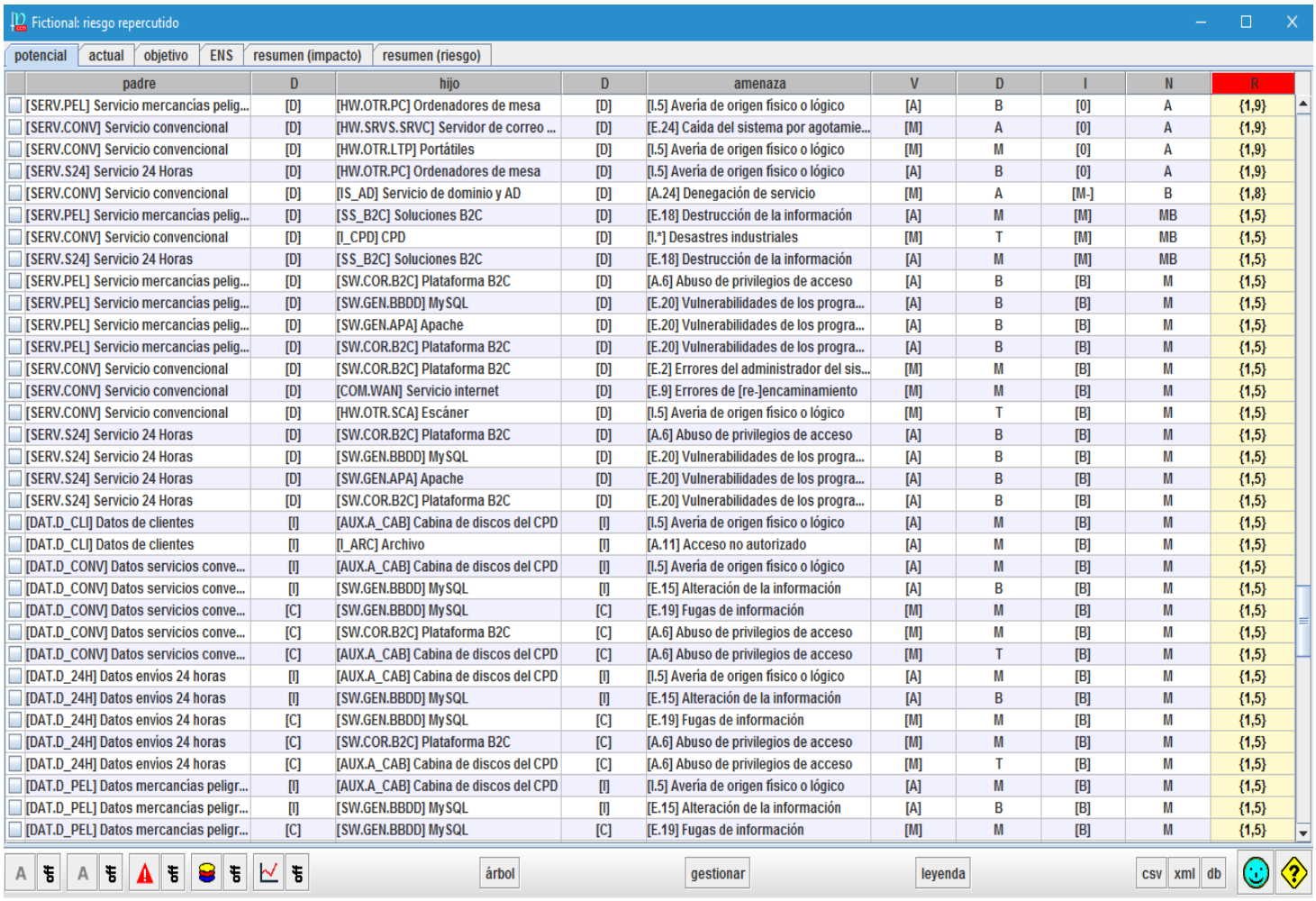
padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.PEL] Servicio mercancías pelig...	[D]	[HW.OTR.LTP] Portátiles	[D]	[E.25] Pérdida de equipos	[A]	M	[M-]	M	{2,8}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.GEN.EXC] Exchange	[D]	[E.18] Destrucción de la información	[A]	A	[M-]	M	{2,8}
[SERV.PEL] Servicio mercancías pelig...	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[A.11] Acceso no autorizado	[A]	M	[M-]	M	{2,8}
[SERV.CONV] Servicio convencional	[D]	[SS_TEL] Telefonica	[D]	[A.24] Denegación de servicio	[M]	A	[M-]	M	{2,8}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.18] Destrucción de la información	[M]	A	[M-]	M	{2,8}
[SERV.CONV] Servicio convencional	[D]	[SS_ELE] Iberdrola	[D]	[I.9] Interrupción de otros servicios o ...	[M]	A	[M-]	M	{2,8}
[SERV.CONV] Servicio convencional	[D]	[SS_B2C] Soluciones B2C	[D]	[A.24] Denegación de servicio	[M]	A	[M-]	M	{2,8}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.LTP] Portátiles	[D]	[E.25] Pérdida de equipos	[A]	M	[M-]	M	{2,8}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.EXC] Exchange	[D]	[E.18] Destrucción de la información	[A]	A	[M-]	M	{2,8}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[A.11] Acceso no autorizado	[A]	M	[M-]	M	{2,8}
[DAT.D_CLI] Datos de clientes	[C]	[IS_BCK] Servicio de backup	[C]	[A.11] Acceso no autorizado	[A]	A	[M-]	M	{2,8}
[DAT.D_CLI] Datos de clientes	[C]	[I_ARC] Archivo	[C]	[A.11] Acceso no autorizado	[A]	A	[M-]	M	{2,8}
[DAT.D_CONV] Datos servicios conve...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.11] Acceso no autorizado	[M]	A	[M-]	M	{2,8}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.11] Acceso no autorizado	[M]	A	[M-]	M	{2,8}
[DAT.D_PEL] Datos mercancías peligr...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.11] Acceso no autorizado	[M]	A	[M-]	M	{2,8}
[SERV.S24] Servicio 24 Horas	[D]	[P_FICT] Personal de Fictional	[D]	[A.28] Indisponibilidad del personal	[A]	M	[M]	B	{2,4}
[DAT.D_CONV] Datos servicios conve...	[I]	[SS_B2C] Soluciones B2C	[I]	[E.15] Alteración de la información	[A]	M	[M]	B	{2,4}
[DAT.D_CONV] Datos servicios conve...	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[E.23] Errores de mantenimiento / act...	[A]	M	[M]	B	{2,4}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SS_B2C] Soluciones B2C	[I]	[E.15] Alteración de la información	[A]	M	[M]	B	{2,4}
[DAT.D_24H] Datos envíos 24 horas	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[E.23] Errores de mantenimiento / act...	[A]	M	[M]	B	{2,4}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SS_B2C] Soluciones B2C	[I]	[E.15] Alteración de la información	[A]	M	[M]	B	{2,4}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[E.23] Errores de mantenimiento / act...	[A]	M	[M]	B	{2,4}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.GEN.APA] Apache	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[SERV.CONV] Servicio convencional	[D]	[COM.WAN] Servicio internet	[D]	[A.7] Uso no previsto	[M]	M	[B]	A	{2,4}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVC] Servidor de correo ...	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[B]	A	{2,4}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.APA] Apache	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.GEN.APA] Apache	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.APA] Apache	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.GEN.APA] Apache	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,4}
[SERV.CONV] Servicio convencional	[D]	[AUX.A_CAB] Cabina de discos del CPD	[D]	[E.24] Caída del sistema por agotamie...	[M]	A	[B]	A	{2,4}
[DAT.D_CLI] Datos de clientes	[I]	[IS_BCK] Servicio de backup	[I]	[A.15] Modificación de la información	[A]	MA	[M]	B	{2,3}
[DAT.D_CLI] Datos de clientes	[I]	[HW.SRVS.SRVAPP] Servidor de aplic...	[I]	[E.23] Errores de mantenimiento / act...	[A]	M	[M]	B	{2,3}
[DAT.D_CONV] Datos servicios conve...	[I]	[IS_BCK] Servicio de backup	[I]	[A.15] Modificación de la información	[A]	MA	[M]	B	{2,3}

Ilustración 51 Riesgo potencial



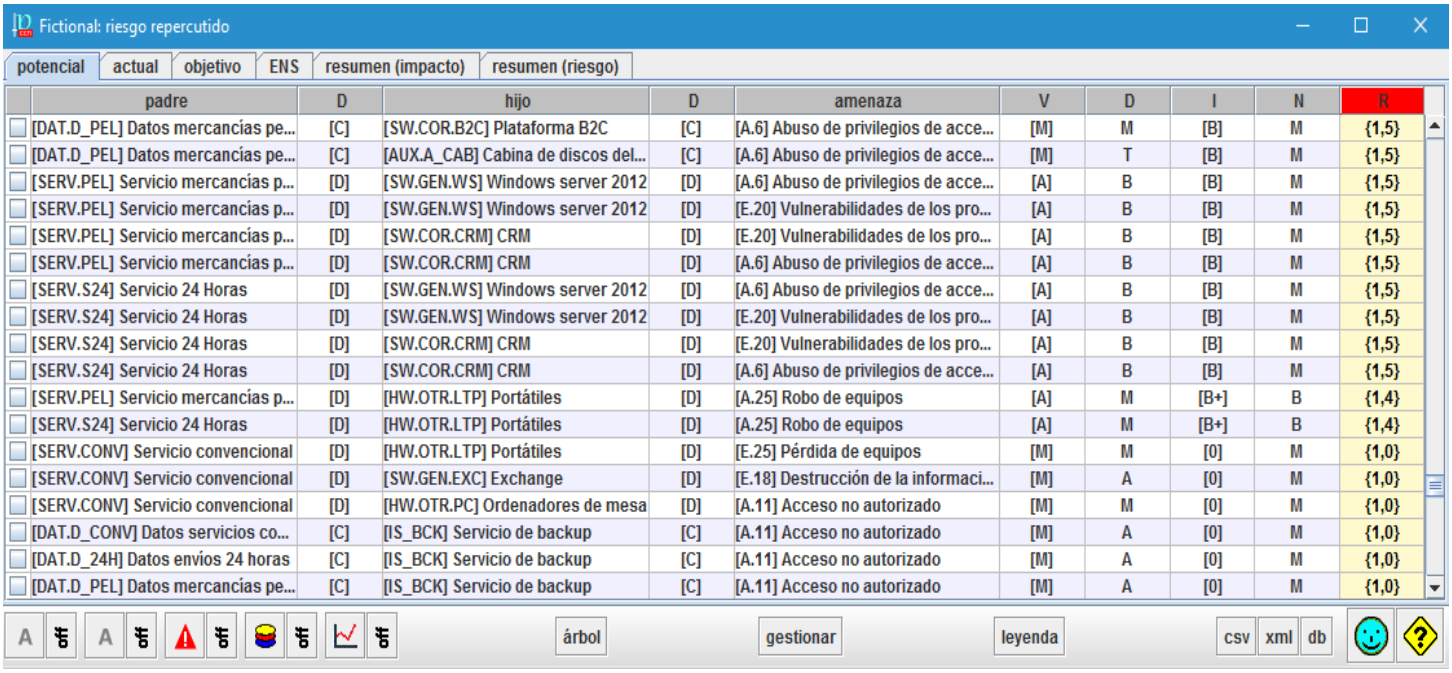
padre	D	hijo	D	amenaza	V	D	I	N	R
[DAT.D_CLI] Datos de clientes	[I]	[HW.SRVS.SRVAPP] Servidor de aplic...	[I]	[E.23] Errores de mantenimiento / act...	[A]	M	[M]	B	{2,3}
[DAT.D_CONV] Datos servicios conve...	[I]	[IS_BCK] Servicio de backup	[I]	[A.15] Modificación de la información	[A]	MA	[M]	B	{2,3}
[DAT.D_24H] Datos envíos 24 horas	[I]	[IS_BCK] Servicio de backup	[I]	[A.15] Modificación de la información	[A]	MA	[M]	B	{2,3}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[IS_BCK] Servicio de backup	[I]	[A.15] Modificación de la información	[A]	MA	[M]	B	{2,3}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.COR.CRM] CRM	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,3}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,3}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.CRM] CRM	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,3}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,3}
[DAT.D_CLI] Datos de clientes	[I]	[SW.COR.CRM] CRM	[I]	[E.21] Errores de mantenimiento / act...	[A]	B	[B]	A	{2,3}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.GEN.EXC] Exchange	[D]	[E.2] Errores del administrador del sis...	[A]	M	[B+]	M	{2,1}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.APA] Apache	[D]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.EXC] Exchange	[D]	[E.2] Errores del administrador del sis...	[A]	M	[B+]	M	{2,1}
[DAT.D_CONV] Datos servicios conve...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[DAT.D_CONV] Datos servicios conve...	[C]	[SW.GEN.APA] Apache	[C]	[E.20] Vulnerabilidades de los progra...	[M]	M	[B+]	M	{2,1}
[DAT.D_CONV] Datos servicios conve...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[DAT.D_CONV] Datos servicios conve...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.20] Vulnerabilidades de los progra...	[M]	M	[B+]	M	{2,1}
[DAT.D_CONV] Datos servicios conve...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.20] Vulnerabilidades de los progra...	[M]	M	[B+]	M	{2,1}
[DAT.D_CONV] Datos servicios conve...	[C]	[SW.GEN.APA] Apache	[C]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.GEN.APA] Apache	[C]	[E.20] Vulnerabilidades de los progra...	[M]	M	[B+]	M	{2,1}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.20] Vulnerabilidades de los progra...	[M]	M	[B+]	M	{2,1}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.20] Vulnerabilidades de los progra...	[M]	M	[B+]	M	{2,1}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.GEN.APA] Apache	[C]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[DAT.D_PEL] Datos mercancías peligr...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[DAT.D_PEL] Datos mercancías peligr...	[C]	[SW.GEN.APA] Apache	[C]	[E.20] Vulnerabilidades de los progra...	[M]	M	[B+]	M	{2,1}
[DAT.D_PEL] Datos mercancías peligr...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[DAT.D_PEL] Datos mercancías peligr...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.20] Vulnerabilidades de los progra...	[M]	M	[B+]	M	{2,1}
[DAT.D_PEL] Datos mercancías peligr...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.20] Vulnerabilidades de los progra...	[M]	M	[B+]	M	{2,1}
[DAT.D_PEL] Datos mercancías peligr...	[C]	[SW.GEN.APA] Apache	[C]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,1}
[SERV.PEL] Servicio mercancías pelig...	[D]	[AUX.A_CAB] Cabina de discos del CPD	[D]	[I.5] Avería de origen físico o lógico	[A]	M	[B+]	M	{2,0}
[SERV.PEL] Servicio mercancías pelig...	[D]	[AUX.A_CAB] Cabina de discos del CPD	[D]	[E.23] Errores de mantenimiento / act...	[A]	M	[B+]	M	{2,0}
[SERV.PEL] Servicio mercancías pelig...	[D]	[AUX.A_CAB] Cabina de discos del CPD	[D]	[A.6] Abuso de privilegios de acceso	[A]	M	[B+]	M	{2,0}
[SERV.S24] Servicio 24 Horas	[D]	[AUX.A_CAB] Cabina de discos del CPD	[D]	[I.5] Avería de origen físico o lógico	[A]	M	[B+]	M	{2,0}
[SERV.S24] Servicio 24 Horas	[D]	[AUX.A_CAB] Cabina de discos del CPD	[D]	[E.23] Errores de mantenimiento / act...	[A]	M	[B+]	M	{2,0}
[SERV.S24] Servicio 24 Horas	[D]	[AUX.A_CAB] Cabina de discos del CPD	[D]	[A.6] Abuso de privilegios de acceso	[A]	M	[B+]	M	{2,0}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.CRM] CRM	[D]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,0}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.2] Errores del administrador del sis...	[M]	M	[B+]	M	{2,0}

Ilustración 52 Riesgo potencial



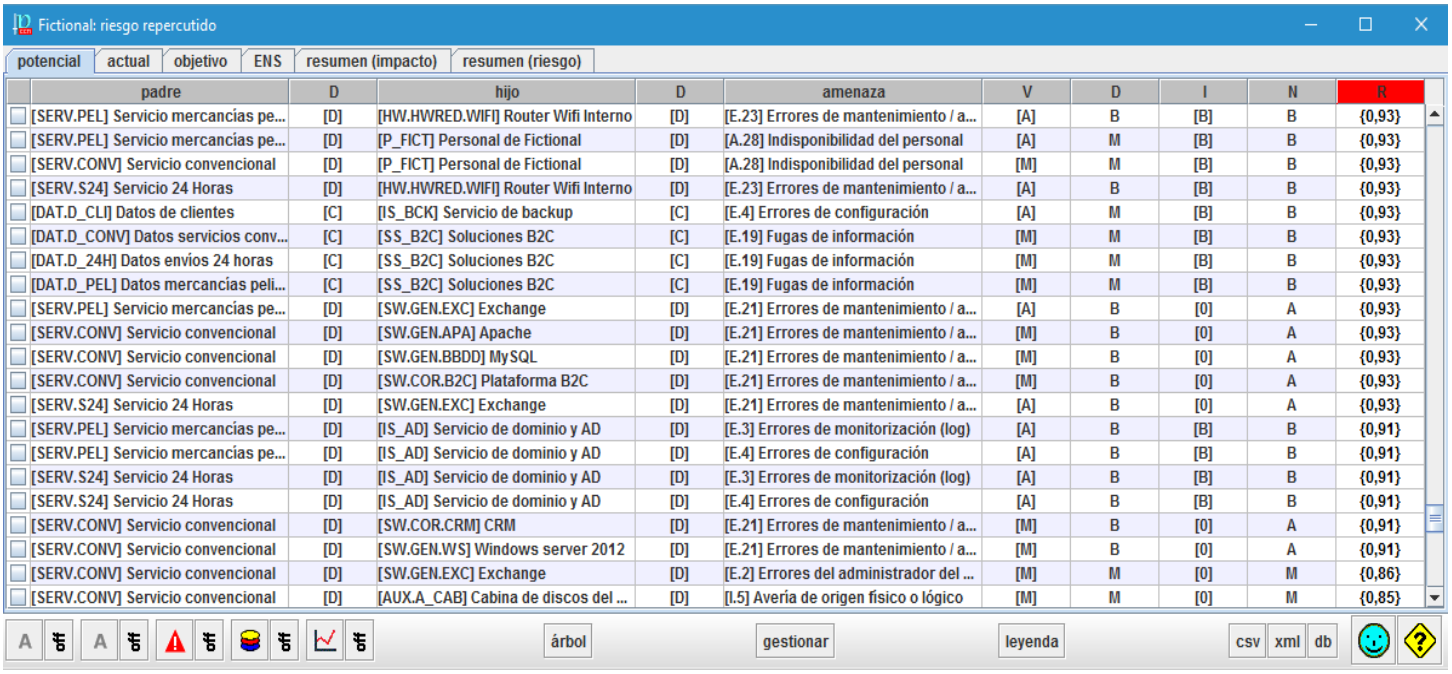
padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.PEL] Servicio mercancías pelig...	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[I.5] Avería de origen físico o lógico	[A]	B	[0]	A	{1,9}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVC] Servidor de correo ...	[D]	[E.24] Caída del sistema por agotamie...	[M]	A	[0]	A	{1,9}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.LTP] Portátiles	[D]	[I.5] Avería de origen físico o lógico	[M]	M	[0]	A	{1,9}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[I.5] Avería de origen físico o lógico	[A]	B	[0]	A	{1,9}
[SERV.CONV] Servicio convencional	[D]	[IS_AD] Servicio de dominio y AD	[D]	[A.24] Denegación de servicio	[M]	A	[M-]	B	{1,8}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SS_B2C] Soluciones B2C	[D]	[E.18] Destrucción de la información	[A]	M	[M]	MB	{1,5}
[SERV.CONV] Servicio convencional	[D]	[I_CPD] CPD	[D]	[I.*] Desastres industriales	[M]	T	[M]	MB	{1,5}
[SERV.S24] Servicio 24 Horas	[D]	[SS_B2C] Soluciones B2C	[D]	[E.18] Destrucción de la información	[A]	M	[M]	MB	{1,5}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[A.6] Abuso de privilegios de acceso	[A]	B	[B]	M	{1,5}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.20] Vulnerabilidades de los progra...	[A]	B	[B]	M	{1,5}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.GEN.APA] Apache	[D]	[E.20] Vulnerabilidades de los progra...	[A]	B	[B]	M	{1,5}
[SERV.PEL] Servicio mercancías pelig...	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.20] Vulnerabilidades de los progra...	[A]	B	[B]	M	{1,5}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.2] Errores del administrador del sis...	[M]	M	[B]	M	{1,5}
[SERV.CONV] Servicio convencional	[D]	[COM.WAN] Servicio internet	[D]	[E.9] Errores de [re-]encaminamiento	[M]	M	[B]	M	{1,5}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.SCA] Escáner	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[B]	M	{1,5}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[A.6] Abuso de privilegios de acceso	[A]	B	[B]	M	{1,5}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.20] Vulnerabilidades de los progra...	[A]	B	[B]	M	{1,5}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.APA] Apache	[D]	[E.20] Vulnerabilidades de los progra...	[A]	B	[B]	M	{1,5}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.20] Vulnerabilidades de los progra...	[A]	B	[B]	M	{1,5}
[DAT.D_CLI] Datos de clientes	[I]	[AUX.A_CAB] Cabina de discos del CPD	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[B]	M	{1,5}
[DAT.D_CLI] Datos de clientes	[I]	[I_ARC] Archivo	[I]	[A.11] Acceso no autorizado	[A]	M	[B]	M	{1,5}
[DAT.D_CONV] Datos servicios conve...	[I]	[AUX.A_CAB] Cabina de discos del CPD	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[B]	M	{1,5}
[DAT.D_CONV] Datos servicios conve...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.15] Alteración de la información	[A]	B	[B]	M	{1,5}
[DAT.D_CONV] Datos servicios conve...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.19] Fugas de información	[M]	M	[B]	M	{1,5}
[DAT.D_CONV] Datos servicios conve...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.6] Abuso de privilegios de acceso	[M]	M	[B]	M	{1,5}
[DAT.D_CONV] Datos servicios conve...	[C]	[AUX.A_CAB] Cabina de discos del CPD	[C]	[A.6] Abuso de privilegios de acceso	[M]	T	[B]	M	{1,5}
[DAT.D_24H] Datos envíos 24 horas	[I]	[AUX.A_CAB] Cabina de discos del CPD	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[B]	M	{1,5}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.15] Alteración de la información	[A]	B	[B]	M	{1,5}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.19] Fugas de información	[M]	M	[B]	M	{1,5}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.6] Abuso de privilegios de acceso	[M]	M	[B]	M	{1,5}
[DAT.D_24H] Datos envíos 24 horas	[C]	[AUX.A_CAB] Cabina de discos del CPD	[C]	[A.6] Abuso de privilegios de acceso	[M]	T	[B]	M	{1,5}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[AUX.A_CAB] Cabina de discos del CPD	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[B]	M	{1,5}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.15] Alteración de la información	[A]	B	[B]	M	{1,5}
[DAT.D_PEL] Datos mercancías peligr...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.19] Fugas de información	[M]	M	[B]	M	{1,5}

Ilustración 54 Riesgo potencial



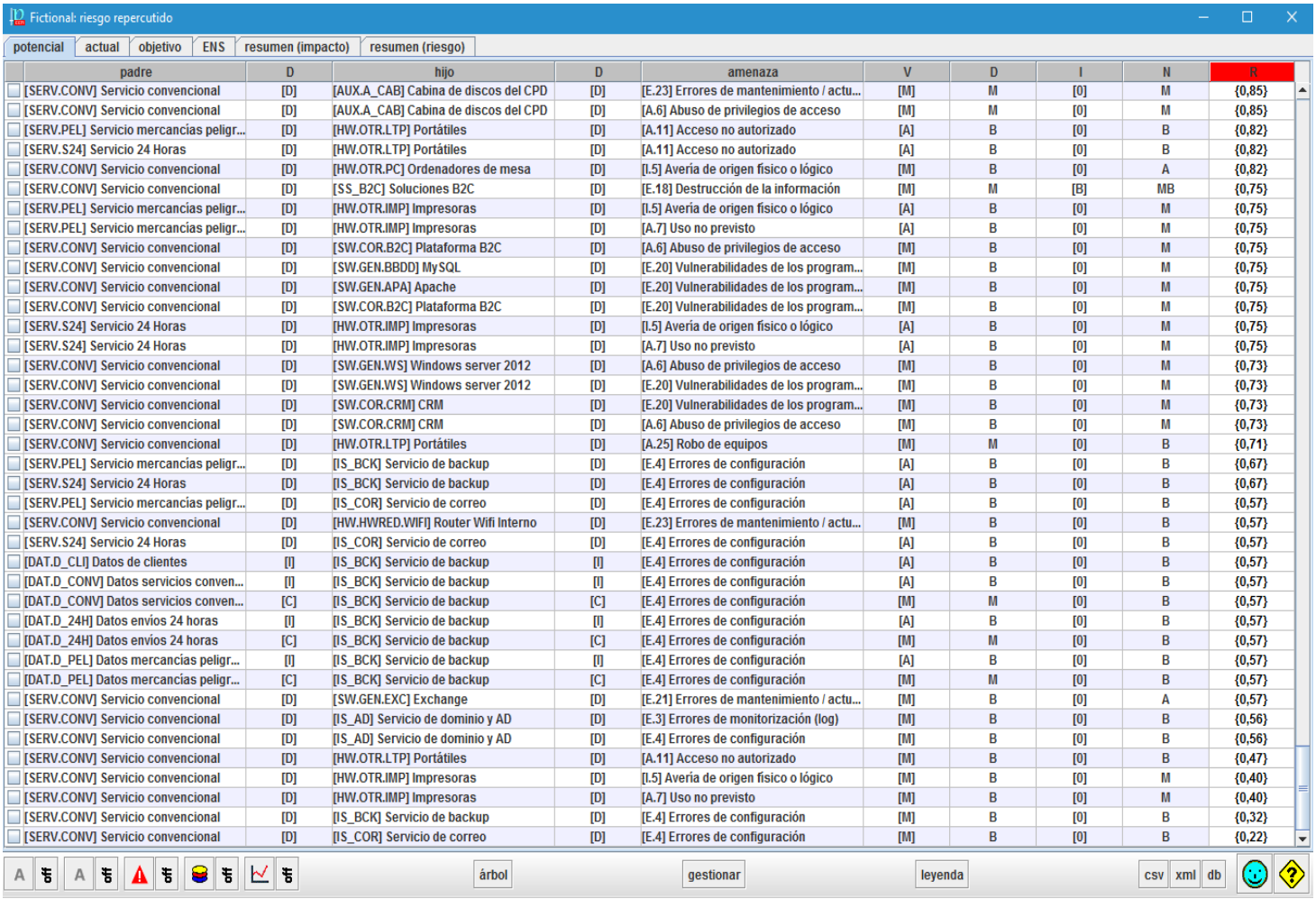
padre	D	hijo	D	amenaza	V	D	I	N	R
[DAT.D_PEL] Datos mercancías pe...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.6] Abuso de privilegios de acce...	[M]	M	[B]	M	{1,5}
[DAT.D_PEL] Datos mercancías pe...	[C]	[AUX.A_CAB] Cabina de discos del...	[C]	[A.6] Abuso de privilegios de acce...	[M]	T	[B]	M	{1,5}
[SERV.PEL] Servicio mercancías p...	[D]	[SW.GEN.WS] Windows server 2012	[D]	[A.6] Abuso de privilegios de acce...	[A]	B	[B]	M	{1,5}
[SERV.PEL] Servicio mercancías p...	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.20] Vulnerabilidades de los pro...	[A]	B	[B]	M	{1,5}
[SERV.PEL] Servicio mercancías p...	[D]	[SW.COR.CRM] CRM	[D]	[E.20] Vulnerabilidades de los pro...	[A]	B	[B]	M	{1,5}
[SERV.PEL] Servicio mercancías p...	[D]	[SW.COR.CRM] CRM	[D]	[A.6] Abuso de privilegios de acce...	[A]	B	[B]	M	{1,5}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.WS] Windows server 2012	[D]	[A.6] Abuso de privilegios de acce...	[A]	B	[B]	M	{1,5}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.20] Vulnerabilidades de los pro...	[A]	B	[B]	M	{1,5}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.CRM] CRM	[D]	[E.20] Vulnerabilidades de los pro...	[A]	B	[B]	M	{1,5}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.CRM] CRM	[D]	[A.6] Abuso de privilegios de acce...	[A]	B	[B]	M	{1,5}
[SERV.PEL] Servicio mercancías p...	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.25] Robo de equipos	[A]	M	[B+]	B	{1,4}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.25] Robo de equipos	[A]	M	[B+]	B	{1,4}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.LTP] Portátiles	[D]	[E.25] Pérdida de equipos	[M]	M	[0]	M	{1,0}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.EXC] Exchange	[D]	[E.18] Destrucción de la informaci...	[M]	A	[0]	M	{1,0}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[A.11] Acceso no autorizado	[M]	M	[0]	M	{1,0}
[DAT.D_CONV] Datos servicios co...	[C]	[IS_BCK] Servicio de backup	[C]	[A.11] Acceso no autorizado	[M]	A	[0]	M	{1,0}
[DAT.D_24H] Datos envíos 24 horas	[C]	[IS_BCK] Servicio de backup	[C]	[A.11] Acceso no autorizado	[M]	A	[0]	M	{1,0}
[DAT.D_PEL] Datos mercancías pe...	[C]	[IS_BCK] Servicio de backup	[C]	[A.11] Acceso no autorizado	[M]	A	[0]	M	{1,0}

Ilustración 53 Riesgo potencial



padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[E.23] Errores de mantenimiento / a...	[A]	B	[B]	B	{0,93}
[SERV.PEL] Servicio mercancías pe...	[D]	[P_FICT] Personal de Fictional	[D]	[A.28] Indisponibilidad del personal	[A]	M	[B]	B	{0,93}
[SERV.CONV] Servicio convencional	[D]	[P_FICT] Personal de Fictional	[D]	[A.28] Indisponibilidad del personal	[M]	M	[B]	B	{0,93}
[SERV.S24] Servicio 24 Horas	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[E.23] Errores de mantenimiento / a...	[A]	B	[B]	B	{0,93}
[DAT.D_CLI] Datos de clientes	[C]	[IS_BCK] Servicio de backup	[C]	[E.4] Errores de configuración	[A]	M	[B]	B	{0,93}
[DAT.D_CONV] Datos servicios conv...	[C]	[SS_B2C] Soluciones B2C	[C]	[E.19] Fugas de información	[M]	M	[B]	B	{0,93}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SS_B2C] Soluciones B2C	[C]	[E.19] Fugas de información	[M]	M	[B]	B	{0,93}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SS_B2C] Soluciones B2C	[C]	[E.19] Fugas de información	[M]	M	[B]	B	{0,93}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.EXC] Exchange	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	A	{0,93}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.APA] Apache	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	A	{0,93}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	A	{0,93}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	A	{0,93}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.EXC] Exchange	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	A	{0,93}
[SERV.PEL] Servicio mercancías pe...	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.3] Errores de monitorización (log)	[A]	B	[B]	B	{0,91}
[SERV.PEL] Servicio mercancías pe...	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.4] Errores de configuración	[A]	B	[B]	B	{0,91}
[SERV.S24] Servicio 24 Horas	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.3] Errores de monitorización (log)	[A]	B	[B]	B	{0,91}
[SERV.S24] Servicio 24 Horas	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.4] Errores de configuración	[A]	B	[B]	B	{0,91}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.CRM] CRM	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	A	{0,91}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	A	{0,91}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.EXC] Exchange	[D]	[E.2] Errores del administrador del ...	[M]	M	[0]	M	{0,86}
[SERV.CONV] Servicio convencional	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[I.5] Avería de origen físico o lógico	[M]	M	[0]	M	{0,85}

Ilustración 55 Riesgo potencial



padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.CONV] Servicio convencional	[D]	[AUX.A_CAB] Cabina de discos del CPD	[D]	[E.23] Errores de mantenimiento / actu...	[M]	M	[0]	M	{0,85}
[SERV.CONV] Servicio convencional	[D]	[AUX.A_CAB] Cabina de discos del CPD	[D]	[A.6] Abuso de privilegios de acceso	[M]	M	[0]	M	{0,85}
[SERV.PEL] Servicio mercancías peligr...	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.11] Acceso no autorizado	[A]	B	[0]	B	{0,82}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.11] Acceso no autorizado	[A]	B	[0]	B	{0,82}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[I.5] Avería de origen físico o lógico	[M]	B	[0]	A	{0,82}
[SERV.CONV] Servicio convencional	[D]	[SS_B2C] Soluciones B2C	[D]	[E.18] Destrucción de la información	[M]	M	[B]	MB	{0,75}
[SERV.PEL] Servicio mercancías peligr...	[D]	[HW.OTR.IMP] Impresoras	[D]	[I.5] Avería de origen físico o lógico	[A]	B	[0]	M	{0,75}
[SERV.PEL] Servicio mercancías peligr...	[D]	[HW.OTR.IMP] Impresoras	[D]	[A.7] Uso no previsto	[A]	B	[0]	M	{0,75}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[A.6] Abuso de privilegios de acceso	[M]	B	[0]	M	{0,75}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.20] Vulnerabilidades de los program...	[M]	B	[0]	M	{0,75}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.APA] Apache	[D]	[E.20] Vulnerabilidades de los program...	[M]	B	[0]	M	{0,75}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.20] Vulnerabilidades de los program...	[M]	B	[0]	M	{0,75}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.IMP] Impresoras	[D]	[I.5] Avería de origen físico o lógico	[A]	B	[0]	M	{0,75}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.IMP] Impresoras	[D]	[A.7] Uso no previsto	[A]	B	[0]	M	{0,75}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.WS] Windows server 2012	[D]	[A.6] Abuso de privilegios de acceso	[M]	B	[0]	M	{0,73}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.20] Vulnerabilidades de los program...	[M]	B	[0]	M	{0,73}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.CRM] CRM	[D]	[E.20] Vulnerabilidades de los program...	[M]	B	[0]	M	{0,73}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.CRM] CRM	[D]	[A.6] Abuso de privilegios de acceso	[M]	B	[0]	M	{0,73}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.25] Robo de equipos	[M]	M	[0]	B	{0,71}
[SERV.PEL] Servicio mercancías peligr...	[D]	[IS_BCK] Servicio de backup	[D]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,67}
[SERV.S24] Servicio 24 Horas	[D]	[IS_BCK] Servicio de backup	[D]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,67}
[SERV.PEL] Servicio mercancías peligr...	[D]	[IS_COR] Servicio de correo	[D]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,57}
[SERV.CONV] Servicio convencional	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[E.23] Errores de mantenimiento / actu...	[M]	B	[0]	B	{0,57}
[SERV.S24] Servicio 24 Horas	[D]	[IS_COR] Servicio de correo	[D]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,57}
[DAT.D_CLI] Datos de clientes	[I]	[IS_BCK] Servicio de backup	[I]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,57}
[DAT.D_CONV] Datos servicios conven...	[I]	[IS_BCK] Servicio de backup	[I]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,57}
[DAT.D_CONV] Datos servicios conven...	[C]	[IS_BCK] Servicio de backup	[C]	[E.4] Errores de configuración	[M]	M	[0]	B	{0,57}
[DAT.D_24H] Datos envíos 24 horas	[I]	[IS_BCK] Servicio de backup	[I]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,57}
[DAT.D_24H] Datos envíos 24 horas	[C]	[IS_BCK] Servicio de backup	[C]	[E.4] Errores de configuración	[M]	M	[0]	B	{0,57}
[DAT.D_PEL] Datos mercancías peligr...	[I]	[IS_BCK] Servicio de backup	[I]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,57}
[DAT.D_PEL] Datos mercancías peligr...	[C]	[IS_BCK] Servicio de backup	[C]	[E.4] Errores de configuración	[M]	M	[0]	B	{0,57}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.EXC] Exchange	[D]	[E.21] Errores de mantenimiento / actu...	[M]	B	[0]	A	{0,57}
[SERV.CONV] Servicio convencional	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.3] Errores de monitorización (log)	[M]	B	[0]	B	{0,56}
[SERV.CONV] Servicio convencional	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.4] Errores de configuración	[M]	B	[0]	B	{0,56}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.11] Acceso no autorizado	[M]	B	[0]	B	{0,47}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.IMP] Impresoras	[D]	[I.5] Avería de origen físico o lógico	[M]	B	[0]	M	{0,40}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.IMP] Impresoras	[D]	[A.7] Uso no previsto	[M]	B	[0]	M	{0,40}
[SERV.CONV] Servicio convencional	[D]	[IS_BCK] Servicio de backup	[D]	[E.4] Errores de configuración	[M]	B	[0]	B	{0,32}
[SERV.CONV] Servicio convencional	[D]	[IS_COR] Servicio de correo	[D]	[E.4] Errores de configuración	[M]	B	[0]	B	{0,22}

Ilustración 56 Riesgo potencial

4.8.1 Criterio de aceptación

A la vista de los resultados obtenidos, el comité de dirección de la organización Fictional ha decidido asumir los riesgos entre los que se encuentra la organización por debajo de 5.

5. Fase 4: Propuestas de proyectos

5.1 Introducción

Tras haber realizado el análisis de riesgos, es el momento de formular una serie de propuestas con el fin de que el riesgo potencial disminuya significativamente.

Para ello se llevará a cabo un Plan de Tratamiento de Riesgos. A continuación se realizará la aplicación de controles correspondiente a la ISO 27002 y se obtendrá el riesgo residual de Fictional, que deberá ser menor que el potencial al haber aplicado las propuestas del PTR.

5.2 Propuestas

Se ha realizado un fichero Excel en el que se encuentran las propuestas a realizar para disminuir el riesgo potencial. Dicho fichero se presentará al Comité de Dirección de Fictional para que valoren las propuestas.

Se ha asignado un propietario y un responsable de ejecución para cada propuesta así como el control asociado a la misma. Además, se ha establecido el tipo de tratamiento que se llevará a cabo, pudiendo ser: mitigar, eliminar, prevenir o asumir. Por último, se ha planificado el tiempo que será necesario para llevar a cabo cada propuesta.

Plan de Tratamiento de Riesgos - Fictional S.L.

TRATAMIENTO
Mitigar
Eliminar
Prevenir
Asumir

PLANIFICACIÓN
Inmediata <1mes
Corta <3 meses
Media <6 meses
Larga >12 meses

ESTADO
Planificada
Abierta
Cerrada
Desestimada

ID	ACTIVO	RIESGO	NIVEL DE RIESGO	TRATAMIENTO	MEDIDA A IMPLANTAR	CONTROL A 27001	PROPIETARIO	RESPONSABLE DE EJECUCION	PLANIFICACIÓN	RECURSOS	ESTADO	FECHA DE PLANIFICADA/CIERRE	OBSERVACIONES
1	Datos de clientes	Acceso no autorizado	6,1	MITIGAR	*Elaborar la normativa de control de acceso (A) *Definir roles con autorización exclusiva para realizar tareas (B) *Implantar una política robusta de contraseñas (C) *Limitar el tiempo de conexión de sesión (D) *Establecer un proceso periódico de revisión de permisos de usuario (E)	A.9.1.1 Política de control de acceso A.9.2.1 Altas y bajas de usuarios A.9.4.1 Sistema de gestión de contraseñas A.9.4.2 Procedimientos de seguros de inicio de sesión	Adrián Núñez	Adrián Núñez	A --> Inmediato B --> Inmediato C --> Corto D --> Inmediato E --> Inmediato	A --> 10 horas B --> 15 horas C --> 40 horas D --> 3 horas E --> 10 horas	Pendiente de valorar	Pendiente de valorar	
2	Servidor web	Avería de origen físico o lógico	5,8	MITIGAR	*Habilitar mecanismos de alta disponibilidad (F) *Identificar proveedor Hosting de respaldo en caso de contingencia del CPD (G) *Elaborar PCN (H) *Revisar contratos de mantenimiento con proveedores hardware (I)	A.11.1.2 Controles físicos de entrada A.11.2.4 Mantenimiento de los equipos	Adrián Núñez	Aurelio Pérez	F --> Corto G --> Inmediato H --> Medio I --> Corto	F --> 40 horas G --> 10 horas H --> 150 horas I --> 30 horas	Pendiente de valorar	Pendiente de valorar	
3	Datos de clientes	Revelación de información	5,8	MITIGAR	*Elaborar normativa sobre uso correcto de las comunicaciones (J) *Suscribir acuerdos de confidencialidad con empleados y proveedores (K)	A.13.1.2 Políticas y procedimientos de trasferencia de información A.13.2.4 Acuerdo de confidencialidad o no divulgación	Adrián Núñez	Silvia Rubio	J --> Inmediato K --> Corto	J --> 10 horas K --> 40 horas	Pendiente de valorar	Pendiente de valorar	
4	Servidor de dominio y AD Servidor de aplicaciones (CRM) y ficheros	Avería de origen físico o lógico	5,7	MITIGAR	*Habilitar mecanismos de alta disponibilidad (L) *Identificar proveedor Hosting de respaldo en caso de contingencia del CPD (M) *Elaborar PCN (N) *Revisar contratos de mantenimiento con proveedores hardware (Ñ)	A.11.1.2 Controles físicos de entrada A.11.2.4 Mantenimiento de los equipos	Adrián Núñez	Aurelio Pérez	L --> Corto M --> Inmediato N --> Medio Ñ --> Corto	L --> 40 horas M --> 10 horas N --> 150 horas Ñ --> 30 horas	Pendiente de valorar	Pendiente de valorar	
5	Datos de clientes Datos servicios convencionales Datos envios 24 horas Datos mercancías peligrosas	Modificación de la información	5,7	MITIGAR	*Habilitar mecanismo de registro de acceso al servidor de fichero (O) *Establecer política de acceso a la información basada en need to know (P)	A.9.4.4 Uso de los recursos del sistema con privilegios especiales A.9.4.5 Control de acceso al código fuente de los programas	Adrián Núñez	Adrián Núñez	O --> Corto P --> Inmediato	O --> 40 horas P --> 10 horas	Pendiente de valorar	Pendiente de valorar	
6	Antonio	Indisponibilidad del personal	5,6	MITIGAR	Contratar empleado con carnet para transportar mercancías peligrosas (Q)	A.17 Continuidad de negocio	Silvia Rubio	Silvia Rubio	Q --> Corto	Q --> 25 horas	Pendiente de valorar	Pendiente de valorar	
7	Servidor de dominio y AD Servidor de aplicaciones (CRM) y ficheros	Caída del sistema por agotamiento de recursos	5,3	MITIGAR	*Establecer/implantar un proceso de gestión de la capacidad y de la demanda (R) *Implantar herramienta de monitorización (S)	A.16.1.2 Notificación de eventos de seguridad de la información A.16.1.3 Notificación de puntos débiles de seguridad	Adrián Núñez	Adrián Núñez	R --> Medio S --> Medio	R --> 150 S --> 150	Pendiente de valorar	Pendiente de valorar	
8	Router Wifi Interno	Avería de origen físico o lógico	5,1	MITIGAR	*Adquirir otro router (T)	A.13.1.2 Seguridad de los servicios de red A.13.1.3 Segregación de redes	Adrián Núñez	Aurelio Pérez	T --> Inmediato	T --> 8 horas	Pendiente de valorar	Pendiente de valorar	
9	Telefónica	Fallo de servicios de comunicac	5,1	MITIGAR	*Contratar una línea de respaldo de comunicaciones (U) *Elaborar PCN (V)	A.15.2.1 Control y revisión de la provisión de servicios del provedor	Adrián Núñez	Aurelio Pérez	U --> Corto V --> Medio	U --> 25 horas V --> 150 horas	Pendiente de valorar	Pendiente de valorar	

Ilustración 57 Captura de pantalla del Plan de Tratamiento de Riesgos

Con el objetivo de tener una visión global de los proyectos en función del tiempo estimado de ejecución y los recursos necesarios se ha realizado el siguiente Diagrama de Gantt:

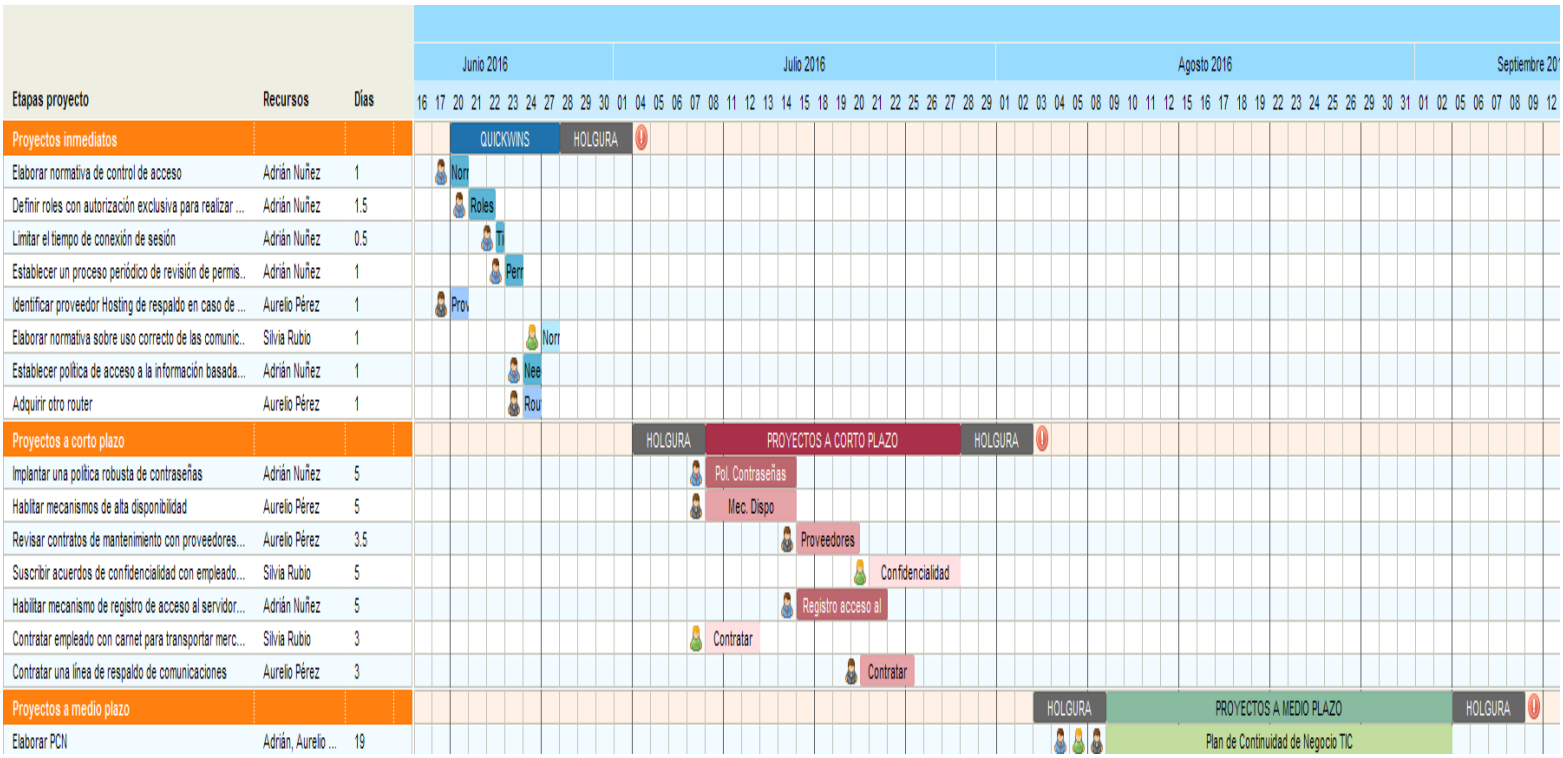


Ilustración 58 Diagrama de Gantt - PTR

Como se puede observar, el Plan de Tratamientos de Riesgos comenzaría el 20 de junio y finalizaría en torno al 2 de septiembre. Las tareas se han distribuido en los siguientes empleados: Adrián Núñez, Silvia Rubio y Aurelio Pérez.

5.3 Aplicación de controles

Una vez se han evaluado los riesgos potenciales y se han implantado en Fictional las propuestas derivadas del Plan de Tratamiento de riesgos, se realiza la aplicación de controles para obtener el riesgo residual.

Se contemplan por tanto las medidas de seguridad previamente implantadas en Fictional al comienzo de la implantación de la ISO 27001 y las propuestas realizadas del Plan de Tratamiento de Riesgos.

La aplicación de controles se realiza en base al CMM al igual que se hizo en el análisis diferencial realizado en la primera fase de la implantación.

La pestaña actual se refiere al estado de madurez inicial en la organización y la pestaña POST PTR al nivel de madurez una implantadas las medidas del Plan de Tratamiento de Riegos.

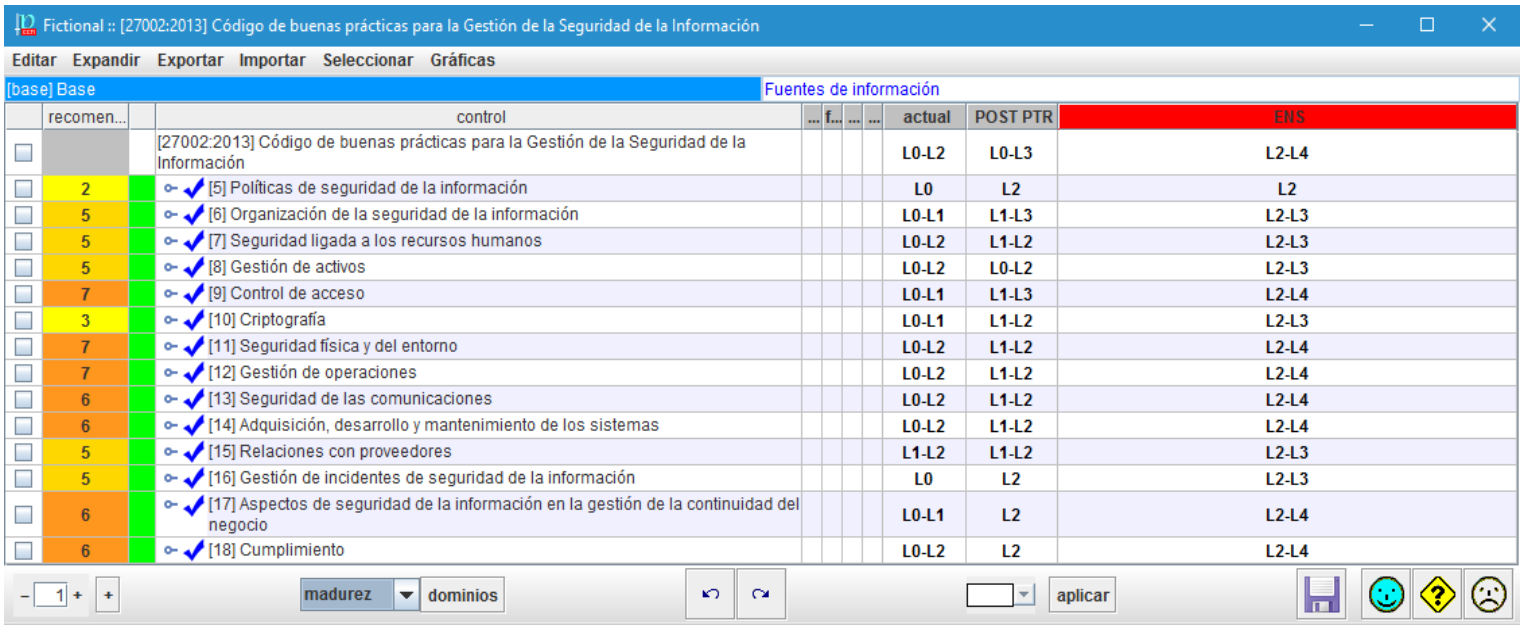


Ilustración 59 Aplicación de controles POST PTR

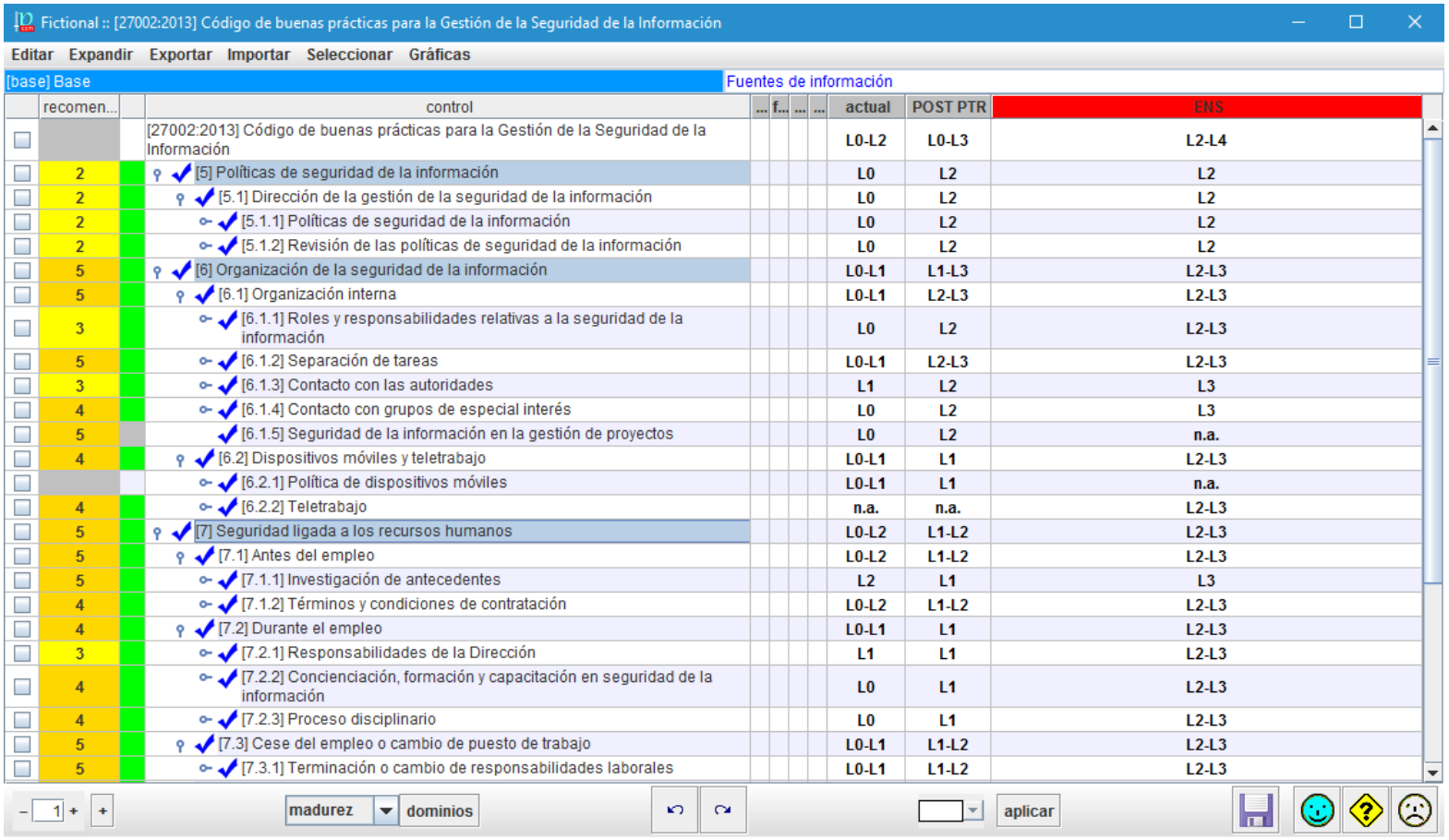


Ilustración 60 Aplicación de controles en dominios 5, 6 y 7 - POST PTR

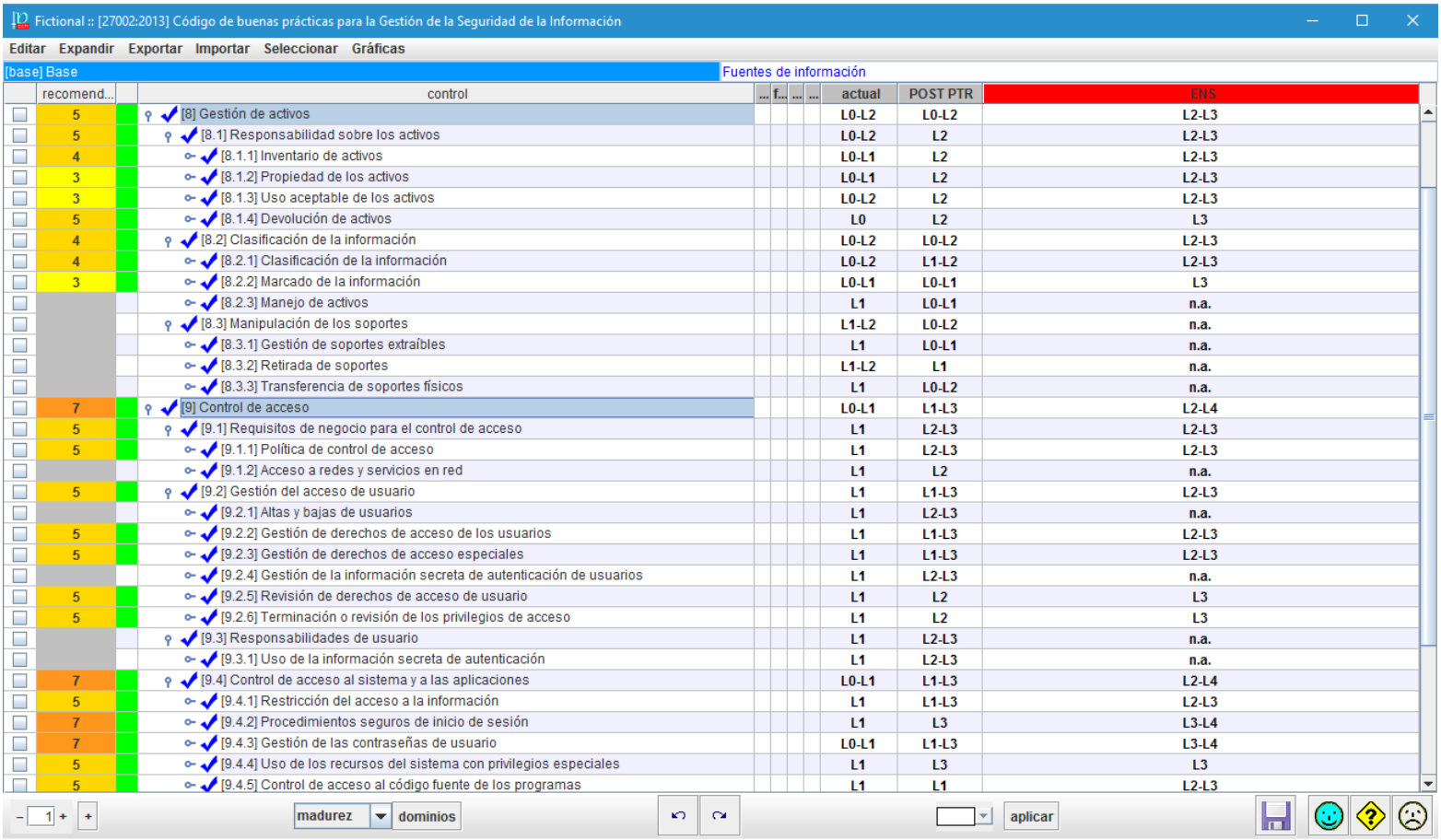


Ilustración 61 Aplicación de controles en dominios 8 y 9 - POST PTR

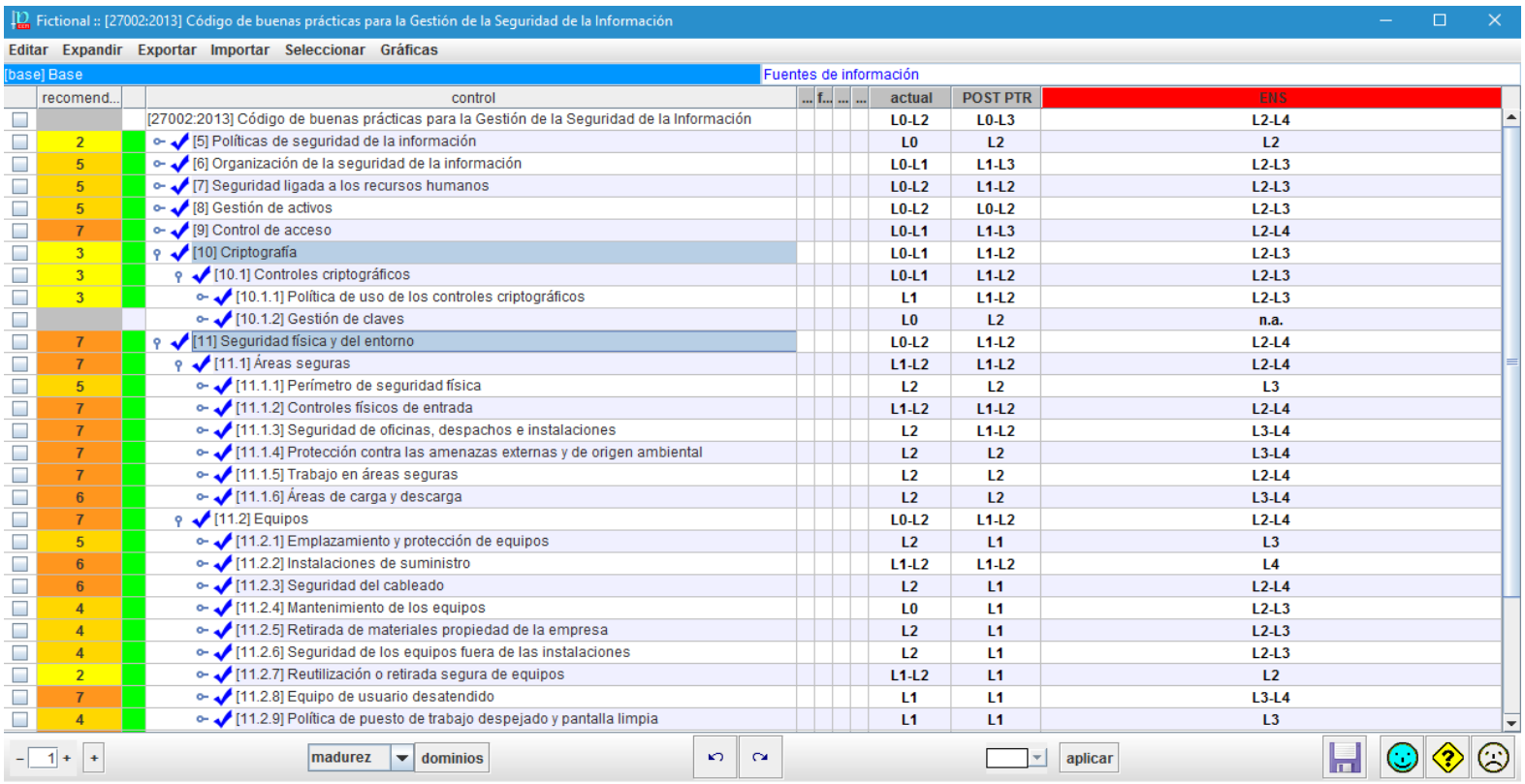


Ilustración 62 Aplicación de controles en dominios 10 y 11 - POST PTR

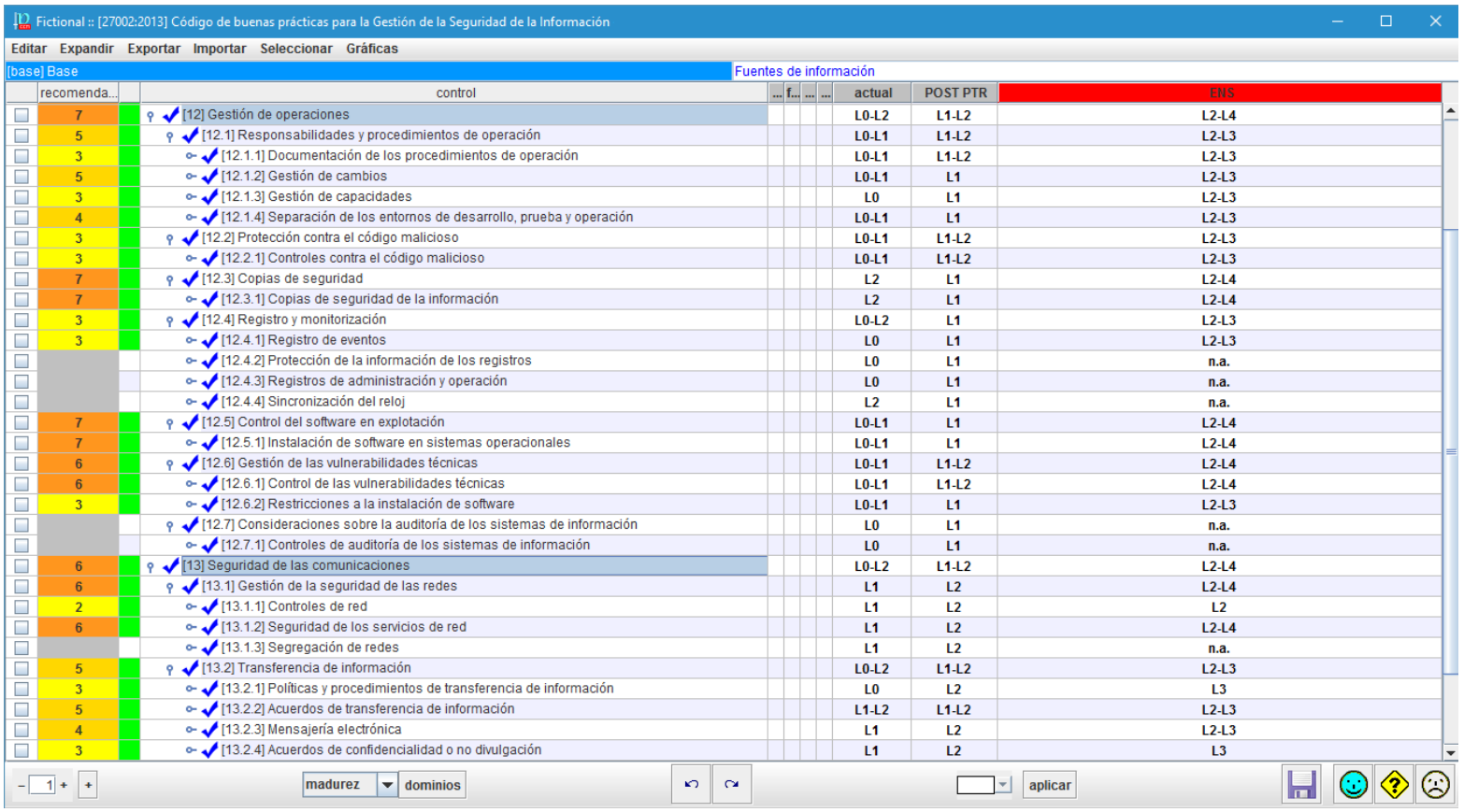


Ilustración 63 Aplicación de controles en dominios 12 y 13 - POST PTR

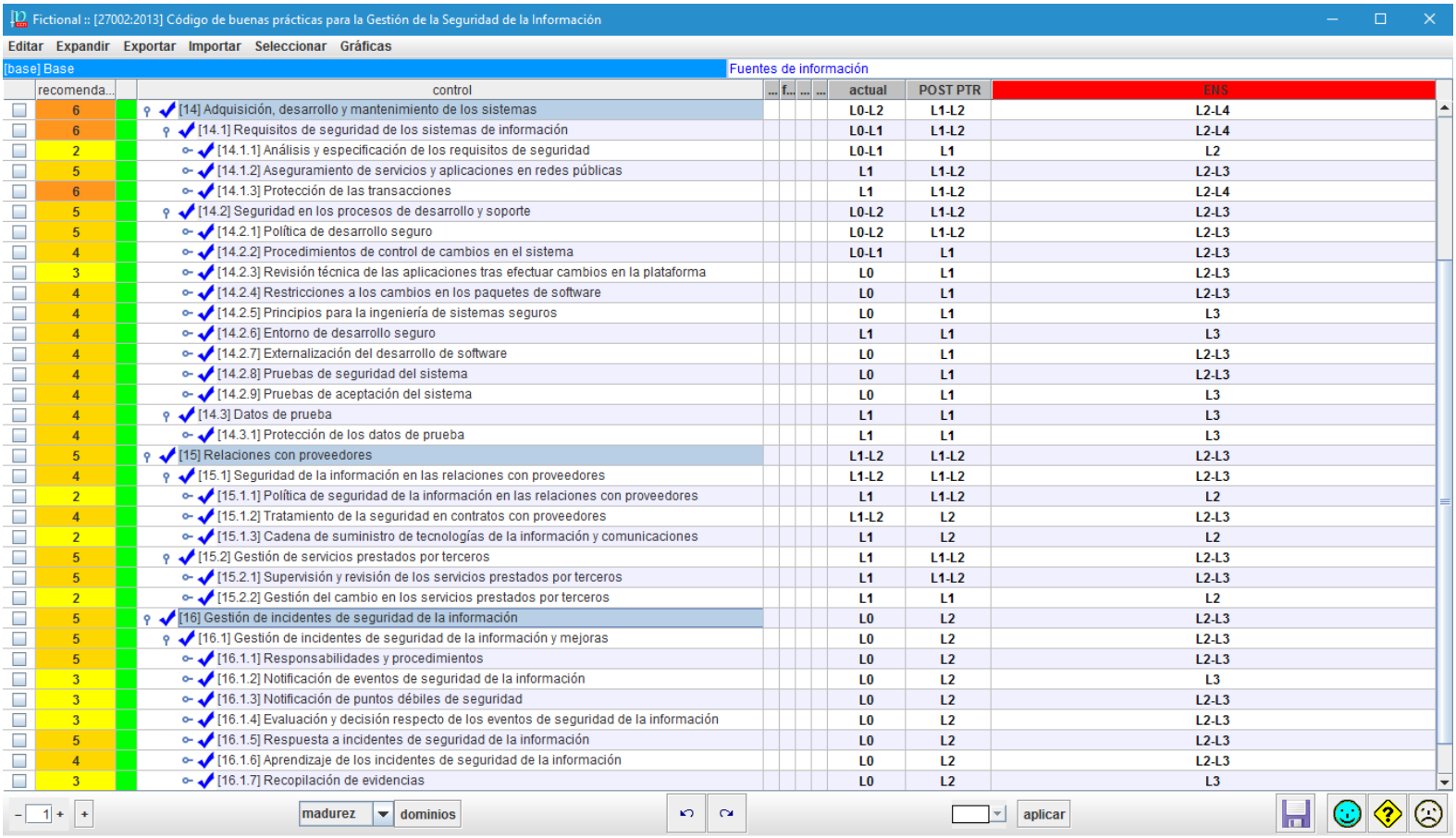


Ilustración 64 Aplicación de controles en dominios 14, 15 y 16 - POST PTR

Fictional :: [27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información

Editar Expandir Exportar Importar Seleccionar Gráficas

[base] Base | Fuentes de información

recomend...	control	actual	POST PTR	ENS
	[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información	L0-L2	L0-L3	L2-L4
2	[5] Políticas de seguridad de la información	L0	L2	L2
5	[6] Organización de la seguridad de la información	L0-L1	L1-L3	L2-L3
5	[7] Seguridad ligada a los recursos humanos	L0-L2	L1-L2	L2-L3
5	[8] Gestión de activos	L0-L2	L0-L2	L2-L3
7	[9] Control de acceso	L0-L1	L1-L3	L2-L4
3	[10] Criptografía	L0-L1	L1-L2	L2-L3
7	[11] Seguridad física y del entorno	L0-L2	L1-L2	L2-L4
7	[12] Gestión de operaciones	L0-L2	L1-L2	L2-L4
6	[13] Seguridad de las comunicaciones	L0-L2	L1-L2	L2-L4
6	[14] Adquisición, desarrollo y mantenimiento de los sistemas	L0-L2	L1-L2	L2-L4
5	[15] Relaciones con proveedores	L1-L2	L1-L2	L2-L3
5	[16] Gestión de incidentes de seguridad de la información	L0	L2	L2-L3
6	[17] Aspectos de seguridad de la información en la gestión de la continuidad del negocio	L0-L1	L2	L2-L4
5	[17.1] Continuidad de la seguridad de la información	L0	L2	L2-L3
4	[17.1.1] Planificar la continuidad de la seguridad de la información	L0	L2	L2-L3
5	[17.1.2] Implementar la continuidad de la seguridad de la información	L0	L2	L2-L3
4	[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información	L0	L2	L3
6	[17.2] Redundancia	L1	L2	L2-L4
6	[17.2.1] Disponibilidad de los medios de procesamiento de información	L1	L2	L2-L4
6	[18] Cumplimiento	L0-L2	L2	L2-L4
3	[18.1] Cumplimiento de los requisitos legales y contractuales	L2	L2	L2-L3
2	[18.1.1] Identificación de legislación aplicable y requisitos contractuales	L2	L2	L2
3	[18.1.2] Derechos de propiedad intelectual (IPR)	L2	L2	L2-L3
	[18.1.3] Protección de los documentos de la organización	L2	L2	n.a.
3	[18.1.4] Protección de datos y privacidad de la información de carácter personal	L2	L2	L2-L3
2	[18.1.5] Regulación de los controles criptográficos	n.a.	L2	L2
6	[18.2] Revisiones de seguridad de la información	L0-L1	L2	L2-L4
4	[18.2.1] Revisión independiente de la seguridad de la información	L1	L2	L2-L3
2	[18.2.2] Cumplimiento de las políticas y normas de seguridad	L0	L2	L2
6	[18.2.3] Comprobación del cumplimiento técnico	L1	L2	L2-L4

madurez | dominios | aplicar

Ilustración 65 Aplicación de controles en dominios 17, y 18 - POST PTR

En la siguiente gráfica se puede comprobar cómo ha aumentado el nivel de madurez en el ámbito de la seguridad respecto a su estado previo a la implantación de la ISO 27001:2013.

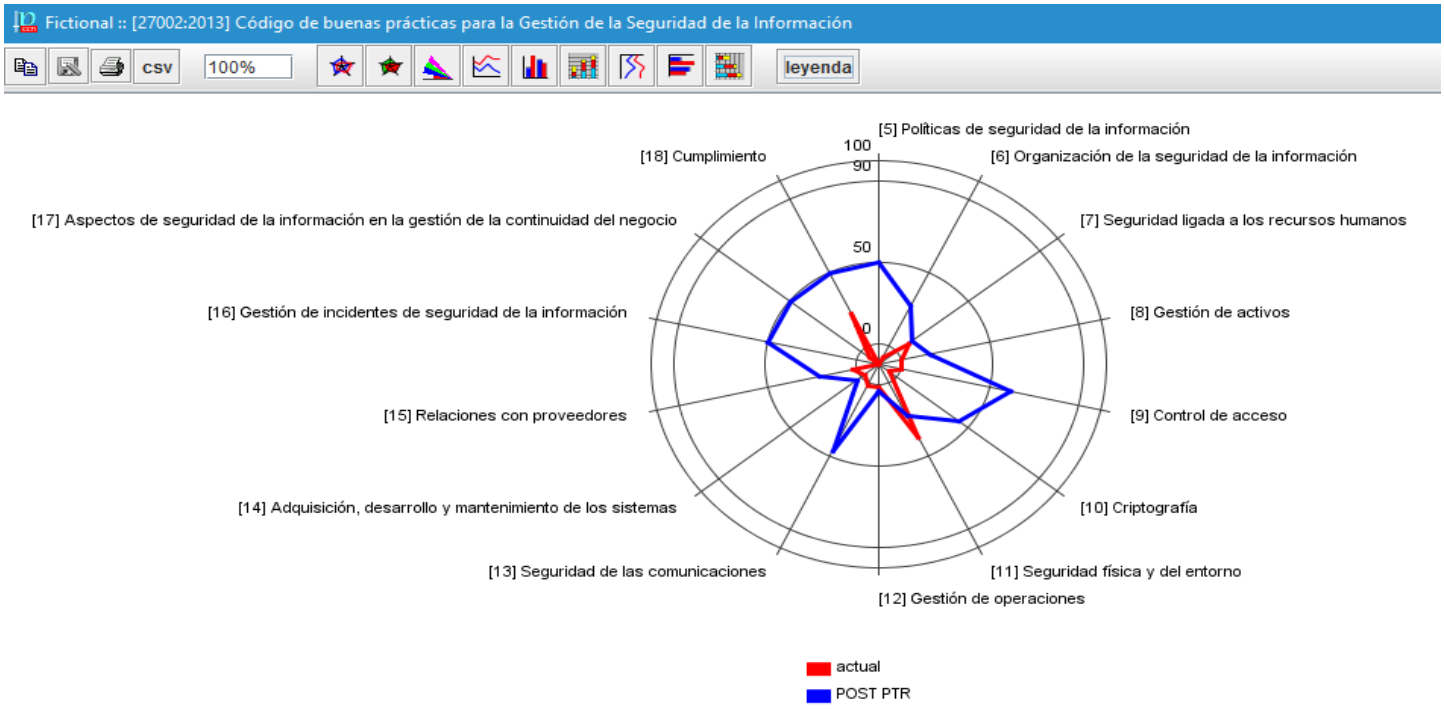
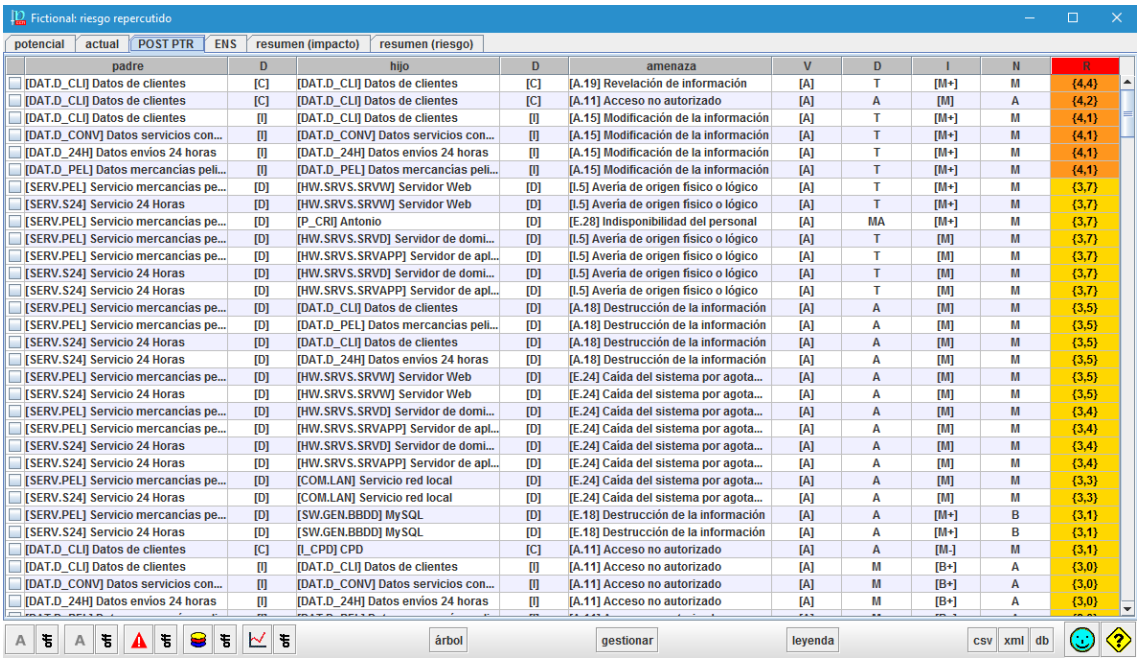


Ilustración 66 Comparación del nivel de madurez de Fictional antes y después del PTR

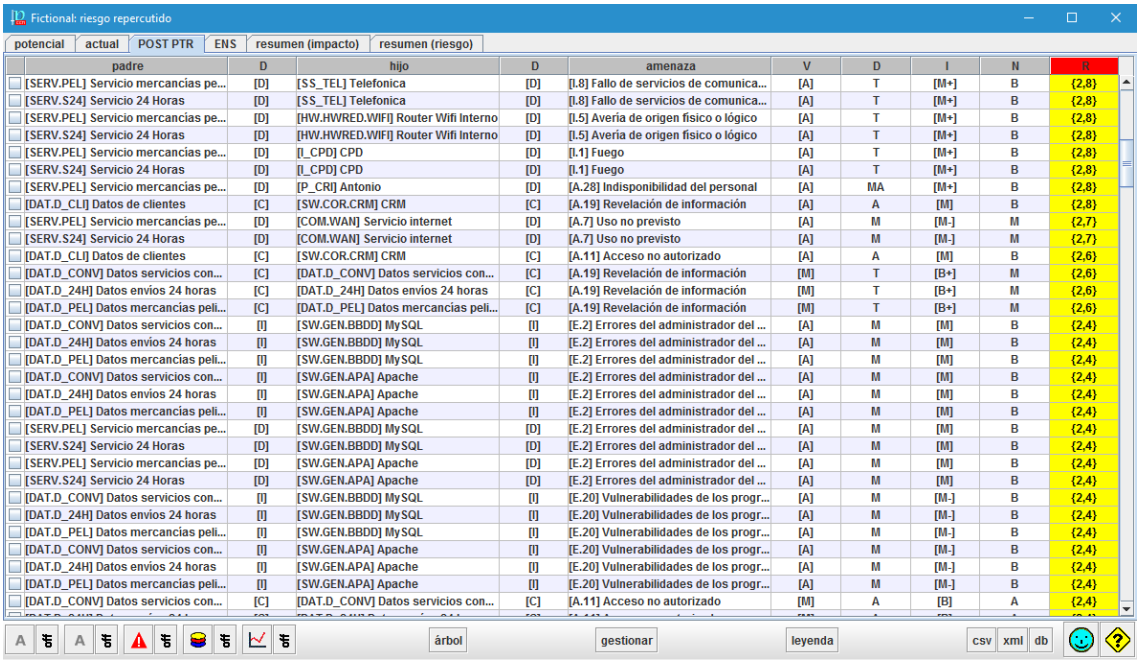
5.4 Riesgo residual

Comprobado que el nivel de seguridad de Fictional ha incrementado, es el momento de obtener el riesgo residual y analizar si ha disminuido o no respecto el potencial.



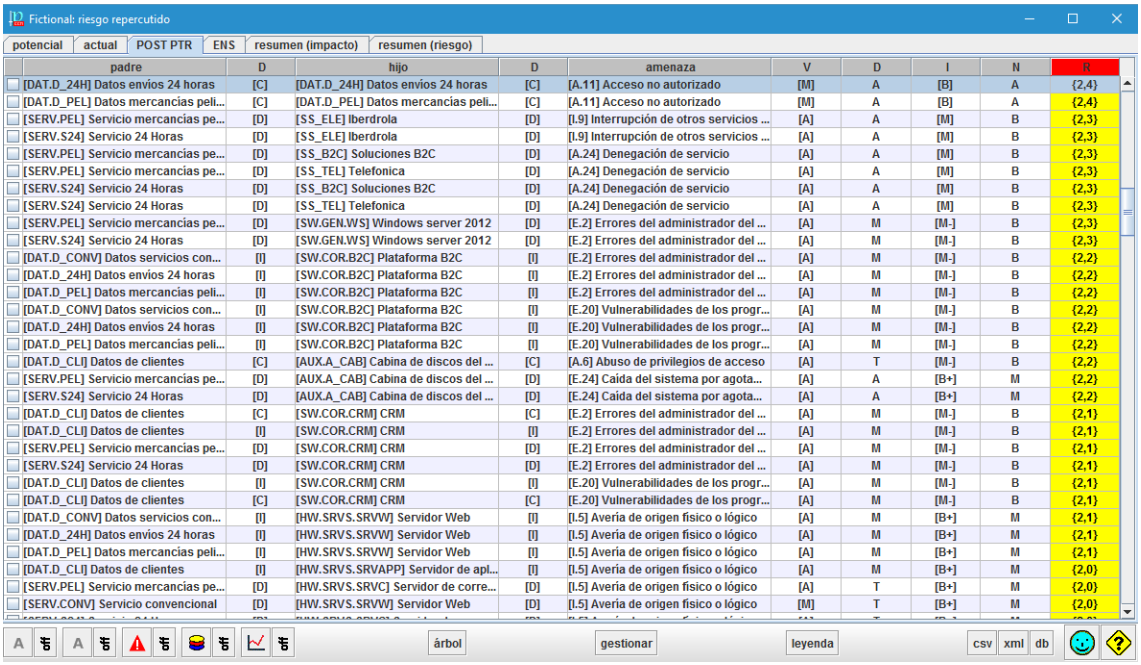
padre	D	hijo	D	amenaza	V	D	I	N	R
[DAT.D_CLI] Datos de clientes	[C]	[DAT.D_CLI] Datos de clientes	[C]	[A.19] Revelación de información	[A]	T	[M+]	M	{4,4}
[DAT.D_CLI] Datos de clientes	[C]	[DAT.D_CLI] Datos de clientes	[C]	[A.11] Acceso no autorizado	[A]	A	[M]	A	{4,2}
[DAT.D_CLI] Datos de clientes	[I]	[DAT.D_CLI] Datos de clientes	[I]	[A.15] Modificación de la información	[A]	T	[M+]	M	{4,1}
[DAT.D_CONV] Datos servicios con...	[I]	[DAT.D_CONV] Datos servicios con...	[I]	[A.15] Modificación de la información	[A]	T	[M+]	M	{4,1}
[DAT.D_24H] Datos envíos 24 horas	[I]	[DAT.D_24H] Datos envíos 24 horas	[I]	[A.15] Modificación de la información	[A]	T	[M+]	M	{4,1}
[DAT.D_PEL] Datos mercancías peli...	[I]	[DAT.D_PEL] Datos mercancías peli...	[I]	[A.15] Modificación de la información	[A]	T	[M+]	M	{4,1}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M+]	M	{3,7}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M+]	M	{3,7}
[SERV.PEL] Servicio mercancías pe...	[D]	[P_CRI] Antonio	[D]	[E.28] Indisponibilidad del personal	[A]	MA	[M+]	M	{3,7}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.SRVS.SRVD] Servidor de domi...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M]	M	{3,7}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.SRVS.SRVAPP] Servidor de apl...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M]	M	{3,7}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVD] Servidor de domi...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M]	M	{3,7}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVAPP] Servidor de apl...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M]	M	{3,7}
[SERV.PEL] Servicio mercancías pe...	[D]	[DAT.D_CLI] Datos de clientes	[D]	[A.18] Destrucción de la información	[A]	A	[M]	M	{3,5}
[SERV.PEL] Servicio mercancías pe...	[D]	[DAT.D_PEL] Datos mercancías peli...	[D]	[A.18] Destrucción de la información	[A]	A	[M]	M	{3,5}
[SERV.S24] Servicio 24 Horas	[D]	[DAT.D_CLI] Datos de clientes	[D]	[A.18] Destrucción de la información	[A]	A	[M]	M	{3,5}
[SERV.S24] Servicio 24 Horas	[D]	[DAT.D_24H] Datos envíos 24 horas	[D]	[A.18] Destrucción de la información	[A]	A	[M]	M	{3,5}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[E.24] Caída del sistema por agota...	[A]	A	[M]	M	{3,5}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[E.24] Caída del sistema por agota...	[A]	A	[M]	M	{3,5}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.SRVS.SRVD] Servidor de domi...	[D]	[E.24] Caída del sistema por agota...	[A]	A	[M]	M	{3,4}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.SRVS.SRVAPP] Servidor de apl...	[D]	[E.24] Caída del sistema por agota...	[A]	A	[M]	M	{3,4}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVD] Servidor de domi...	[D]	[E.24] Caída del sistema por agota...	[A]	A	[M]	M	{3,4}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVAPP] Servidor de apl...	[D]	[E.24] Caída del sistema por agota...	[A]	A	[M]	M	{3,4}
[SERV.PEL] Servicio mercancías pe...	[D]	[COM.LAN] Servicio red local	[D]	[E.24] Caída del sistema por agota...	[A]	A	[M]	M	{3,3}
[SERV.S24] Servicio 24 Horas	[D]	[COM.LAN] Servicio red local	[D]	[E.24] Caída del sistema por agota...	[A]	A	[M]	M	{3,3}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.18] Destrucción de la información	[A]	A	[M+]	B	{3,1}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.18] Destrucción de la información	[A]	A	[M+]	B	{3,1}
[DAT.D_CLI] Datos de clientes	[C]	[I_CPD] CPD	[C]	[A.11] Acceso no autorizado	[A]	A	[M-]	M	{3,1}
[DAT.D_CLI] Datos de clientes	[I]	[DAT.D_CLI] Datos de clientes	[I]	[A.11] Acceso no autorizado	[A]	M	[B+]	A	{3,0}
[DAT.D_CONV] Datos servicios con...	[I]	[DAT.D_CONV] Datos servicios con...	[I]	[A.11] Acceso no autorizado	[A]	M	[B+]	A	{3,0}
[DAT.D_24H] Datos envíos 24 horas	[I]	[DAT.D_24H] Datos envíos 24 horas	[I]	[A.11] Acceso no autorizado	[A]	M	[B+]	A	{3,0}

Ilustración 67 Riesgo residual



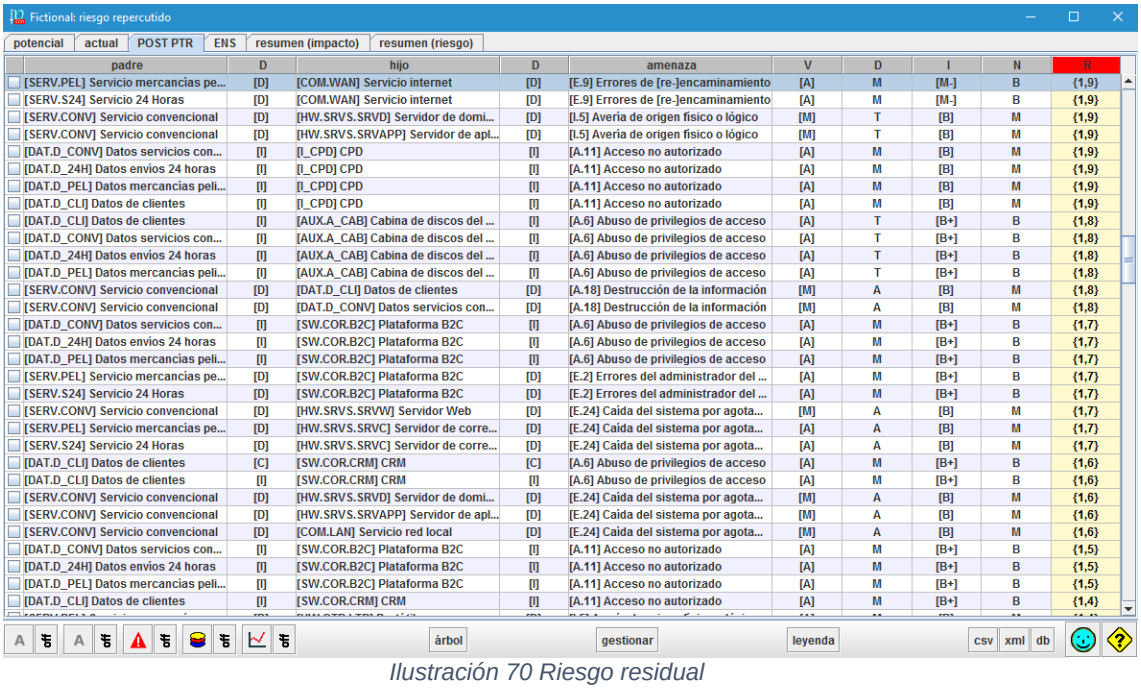
padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.PEL] Servicio mercancías pe...	[D]	[SS_TEL] Telefonica	[D]	[I.8] Fallo de servicios de comunica...	[A]	T	[M+]	B	{2,8}
[SERV.S24] Servicio 24 Horas	[D]	[SS_TEL] Telefonica	[D]	[I.8] Fallo de servicios de comunica...	[A]	T	[M+]	B	{2,8}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M+]	B	{2,8}
[SERV.S24] Servicio 24 Horas	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[M+]	B	{2,8}
[SERV.PEL] Servicio mercancías pe...	[D]	[I_CPD] CPD	[D]	[I.1] Fuego	[A]	T	[M+]	B	{2,8}
[SERV.S24] Servicio 24 Horas	[D]	[I_CPD] CPD	[D]	[I.1] Fuego	[A]	T	[M+]	B	{2,8}
[SERV.PEL] Servicio mercancías pe...	[D]	[P_CRI] Antonio	[D]	[A.28] Indisponibilidad del personal	[A]	MA	[M+]	B	{2,8}
[DAT.D_CLI] Datos de clientes	[C]	[SW.COR.CRM] CRM	[C]	[A.19] Revelación de información	[A]	A	[M]	B	{2,8}
[SERV.PEL] Servicio mercancías pe...	[D]	[COM.WAN] Servicio internet	[D]	[A.7] Uso no previsto	[A]	M	[M-]	M	{2,7}
[SERV.S24] Servicio 24 Horas	[D]	[COM.WAN] Servicio internet	[D]	[A.7] Uso no previsto	[A]	M	[M-]	M	{2,7}
[DAT.D_CLI] Datos de clientes	[C]	[SW.COR.CRM] CRM	[C]	[A.11] Acceso no autorizado	[A]	A	[M]	B	{2,6}
[DAT.D_CONV] Datos servicios con...	[C]	[DAT.D_CONV] Datos servicios con...	[C]	[A.19] Revelación de información	[A]	T	[B+]	M	{2,6}
[DAT.D_24H] Datos envíos 24 horas	[C]	[DAT.D_24H] Datos envíos 24 horas	[C]	[A.19] Revelación de información	[M]	T	[B+]	M	{2,6}
[DAT.D_PEL] Datos mercancías peli...	[C]	[DAT.D_PEL] Datos mercancías peli...	[C]	[A.19] Revelación de información	[M]	T	[B+]	M	{2,6}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.GEN.APA] Apache	[I]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.APA] Apache	[I]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.GEN.APA] Apache	[I]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.APA] Apache	[D]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.APA] Apache	[D]	[E.2] Errores del administrador del ...	[A]	M	[M]	B	{2,4}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,4}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,4}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,4}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.GEN.APA] Apache	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,4}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.APA] Apache	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,4}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.GEN.APA] Apache	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,4}
[DAT.D_CONV] Datos servicios con...	[C]	[DAT.D_CONV] Datos servicios con...	[C]	[A.11] Acceso no autorizado	[M]	A	[B]	A	{2,4}

Ilustración 68 Riesgo residual



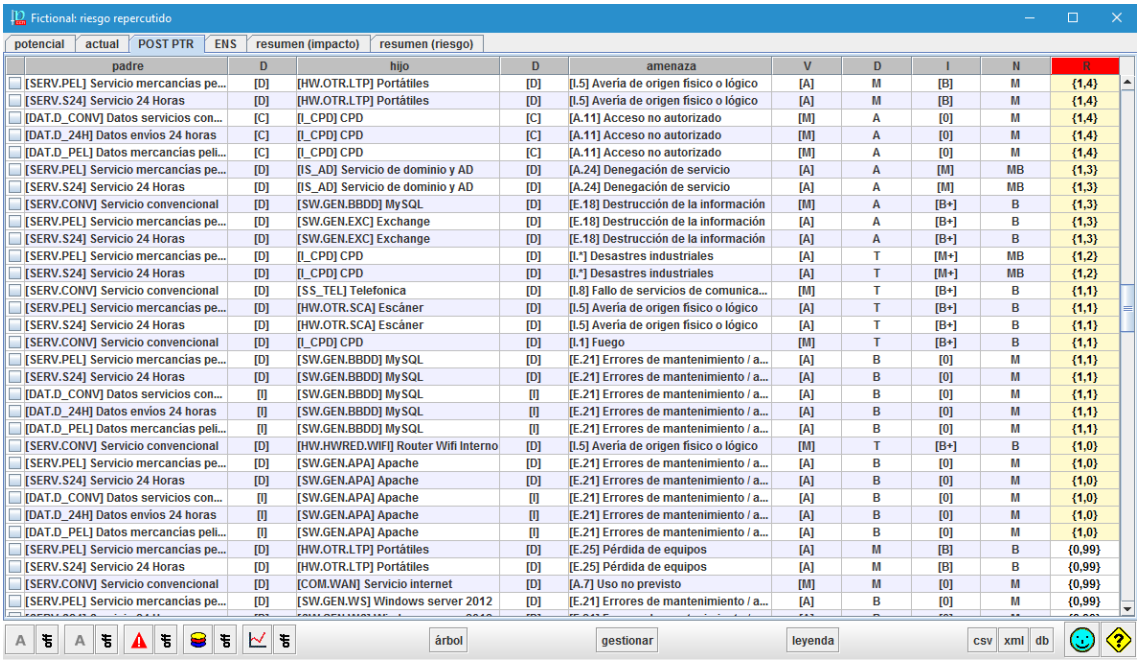
padre	D	hijo	D	amenaza	V	D	I	N	R
[DAT.D_24H] Datos envíos 24 horas	[C]	[DAT.D_24H] Datos envíos 24 horas	[C]	[A.11] Acceso no autorizado	[M]	A	[B]	A	{2,4}
[DAT.D_PEL] Datos mercancías peli...	[C]	[DAT.D_PEL] Datos mercancías peli...	[C]	[A.11] Acceso no autorizado	[M]	A	[B]	A	{2,4}
[SERV.PEL] Servicio mercancías pe...	[D]	[SS_ELE] Iberdrola	[D]	[I.9] Interrupción de otros servicios ...	[A]	A	[M]	B	{2,3}
[SERV.S24] Servicio 24 Horas	[D]	[SS_ELE] Iberdrola	[D]	[I.9] Interrupción de otros servicios ...	[A]	A	[M]	B	{2,3}
[SERV.PEL] Servicio mercancías pe...	[D]	[SS_B2C] Soluciones B2C	[D]	[A.24] Denegación de servicio	[A]	A	[M]	B	{2,3}
[SERV.PEL] Servicio mercancías pe...	[D]	[SS_TEL] Telefonica	[D]	[A.24] Denegación de servicio	[A]	A	[M]	B	{2,3}
[SERV.S24] Servicio 24 Horas	[D]	[SS_B2C] Soluciones B2C	[D]	[A.24] Denegación de servicio	[A]	A	[M]	B	{2,3}
[SERV.S24] Servicio 24 Horas	[D]	[SS_TEL] Telefonica	[D]	[A.24] Denegación de servicio	[A]	A	[M]	B	{2,3}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.2] Errores del administrador del ...	[A]	M	[M-]	B	{2,3}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.2] Errores del administrador del ...	[A]	M	[M-]	B	{2,3}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.2] Errores del administrador del ...	[A]	M	[M-]	B	{2,2}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.2] Errores del administrador del ...	[A]	M	[M-]	B	{2,2}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.2] Errores del administrador del ...	[A]	M	[M-]	B	{2,2}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,2}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,2}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,2}
[DAT.D_CLI] Datos de clientes	[C]	[AUX.A_CAB] Cabina de discos del ...	[C]	[A.6] Abuso de privilegios de acceso	[A]	T	[M-]	B	{2,2}
[SERV.PEL] Servicio mercancías pe...	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[E.24] Caída del sistema por agota...	[A]	A	[B+]	M	{2,2}
[SERV.S24] Servicio 24 Horas	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[E.24] Caída del sistema por agota...	[A]	A	[B+]	M	{2,2}
[DAT.D_CLI] Datos de clientes	[C]	[SW.COR.CRM] CRM	[C]	[E.2] Errores del administrador del ...	[A]	M	[M-]	B	{2,1}
[DAT.D_CLI] Datos de clientes	[I]	[SW.COR.CRM] CRM	[I]	[E.2] Errores del administrador del ...	[A]	M	[M-]	B	{2,1}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.COR.CRM] CRM	[D]	[E.2] Errores del administrador del ...	[A]	M	[M-]	B	{2,1}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.CRM] CRM	[D]	[E.2] Errores del administrador del ...	[A]	M	[M-]	B	{2,1}
[DAT.D_CLI] Datos de clientes	[I]	[SW.COR.CRM] CRM	[I]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,1}
[DAT.D_CLI] Datos de clientes	[C]	[SW.COR.CRM] CRM	[C]	[E.20] Vulnerabilidades de los progr...	[A]	M	[M-]	B	{2,1}
[DAT.D_CONV] Datos servicios con...	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[B+]	M	{2,1}
[DAT.D_24H] Datos envíos 24 horas	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[B+]	M	{2,1}
[DAT.D_PEL] Datos mercancías peli...	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[B+]	M	{2,1}
[DAT.D_CLI] Datos de clientes	[I]	[HW.SRVS.SRVAPP] Servidor de apl...	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[B+]	M	{2,0}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.SRVS.SRVC] Servidor de corre...	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[B+]	M	{2,0}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[B+]	M	{2,0}

Ilustración 69 Riesgo residual



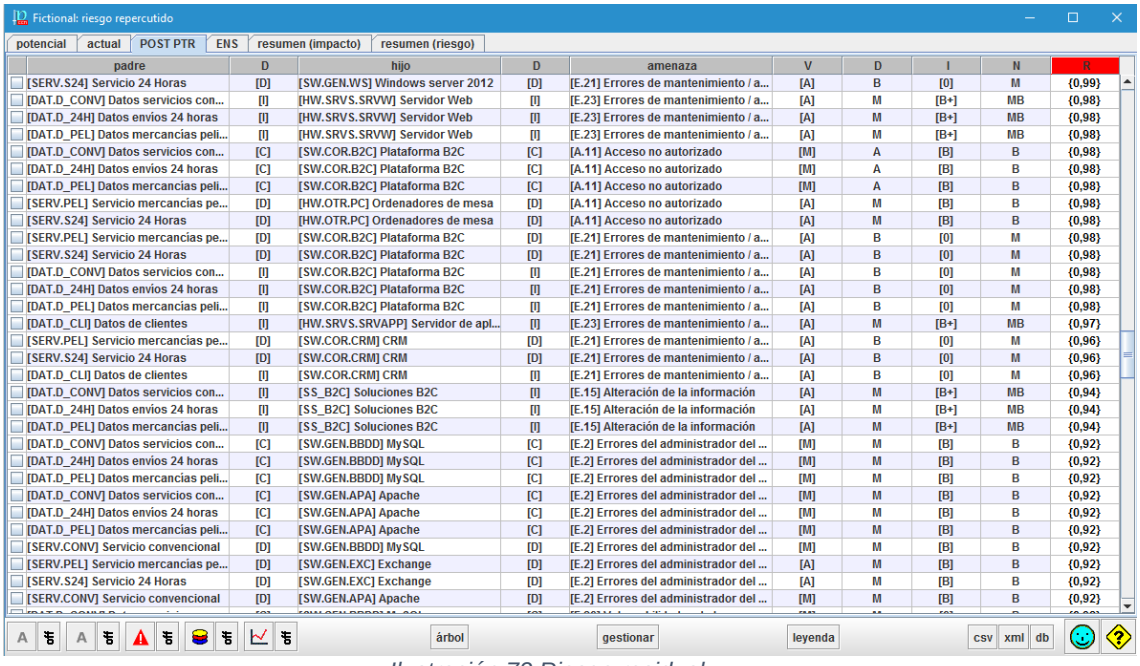
padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.PEL] Servicio mercancías pe...	[D]	[COM.WAN] Servicio internet	[D]	[E.9] Errores de [re-]encaminamiento	[A]	M	[M-]	B	{1,9}
[SERV.S24] Servicio 24 Horas	[D]	[COM.WAN] Servicio internet	[D]	[E.9] Errores de [re-]encaminamiento	[A]	M	[M-]	B	{1,9}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVD] Servidor de domi...	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[B]	M	{1,9}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVAPP] Servidor de apl...	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[B]	M	{1,9}
[DAT.D_CONV] Datos servicios con...	[I]	[I_CPD] CPD	[I]	[A.11] Acceso no autorizado	[A]	M	[B]	M	{1,9}
[DAT.D_24H] Datos envíos 24 horas	[I]	[I_CPD] CPD	[I]	[A.11] Acceso no autorizado	[A]	M	[B]	M	{1,9}
[DAT.D_PEL] Datos mercancías peli...	[I]	[I_CPD] CPD	[I]	[A.11] Acceso no autorizado	[A]	M	[B]	M	{1,9}
[DAT.D_CLI] Datos de clientes	[I]	[I_CPD] CPD	[I]	[A.11] Acceso no autorizado	[A]	M	[B]	M	{1,9}
[DAT.D_CLI] Datos de clientes	[I]	[AUX.A_CAB] Cabina de discos del ...	[I]	[A.6] Abuso de privilegios de acceso	[A]	T	[B+]	B	{1,8}
[DAT.D_CONV] Datos servicios con...	[I]	[AUX.A_CAB] Cabina de discos del ...	[I]	[A.6] Abuso de privilegios de acceso	[A]	T	[B+]	B	{1,8}
[DAT.D_24H] Datos envíos 24 horas	[I]	[AUX.A_CAB] Cabina de discos del ...	[I]	[A.6] Abuso de privilegios de acceso	[A]	T	[B+]	B	{1,8}
[DAT.D_PEL] Datos mercancías peli...	[I]	[AUX.A_CAB] Cabina de discos del ...	[I]	[A.6] Abuso de privilegios de acceso	[A]	T	[B+]	B	{1,8}
[SERV.CONV] Servicio convencional	[D]	[DAT.D_CLI] Datos de clientes	[D]	[A.18] Destrucción de la información	[M]	A	[B]	M	{1,8}
[SERV.CONV] Servicio convencional	[D]	[DAT.D_CONV] Datos servicios con...	[D]	[A.18] Destrucción de la información	[M]	A	[B]	M	{1,8}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[A.6] Abuso de privilegios de acceso	[A]	M	[B+]	B	{1,7}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[A.6] Abuso de privilegios de acceso	[A]	M	[B+]	B	{1,7}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[A.6] Abuso de privilegios de acceso	[A]	M	[B+]	B	{1,7}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.2] Errores del administrador del ...	[A]	M	[B+]	B	{1,7}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.2] Errores del administrador del ...	[A]	M	[B+]	B	{1,7}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVW] Servidor Web	[D]	[E.24] Caída del sistema por agota...	[M]	A	[B]	M	{1,7}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.SRVS.SRVC] Servidor de corre...	[D]	[E.24] Caída del sistema por agota...	[A]	A	[B]	M	{1,7}
[SERV.S24] Servicio 24 Horas	[D]	[HW.SRVS.SRVC] Servidor de corre...	[D]	[E.24] Caída del sistema por agota...	[A]	A	[B]	M	{1,7}
[DAT.D_CLI] Datos de clientes	[C]	[SW.COR.CRM] CRM	[C]	[A.6] Abuso de privilegios de acceso	[A]	M	[B+]	B	{1,6}
[DAT.D_CLI] Datos de clientes	[I]	[SW.COR.CRM] CRM	[I]	[A.6] Abuso de privilegios de acceso	[A]	M	[B+]	B	{1,6}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVD] Servidor de domi...	[D]	[E.24] Caída del sistema por agota...	[M]	A	[B]	M	{1,6}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVAPP] Servidor de apl...	[D]	[E.24] Caída del sistema por agota...	[M]	A	[B]	M	{1,6}
[SERV.CONV] Servicio convencional	[D]	[COM.LAN] Servicio red local	[D]	[E.24] Caída del sistema por agota...	[M]	A	[B]	M	{1,6}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[A.11] Acceso no autorizado	[A]	M	[B+]	B	{1,5}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[A.11] Acceso no autorizado	[A]	M	[B+]	B	{1,5}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[A.11] Acceso no autorizado	[A]	M	[B+]	B	{1,5}
[DAT.D_CLI] Datos de clientes	[I]	[SW.COR.CRM] CRM	[I]	[A.11] Acceso no autorizado	[A]	M	[B+]	B	{1,4}

Ilustración 70 Riesgo residual



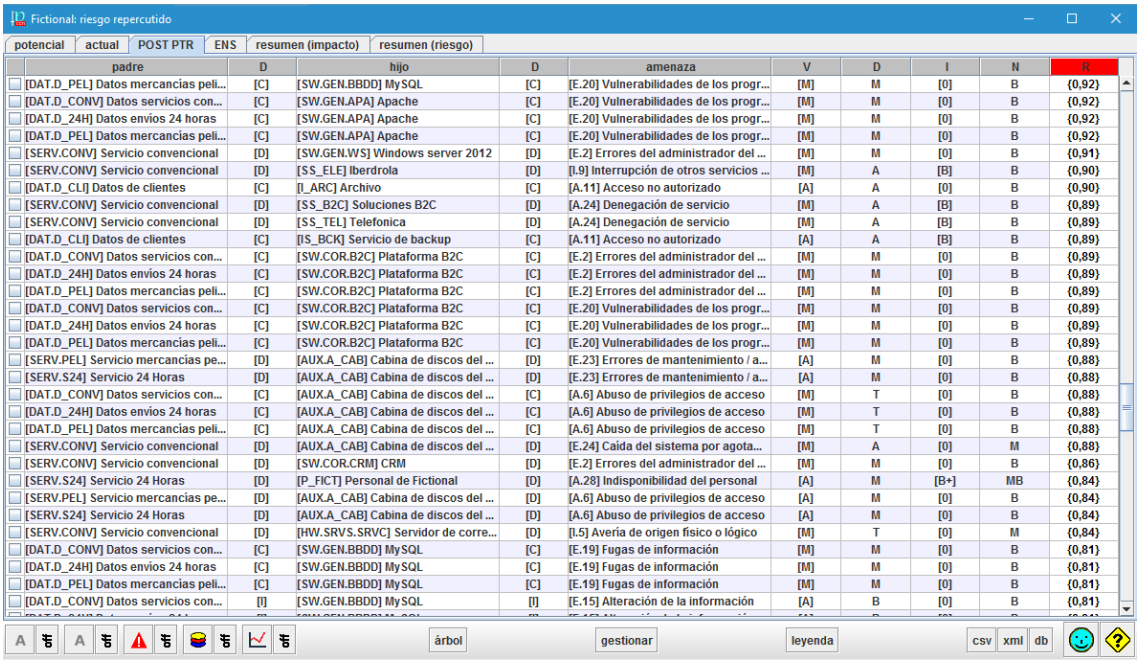
padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.OTR.LTP] Portátiles	[D]	[I.5] Avería de origen físico o lógico	[A]	M	[B]	M	{1,4}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.LTP] Portátiles	[D]	[I.5] Avería de origen físico o lógico	[A]	M	[B]	M	{1,4}
[DAT.D_CONV] Datos servicios con...	[C]	[I_CPD] CPD	[C]	[A.11] Acceso no autorizado	[M]	A	[0]	M	{1,4}
[DAT.D_24H] Datos envíos 24 horas	[C]	[I_CPD] CPD	[C]	[A.11] Acceso no autorizado	[M]	A	[0]	M	{1,4}
[DAT.D_PEL] Datos mercancías peli...	[C]	[I_CPD] CPD	[C]	[A.11] Acceso no autorizado	[M]	A	[0]	M	{1,4}
[SERV.PEL] Servicio mercancías pe...	[D]	[IS_AD] Servicio de dominio y AD	[D]	[A.24] Denegación de servicio	[A]	A	[M]	MB	{1,3}
[SERV.S24] Servicio 24 Horas	[D]	[IS_AD] Servicio de dominio y AD	[D]	[A.24] Denegación de servicio	[A]	A	[M]	MB	{1,3}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.18] Destrucción de la información	[M]	A	[B+]	B	{1,3}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.EXC] Exchange	[D]	[E.18] Destrucción de la información	[A]	A	[B+]	B	{1,3}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.EXC] Exchange	[D]	[E.18] Destrucción de la información	[A]	A	[B+]	B	{1,3}
[SERV.PEL] Servicio mercancías pe...	[D]	[I_CPD] CPD	[D]	[I.*] Desastres industriales	[A]	T	[M+]	MB	{1,2}
[SERV.S24] Servicio 24 Horas	[D]	[I_CPD] CPD	[D]	[I.*] Desastres industriales	[A]	T	[M+]	MB	{1,2}
[SERV.CONV] Servicio convencional	[D]	[SS_TEL] Telefonica	[D]	[I.8] Fallo de servicios de comunica...	[M]	T	[B+]	B	{1,1}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.OTR.SCA] Escáner	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[B+]	B	{1,1}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.SCA] Escáner	[D]	[I.5] Avería de origen físico o lógico	[A]	T	[B+]	B	{1,1}
[SERV.CONV] Servicio convencional	[D]	[I_CPD] CPD	[D]	[I.1] Fuego	[M]	T	[B+]	B	{1,1}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,1}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,1}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,1}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,1}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,1}
[SERV.CONV] Servicio convencional	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[B+]	B	{1,0}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.APA] Apache	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,0}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.APA] Apache	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,0}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.GEN.APA] Apache	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,0}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.APA] Apache	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,0}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.GEN.APA] Apache	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{1,0}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.OTR.LTP] Portátiles	[D]	[E.25] Pérdida de equipos	[A]	M	[B]	B	{0,99}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.LTP] Portátiles	[D]	[E.25] Pérdida de equipos	[A]	M	[B]	B	{0,99}
[SERV.CONV] Servicio convencional	[D]	[COM.WAN] Servicio internet	[D]	[A.7] Uso no previsto	[M]	M	[0]	M	{0,99}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,99}

Ilustración 71 Riesgo residual



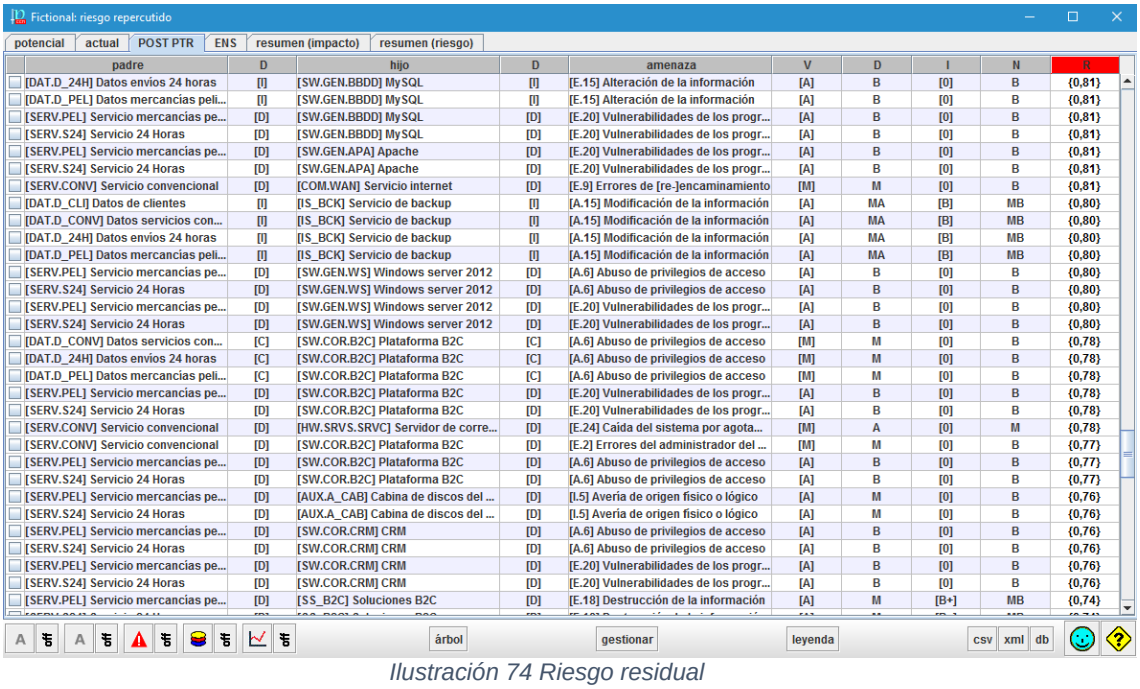
padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,99}
[DAT.D_CONV] Datos servicios con...	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[E.23] Errores de mantenimiento / a...	[A]	M	[B+]	MB	{0,98}
[DAT.D_24H] Datos envíos 24 horas	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[E.23] Errores de mantenimiento / a...	[A]	M	[B+]	MB	{0,98}
[DAT.D_PEL] Datos mercancías peli...	[I]	[HW.SRVS.SRVW] Servidor Web	[I]	[E.23] Errores de mantenimiento / a...	[A]	M	[B+]	MB	{0,98}
[DAT.D_CONV] Datos servicios con...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.11] Acceso no autorizado	[M]	A	[B]	B	{0,98}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.11] Acceso no autorizado	[M]	A	[B]	B	{0,98}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.11] Acceso no autorizado	[M]	A	[B]	B	{0,98}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[A.11] Acceso no autorizado	[A]	M	[B]	B	{0,98}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[A.11] Acceso no autorizado	[A]	M	[B]	B	{0,98}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,98}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,98}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,98}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,98}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.COR.B2C] Plataforma B2C	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,98}
[DAT.D_CLI] Datos de clientes	[I]	[HW.SRVS.SRVAPP] Servidor de apl...	[I]	[E.23] Errores de mantenimiento / a...	[A]	M	[B+]	MB	{0,97}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.COR.CRM] CRM	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,96}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.CRM] CRM	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,96}
[DAT.D_CLI] Datos de clientes	[I]	[SW.COR.CRM] CRM	[I]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,96}
[DAT.D_CONV] Datos servicios con...	[I]	[SS_B2C] Soluciones B2C	[I]	[E.15] Alteración de la información	[A]	M	[B+]	MB	{0,94}
[DAT.D_24H] Datos envíos 24 horas	[I]	[SS_B2C] Soluciones B2C	[I]	[E.15] Alteración de la información	[A]	M	[B+]	MB	{0,94}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SS_B2C] Soluciones B2C	[I]	[E.15] Alteración de la información	[A]	M	[B+]	MB	{0,94}
[DAT.D_CONV] Datos servicios con...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.2] Errores del administrador del ...	[M]	M	[B]	B	{0,92}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.2] Errores del administrador del ...	[M]	M	[B]	B	{0,92}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.2] Errores del administrador del ...	[M]	M	[B]	B	{0,92}
[DAT.D_CONV] Datos servicios con...	[C]	[SW.GEN.APA] Apache	[C]	[E.2] Errores del administrador del ...	[M]	M	[B]	B	{0,92}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.GEN.APA] Apache	[C]	[E.2] Errores del administrador del ...	[M]	M	[B]	B	{0,92}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SW.GEN.APA] Apache	[C]	[E.2] Errores del administrador del ...	[M]	M	[B]	B	{0,92}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.2] Errores del administrador del ...	[M]	M	[B]	B	{0,92}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.EXC] Exchange	[D]	[E.2] Errores del administrador del ...	[A]	M	[B]	B	{0,92}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.EXC] Exchange	[D]	[E.2] Errores del administrador del ...	[A]	M	[B]	B	{0,92}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.APA] Apache	[D]	[E.2] Errores del administrador del ...	[M]	M	[B]	B	{0,92}

Ilustración 72 Riesgo residual



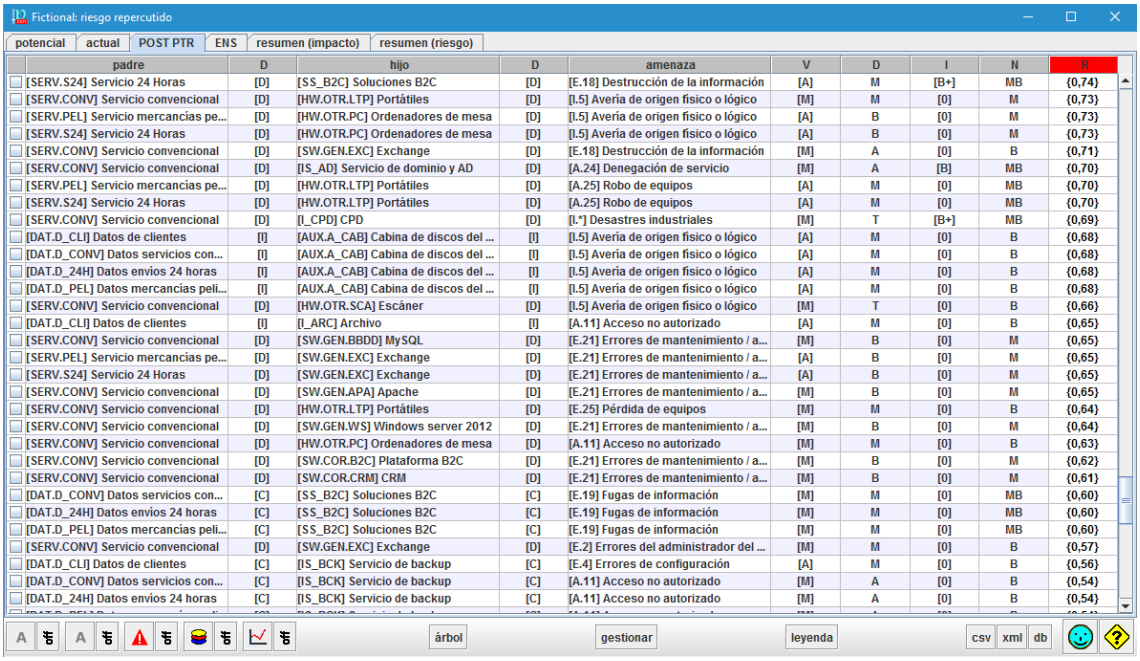
padre	D	hijo	D	amenaza	V	D	I	N	R
[DAT.D_PEL] Datos mercancías peli...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.20] Vulnerabilidades de los progr...	[M]	M	[0]	B	{0,92}
[DAT.D_CONV] Datos servicios con...	[C]	[SW.GEN.APA] Apache	[C]	[E.20] Vulnerabilidades de los progr...	[M]	M	[0]	B	{0,92}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.GEN.APA] Apache	[C]	[E.20] Vulnerabilidades de los progr...	[M]	M	[0]	B	{0,92}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SW.GEN.APA] Apache	[C]	[E.20] Vulnerabilidades de los progr...	[M]	M	[0]	B	{0,92}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.2] Errores del administrador del ...	[M]	M	[0]	B	{0,91}
[SERV.CONV] Servicio convencional	[D]	[SS_ELE] Iberdrola	[D]	[I.9] Interrupción de otros servicios ...	[M]	A	[B]	B	{0,90}
[DAT.D_CLI] Datos de clientes	[C]	[I_ARC] Archivo	[C]	[A.11] Acceso no autorizado	[A]	A	[0]	B	{0,90}
[SERV.CONV] Servicio convencional	[D]	[SS_B2C] Soluciones B2C	[D]	[A.24] Denegación de servicio	[M]	A	[B]	B	{0,89}
[SERV.CONV] Servicio convencional	[D]	[SS_TEL] Telefonica	[D]	[A.24] Denegación de servicio	[M]	A	[B]	B	{0,89}
[DAT.D_CLI] Datos de clientes	[C]	[IS_BCK] Servicio de backup	[C]	[A.11] Acceso no autorizado	[A]	A	[B]	B	{0,89}
[DAT.D_CONV] Datos servicios con...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.2] Errores del administrador del ...	[M]	M	[0]	B	{0,89}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.2] Errores del administrador del ...	[M]	M	[0]	B	{0,89}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.2] Errores del administrador del ...	[M]	M	[0]	B	{0,89}
[DAT.D_CONV] Datos servicios con...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.20] Vulnerabilidades de los progr...	[M]	M	[0]	B	{0,89}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.20] Vulnerabilidades de los progr...	[M]	M	[0]	B	{0,89}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[E.20] Vulnerabilidades de los progr...	[M]	M	[0]	B	{0,89}
[SERV.PEL] Servicio mercancías pe...	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[E.23] Errores de mantenimiento / a...	[A]	M	[0]	B	{0,88}
[SERV.S24] Servicio 24 Horas	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[E.23] Errores de mantenimiento / a...	[A]	M	[0]	B	{0,88}
[DAT.D_CONV] Datos servicios con...	[C]	[AUX.A_CAB] Cabina de discos del ...	[C]	[A.6] Abuso de privilegios de acceso	[M]	T	[0]	B	{0,88}
[DAT.D_24H] Datos envíos 24 horas	[C]	[AUX.A_CAB] Cabina de discos del ...	[C]	[A.6] Abuso de privilegios de acceso	[M]	T	[0]	B	{0,88}
[DAT.D_PEL] Datos mercancías peli...	[C]	[AUX.A_CAB] Cabina de discos del ...	[C]	[A.6] Abuso de privilegios de acceso	[M]	T	[0]	B	{0,88}
[SERV.CONV] Servicio convencional	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[E.24] Caída del sistema por agota...	[M]	A	[0]	M	{0,88}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.CRM] CRM	[D]	[E.2] Errores del administrador del ...	[M]	M	[0]	B	{0,86}
[SERV.S24] Servicio 24 Horas	[D]	[P_FICT] Personal de Fictional	[D]	[A.28] Indisponibilidad del personal	[A]	M	[B+]	MB	{0,84}
[SERV.PEL] Servicio mercancías pe...	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[A.6] Abuso de privilegios de acceso	[A]	M	[0]	B	{0,84}
[SERV.S24] Servicio 24 Horas	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[A.6] Abuso de privilegios de acceso	[A]	M	[0]	B	{0,84}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVC] Servidor de corre...	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[0]	M	{0,84}
[DAT.D_CONV] Datos servicios con...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.19] Fugas de información	[M]	M	[0]	B	{0,81}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.19] Fugas de información	[M]	M	[0]	B	{0,81}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SW.GEN.BBDD] MySQL	[C]	[E.19] Fugas de información	[M]	M	[0]	B	{0,81}
[DAT.D_CONV] Datos servicios con...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.15] Alteración de la información	[A]	B	[0]	B	{0,81}

Ilustración 73 Riesgo residual



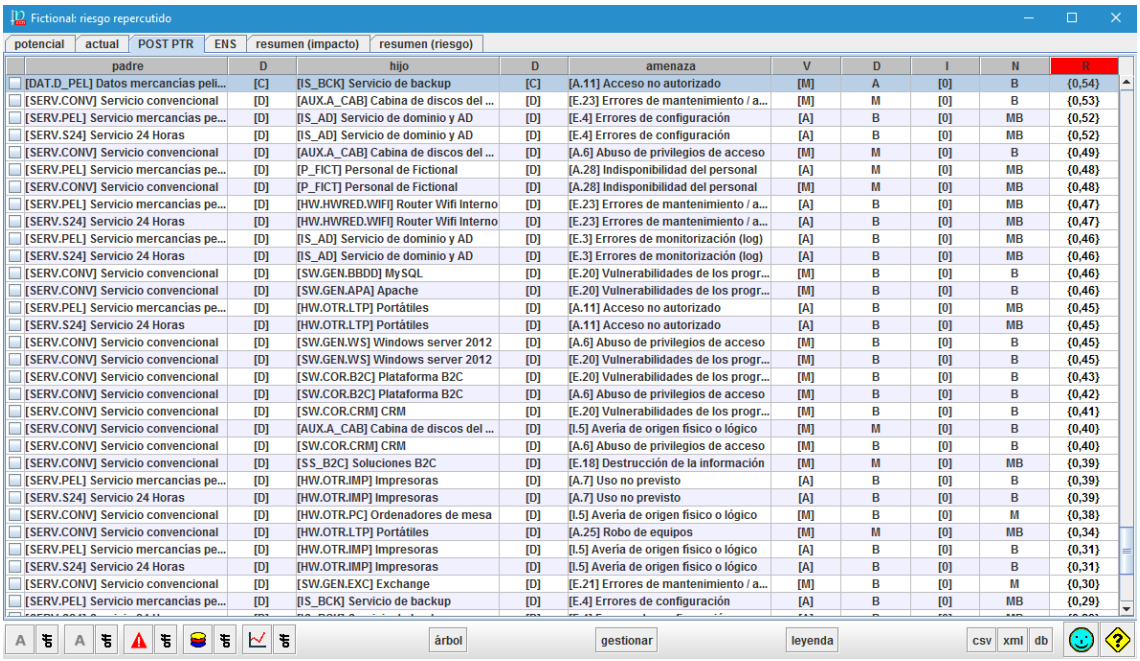
padre	D	hijo	D	amenaza	V	D	I	N	R
[DAT.D_24H] Datos envíos 24 horas	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.15] Alteración de la información	[A]	B	[0]	B	{0,81}
[DAT.D_PEL] Datos mercancías peli...	[I]	[SW.GEN.BBDD] MySQL	[I]	[E.15] Alteración de la información	[A]	B	[0]	B	{0,81}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,81}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,81}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.APA] Apache	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,81}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.APA] Apache	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,81}
[SERV.CONV] Servicio convencional	[D]	[COM.WAN] Servicio internet	[D]	[E.9] Errores de [re-]encaminamiento	[M]	M	[0]	B	{0,81}
[DAT.D_CLI] Datos de clientes	[I]	[IS_BCK] Servicio de backup	[I]	[A.15] Modificación de la información	[A]	MA	[B]	MB	{0,80}
[DAT.D_CONV] Datos servicios con...	[I]	[IS_BCK] Servicio de backup	[I]	[A.15] Modificación de la información	[A]	MA	[B]	MB	{0,80}
[DAT.D_24H] Datos envíos 24 horas	[I]	[IS_BCK] Servicio de backup	[I]	[A.15] Modificación de la información	[A]	MA	[B]	MB	{0,80}
[DAT.D_PEL] Datos mercancías peli...	[I]	[IS_BCK] Servicio de backup	[I]	[A.15] Modificación de la información	[A]	MA	[B]	MB	{0,80}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.WS] Windows server 2012	[D]	[A.6] Abuso de privilegios de acceso	[A]	B	[0]	B	{0,80}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.WS] Windows server 2012	[D]	[A.6] Abuso de privilegios de acceso	[A]	B	[0]	B	{0,80}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,80}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,80}
[DAT.D_CONV] Datos servicios con...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.6] Abuso de privilegios de acceso	[M]	M	[0]	B	{0,78}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.6] Abuso de privilegios de acceso	[M]	M	[0]	B	{0,78}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SW.COR.B2C] Plataforma B2C	[C]	[A.6] Abuso de privilegios de acceso	[M]	M	[0]	B	{0,78}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,78}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,78}
[SERV.CONV] Servicio convencional	[D]	[HW.SRVS.SRVC] Servidor de corre...	[D]	[E.24] Caída del sistema por agota...	[M]	A	[0]	M	{0,78}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.2] Errores del administrador del ...	[M]	M	[0]	B	{0,77}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[A.6] Abuso de privilegios de acceso	[A]	B	[0]	B	{0,77}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[A.6] Abuso de privilegios de acceso	[A]	B	[0]	B	{0,77}
[SERV.PEL] Servicio mercancías pe...	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[I.5] Avería de origen físico o lógico	[A]	M	[0]	B	{0,76}
[SERV.S24] Servicio 24 Horas	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[I.5] Avería de origen físico o lógico	[A]	M	[0]	B	{0,76}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.COR.CRM] CRM	[D]	[A.6] Abuso de privilegios de acceso	[A]	B	[0]	B	{0,76}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.CRM] CRM	[D]	[A.6] Abuso de privilegios de acceso	[A]	B	[0]	B	{0,76}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.COR.CRM] CRM	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,76}
[SERV.S24] Servicio 24 Horas	[D]	[SW.COR.CRM] CRM	[D]	[E.20] Vulnerabilidades de los progr...	[A]	B	[0]	B	{0,76}
[SERV.PEL] Servicio mercancías pe...	[D]	[SS_B2C] Soluciones B2C	[D]	[E.18] Destrucción de la información	[A]	M	[B+]	MB	{0,74}

Ilustración 74 Riesgo residual



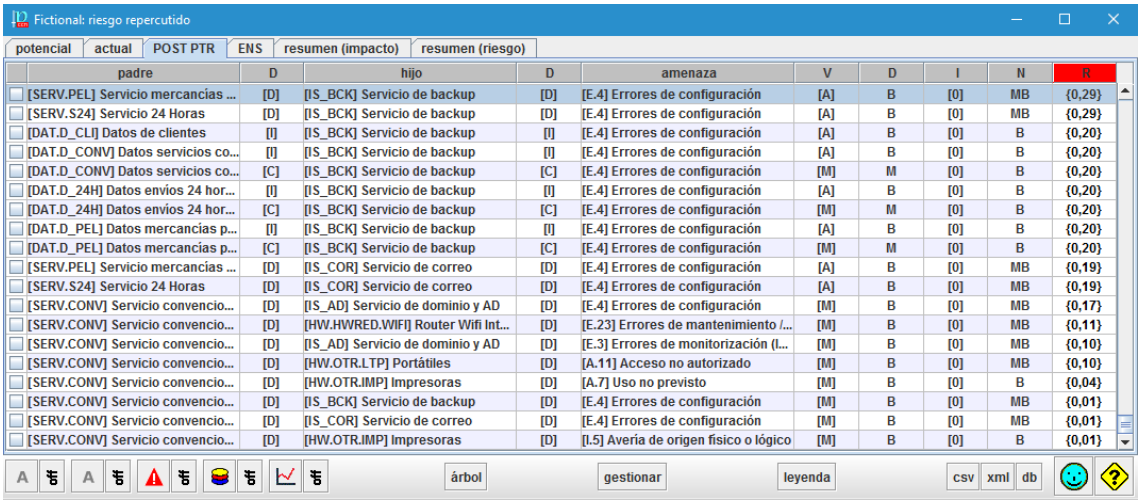
padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.S24] Servicio 24 Horas	[D]	[SS_B2C] Soluciones B2C	[D]	[E.18] Destrucción de la información	[A]	M	[B+]	MB	{0,74}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.LTP] Portátiles	[D]	[I.5] Avería de origen físico o lógico	[M]	M	[0]	M	{0,73}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[I.5] Avería de origen físico o lógico	[A]	B	[0]	M	{0,73}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[I.5] Avería de origen físico o lógico	[A]	B	[0]	M	{0,73}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.EXC] Exchange	[D]	[E.18] Destrucción de la información	[M]	A	[0]	B	{0,71}
[SERV.CONV] Servicio convencional	[D]	[IS_AD] Servicio de dominio y AD	[D]	[A.24] Denegación de servicio	[M]	A	[B]	MB	{0,70}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.25] Robo de equipos	[A]	M	[0]	MB	{0,70}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.25] Robo de equipos	[A]	M	[0]	MB	{0,70}
[SERV.CONV] Servicio convencional	[D]	[I_CPD] CPD	[D]	[I.*] Desastres industriales	[M]	T	[B+]	MB	{0,69}
[DAT.D_CLI] Datos de clientes	[I]	[AUX.A_CAB] Cabina de discos del ...	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[0]	B	{0,68}
[DAT.D_CONV] Datos servicios con...	[I]	[AUX.A_CAB] Cabina de discos del ...	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[0]	B	{0,68}
[DAT.D_24H] Datos envíos 24 horas	[I]	[AUX.A_CAB] Cabina de discos del ...	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[0]	B	{0,68}
[DAT.D_PEL] Datos mercancías peli...	[I]	[AUX.A_CAB] Cabina de discos del ...	[I]	[I.5] Avería de origen físico o lógico	[A]	M	[0]	B	{0,68}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.SCA] Escáner	[D]	[I.5] Avería de origen físico o lógico	[M]	T	[0]	B	{0,66}
[DAT.D_CLI] Datos de clientes	[I]	[I_ARC] Archivo	[I]	[A.11] Acceso no autorizado	[A]	M	[0]	B	{0,65}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	M	{0,65}
[SERV.PEL] Servicio mercancías pe...	[D]	[SW.GEN.EXC] Exchange	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,65}
[SERV.S24] Servicio 24 Horas	[D]	[SW.GEN.EXC] Exchange	[D]	[E.21] Errores de mantenimiento / a...	[A]	B	[0]	M	{0,65}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.APA] Apache	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	M	{0,65}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.LTP] Portátiles	[D]	[E.25] Pérdida de equipos	[M]	M	[0]	B	{0,64}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	M	{0,64}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[A.11] Acceso no autorizado	[M]	M	[0]	B	{0,63}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	M	{0,62}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.CRM] CRM	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	M	{0,61}
[DAT.D_CONV] Datos servicios con...	[C]	[SS_B2C] Soluciones B2C	[C]	[E.19] Fugas de información	[M]	M	[0]	MB	{0,60}
[DAT.D_24H] Datos envíos 24 horas	[C]	[SS_B2C] Soluciones B2C	[C]	[E.19] Fugas de información	[M]	M	[0]	MB	{0,60}
[DAT.D_PEL] Datos mercancías peli...	[C]	[SS_B2C] Soluciones B2C	[C]	[E.19] Fugas de información	[M]	M	[0]	MB	{0,60}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.EXC] Exchange	[D]	[E.2] Errores del administrador del ...	[M]	M	[0]	B	{0,57}
[DAT.D_CLI] Datos de clientes	[C]	[IS_BCK] Servicio de backup	[C]	[E.4] Errores de configuración	[A]	M	[0]	B	{0,56}
[DAT.D_CONV] Datos servicios con...	[C]	[IS_BCK] Servicio de backup	[C]	[A.11] Acceso no autorizado	[M]	A	[0]	B	{0,54}
[DAT.D_24H] Datos envíos 24 horas	[C]	[IS_BCK] Servicio de backup	[C]	[A.11] Acceso no autorizado	[M]	A	[0]	B	{0,54}

Ilustración 75 Riesgo residual



padre	D	hijo	D	amenaza	V	D	I	N	R
[DAT.D_PEL] Datos mercancías peli...	[C]	[IS_BCK] Servicio de backup	[C]	[A.11] Acceso no autorizado	[M]	A	[0]	B	{0,54}
[SERV.CONV] Servicio convencional	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[E.23] Errores de mantenimiento / a...	[M]	M	[0]	B	{0,53}
[SERV.PEL] Servicio mercancías pe...	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.4] Errores de configuración	[A]	B	[0]	MB	{0,52}
[SERV.S24] Servicio 24 Horas	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.4] Errores de configuración	[A]	B	[0]	MB	{0,52}
[SERV.CONV] Servicio convencional	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[A.6] Abuso de privilegios de acceso	[M]	M	[0]	B	{0,49}
[SERV.PEL] Servicio mercancías pe...	[D]	[P_FICT] Personal de Fictional	[D]	[A.28] Indisponibilidad del personal	[A]	M	[0]	MB	{0,48}
[SERV.CONV] Servicio convencional	[D]	[P_FICT] Personal de Fictional	[D]	[A.28] Indisponibilidad del personal	[M]	M	[0]	MB	{0,48}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[E.23] Errores de mantenimiento / a...	[A]	B	[0]	MB	{0,47}
[SERV.S24] Servicio 24 Horas	[D]	[HW.HWRED.WIFI] Router Wifi Interno	[D]	[E.23] Errores de mantenimiento / a...	[A]	B	[0]	MB	{0,47}
[SERV.PEL] Servicio mercancías pe...	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.3] Errores de monitorización (log)	[A]	B	[0]	MB	{0,46}
[SERV.S24] Servicio 24 Horas	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.3] Errores de monitorización (log)	[A]	B	[0]	MB	{0,46}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.BBDD] MySQL	[D]	[E.20] Vulnerabilidades de los progr...	[M]	B	[0]	B	{0,46}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.APA] Apache	[D]	[E.20] Vulnerabilidades de los progr...	[M]	B	[0]	B	{0,46}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.11] Acceso no autorizado	[A]	B	[0]	MB	{0,45}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.11] Acceso no autorizado	[A]	B	[0]	MB	{0,45}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.WS] Windows server 2012	[D]	[A.6] Abuso de privilegios de acceso	[M]	B	[0]	B	{0,45}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.WS] Windows server 2012	[D]	[E.20] Vulnerabilidades de los progr...	[M]	B	[0]	B	{0,45}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[E.20] Vulnerabilidades de los progr...	[M]	B	[0]	B	{0,43}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.B2C] Plataforma B2C	[D]	[A.6] Abuso de privilegios de acceso	[M]	B	[0]	B	{0,42}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.CRM] CRM	[D]	[E.20] Vulnerabilidades de los progr...	[M]	B	[0]	B	{0,41}
[SERV.CONV] Servicio convencional	[D]	[AUX.A_CAB] Cabina de discos del ...	[D]	[I.5] Avería de origen físico o lógico	[M]	M	[0]	B	{0,40}
[SERV.CONV] Servicio convencional	[D]	[SW.COR.CRM] CRM	[D]	[A.6] Abuso de privilegios de acceso	[M]	B	[0]	B	{0,40}
[SERV.CONV] Servicio convencional	[D]	[SS_B2C] Soluciones B2C	[D]	[E.18] Destrucción de la información	[M]	M	[0]	MB	{0,39}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.OTR.IMP] Impresoras	[D]	[A.7] Uso no previsto	[A]	B	[0]	B	{0,39}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.IMP] Impresoras	[D]	[A.7] Uso no previsto	[A]	B	[0]	B	{0,39}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.PC] Ordenadores de mesa	[D]	[I.5] Avería de origen físico o lógico	[M]	B	[0]	M	{0,38}
[SERV.CONV] Servicio convencional	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.25] Robo de equipos	[M]	M	[0]	MB	{0,34}
[SERV.PEL] Servicio mercancías pe...	[D]	[HW.OTR.IMP] Impresoras	[D]	[I.5] Avería de origen físico o lógico	[A]	B	[0]	B	{0,31}
[SERV.S24] Servicio 24 Horas	[D]	[HW.OTR.IMP] Impresoras	[D]	[I.5] Avería de origen físico o lógico	[A]	B	[0]	B	{0,31}
[SERV.CONV] Servicio convencional	[D]	[SW.GEN.EXC] Exchange	[D]	[E.21] Errores de mantenimiento / a...	[M]	B	[0]	M	{0,30}
[SERV.PEL] Servicio mercancías pe...	[D]	[IS_BCK] Servicio de backup	[D]	[E.4] Errores de configuración	[A]	B	[0]	MB	{0,29}

Ilustración 76 Riesgo residual



padre	D	hijo	D	amenaza	V	D	I	N	R
[SERV.PEL] Servicio mercancías ...	[D]	[IS_BCK] Servicio de backup	[D]	[E.4] Errores de configuración	[A]	B	[0]	MB	{0,29}
[SERV.S24] Servicio 24 Horas	[D]	[IS_BCK] Servicio de backup	[D]	[E.4] Errores de configuración	[A]	B	[0]	MB	{0,29}
[DAT.D_CLI] Datos de clientes	[I]	[IS_BCK] Servicio de backup	[I]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,20}
[DAT.D_CONV] Datos servicios co...	[I]	[IS_BCK] Servicio de backup	[I]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,20}
[DAT.D_CONV] Datos servicios co...	[C]	[IS_BCK] Servicio de backup	[C]	[E.4] Errores de configuración	[M]	M	[0]	B	{0,20}
[DAT.D_24H] Datos envíos 24 hor...	[I]	[IS_BCK] Servicio de backup	[I]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,20}
[DAT.D_24H] Datos envíos 24 hor...	[C]	[IS_BCK] Servicio de backup	[C]	[E.4] Errores de configuración	[M]	M	[0]	B	{0,20}
[DAT.D_PEL] Datos mercancías p...	[I]	[IS_BCK] Servicio de backup	[I]	[E.4] Errores de configuración	[A]	B	[0]	B	{0,20}
[DAT.D_PEL] Datos mercancías p...	[C]	[IS_BCK] Servicio de backup	[C]	[E.4] Errores de configuración	[M]	M	[0]	B	{0,20}
[SERV.PEL] Servicio mercancías ...	[D]	[IS_COR] Servicio de correo	[D]	[E.4] Errores de configuración	[A]	B	[0]	MB	{0,19}
[SERV.S24] Servicio 24 Horas	[D]	[IS_COR] Servicio de correo	[D]	[E.4] Errores de configuración	[A]	B	[0]	MB	{0,19}
[SERV.CONV] Servicio convencio...	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.4] Errores de configuración	[M]	B	[0]	MB	{0,17}
[SERV.CONV] Servicio convencio...	[D]	[HW.HWRED.WIFI] Router Wifi Int...	[D]	[E.23] Errores de mantenimiento /...	[M]	B	[0]	MB	{0,11}
[SERV.CONV] Servicio convencio...	[D]	[IS_AD] Servicio de dominio y AD	[D]	[E.3] Errores de monitorización (I...	[M]	B	[0]	MB	{0,10}
[SERV.CONV] Servicio convencio...	[D]	[HW.OTR.LTP] Portátiles	[D]	[A.11] Acceso no autorizado	[M]	B	[0]	MB	{0,10}
[SERV.CONV] Servicio convencio...	[D]	[HW.OTR.IMP] Impresoras	[D]	[A.7] Uso no previsto	[M]	B	[0]	B	{0,04}
[SERV.CONV] Servicio convencio...	[D]	[IS_BCK] Servicio de backup	[D]	[E.4] Errores de configuración	[M]	B	[0]	MB	{0,01}
[SERV.CONV] Servicio convencio...	[D]	[IS_COR] Servicio de correo	[D]	[E.4] Errores de configuración	[M]	B	[0]	MB	{0,01}
[SERV.CONV] Servicio convencio...	[D]	[HW.OTR.IMP] Impresoras	[D]	[I.5] Avería de origen físico o lógico	[M]	B	[0]	B	{0,01}

Ilustración 77 Riesgo residual

De los resultados obtenidos, vemos como efectivamente ha disminuido el riesgo de la organización, llegando a no tener ninguna amenaza por encima de 5. Podemos afirmar por tanto que el Plan de Tratamiento de Riesgos ha sido todo un éxito en la organización Fictional.

6. Fase 5: Auditoría de cumplimiento

6.1 Introducción

Concluido el análisis de riesgos y la implantación de las propuestas necesarias en materia de seguridad, es momento de identificar las posibles deficiencias generadas a partir de dichas propuestas y las oportunidades de mejora asociadas a las mismas.

Para ello se va a realizar una auditoría basada en la normativa ISO/IEC 27001:2013, así como en el Anexo A o ISO 27002:2013. Este ejercicio es necesario puesto que la organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de seguridad de la información cumple con los requisitos propios de la organización para su sistema de gestión de seguridad de la información y los requisitos de esta norma internacional.

6.2 Metodología

Todo sistema implantado requiere de un mantenimiento que permita la prevención y corrección de anomalías detectadas, la norma ISO 27001 así lo contempla dentro del establecimiento y gestión del Sistema de Gestión de Seguridad de la Información.

A partir de la acción correctiva la organización tiene la posibilidad de eliminar la causa de las no conformidades que se hayan encontrado durante la auditoría del SGSI. Las acciones correctivas se deben de documentar e incluir los siguientes requisitos:

1. Identificar las no conformidades.
2. Determinar las causas de las no conformidades.
3. Evaluar acciones que logren eliminar las no conformidades.
4. Determinar e implementar la acción correctiva necesaria.
5. Registrar los resultados de la acción realizada.
6. Revisar la acción correctiva.

6.3 Evaluación de la madurez

En primera instancia se ha auditado los requerimientos para establecer, implementar, mantener y continuamente mejorar el Sistema de Gestión de Seguridad de la Información, agrupado en 7 cláusulas.

Se ha podido comprobar la evolución de la madurez en la organización Fictional. En la siguiente tabla y gráfico se puede observar el avance logrado:

Cláusulas	CMM Inicial	CMM Actual
Contexto de la organización	L1	L3
Liderazgo	L1	L2
Planificación	L0	L3
Soporte	L0	L2
Operación	L1	L3
Evaluación del desempeño	L0	L2
Mejora	L0	L3

Tabla 11 Comparación de cláusulas ISO 27001:2013

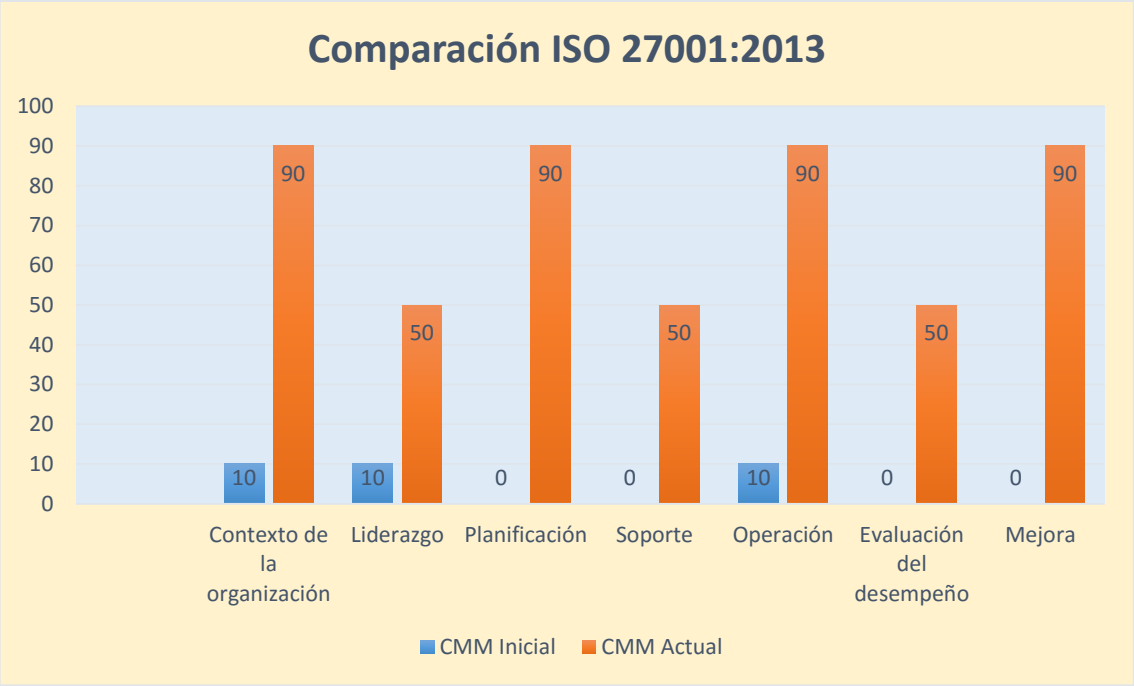


Ilustración 78 Comparación de cláusulas ISO 27001:2013

Respecto a la ISO 27002:2013 se ha podido auditar el nivel de madurez de los controles obteniendo la siguiente evolución respecto a su estado inicial:

Fictional :: [27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información

Editar Expandir Exportar Importar Seleccionar Gráficas

[base] Base | Fuentes de información

recomendación	control	inicial	Actual
	[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información	11%	36%
2	[5] Políticas de seguridad de la información	0%	50%
5	[6] Organización de la seguridad de la información	4%	32%
5	[7] Seguridad ligada a los recursos humanos	17%	18%
5	[8] Gestión de activos	10%	23%
7	[9] Control de acceso	10%	60%
3	[10] Criptografía	5%	45%
7	[11] Seguridad física y del entorno	40%	28%
7	[12] Gestión de operaciones	11%	14%
6	[13] Seguridad de las comunicaciones	11%	47%
6	[14] Adquisición, desarrollo y mantenimiento de los sistemas	8%	13%
5	[15] Relaciones con proveedores	12%	27%
5	[16] Gestión de incidentes de seguridad de la información	0%	50%
6	[17] Aspectos de seguridad de la información en la gestión de la continuidad del negocio	5%	50%
6	[18] Cumplimiento	28%	50%

porcentaje dominios aplicar

Ilustración 79 Comparación de dominios ISO 27002:2013

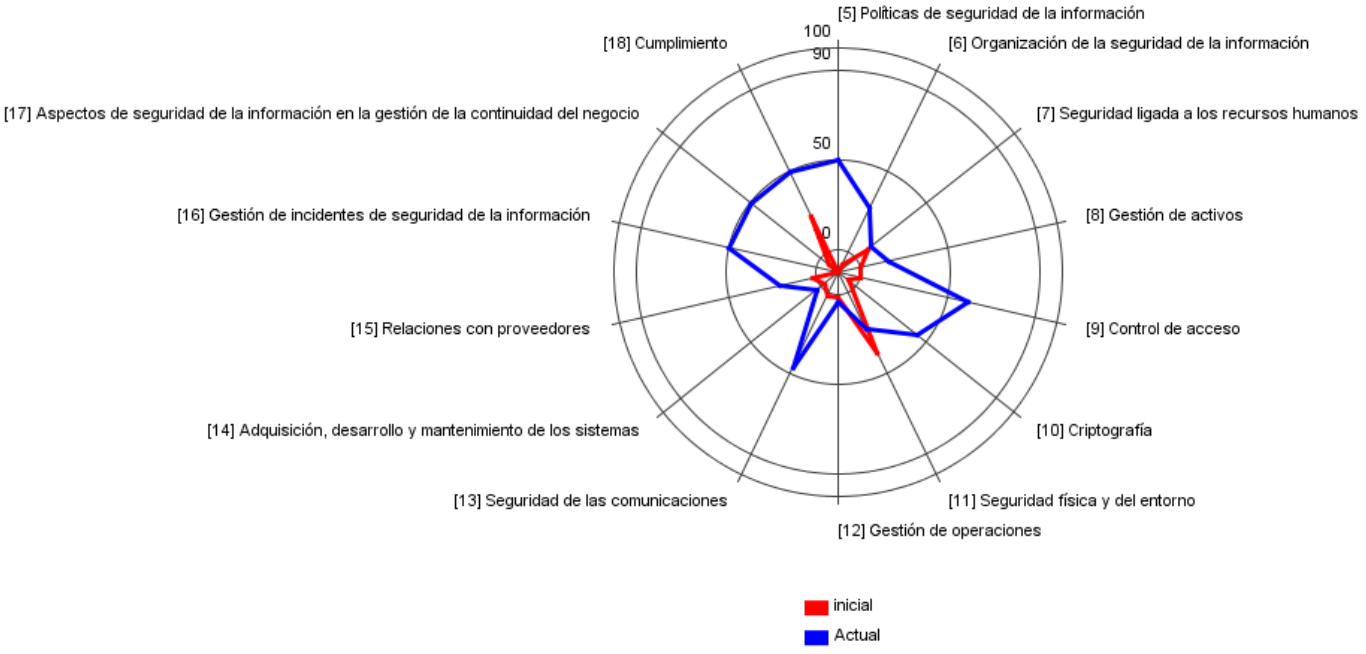


Ilustración 80 Comparación de dominios ISO 27002:2013

Por último, con el fin de conocer de forma concreta el nivel de madurez del SGSI de Fictional se ha realizado la siguiente gráfica donde se puede observar el porcentaje de madurez de cada nivel respecto a los controles de la ISO 27002:2013.

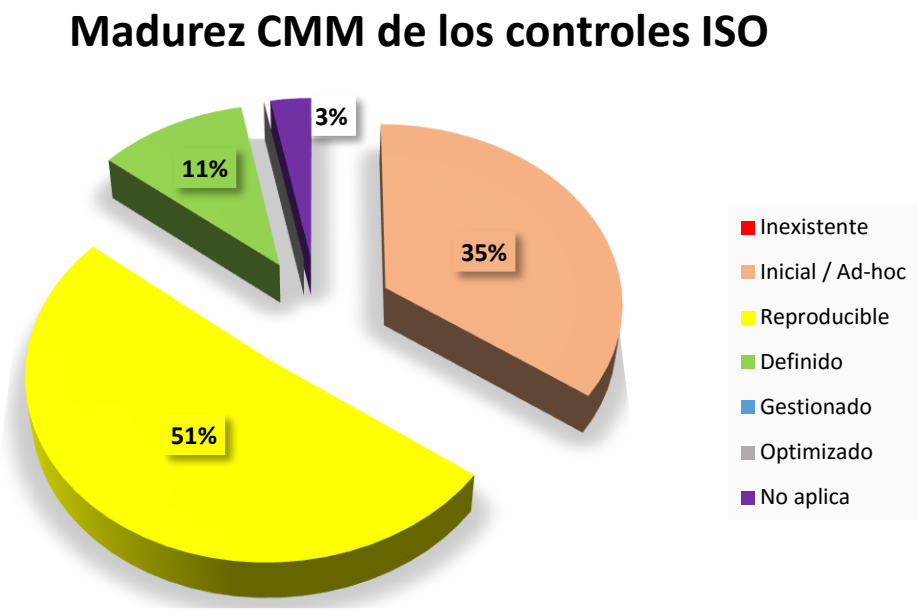


Ilustración 81 Porcentaje de madurez de los niveles de CMM en SGSI

6.4 Informe no conformidades

Se ha elaborado un fichero con las no conformidades detectadas durante la auditoría de cumplimiento y las acciones correctivas asociadas a las mismas. Tal y como requiere la ISO 27001:2013, para cada no conformidad se han detallado los siguientes aspectos:

- Origen de la no conformidad
- Descripción de la no conformidad detectada
- Acción inmediata a realizar
- Análisis de la causa
- Acción correctiva
- Coste de aplicar la acción correctiva
- Responsable de cada no conformidad
- Fecha de inicio de la acción correctiva
- Medición de la eficacia
- Fecha prevista de cierre
- Estado
- Fecha de cierre
- Observaciones

Se han hallado un total de 11 No conformidades durante la auditoría de cumplimiento. Sobre las mismas se realizará un seguimiento en el fichero SGSI-NoConformidades_AccionesCorrectivas-Fictional.xls

Ficha No Conformidades - Fictional S.L.

ID	ORIGEN	NO CONFORMIDAD	CONTROL ASOCIADO 27001:2013	ACCIONES INMEDIATAS	ANÁLISIS DE CAUSA	ACCIÓN CORRECTIVA	COSTE	RESPONSABLE	FECHA DE INICIO	MEDICION DE LA EFICACIA	FECHA PREVISTA DE CIERRE	ESTADO	FECHA DE CIERRE	OBSERVACIONES
1	Auditoría Interna	NC01.A) Información documentada. La documentación del SGSI no encuentra pendiente de aprobación a fecha de la auditoría.	Apartado 7.5 Información documentada	Aprobación en la Revisión por la Dirección de la documentación del SGSI	En el momento de la auditoría interna no se había realizado la revisión por la dirección donde se aprobaría la documentación del SGSI. SGSI inmadura	Llevar a cabo una seguimiento de la aprobación de la documentación	4h.	Comité de Seguridad	01/06/2016	Verificar que la documentación vigente se encuentra aprobada	01/06/2017	Abierta		
2	Auditoría Interna	NC01.B) Información documentada. Asimismo, cómo nace dispone de gran parte de los registros que se derivan de la aplicación de los procedimientos del SGSI.	Apartado 7.5 Información documentada	Hacer una primera medición de los registros que se posible.	El Sistema de Gestión de Seguridad de la Información de Fictional aún no ha desarrollado por lo que en el momento de la auditoría no se dispone de todos los registros exigidos al mismo. SGSI inmadura	Llevar a cabo una implantación efectiva de los procedimientos definidos en el SGSI	80h.	Comité de Seguridad	01/06/2016	Verificar registros	01/06/2017	Abierta		
3	Auditoría Interna	NC02. Seguimiento, medición, análisis y evaluación. No se han implantado, a fecha de la auditoría, las métodos provistos para el seguimiento, medición, análisis y evaluación del desempeño de la seguridad de la información y la eficacia del SGSI.	Apartado **9. Seguimiento, medición, análisis y evaluación**	Aprobación en la Revisión por la Dirección de los indicadores y realización de una primera medición	En el momento de la auditoría no se había previsto los métodos de seguimiento, medición, análisis y evaluación. SGSI inmadura	Establecer indicadores para poder realizar un seguimiento del Sistema de Gestión de forma que se mida el desempeño de la seguridad de la información y su eficacia.	5h.	Comité de Seguridad	01/06/2016	Verificar la medición efectiva de indicadores	01/06/2017	Abierta		
4	Auditoría Interna	NC03.A) DC4. Organización de la seguridad de la información. No se ha definido las propietarios de los activos de la organización, conforme a lo indicado en el procedimiento SGSI-P-A.06-01 de Asignación de responsabilidades	Dominio de control 6 del Anexo A. **Organización de la seguridad de la información.**	La propiedad de los activos: Servidores, electrónicos de red y aplicaciones no ha asignada al área de sistemas.	No existe una adecuada definición de la propiedad de los activos	Se ha establecido una asignación orientativa para la propiedad de los sistemas de información dependiendo del área de sistemas	3h.	Comité de Seguridad	01/06/2016	Verificar la asignación de la propiedad de activos	01/06/2017	Abierta		
5	Auditoría Interna	NC03.B) DC4. Organización de la seguridad de la información. No se dispone de los acuerdos de confidencialidad de terceros y fichas de especificación de requerimientos de seguridad de la información previstos por el procedimiento SGSI-P-A.06-01 de Asignación de responsabilidades	Dominio de control 6 del Anexo A. **Organización de la seguridad de la información.**	Solicitar a los proveedores la firma de acuerdos de confidencialidad.	Hasta ahora no implantada, a fecha de la auditoría interna, todavía no dio definitivo en los procedimientos que dan cumplimiento al SGSI al ser parte de reciente creación y estar en proceso de implantación. SGSI inmadura	Establecer un proceso previo a la contratación/adquisición con terceros de requerimientos de seguridad	2h.	Comité de Seguridad	01/06/2016	Verificar la firma de acuerdos de confidencialidad y cumplimentación de hojas de requerimientos de seguridad	01/06/2017	Abierta		
6	Auditoría Interna	NC03.C) DC4. Organización de la seguridad de la información. Tampoco se ha podido evidenciar la comunicación de la política de seguridad de la organización al personal externo a Fictional que desarrolla tareas para la organización en las que pueden estar implicados sistemas de información de su dominio protegible conforme a lo indicado en el apartado 8.1 de dicho procedimiento	Dominio de control 6 del Anexo A. **Organización de la seguridad de la información.**	Se ha propuesto la comunicación de la política de seguridad a terceros en próximas renovaciones contractuales o nuevos contratos	Hasta hoy la consideración no ocurrió la comunicación de la política de seguridad.	Comunicar la política de seguridad de la organización a las entidades externas que dispongan de acceso a la información de Fictional	1h.	Comité de Seguridad	01/06/2016	Verificación de la comunicación de la política de seguridad a terceros	01/06/2017	Abierta		
7	Auditoría Interna	NC04.A) DC9. Control de acceso. Se ha constatado la utilización de usuarios genéricos para el acceso a activos de la organización vía VPN. Además, los contraseñas compartidas utilizadas no satisfacen todas las políticas de seguridad de contraseñas definidas para la organización. Asimismo, dichas contraseñas no son cambiadas cuando alguno de los usuarios de los cuentas genéricas cause baja en la organización.	Dominio de control 9 del Anexo A. **Control de acceso**	Cambiar las contraseñas genéricas tras la baja de un usuario y establecer cuentas nominales para el acceso a los activos de la organización vía VPN.	Hasta la implantación del Sistema de Gestión no se había considerado la falta de seguridad en la gestión de contraseñas y tras la implantación no se había corregido esta desviación.	Limitación en la utilización de usuarios genéricos y estudio de la posible eliminación de los existentes Evaluación de requisitos de autenticación en la adquisición de nuevos activos	20h.	Comité de Seguridad	01/06/2016	Verificación de políticas de contraseñas de los aplicaciones corporativas	01/06/2017	Abierta		
8	Auditoría Interna	NC05. A) DC11. Seguridad física y del entorno. El armario que alberga los servidores de fichaje y los electrónicos de red en las oficinas de Fictional no encontraba abierta en el momento de la auditoría.	Dominio de control 11 del Anexo A. **Seguridad física y del entorno**	Cerrar el armario que alberga los servidores de fichaje y los electrónicos de red.	Concienciación inadecuada.	Establecer formación sobre el SGSI y llevar a cabo diferentes medidas de concienciación de seguridad de la información.	6h.	Comité de Seguridad	01/06/2016	Verificación de que los registros encuentra cerrados	01/06/2017	Abierta		
9	Auditoría Interna	NC06.A) DC12. Seguridad de las operaciones. El sistema de protección antivirus de la organización no encuentra operativo las últimas meses.	Dominio de control 12 del Anexo A. **Seguridad de las operaciones**	Actualmente se está instalando el nuevo sistema antivirus Microsoft	Desde Microsoft se realizó una actualización que provocó incompatibilidades, por cual llevando a cabo la actualización de los sistemas	Realizar prueba de migración en entornos de preproducción	40d.	Comité de Seguridad	01/06/2016	Verificar el estado de implantación de los sistemas antivirus	01/06/2017	Abierta		
10	Auditoría Interna	NC07.A) DC15. Relación con proveedores. No se dispone de cláusulas y acuerdos de responsabilidades y obligaciones en materia de seguridad para todos los suministradores de servicios conforme a lo indicado en los procedimientos SGSI-P-A.06-01 de Asignación de responsabilidades	Dominio de control 15 del Anexo A. **Relación con proveedores**	Se ha solicitado los acuerdos de confidencialidad pertinentes a los proveedores.	Procedimiento de reciente creación por lo que en el tiempo en viger del mismo no se han podido implementar las medidas de forma completa y efectiva. Se ha delegado en los proveedores la suscripción de acuerdos de confidencialidad	Establecer acuerdos de responsabilidades y obligaciones en materia de seguridad con los proveedores de Fictional	8h.	Comité de Seguridad	01/06/2016	Verificar la existencia de acuerdos de confidencialidad con los principales proveedores	01/06/2017	Abierta		
11	Auditoría Interna	NC08. DC17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio. A fecha de la auditoría no se ha desarrollado ni aprobado un Plan de continuidad del negocio	Dominio de control 17 del Anexo A. **Aspectos de seguridad de la información para la gestión de la continuidad del negocio**	Definición del PCN	SGSI inmadura	Se ha desarrollado un plan de contingencia y ha establecido en los tres próximos años la realización de pruebas en fechas que tengan un impacto mínimo para la operativa de Fictional. Por otra parte, durante 2016 no va a llevar a cabo un proyecto que contemple la definición de planes de continuidad de negocio	40d.	Comité de Seguridad	01/06/2016	Verificar la realización de planes de continuidad de negocio y la realización de las pruebas aportadas	01/06/2017	Abierta		

Ilustración 82 No conformidades detectas en auditoría de cumplimiento SGSI

7. Fase 6: Presentación de resultados y entrega de informes

7.1 Introducción

Fictional ya dispone de un Sistema de Gestión de Seguridad de la Información, se trata de un SGSI inmaduro puesto que es de reciente implantación, no obstante el primer paso es asentar las bases y la organización lo ha conseguido.

El siguiente paso a realizar es recopilar la información y resultados obtenidos con el fin de darle el formato pertinente para su posterior presentación.

7.2 Objetivos de la fase y entregables

El objetivo principal de esta fase es la generación de la documentación que contenga los resultados obtenidos a lo largo del proyecto. Se realizarán cuatro presentaciones en formato PowerPoint:

- **Resumen ejecutivo**: Documento en el que se resume las diferentes fases del proyecto, así como las principales actividades que se han desarrollado en cada fase.

- **Presentación a la compañía**: Documento en el que se presenta el proyecto de implantación del SGSI desarrollado a la organización

- **Presentación del estado de cumplimiento de los controles**: Documento en el que se resume el estado de implementación de los controles que han sido necesarios implementar.

- **Presentación a la dirección**: Documento en el que se recogen las conclusiones del proyecto, sin utilizar lenguaje técnico, con el objetivo de presentarlo a la dirección.

8. Conclusiones

Una vez finalizado el proyecto es momento de analizar las lecciones aprendidas durante el transcurso de la implantación de la ISO/IEC 27001:2013 en una organización ficticia.

En primer lugar considero necesario que las organizaciones que disponen de sistemas de información y por tanto de empleados encargados de gestionar dichos sistemas, dispongan de un Sistema de Gestión de Seguridad de la Información. El primer paso para proteger en materia de seguridad de la información tu organización, es creer en ello. Ser consciente de que existen unas vulnerabilidades en tus activos y que por tanto están expuestos a ataques o incidentes de seguridad con la consecuente pérdida económica.

En segundo lugar considero que el proyecto es una práctica muy realista, puesto que la implantación de la ISO/IEC 27001:2013 es una tarea demandada en el sector TI, así como las auditorías sobre los Sistemas de Gestión de Seguridad de la Información.

Por otro lado, el hecho de haber desarrollado un análisis de riesgos con la herramienta PILAR me ha servido por partida doble. Primero por conocer la metodología MAGERIT y las etapas de un análisis de riesgos; segundo por haber conocido la herramienta PILAR y poder saber utilizarla.

Además, el hecho de valorar que propuestas puede llevar a cabo una empresa para mitigar o reducir los riesgos a los que se encuentra expuesta, te hace reflexionar sobre diferentes medidas que el día de mañana como consultor puedo proponer a una entidad con una casuística similar.

Respecto a las fases del proyecto, el tiempo establecido para desarrollar cada una era acorde al contenido que se demandaba. Por ello, no he tenido ningún problema para ir completando cada etapa del trabajo.

Por último, considero que se trata de un Trabajo Final de Máster muy apropiado para la especialidad de Gestión y auditoría de la seguridad informática.

9. Glosario

Acción correctiva: Acción tomada para eliminar la causa de una no-conformidad detectada u otra situación indeseable.

Activo: Elemento, lógico, físico o intangible, disponible para garantizar el correcto funcionamiento de los sistemas de información de Fictional.

Análisis del riesgo: proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Ataque: Conjunto de acciones cuyo objetivo es comprometer cualquiera de los aspectos que conforman la seguridad de un recurso (esto es, la integridad, confidencialidad o disponibilidad del mismo).

Incidente: Violación grave o potencial violación grave de las normativas de seguridad definidas en Fictional, por parte de usuarios externos o internos a la organización.

No conformidad: Actividad, servicio o proceso que no cumple con los requisitos especificados en el Sistema de Gestión de la Seguridad de la Información (SGSI) de Fictional.

Política de seguridad: Documento en el que se establece el compromiso de la Dirección de Fictional y el enfoque de la organización para gestionar la seguridad de la información. Es de conocimiento y cumplimiento **obligado** para todo el personal de la compañía y para terceros que puedan verse afectados por el contenido de la misma en cualquier relación con Fictional.

Recurso: Conjunto de elementos, lógicos y físicos, disponibles para garantizar el correcto funcionamiento de los sistemas de información de Fictional.

Riesgo: efecto de la incertidumbre sobre la consecución de los objetivos. Con frecuencia, el riesgo se expresa en términos de combinación entre impacto y probabilidad.

Riesgo residual: riesgo remanente después del tratamiento del riesgo.

Sistema de Gestión de la Seguridad de la Información: Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información; es la herramienta de que dispone el Responsable Técnico del SGSI para llevar a cabo las políticas y los objetivos de seguridad dentro de la organización.

Tratamiento del riesgo: proceso destinado a modificar el riesgo.

10. Bibliografía

[0] **International Organization for Standardization.** Information technology - Security techniques - Information security management systems - Requirements. ISO/IEC, 2013. ISO 27001:2013.

[1]http://www.pmg-ssi.com/2013/12/iso27001-origen/
[Consulta: 2 de marzo 2016]

[2]http://www.pdcahome.com/5202/ciclo-pdca/
[Consulta: 4 de marzo de 2016]

[3]http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/41_leccin_16_cmo_definir_el_alcance_del_sgsi.html
[Consulta: 5 de 2016]

[4]http://www.globales.es/imagen/internet/Informaci%C3%B3n%20General%20CMMI.pdf
[Consulta: 6 de marzo de 2016]

[5]http://www.gmv.com/es/Seguridad/GestionSeguridadInformacion/GestionSeguridad.html
[Consulta: 18 de marzo de 2016]

[6]https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Politicas_normas_procedimientos_de_seguridad_y_otros_documentos_de_un_SGSI
[Consulta: 23 de marzo de 2016]

[7]**Ministerio de Hacienda y Administraciones Públicas.** *MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[8]http://www.pmg-ssi.com/2014/03/iso-27001-y-el-inventario-de-activos-de-la-informacion/
[Consulta: 20 de abril de 2016]

11. Anexos

- SGSI-PS-Política de seguridad.docx
- SGSI-P-09-01_Gestión de indicadores.docx
- SGSI-P-10-02_Procedimiento de acciones correctivas y no conformidades.docx
- SGSI-P-A.06-01_Asignación de responsabilidades.docx
- SGSI-P-A.08-01_Clasificación y tratamiento de la información.docx
- SGSI-P-A.18-01_Procedimiento de Auditorías Internas.docx
- SGSI_PTR_Fictional.xlsx
- SGSI_NoConformidades_AccionesCorrectivas_Fictional.xlsx
- Valoración_CMM_ISO27002_Fictional.xlsx
- Diagrama de Gantt Planificación_TFM.png
- Diagrama de Gantt Planificación_PTR.png
- Organigrama.pptx
- Cumplimiento de los controles.pptx
- Presentación a la compañía.pptx
- Presentación a la dirección.pptx
- Resumen ejecutivo.pptx