Gestión de Auditoría y Seguridad

José Antonio Riaza Valverde Cristian Cuerda González
José Roldán Gómez

19 de diciembre de 2017

Índice

1. Introducción

En la actualidad manejar correctamente la información es crucial para cualquier organización. Esto se debe a que vivimos en mundo completamente globalizado y con unas condiciones que cambian de forma rápida y repentina.

Es necesario realizar una correcta estrategia y planificación que nos permita evitar y responder antes posibles problemas que nuestro sistema de información pueda sufrir.Por eso es importante realizar y documentar correctamente un sistema de gestión de la seguridad de la información (SGSI).

GoodSound$^{\text{TM}}$ es una empresa de base tecnológica cuyo objetivo es reducir la contaminación acústica en las grandes ciudades y mejorar la calidad de vida de todos los ciudadanos. Para ello nuestra principal herramienta es la información que podamos recoger para llevar a cabo las medidas pertinentes en base a esta información. Esta necesidad imperante de información provoca que sea crucial para nosotros ceñirnos a un SGSI.

Para lograr este objetivo emplearemos sensores capaces de medir los decibelios de las zonas de ocio de las urbes, que posteriormente preprocesamos para evitar los posibles errores introducidos por los sensores de ruido. A continuación se enviarán a un motor de eventos complejos, el cual es capaz de detectar patrones predefinidos por nosotros y realizar acciones en función de los mismos. En nuestro caso, el motor CEP nos permitirá modificar los LEDs de una columna que permita al viandante comprender el estado del ruido de la zona.

Además, se pretende implementar una aplicación móvil que permita a los usuarios concienciados obtener ventajas como descuentos, y a los locales que cumplan con la normativa tener publicidad de forma gratuita.

Este documento pretende ser una guia aproximada de cómo implantar un Sistema de Gestión de Seguridad de la Información. En la siguiente sección veremos los conceptos relativos a los SGSI, ya que es obligatorio para comprender correctamente el resto del trabajo. En la tercera sección se realiza un análisis de riesgos identificando los activos de la empresa y asignándoles un valor de acuerdo a los objetivos de negocio de la empresa; además se identifican las posibles amenazas que afectan a cada activo, así como el impacto negativo que pueden tener de ocurrir en base a nuestro modelo de negocio, y la probabilidad de que estos ocurran. En la cuata sección vamos a ver posibles salvaguardas y controles para reducir estos riesgos, además también vamos a ver cómo podemos gestionar los riesgos residuales que quedan tras aplicar las salvaguardas. En la última sección analizaremos las conclusiones obtenidas durante la realización del trabajo.

2. Sistemas de gestión de la seguridad de la información

Un SGSI proporciona un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio, basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos.

El SGSI debe contener un análisis de riesgos para conformar una estrategia sobre cómo tratar los aspectos relacionados con la seguridad e implementación de los controles necesarios. Dicho análisis debe incluir los siguientes puntos:

- Determinar que se trata de proteger
- Determinar de que es necesario protegerse
- Determinar cuan probables son las amenazas
- Implementar los controles que protejan bienes informáticos de una manera rentable.
- Revisar continuamente este proceso y perfeccionarlo cada vez que se encuentra una debilidad (vulnerabilidad).

En resumen, esta metodología promueve la adopción de un enfoque basado en procesos "Planificar-Hacer-Verificar-Actuar", el cual se aplica para estructurar todos los procesos del SGSI como se indica en la ISO/IEC 27001 [1].

2.1. Margerit

Tal y como indica *PILAR* en [2], la metodología que se utiliza para el análisis y la gestión de riesgos es *Magerit*. Los activos de la empresa están continuamente expuestos a amenazas que, cuando se materializan, degradan el activo produciendo un impacto. Si estimamos la frecuencia con que se materializan las amenazas, podemos deducir el riesgo al que está expuesto el sistema.

Por otro lado, la degradación y la frecuencia califican la vulnerabilidad del sistema. El gestor del sistema de información dispone de salvaguardas, que o bien reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto. Dependiendo del grado de implantación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo que se denomina *riesgo residual*. En la Figura 1 se muestra el funcionamiento de *Magerit*.

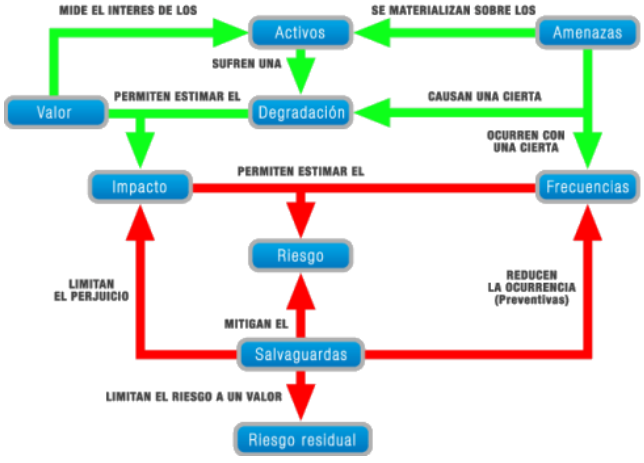

Figura 1: Proceso de *Margerit*

PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

- ISO/IEC 27002 (2005, 2013)- Código de buenas prácticas para la Gestión de la Seguridad de la Información.
- ENS - Esquema Nacional de Seguridad.

2.2. Fases del proceso

Para la implantación de un SGSI es necesario llevar a cabo una serie de pasos que se dividen en distintas fases. En nuestro caso, el proyecto arranca dando por supuesto que se han realizado anteriormente las fases 1 y 2 mostradas en la Figura 2. Hemos llevado a cabo las fases 3, 4, 5 y 6, a la espera de realizar la auditoria interna en la siguiente parte de la asignatura.

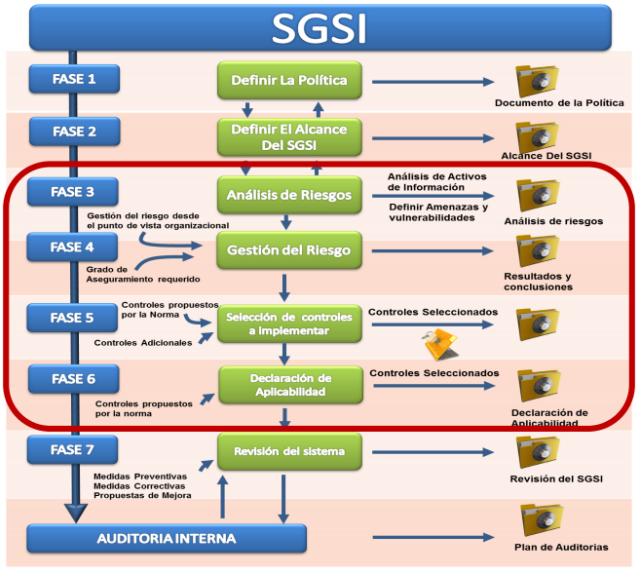

Figura 2: Fases del proceso

Como las fases 1 y 2 no se han llevado a cabo, vamos a explicar brevemente en qué consisten de forma teórica.

En la fase 1 se recogen las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la organización y legislación vigente. Se debe establecer cómo actuar en caso de incidente y definir responsabilidades. Además es necesario indicar qué se va a proteger, de quién queremos protegerlo y por qué y determinar dónde está el límite de un comportamiento aceptable y que ocurre si se sobrepasa ese comportamiento. Toda esta información se recoge en el *Documento de la Política*, el cual debe cumplir las siguientes especificaciones:

- Accesible a toda la organización corta, preciso y fácil de entender.
- Aprobado y publicada por la dirección

- De dominio público a la organización.
- Referencia en resolución de conflictos.
- Definir responsabilidades
- Personalizado para la organización.
- Indicar las normas de comportamiento y seguridad.

En la fase 2 se establece cuál va a ser el alcance del SGSI, es decir, qué partes o procesos de la organización forman parte del mismo. Para llevar a cabo esta tarea hay que i) identificar los procesos críticos; ii) estimar los recursos económicos y de personal necesarios para implantar y mantener el SGSI; y iii) definir cuáles son las actividades de la organización, las ubicaciones físicas involucradas, la tecnología que usa la organización y qué áreas están excluidas.

3. Análisis de riesgos

El análisis de riesgos consiste en una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados. En esta sección se van a enumerar aquellos activos que se han encontrado más relevantes en nuestra empresa y la valoración que hemos realizado en cuanto a confidencialidad, disponibilidad e integridad de cada uno de ellos. Después, se enumeran las amenazas más significativas que se han encontrado y que afectan a dichos activos. Dichas amenazas son las que tienen más probabilidad de ocurrir y por lo tanto, aquellas que implican un mayor riesgo.

3.1. Activos

En un sistema de información hay dos cosas esenciales: la información que maneja y los servicios que presta. Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema [3].

Definición 1. Activo, (véase en [3]). *Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.*

Subordinados a dicha esencia se pueden identificar otros activos relevantes, que se especifican en la siguiente sección.

3.1.1. Tipos de activos

La clasificacion que sigue lista los activos tal y como se contemplan en [4], determinando para cada uno un código, un nombre y una breve descripción. Nótese que la pertenencia de un activo a un tipo no es excluyente de su pertenencia a otro tipo; es decir, un activo puede ser simultáneamente de varios tipos.

[S] Servicios. Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio se requieren una serie de medios.

[D] **Datos**. Elementos de información que, de forma singular o agrupados de alguna forma, representan el conocimiento que se tiene de algo.

[SW] **Aplicaciones**. Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

[HW] **Equipos informáticos**. Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

[COM] **Redes de comunicaciones**. Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

[SI] **Soporte de información**. Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[AUX] **Equipamiento auxiliar**. Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

[L] **Instalaciones**. Lugares donde se hospedan los sistemas de información y comunicaciones.

[P] **Personal**. Personas relacionadas con los sistemas de información.

3.1.2. Activos identificados

En la Tabla 1 se muestran resumidos los activos identificados en nuestra empresa *GoodSound*$^{\text{TM}}$, clasificados por el tipo de activo del que se trata. A continuación se enumeran los activos más importantes de la empresa junto a uan breve descripción:

- **PILAR**. Programa (software) utilizado para la gestión de riesgos en la empresa.
- **MATLAB**. Programa (software) utilizado en el modelado del sistema hardware que se va a desarrollar.
- **Motor CEP**. Programa (software) utilizado para trabajar con los datos detectados por los sensores de ruido, crear patrones y lanzar eventos complejos.
- **Ordenadores**. Dispositivos físicos que se utilizan para desarrollar nuestro sistema, elaborar la documentación, instalar los servidores con los que se comunicaran los distintos componentes, etc.

Tipo		Activo
Equipos informáticos	[**HW**]	Ordenadores Arduinos Raspberrys Sensores
Aplicaciones	[**SW**]	PILAR Motor CEP MATLAB
Personal	[**P**]	José Antonio Riaza Valverde José Roldán Gómez Cristian Cuerda González Yuri Coicca
Servicios	[**S**]	Gestoria Fiscal y Financiera Empresa de instalación
Instalaciones	[**L**]	Oficinas
Redes de comunicación	[**COM**]	Conexión a internet

Tabla 1: Activos de *GoodSound*$^{\text{TM}}$

- **Arduinos**. Plataforma de hardware libre, basada en una placa con un microcontrolador y un entorno de desarrollo, diseñada para facilitar el uso de la electrónica en proyectos multidisciplinares. Se utilizan para recoger la información que proporcionan los sensores de ruido y realizar un primer procesamiento y eliminar anomalías.
- **Raspberrys**. Placa que soporta varios componentes necesarios en un ordenador común. Una vez recogida la información en los Arduinos, las Raspberrys ejecutan el motor CEP y envían información a la columna de la conciencia y a nuestro web service.
- **Sensores**. Micrófonos que se encargan de medir los niveles de ruidos que hay en una zona determinada.
- **Conexión a Internet**. Conexión que se utiliza tanto para trabajar en nuestra oficina como para comunicar los diferentes componentes del sistema.
- **Gestoría Fiscal y Financiera**. Empresa subcontratada encargada de llevar a cabo las tareas de contabilidad, impuestos, hacienda, etc.
- **Consultoría (profesores)**. Empresa subcontratada para realizar tareas de consultoría y asesoramiento.
- **Empresa de instalación**. Empresa encargada de instalar los sistemas desarrollados en los distintos bares de la Zona.
- **Oficinas**. Oficinas centrales de nuestra empresa, donde se lleva a cabo el desarrollo del sistema, se alojan los servidores y se realizan las tareas de mantenimiento.
- **Trabajadores**. Cada uno de los trabajadores con los que cuenta la empresa.

3.2. Amenazas

Definición 2. Amenaza. *Situación de daño hacia una empresa o sus activos cuyo riesgo de producirse es significativo o relevante.*

3.2.1. Amenazas identificadas

En esta sección vamos a describir en qué consisten algunas de las amenazas más significativas. Como a menudo las amenazas se repiten entre activos que pertenecen a una misma categoría, vamos a clasificar las amenazas en esas mismas categorías para explicarlas más fácilmente:

- **Software**:
  - **Vulnerabilidades de los programas (software)**. Errores de código que pueden permitir el acceso de virus o malware a nuestro sistema mediante el uso de técnicas como los exploit.
  - **Errores de mantenimiento / actualización de programas (software)**. Problemas de compatibilidad al actualizar un software con las versiones anteriores, perdidas de información durante la actualización, etc.
  - **Manipulación de programas**. Alteración malintencionada de nuestros sistemas con la finalidad de causar algún perjuicio.
- **Hardware**:
  - **Fuego**. Daños causados por incendios o pequeños fuegos no controlados.
  - **Daños por agua**. Averías y daños causados por el agua debido a una inundación, una gotera o un derrame de una botella por ejemplo, o la humedad.
  - **Desastres naturales**. Desastres naturales como terremotos, huracanes, tsunamis y demás, que puedan afectar a nuestros equipos dejándolos inutilizables.
  - **Corte del suministro eléctrico**. Cortes provocados por averías en la línea, impagos, averías dentro de la oficina, mantenimiento, etc.
  - **Condiciones inadecuadas de temperatura o humedad**. Daño continuado en el tiempo debido a temperaturas extremas o condiones de humedad que afecten negativamente a los componentes hardware.
  - **Errores de mantenimiento / actualización de equipos (hardware)**. Problemas surgidos al actualizar los equipos o al llevar a cabo las tareas de mantenimiento, como componentes defectuosos, componentes que no son compatibles entre ellos, etc.
  - **Caída del sistema por agotamiento de recursos**. Indisponibilidad temporal del sistema debido a una sobrecarga del mismo.
  - **Pérdida de equipos**. Perdida de pequeños componetes hardware de forma accidental.
  - **Acceso no autorizado**. Acceso a nuestros equipos por personal no autorizado.

- **Manipulación del hardware**. Alteración de los componentes hardware de forma malintencionada o indebida.
- **Denegación de servicio**. Ataque a nuestro sistema para que no pueda proporcionar uno o varios servicios.
- **Robo de equipos**. Sustracción de los equipos hardware.
- **Ataque destructivo**. Ataque físico contra nuestros equipos, como por ejemplo, lanzar piedras a los sensores, mojarlos, golpearlos, etc.
- **Conexiones**.
- **Fallo de servicios de comunicaciones**. Cualquier error que se produzca de forma no intencionada durante la comunicación.
- **Errores del administrador del sistema / de la seguridad**. Defectos en la configuración de la red o problemas no tratados que posteriormente den lugar a fallos o errores.
- **Suplantación de la identidad**. Acceso no autorizado a nuestra red por parte de personas ajenas al sistema haciéndose pasar por una persona que si tiene acceso.
- **Reencaminamiento de mensajes**. Redirección de los mensajes de nuestra red hacia una maquina no autorizada con fines perjudiciales.
- **Análisis de tráfico**. Comprobación del tráfico de nuestra red de forma no autorizada con fines perjudiciales.
- **Interceptación de información (escucha)**. Captación de mensajes que se transmiten en nuestra red por personal no autorizado con fines perjudiciales.
- **Modificación de la información**. Alteración de mensajes que se transmiten en nuestra red por personal no autorizado con fines perjudiciales.

- **Servicios subcontratados**:
  - **Repudio (negación de actuaciones)**. Negación de hechos, comportamientos o actividades llevados a cabo por parte la empresa subcontratada.
  - **Revelación de información**. Proporcionar nuestra información confidencial de forma intencionada o no a personas no autorizadas a acceder a ella.
  - **Indisponibilidad del personal**. Problemas de salud, de horarios o de cualquier otra índole que no permita que el personal contratado trabaje cuando se le necesita.
  - **Distracción**. Falta de atención que provoque otros fallos mayores, como revelación de información o errores.
  - **Extorsión**. Chantaje hacia nuestra empresa, pidiendo algún tipo de beneficio a cambio de no perjudicarnos.
  - **Ingeniería social (picaresca)**. Problemas con hacienda por impago de impuestos, blanqueo de dinero, empresas en paraísos fiscales, etc.

- **Instalaciones**:

- **Abuso de privilegios de acceso**. Utilizar los permisos que la persona tiene para acceder a nuestras instalaciones con unos fines distintos a los puramente laborales. Por ejemplo, acceder a expedientes de nuestros clientes para obtener información personal y chantajearlos después.
- **Uso no previsto**. Uso de nuestras instalaciones con unos fines distintos a los laborales, como por ejemplo, conectarse a las redes sociales personales en el trabajo.
- **Ocupación enemiga**. Ocupación de nuestras instalaciones por parte de algún tipo de competidor o enemigo, imposibilítanos el acceso.

- **Personal**:
  - **Destrucción de la información**. Eliminación de forma intencionada o no de información de la empresa.

3.2.2. Amenazas por activos

A continuación se listan las amenazas anteriormente explicadas, asociados a los activos de nuestra empresa.

Amenaza	**Prob.**	**[D]**	**[I]**	**[C]**
[E.20] Vulnerabilidades de los programas (software)	P	B	A	B
[E.21] Errores de mantenimiento / actualización de programas (software)	PP	B	A	B
[A.22] Manipulación de programas	PP	B	A	B

Tabla 2: Amenazas del activo **[S1] Pilar**

Amenaza	**Prob.**	**[D]**	**[I]**	**[C]**
[E.20] Vulnerabilidades de los programas (software)	P	M	A	M
[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	A	M
[A.22] Manipulación de programas	PP	M	A	M

Tabla 3: Amenazas del activo **[S2] Matlab**

Amenaza	**Prob.**	**[D]**	**[I]**	**[C]**
[E.20] Vulnerabilidades de los programas (software)	P	A	MA	-
[E.21] Errores de mantenimiento / actualización de programas (software)	PP	A	MA	-
[A.22] Manipulación de programas	PP	A	MA	-

Tabla 4: Amenazas del activo **[S3] Motor CEP**

Amenaza	**Prob.**	**[D]**	**[I]**	**[C]**
[N.1] Fuego	MR	T	MA	A
[N.2] Daños por agua	MR	T	MA	A
[N.*] Desastres naturales	MR	T	MA	A
[I.6] Corte del suministro eléctrico	P	MA	A	A
[I.7] Condiciones inadecuadas de temperatura o humedad	PP	T	MA	A
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	T	MA	A
[E.24] Caída del sistema por agotamiento de recursos	P	MA	A	A
[E.25] Pérdida de equipos	PP	T	MA	A
[A.11] Acceso no autorizado	P	T	MA	A

Tabla 5: Amenazas del activo **[E1] Ordenadores**

Amenaza	Prob.	[D]	[I]	[C]
[N.*] Desastres naturales	MR	MA	M	-
[I.3] Contaminación medioambiental	MR	MA	M	-
[E.24] Caída del sistema por agotamiento de recursos	MR	MA	M	-
[A.23] Manipulación del hardware	P	MA	M	-
[A.24] Denegación de servicio	P	MA	M	-
[A.25] Robo de equipos	MA	MA	M	-
[A.26] Ataque destructivo	CS	MA	M	-

Tabla 6: Amenazas del activo **[E2] Arduinos**

Amenaza	Prob.	[D]	[I]	[C]
[N.*] Desastres naturales	MR	MA	A	-
[I.3] Contaminación medioambiental	MR	MA	A	-
[E.24] Caída del sistema por agotamiento de recursos	MR	MA	A	-
[A.23] Manipulación del hardware	PP	MA	A	B
[A.24] Denegación de servicio	P	MA	A	-
[A.25] Robo de equipos	PP	MA	A	B
[A.26] Ataque destructivo	PP	MA	A	B

Tabla 7: Amenazas del activo **[E3] Raspberrys**

Amenaza	Prob.	[D]	[I]	[C]
[N.*] Desastres naturales	PP	M	B	-
[I.3] Contaminación medioambiental	MR	M	B	-
[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	B	-
[E.24] Caída del sistema por agotamiento de recursos	PP	M	B	-
[E.25] Pérdida de equipos	MA	M	B	-
[A.23] Manipulación del hardware	PP	M	B	-
[A.24] Denegación de servicio	PP	M	B	-
[A.26] Ataque destructivo	MA	M	B	-

Tabla 8: Amenazas del activo **[E4] Sensores**

Amenaza	Prob.	[D]	[I]	[C]
[I.8] Fallo de servicios de comunicaciones	P	T	MA	A
[E.2] Errores del administrador del sistema / de la seguridad	MA	T	MA	A
[A.5] Suplantación de la identidad	PP	-	MA	A
[A.9] [Re-]encaminamiento de mensajes	PP	T	MA	A
[A.11] Acceso no autorizado	MR	T	MA	A
[A.12] Análisis de tráfico	P	B	B	A
[A.14] Interceptación de información (escucha)	PP	-	MA	A
[A.15] Modificación de la información	PP	B	MA	-
[A.24] Denegación de servicio	PP	T	MA	-

Tabla 9: Amenazas del activo **[C1] Conexion Internet**

Amenaza	Prob.	[D]	[I]	[C]
[E] Errores y fallos no intencionados	P	B	MA	A
[A.28] Indisponibilidad del personal	P	B	-	-
[A.29] Extorsión	MR	B	MA	A
[A.30] Ingeniería social (picaresca)	PP	B	MA	A

Tabla 10: Amenazas del activo **[SS1] Gestoria Fiscal y Financiera**

Amenaza	Prob.	[D]	[I]	[C]
[A.13] Repudio (negación de actuaciones)	MR	MA	-	-
[A.28] Indisponibilidad del personal	PP	MA	-	-
[A.31] Distracción	P	MA	MA	MA

Tabla 11: Amenazas del activo **[SS2] Consultoria (Profesores)**

Amenaza	Prob.	[D]	[I]	[C]
[A.13] Repudio (negación de actuaciones)	P	A	B	-
[A.19] Revelación de información	PP	B	-	B
[A.28] Indisponibilidad del personal	PP	A	-	-
[A.31] Distracción	MA	A	B	B

Tabla 12: Amenazas del activo **[SS3] Empresa de instalacion**

Amenaza	Prob.	[D]	[I]	[C]
[I.1] Fuego	PP	T	-	-
[I.2] Daños por agua	PP	MA	-	-
[I.*] Desastres industriales	MR	M	-	-
[A.6] Abuso de privilegios de acceso	P	M	MA	A
[A.7] Uso no previsto	MA	M	MA	A
[A.26] Ataque destructivo	MR	A	B	B
[A.27] Ocupación enemiga	MR	A	MA	A

Tabla 13: Amenazas del activo **[I1] Oficinas**

Amenaza	Prob.	[D]	[I]	[C]
[A.15] Modificación de la información	MR	B	MA	B
[A.18] Destrucción de la información	PP	A	-	-
[A.19] Revelación de información	PP	B	B	MA
[A.28] Indisponibilidad del personal	P	B	-	-
[A.29] Extorsión	MR	A	A	MA
[A.30] Ingeniería social (picaresca)	MR	A	A	MA

Tabla 14: Amenazas del activo **[T1] Jose Antonio Riaza**

Amenaza	Prob.	[D]	[I]	[C]
[A.15] Modificación de la información	MR	B	MA	B
[A.18] Destrucción de la información	PP	A	-	-
[A.19] Revelación de información	PP	B	B	MA
[A.28] Indisponibilidad del personal	P	B	-	-
[A.29] Extorsión	MR	A	A	MA
[A.30] Ingeniería social (picaresca)	MR	A	A	MA

Tabla 15: Amenazas del activo **[T2] Jose Roldan Gomez**

Amenaza	Prob.	[D]	[I]	[C]
[A.15] Modificación de la información	MR	B	MA	B
[A.18] Destrucción de la información	PP	A	-	-
[A.19] Revelación de información	PP	B	B	MA
[A.28] Indisponibilidad del personal	P	B	-	-
[A.29] Extorsión	MR	A	A	MA
[A.30] Ingeniería social (picaresca)	MR	A	A	MA

Tabla 16: Amenazas del activo **[T3] Cristian Cuerda Gonzalez**

Amenaza	Prob.	[D]	[I]	[C]
[A.15] Modificación de la información	MR	B	MA	B
[A.18] Destrucción de la información	PP	A	-	-
[A.19] Revelación de información	PP	B	B	MA
[A.28] Indisponibilidad del personal	P	B	-	-
[A.29] Extorsión	MR	A	A	MA
[A.30] Ingeniería social (picaresca)	MR	A	A	MA

Tabla 17: Amenazas del activo **[T4] Yuri**

4. Gestión del riesgo

4.1. Salvaguardas

Definición 3. Salvaguarda. *Una salvaguarda es una medida que se adquiere o implementa con el objetivo de reducir o eliminar el riesgo generado por una determinada amenaza.*

4.1.1. Salvaguardas generales

En esta categoría hemos incluido aquellas salvaguardas que PILAR propone a nivel general y que no se enfocan entorno a una categoría concreta en las que clasificamos nuestros activos. Podemos encontrar medidas enfocadas a la gestión de privilegios o al acceso a nuestros sistemas; protección básica de servicios como el correo electrónico, las aplicaciones web, el servidor DNS, servicios de Voz IP, los contratos de prestación de servicios; aspectos relacionados con la gestión de incidentes en la organización, como disponer de un registro de los incidentes, revisar y corregir estos incidentes, formar al personal para evitarlos en el futuro; y por ultimo aspectos relacionados con la continuidad del negocio, la organización interna de la empresa, el cuidado de las relaciones externas y medidas de seguridad a tener en cuenta a la hora de adquirir o desarrollar determinados tipos de activos nuevos.

Salvaguardas	R	Actual
[AC] Control de acceso lógico	7	L2
[AC.1] Gestión de privilegios	5	L2
[AC.2] Imposición del control de acceso	6	L2
[H.ST] Segregación de tareas	7	L2

Tabla 18: Salvaguardas de **[AC] Control de acceso lógico**

4.1.2. [SW] Protección de las Aplicaciones Informáticas (SW)

A nivel de proteger las aplicaciones software, vemos que PILAR ofrece salvaguardas que se enfocan en disponer de inventarios, normativas, manuales de instrucciones y en general toda la documentación posible asociada a las aplicaciones, además de realizar copias de seguridad y contar con protección frente a ataques malintencionados. Además hay que prestar atención al mantenimiento y actualizaciones de las aplicaciones, para evitar posibles fallos o incompatibilidades.

Salvaguardas	R	Actual
[S] Protección de los Servicios	3	L1
[S.1] Prestación de los servicios		L1
[S.1.1] Se dispone de normativa relativa al uso de los servicios		L1
[S.1.2] Se dispone de un inventario de servicios		L1
[S.cont] Aseguramiento de la disponibilidad		L1
[S.SC] Se aplican perfiles de seguridad		L1
[S.op] Explotación		L1
[S.CM] Gestión de cambios (mejoras y sustituciones)		L1
[S.end] Desmantelamiento		L1
[S.www] Protección de servicios y aplicaciones web		L1
[S.email] Protección del correo electrónico		L1
[S.1.a] Seguridad del comercio electrónico		L1
[S.dir] Protección del directorio		L1
[S.dns] Protección del servidor de nombres de dominio (DNS)		L1
[S.1.e] Prestación de servicios de infraestructura de clave pública (CSP)		L1
[S.voip] Voz sobre IP		L1
[S.2] Servicios subcontratados		L1
[S.2.1] Aspectos generales		L1
[S.2.2] Contratos de prestación de servicios		L1
[S.2.3] Operación		L1
[S.2.4] Gestión de cambios		L1
[S.2.5] Autenticación del servidor		L1
[S.2.6] Continuidad de operaciones		L1
[S.2.7] Desmantelamiento		L1
[S.3] Medios alternativos sujetos a mismas garantías de protección que habituales	3	L1

Tabla 19: Salvaguardas de **[S] Protección de los Servicios**

Salvaguardas	R	Actual
[IR] Gestión de incidentes	7	L2
[IR.1] Se dispone de normativa de actuación para la gestión de incidentes	2	L2
[IR.2] Se dispone de procedimientos para la gestión de incidentes	5	L2
[IR.3] Contención del incidente	7	L2
[IR.4] Gestión del incidente	4	L2
[IR.5] Cooperación con otras organizaciones	5	L2
[IR.6] Comunicación de los incidentes de seguridad	3	L2
[IR.7] Comunicación de las deficiencias de seguridad	2	L2
[IR.8] Comunicación de los fallos del software		L2
[IR.9] Se dispone de un registro de incidentes		L2
[IR.a] Los fallos y las medidas correctoras se registran y se revisan	3	L2
[IR.b] Control formal del proceso de recuperación ante el incidente	3	L2
[IR.c] Formación y concienciación	3	L2
[IR.d] Se aprende de los incidentes	3	L2
[IR.e] Se toman medidas para prevenir la repetición	4	L2

Tabla 20: Salvaguardas de **[IR] Gestión de incidentes**

Salvaguardas	R	Actual
[tools] Herramientas de seguridad	7	L3
[tools.AV] Herramienta contra código dañino		L3
[tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión	7	L3
[tools.conf] Herramienta de chequeo de configuración		L3
[tools.traffic] Herramienta de monitorización de tráfico	6	L3
[tools.DLP] DLP: Herramienta de monitorización de contenidos		L3
[tools.HP] Honey net / honey pot		L3
[tools.SFV] Verificación de las funciones de seguridad	6	L3

Tabla 21: Salvaguardas de **[tools] Herramientas de seguridad**

4.1.3. [HW] Protección de los Equipos Informáticos (HW)

Respecto a la protección de los equipos informáticos, PILAR nos ofrece unas salvaguardas similares al que ofrecia con las aplicaciones software, añadiendo algunas específicas como por ejemplo, la prevención de emanaciones electromagnéticas, el uso de máquinas virtuales, disponer de la normativa de uso del hardware, etc.

Salvaguardas	R	Actual
[V] Gestión de vulnerabilidades	6	L2
[V.1] Se dispone de personas dedicadas a la gestión de vulnerabilidades	3	L2
[V.2] Se han previsto mecanismos para estar informados de vulnerabilidades ...	4	L2
[tools.V] Herramienta de análisis de vulnerabilidades	6	L2
[V.4] Se analiza el impacto potencial (estimación de riesgos)	3	L2
[V.5] Pruebas de penetración	4	L2
[V.6] Se dispone de procedimientos de reacción	3	L2
[V.7] Reparación de las vulnerabilidades detectadas	5	L2

Tabla 22: Salvaguardas de **[V] Gestión de vulnerabilidades**

Salvaguardas	R	Actual
[BC] Continuidad del negocio	5	L2
[BC.1] Gestión de la continuidad	3	L2
[BC.BIA] Se ha realizado un análisis de impacto (BIA)	2	L2
[BC.3] Actividades preparatorias	3	L2
[BC.4] Reacción (gestión de crisis)	3	L2
[BC.DRP] Plan de Recuperación de Desastres (DRP)	5	L2
[BC.6] Restitución (retorno a condiciones normales de trabajo)	2	L2

Tabla 23: Salvaguardas de **[BC] Continuidad del negocio**

Salvaguardas	R	Actual
[G] Organización	5	L2
[G.1] Organización interna	3	L2
[G.2] Documentación técnica (componentes)	3	L2
[G.3] Documentación organizativa (normas y procedimientos)	3	L2
[G.4] Protección de datos de carácter personal (Documento de seguridad - LOPD)		L2
[RM] Gestión de riesgos	3	L2
[G.plan] Planificación de la seguridad	3	L2
[G.exam] Inspecciones de seguridad	5	L2
[G.8] Salvaguarda de los registros de la Organización (vital records)		L2

Tabla 24: Salvaguardas de **[G] Organización**

Salvaguardas	R	Actual
[E] Relaciones Externas	6	L2
[E.1] Acuerdos para intercambio de información y software	6	L2
[E.2] Acceso externo	5	L2

Tabla 25: Salvaguardas de **[E] Relaciones Externas**

Salvaguardas	R	Actual
[NEW] Adquisición / desarrollo	5	L2
[NEW.1] Gestión de proyectos	2	L2
[NEW.SW] Aplicaciones: Adquisición o desarrollo	4	L2
[NEW.HW] Equipos: Adquisición o desarrollo	4	L2
[NEW.COM] Comunicaciones: Adquisición o contratación	3	L2
[NEW.MP] Soportes de Información: Adquisición		L2
[NEW.C] Productos certificados o acreditados	5	L2

Tabla 26: Salvaguardas de **[NEW] Adquisición / desarrollo**

4.1.4. [COM] Protección de las Comunicaciones

A la hora de proteger las comunicaciones, PILAR propone distintas medidas de control sobre el acceso a la red que utiliza nuestra empresa, la autenticación, la protección de las redes WiFi, la encriptación de las comunicaciones, el uso de redes privadas, la segregación de nuestras redes en diferentes dominios con diferentes permisos de acceso, etcétera.

Salvaguardas	R	Actual
[SW] Protección de las Aplicaciones Informáticas (SW)	7	L2
[SW.1] Se dispone de un inventario de aplicaciones (SW)	3	L2
[SW.2] Se dispone de normativa relativa a las aplicaciones (SW)	2	L2
[SW.3] Se dispone de procedimientos de uso de las aplicaciones	2	L2
[SW.4] IPR: Se protegen los derechos de propiedad intelectual de las aplicaciones (SW)	3	L2
[SW.backup] Copias de seguridad (backup) (SW)	5	L2
[SW.start] Puesta en producción	3	L2
[SW.SC] Se aplican perfiles de seguridad	7	L2
[SW.op] Explotación / Producción	5	L2
[SW.CM] Cambios (actualizaciones y mantenimiento)	4	L2
[SW.end] Desmantelamiento	2	L2

Tabla 27: Salvaguardas de **1.2. [SW]Protección de las Aplicaciones Informáticas (SW)**

Salvaguardas	R	Actual
[HW] Protección de los Equipos Informáticos (HW)	7	L2
[HW.1] Se dispone de un inventario de equipos (HW)	2	L2
[HW.2] Se dispone de normativa sobre el uso correcto de los equipos	2	L2
[HW.3] Se dispone de procedimientos de uso del equipamiento	2	L2
[HW.start] Puesta en producción	4	L2
[HW.SC] Se aplican perfiles de seguridad	7	L2
[HW.cont] Aseguramiento de la disponibilidad	6	L2
[HW.7] Medios alternativos sujetos a mismas garantías de protección que habituales	3	L2
[HW.8] Contenedores criptográficos (HW, HW virtual)	6	L2
[HW.9] xor Prevención de emanaciones electromagnéticas (TEMPEST equipment)		L2
[HW.a] Instalación	3	L2
[HW.op] Operación	5	L2
[HW.CM] Cambios (actualizaciones y mantenimiento)	4	L2
[HW.end] Desmantelamiento	3	L2
[HW.f] Maquinas virtuales		L2
[HW.i] Voz, facsímil y video	3	L2

Tabla 28: Salvaguardas de **1.3. [HW]Protección de los Equipos Informáticos (HW)**

Salvaguardas	R	Actual
[COM] Protección de las Comunicaciones	9	L2
[COM.1] Se dispone de un inventario de servicios de comunicación	2	L2
[COM.2] Se dispone de normativa sobre el uso correcto de las comunicaciones	3	L2
[COM.3] Se dispone de procedimientos de uso de las comunicaciones	3	L2
[COM.start] Entrada en servicio	4	L2
[COM.SC] Se aplican perfiles de seguridad	9	L2
[COM.cont] Aseguramiento de la disponibilidad	6	L2
[COM.7] Medios alternativos sujetos a mismas garantías de protección que habituales	3	L2
[COM.aut] Autenticación del canal	5	L2
[COM.I] xor Protección de la integridad de los datos intercambiados	6	L2
[COM.a] Se toman medidas frente a la inyección de información espuria	7	L2
[COM.C] Protección criptográfica de la confidencialidad de los datos intercambiados	5	L2
[COM.op] Operación	5	L2
[COM.CM] Cambios (actualizaciones y mantenimiento)	5	L2
[COM.end] Desmantelamiento	3	L2
[COM.wifi] Seguridad Wireless (WiFi)		L2
[COM.mobile] Telefonía móvil		L2
[COM.DS] Segregación de las redes en dominios		L2
[COM.i] Redes privadas virtuales		L2

Tabla 29: Salvaguardas de **1.4. [COM]Protección de las Comunicaciones**

4.1.5. [AUX] Elementos Auxiliares

Respecto a los elementos auxiliares, PILAR realiza un enfoque principal en la protección frente a inclemencias climáticas, posibles cortes de la red eléctrica, subidas de tensión, medidas de protección frente a robos o a ataques destructivos, así como seguimiento de los protocolos de instalación y mantenimiento

recomendados por los fabricantes.

Salvaguardas	R	Actual
[AUX] Elementos Auxiliares	6	L2
[AUX.1] Se dispone de un inventario de equipamiento auxiliar	3	L2
[AUX.cont] Aseguramiento de la disponibilidad		L2
[AUX.start] Instalación		L2
[AUX.power] Suministro eléctrico	5	L2
[AUX.AC] Climatización	5	L2
[AUX.wires] Protección del cableado	6	L2
[AUX.7] Se disponen medidas frente a posibles robos		L2
[AUX.8] Se prevén medidas frente a todos los problemas graves identificados en el análisis de riesgos		L2

Tabla 30: Salvaguardas de **1.5. [AUX]Elementos Auxiliares**

4.1.6. [L] Protección de las Instalaciones

En esta categoría en concreto, PILAR diferencia entre la protección de las instalaciones físicas y el de su perímetro. En el caso del perímetro, PILAR no observa un posible riesgo sobre nuestros activos, algo que consideramos erróneo, puesto que gran parte de nuestros activos se encuentran en nuestras oficinas (servidores, información, personal, etc) y consideramos que es fundamental la defensa del mismo. Por eso, a pesar de que PILAR no aplica salvaguardas en este ámbito, nosotros hemos considerado importante asignarle un buen nivel de madurez objetivo. En reglas generales, se habla de la protección de las instalaciones frente a desastres naturales, reglas de diseño, protección de puertas y ventanas, uso de muros exteriores, etc.

Salvaguardas	R	Actual
[L] Protección de las Instalaciones	7	L2
[L.1] Se dispone de normativa de seguridad	2	L2
[L.2] Se dispone de un inventario de instalaciones	5	L2
[L.3] Entrada en servicio	5	L2
[L.design] Diseño	5	L2
[L.5] xor Existe protección frente a emanaciones (TEMPEST facility zoning)		L2
[L.6] Protección frente a desastres	7	L2
[L.cont] Continuidad de operaciones	5	L2
[L.end] Desmantelamiento	3	L2

Tabla 31: Salvaguardas de **1.6. [L]Protección de las Instalaciones**

4.1.7. [PS] Gestión del Personal

En la categoría de personal, PILAR propone una serie de normativas a seguir a la hora de contratar a nuevo personal, formarlo, cambiar su puesto de trabajo, la relación que se tiene que tener con el personal, proteger a los trabajadores frente a posibles coacciones y por otro lado, también habla de la necesidad de proporcionar una normativa sobre seguridad al personal para que la estudien y la cumplan adecuadamente.

Salvaguardas	R	Actual
[PPS] Protección del perímetro físico		L3
[L.depth] Defensa en profundidad		L3
[PPS.2] Diseño		L3
[PPS.3] Puertas		L3
[PPS.4] Ventanas		L3
[PPS.5] Barrotes o rejas		L3
[PPS.6] Muros exteriores		L3
[PPS.7] Entradas exteriores		L3
[PPS.8] Control de llaves, combinaciones o dispositivos de seguridad		L3
[L.IA] xor Mecanismo de autenticación		L3
[L.AC] Control de los accesos físicos		L3
[PPS.b] Se dispone de un sistema de detección de intrusión perimetral		L3
[PPS.c] Se dispone de cámaras de vídeo de vigilancia (CCTV)		L3
[PPS.d] Personal concienciado en detección y reacción frente actividades sospechosas en las cercanías		L3
[PPS.e] Iluminación de seguridad		L3
[PPS.f] Vigilancia		L3
[PPS.g] La seguridad de la instalación no es responsabilidad de un único guarda		L3
[PPS.h] Registros de eventos		L3

Tabla 32: Salvaguardas de **[PPS] Protección del perímetro físico**

Salvaguardas	R	Actual
[PS] Gestión del Personal	6	L2
[PS.1] Se dispone de normativa relativa a la gestión de personal (en materia de seguridad)	3	L2
[PS.2] Se dispone de procedimientos para la gestión de personal (en materia de seguridad)	3	L2
[PS.3] Relación de personal	3	L2
[PS.4] Puestos de trabajo	3	L2
[PS.5] Contratación	5	L2
[PS.6] Cambio de puesto de trabajo	3	L2
[PS.AT] Formación y concienciación	3	L2
[PS.8] Procedimientos de prevención y reacción	6	L2
[PS.9] Protección del usuario frente a coacciones	5	L2
[PS.cont] Aseguramiento de la disponibilidad	4	L2

Tabla 33: Salvaguardas de **1.7. [PS]Gestión del Personal**

5. Conclusiones

5.1. Valor activo

Como podemos observar en la Figura 3, desde el punto de vista de la confidencialidad, el activo con mayor impacto negativo de ser vulnerado somos nosotros. Esto se debe a que mientras que el resto de activos actuales están orientados a este proyecto (proyecto que es bastante trasparente porque no nos preocupa que se conozcan los detalles), nosotros podemos tener información de futuros planes. Esta información es más sensible para la organización. Por esta razón, los siguientes activos con impactos de confidencialidad altos son la gestoría, nuestros ordenadores, y la conexión a internet que podemos usar para comunicarnos.

En cuanto a la disponibilidad se refiere, nosotros somos fácilmente sustituibles, sin embargo es bastante crítico que tengamos hardware y software disponible para trabajar y mantener el sistema.

En la parte de integridad, puede parecer extraño que estimemos un impacto tan bajo para nosotros como activo, esto es así porque suponemos auditorias de cuentas de nuestra gestoría fiscal (sólo sería problemático si todos fuéramos corruptos) y, si alguien no tuviese integridad, podría corregirse rápido porque nuestra gestora sirve como intermediaria en nuestros trámites.

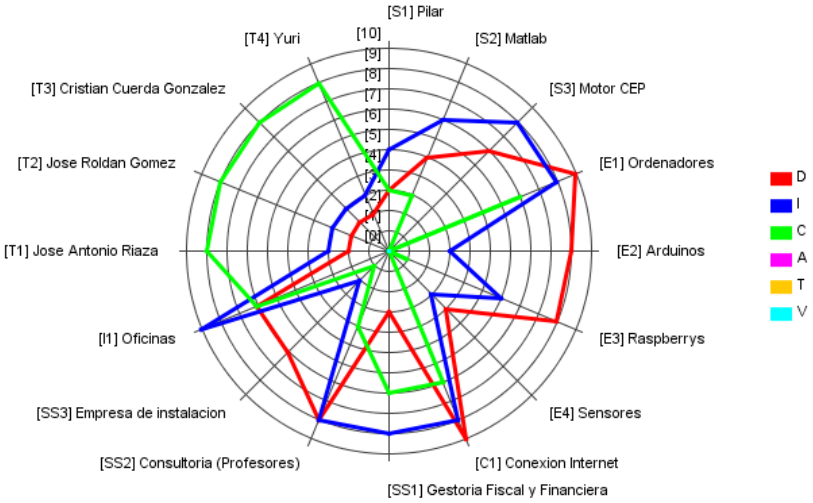

Figura 3: Gráfica del Valor activo generada por *PILAR*

5.2. Impacto acumulado

En la Figura 4 se muestra el gráfico de impacto acumulado, que es más claro que el anterior, ya que nos muestra el impacto acumulado de cada activo en función de nuestra situación actual (rojo), suponiendo que implementamos solo las salvaguardas que recomienda PILAR (verde), y suponiendo que implementamos todas las medidas que nosotros consideramos (azul).

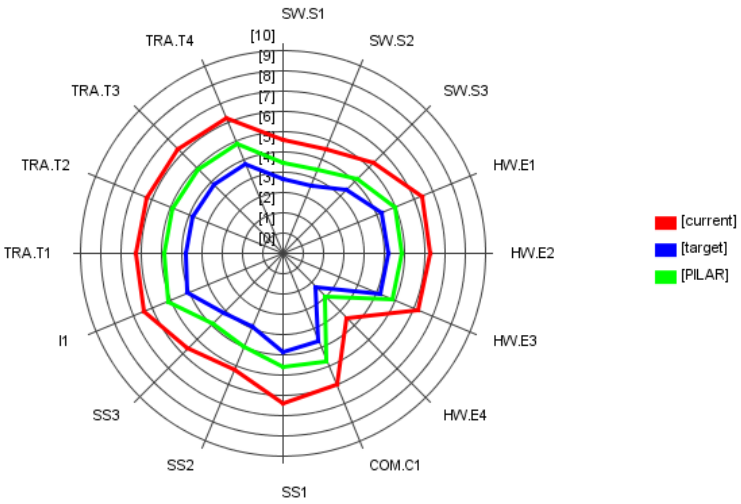

Figura 4: Gráfica del Impacto acumulado generada por *PILAR*

Es un gráfico muy útil de cara a conocer qué activos son más críticos, aunque no tiene en cuenta la probabilidad de que la amenazas ocurran.

5.3. Riesgo acumulado

En la Figura 5 se muestra el riesgo acumulado. Este gráfico tiene la particularidad de combinar el impacto con la probabilidad de que ocurran las amenazas, por eso es extremadamente útil para identificar que activos presentan un riesgo real. En este caso los arduinos presentan un riesgo muy importante porque son fácilmente accesibles por terceros.

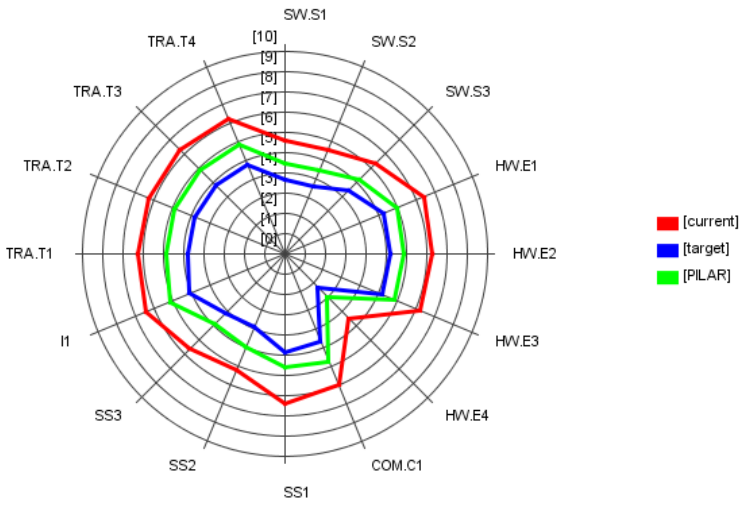

Figura 5: Gráfica del Riesgo acumulado generada por *PILAR*

Las instalaciones son críticas porque consideramos que los servidores y nuestros ordenadores están dentro. Por otra parte la conexión a internet es sensible también porque todo nuestro modelo de negocio se basa en el correcto funcionamiento de la misma.

5.4. Salvaguardas de protección

En la Figure 6 se muestran las salvaguardas de protección. Este gráfico muestra el estado de las salvaguardas por tipo, así como nuestro objetivo y el recomendado por pilar.

En nuestro caso creemos que todos los tipos de salvaguardas deben de tenerse en cuenta y mejorarse, aunque pilar no ve necesario aumentar salvaguardas de disuasión.

Nuestro estado actual deja bastante que desear en todos los tipos de salvaguardas, pero el objetivo es mejorar.

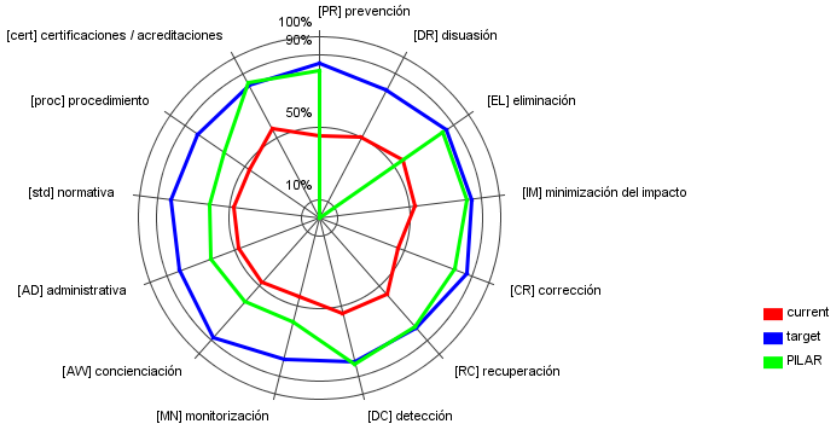

Figura 6: Gráfica de las Salvaguardas de protección generada por *PILAR*

Referencias

[1] James Zhou. ISO 27001 Information Security Management. `http://enewsletter.ntu.edu.sg/itconnect/2011-03/Pages/ISO27001-ISM.aspx`, Marzo 2011.

[2] PILAR. Herramientas para el anásis de riesgos. `http://www.pilar-tools.com`, Diciembre 2017.

[3] Ministerio de Administraciones Públicas. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. `http://publicaciones.administracion.es`, Octubre 2012.

[4] Ministerio de Administraciones Públicas. MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II - Catálogo de Elementos. `http://publicaciones.administracion.es`, Junio 2006.