Trabajo Final de Máster

Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 para empresa de apuestas deportivas online

Universitat Oberta de Catalunya

Máster Universitario en Seguridad de las TIC - MISTIC

Adrián Capdevila Dueñas

Resumen del trabajo

El presente trabajo aborda la adecuación de una organización a la norma ISO-IEC 27001:2013, la norma de seguridad de la información más extendida e implantada mundialmente.

Para ello, tras presentar la empresa, sus líneas de negocio y sus servicios TI, se analizará el estado de seguridad de la misma haciendo un primer análisis diferencial de su nivel de cumplimiento de la norma.

Posteriormente se definirá el esquema documental que la empresa debería desarrollar para cubrir todos los apartados de la norma, incluyendo políticas, normativas, procedimientos y registros.

La siguiente fase constará en un análisis de riesgos formal utilizando la metodología MAGERIT V3, apoyado en la herramienta PILAR.

A continuación se establecerá el plan de tratamiento de riesgos, el cual dará como resultado una serie de proyectos o tareas enfocados a minimizar los riesgos detectados durante el análisis y mejorar el nivel de cumplimiento de la norma.

La última fase de la adecuación consistirá en una auditoría de cumplimiento en la que se analizarán tanto los puntos de la norma como los controles del Anexo A.

Summary

This paper explains the adequation of an organization to the standard ISO-IEC 27001:2013, the worldwide most implemented information security standard.

After explaining the company, its business cases and the IT services, the IT security will be analyzed by a GAP analysis.

Subsequently, the mandatory documentation will be created, including policies, rules, procedures and records.

The next phase will consist in a formal risk assessment using the MAGERIT V3 methodology, implemented with the tool “PILAR”.

After that, the plan to reduce the risks will be established, which will contain projects to minimize the risks of the analysis and to improve the level of compliance with the standard.

The last phase will consist in a compliance audit where the standard and the controls from “Annex A” will be analyzed.

Índice

Resumen del trabajo....2

1 Introducción....5

1.1 Objetivo y justificación....5

1.2 Planificación del trabajo....5

1.3 Organización de la memoria....5

1.4 Definiciones....6

1.5 Acerca de las normas ISO 27001 / ISO 27002....8

1.6 Contexto: organización objeto del plan....9

1.7 Conclusiones....9

2 Acerca de Divertiapuesta y estado inicial....10

2.1 Motivación de la adecuación y alcance del SGSI....13

3 Objetivos de seguridad de la información....13

4 Análisis diferencial contra ISO 27001....14

5 Esquema documental....16

6 Análisis de riesgos....17

6.1 Identificación de activos y dependencias....17

6.2 Valoración de activos y dimensiones....23

6.3 Identificación y valoración de amenazas....26

6.4 Riesgo potencial....31

5 Declaración de aplicabilidad....35

7 Plan de tratamiento del riesgo....36

7.1 Proyecto 1 - Definir la política y normativas de seguridad de la organización....37

7.2 Proyecto 2 - Formalizar el proceso de acceso a la información, inventariarla y clasificarla....39

7.3 Proyecto 3 - Planificación, documentación y control de tareas periódicas....41

7.4 Proyecto 4 - Implantar un control de cambios gestionado.....44
7.5 Proyecto 5 - Cifrado de la información sensible.....46
7.6 Proyecto 6 – Aproximación a la continuidad de negocio.....48
7.7 Planificación.....50
7.8 Análisis del nivel de riesgo residual.....51
8 Auditoría de cumplimiento.....52
9 Anexo I – Listado de documentación adjunta.....53
10 Bibliografía.....54

1 Introducción

El presente apartado es una introducción a la creación y organización del Trabajo Fin de Master (en adelante *"TFM"*), mientras que el resto del documento contendrá la adecuación obviando que se trata de un documento académico.

1.1 Objetivo y justificación

El presente TFM muestra los pasos a seguir por una organización para adecuarse a la norma ISO 27001. Así pues, **su objetivo es** mostrar con un caso práctico los pasos que debe seguir cualquier organización de similares características para conseguir la adecuación y posible certificación, así como ofrecer ideas y ejemplos de como abordar cada una de las fases.

La justificación del TFM es ofrecer a aquellas organizaciones o profesionales que lo necesiten, un modelo de proyecto y documentación que puedan utilizar en procesos de adecuación a la norma o de mejora de la seguridad de la información.

1.2 Planificación del trabajo

La elaboración del TFM ha llevado cerca de tres meses naturales, habiéndose planificado con entregas generalmente cada 15 días, de modo que con cada entrega los diferentes documentos han ido creciendo y mejorando en un proceso evolutivo.

1.3 Organización de la memoria

Esta memoria se encuentra organizada en tres grandes bloques:

- **Apartado de introducción:** este apartado, junto a la conclusión, es el único que hace referencia al documento académico como un TFM, siendo el resto del documento y anexos perfectamente trasladables a un entorno real.
- **Conclusiones:** recoge las conclusiones finales del TFM.
- **Cuerpo del documento (apartados del 2 al 9):** explica el desarrollo del proyecto de adecuación desde el punto de vista de la empresa. Puede considerarse una bitácora del trabajo que cualquier organización debería seguir para la adecuación.
- **Documentos anexos:** se han extraído de esta bitácora aquellos documentos generados que deberían pasar a formar parte como tal del SGSI de DivertiApuesta. También se incluyen documentos de trabajo como hojas de cálculo, presentaciones o el fichero de análisis de riesgos de la herramienta PILAR.

1.4 Definiciones

- **Análisis de riesgos:** también abreviado como “AR”. Metodología sistemática que permite evaluar los riesgos para la seguridad de la información de la organización analizada. Se contemplan todos los activos del sistema de información, las posibles amenazas (tecnológicas o no), y se calculan los niveles de riesgo pertinentes.
- **Ciclo de Deming:** también abreviado como “PDCA”. Se trata de un modelo de mejora continua de procesos que se aplica ampliamente en implantaciones de la norma ISO 27001 y otros sistemas de gestión. Consta de 4 fases que en inglés dan origen a las siglas PDCA; Plan, Do, Check y Act. Consiste en abordar la mejora continua con una primera fase de planificación y diseño, se continúa con la implementación y operación del SGSI, se hacen revisiones (checks) periódicas y continuas, y se actúa mejorando el sistema.
- **CEO, CIO y CISO:** son siglas utilizadas en el ámbito de los sistemas de información para referirse a diferentes roles. El CEO acostumbra a ser el máximo responsable de la organización o a ocupar un puesto ejecutivo en la dirección. El CIO es el encargado de que el sistema de información funcione correctamente, y el CISO es el encargado de proteger los sistemas de información y por consiguiente los procesos de negocio.
- **Centro de proceso de datos:** también conocido como CPD. Es la sala o recinto donde se ubican los servidores y equipos de comunicaciones. Acostumbra a tener requisitos especiales en cuanto a climatización, protecciones industriales y control de acceso.
- **Declaración de aplicabilidad:** también abreviado como “SOA”. Documento del SGSI donde se seleccionan aquellos controles que la organización decide implantar. Este documento es aprobado por la alta dirección e incluye tanto los requisitos de la norma como cualquier otro que se haya identificado, como pueden ser legislación aplicable o requisitos de certificaciones ajenas a ISO27001.
- **DMZ:** también conocida como zona desmilitarizada, se trata de un segmento de la red de las organizaciones donde se ubican aquellos servidores más expuestos a Internet. Se trata pues de un potencial objetivo de ataques, pero es necesaria, por lo que están especialmente monitorizadas y sus equipos disponen de mayores medidas de seguridad.
- **ISO 27001**: norma internacional que define los requisitos de un Sistema de Gestión de Seguridad de la Información. Consta de una primera parte organizativa que detalla los como crear un SGSI a alto nivel, y de un anexo más operativo donde se indican qué controles de seguridad deberían implantarse.

- **ISO 27002**: norma internacional con propuestas para la implantación de controles de seguridad de la información. Generalmente se utiliza como complemento del anexo de la norma ISO 27001, o como checklist para organizaciones con poca cultura de seguridad que quieren empezar por pequeñas tareas sin abordar un SGSI completo.
- **Plan de continuidad de negocio:** también abreviado como PCN, es un plan a ejecutar ante eventos que afecten de forma significativa a la operativa del sistema de información. Debe contener instrucciones claras y concisas sobre qué hacer según diferentes casuísticas, con el fin de reducir al mínimo el impacto de una incidencia grabe sobre los servicios críticos, ya sea de origen natural, una avería, o incluso la indisponibilidad de las oficinas.
- **PILAR**: herramienta para la realización de análisis de riesgos en el ámbito de la seguridad de la información. Es de las más extendidas a nivel nacional y permite evaluar tanto el cumplimiento de la ISO27001, como del Esquema Nacional de Seguridad o el reciente Reglamento Europeo de Protección de Datos.
- **Sistema de alimentación in interrumpida:** también conocido como SAI. Se trata de un conjunto de baterías conectadas generalmente a los servidores para protegerlos de subidas y bajadas repentinas de electricidad. Si bien los hay de diferentes tamaños, su finalidad es poder hacer un apagado controlado de equipos en caso de fallo de la acometida habitual, o dar margen de maniobra hasta que entre en funcionamiento el grupo electrógeno, si existiera.
- **Sistema de Gestión de Seguridad de la Información:** también abreviado como “SGSI”. Conjunto de prácticas, procedimientos y normativas creados para implantar, evaluar y mejorar las mejores prácticas en seguridad de la información. Se trata de un proceso evolutivo que no solo implanta controles de seguridad, sino que analiza las necesidades en conjunto, encuentra los mejores controles a aplicar y los evalúa periódicamente para mejorar los niveles de seguridad.
- **Sistema de información:** también abreviado como “SI”. Conjunto de activos que intervienen en el tratamiento de la información. Contiene desde servidores, ordenadores, impresoras, hasta información en papel.
- **VPN:** conexión segura que permite a dispositivos conectados a Internet, conectarse a la red interna de una organización sin estar físicamente allí.

1.5 Acerca de las normas ISO 27001 / ISO 27002

Las normas ISO 27001 e ISO 27002 forman parte de la serie ISO 27000, orientada a la seguridad de los sistemas de información.

Contiene multitud de documentos que tratan temas asociados a la ciberseguridad, como la definición de métricas para la seguridad de la información (ISO 27004), la gestión de los riesgos (ISO 27005) o guías de gobierno de la seguridad de la información (ISO 27014). No obstante, son las normas 27001 y 27002 las más extendidas y utilizadas.

Para comprender la importancia y relevancia de estas dos normas, debemos remontarnos al año 1995 cuando se publicó el *standar* BS7799-1. Este documento contenía una serie de recomendaciones de seguridad para los sistemas de información, así como recomendaciones y sugerencias para su implantación en organizaciones de distinta índole. Dichas recomendaciones, recopilaban no solo medidas técnicas como la segmentación de redes, o la protección contra *malware*, sino que incluían medidas organizativas como pueden ser la segregación de tareas, la recomendación de establecer políticas de seguridad, o controlar la gestión de cambios en los sistemas.

Ante la ausencia de documentación previa tan completa, dicho documento se convirtió rápidamente en la hoja de ruta de muchas organizaciones que querían proteger sus sistemas, y en el año 2000 fue adaptado por ISO e IEC dando como resultado la norma ISO/IEC 17799.

Con el paso del tiempo, la gestión de la seguridad maduró, y las recomendaciones de la ISO 17799 no conseguían abarcar la seguridad de la información como un proceso global, por lo que reutilizando parte de la BS 7799, en 2005 nació la norma ISO 27001, la cual definía como debía ser un Sistema de Gestión de Seguridad de la Información, e incorporaba en forma de anexo las recomendaciones de la ISO 17799 que pasó a llamarse ISO 27002.

En 2013, ambas normas sufrieron una revisión profunda para facilitar su implementación junto a otros sistemas de gestión (como ISO 9000 e ISO 20000), siendo hasta la fecha las últimas versiones de la norma.

Aunque puedan parecer muy similares, son dos normas independientes que se complementan:

- **ISO 27001 define como gestionar la seguridad de la información**, obligando a planificar la seguridad a alto nivel, a implantar un modelo de seguridad que realmente se alinee con los objetivos del negocio, a medir la evolución de la seguridad de la información (y no solo de las medidas de seguridad), a analizar y gestionar los riesgos y en general a mejorar la seguridad de forma continua.

- **ISO 27002 ofrece propuestas de cómo implantar las medidas de seguridad** que la ISO 27001 requiere. Por ejemplo, ISO 27001 indica que se deberán establecer medidas contra el *malware*, pero no especifica cómo, mientras que en ISO 27002

pueden encontrarse diferentes modos y sugerencias de cómo implantar estas medidas.

Así pues, ISO 27001 puede implantarse sin basarse en ISO 27002, e ISO 27002 puede utilizarse sin la 27001 a modo de *checklist* de controles de seguridad que cualquier organización que desee mejorar su seguridad, puede implantar.

Por último cabe destacar que de forma general ninguna de las dos son de obligado cumplimiento, aunque existen sectores, proveedores u organizaciones que pueden exigir a las organizaciones el cumplimiento de alguna de estas dos normas. Para ello, ISO 27001 puede ser certificada oficialmente por una organización acreditada, mientras que tal certificación no existe para ISO 27002 ni el resto de la serie 27000.

1.6 Contexto: organización objeto del plan

Para el presente TFM se ha decidido utilizar una empresa ficticia a la que se ha llamado “DivertiApuesta”, cuya línea principal de negocio serán las apuestas deportivas online.

La elección de una empresa ficticia se debe a que por dedicarme a la campo de cumplimiento normativo en ciberseguridad, todas las empresas con las que colaboro ya disponen de un SGSI certificado, y por motivos de confidencialidad no podría utilizar un cliente en proceso de adecuación aunque ocultase sus datos.

No obstante, lejos de poder ser un inconveniente, considero que la elección de una empresa de apuestas deportivas online puede resultar muy enriquecedora ya que dispone de ciertos requisitos de seguridad que la hacen particular, tanto por el nivel de integridad que requieren sus datos y transacciones, como por ser un potencial objetivo de posibles atacantes, tanto internos como externos.

Además, por motivos laborales he participado proyectos de seguridad con empresas con requisitos de seguridad similares, por lo que, a pesar de no poder ofrecer datos reales, conozco la casuística a la que se enfrentan, así como la estructura que acostumbran a utilizar en sus sistemas.

1.7 Conclusiones

Desde el punto de vista académico, el TFM ha resultado muy interesante, ya que el planteamiento del proyecto es relativamente diferente a lo que vengo estando acostumbrado por trabajo. He jugado un triple rol como implantador, empresa que implanta el SGSI y como auditor externo, lo que me ha aportado diferentes puntos de vista de un mismo SGSI, que rara vez sucede en el mundo real. Además, algunos detalles como la estructura del SOA, algunas de las presentaciones finales, o la valoración de los riesgos directamente con las salvaguardas implantadas, han sido nuevos para mi, con el consiguiente aporte de conocimientos.

Desde el punto de vista de la implantación del SGSI en DivertiApuesta, a pesar de ser un caso ficticio, queda patente la importante mejora de la seguridad entre el inicio y el final

del proyecto, así como las ventajas que la nueva estructura y cultura de ciberseguridad creada, harían mejorar a la organización con cada iteración del ciclo de mejora continua.

Lejos de ser una moda, queda patente que la implantación de un SGSI es hoy por hoy el mejor modo de abordar la mejora de la ciberseguridad en una organización, ya sea mediante la norma ISO 27001, el Esquema Nacional de Seguridad, o cualquier otro referente contrastado.

2 Acerca de Divertiapuesta y estado inicial

DivertiApuesta es una empresa de 45 empleados cuya principal línea de negocio es permitir a sus usuarios hacer apuestas deportivas tanto online como desde terminales físicos en bares y salas de juego.

Dado que DivertiApuesta lleva algunos años en el sector, son muy conscientes de la importancia de la seguridad de la información y de la criticidad de la misma en su negocio, por lo que cuenta con **personal técnico muy competente**, aunque ligeramente desorganizado en cuanto a lo que a seguridad se refiere.

A continuación se incluye un esquema de los diferentes departamentos así como de los principales roles en cuanto a la seguridad de la información:

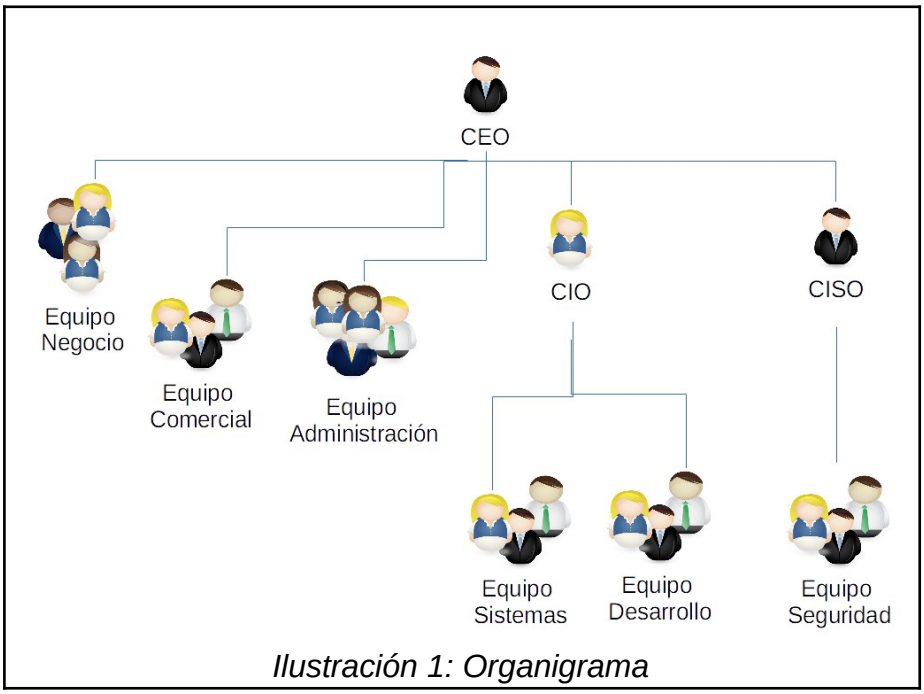


Ilustración 1: Organigrama

Como se puede apreciar, DivertiApuesta cuenta con los siguientes departamentos:

- **Un área de administración** formada por 4 personas que se encarga de la gestión económica, finanzas y recursos humanos, a la que se refieren como “Administración”
- **Un área de sistemas** formada por 8 empleados, entre los que se encuentra el CIO. Este área gestiona tanto los servidores como el parque de equipos de usuario.
- **Un equipo de desarrollo** formado por 15 empleados que se encargan de mantener y evolucionar la plataforma de apuestas.
- **Un equipo comercial** de 10 empleados que se encargan del marketing, gestión de la web corporativa, captación de nuevos locales para ubicar los terminales, y de buscar patrocinios con terceras empresas.
- **Un equipo de negocio** de 6 personas, entre quienes se encuentra el CEO, que definen las estrategias de las apuestas, las promociones, la cuantía de los premios y las comisiones.
- Un reciente **equipo de seguridad** formado por 2 personas, una de ellas está empezando a ejercer de CISO. Se encargan actualmente de pruebas de *pentest*, análisis de código, detección de intrusos y del reciente procedimiento de gestión de incidentes de seguridad de la información.

La única sede está en un parque empresarial y disponen de un edificio propio donde tienen tanto las oficinas centrales como el CPD. Dicho edificio cuenta con control de accesos general con tarjeta RFID más *PIN*, y el CPD dispone de las medidas de protección habituales: aire acondicionado redundante, SAI, suelo técnico, una sola acometida eléctrica que compensan con un grupo electrógeno, y lineas de comunicaciones con el exterior redundadas.

En cuanto a la **plataforma TI**, tanto los servidores que prestan servicio, los puestos de usuario y la electrónica de red son relativamente nuevos, disponen de mantenimiento y están adecuadamente dimensionados, aunque no existe un control formal sobre la gestión de los mismos, ya que se considera que todo el personal es competente y que velará por la protección de los mismos.

A grandes rasgos, la infraestructura es la siguiente:

- Una gran base de datos donde se almacenan todos los datos de usuarios y apuestas deportivas
- Dos servidores WEB en DMZ que recogen los datos de los usuarios que apuestan online
- Un servidor que recibe las peticiones de los terminales físicos mediante VPN y los vuelca en la base de datos principal
- 4 servidores de desarrollo para los 4 servidores anteriormente mencionados

- Un servidor de VPN y correo electrónico
- Un servidor de gestión general para la documentación, sistema de *ticketing* y aplicaciones del departamento de administración
- Un robot de copias de seguridad
- Un cortafuegos externo que protege la organización de Internet y a la DMZ a la vez que balancea entre las 2 conexiones con el exterior.
- Un cortafuegos interno que separa a los usuarios, de los servidores internos de gestión y a los servidores críticos.

Se adjunta el diagrama de red:

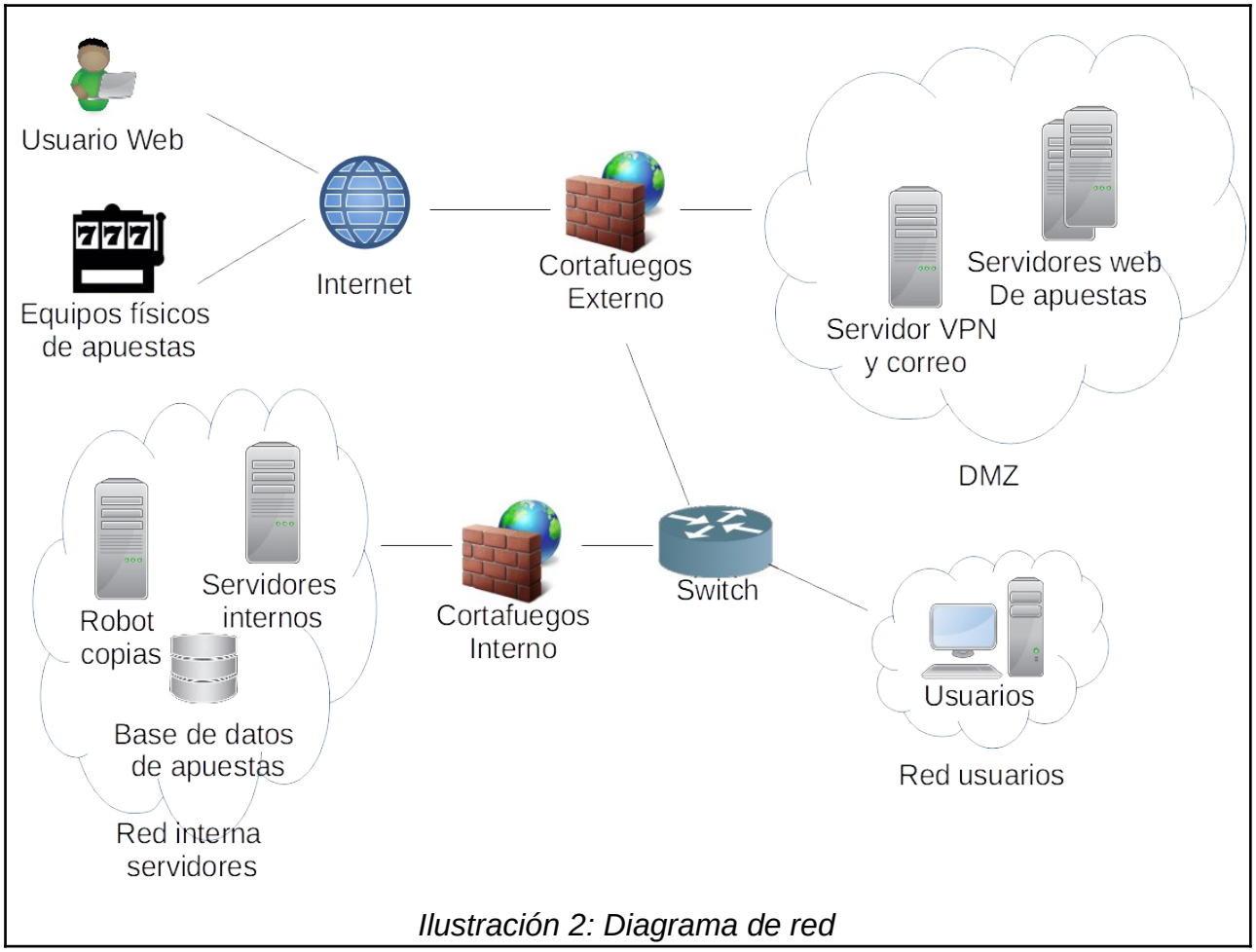


Ilustración 2: Diagrama de red

2.1 Motivación de la adecuación y alcance del SGSI

Debido a la criticidad que la seguridad de la información tiene para el negocio, DivertiApuesta dedica grandes esfuerzos a asegurar sus sistemas de información.

Para ello cuentan con un equipo de sistemas muy competente que vela por la correcta configuración de los dispositivos y servidores, además del reciente equipo de seguridad, que de momento centra la mayoría de su dedicación a tareas de detección y prevención de ataques informáticos.

No obstante, a medida que la empresa y la plataforma han crecido, el responsable de sistemas ha detectado que el número de incidentes debidos a errores humanos ha aumentado considerablemente, ya que no disponen de una gestión robusta más allá del seguimiento que se pueda hacer de las diferentes tareas mediante el sistema de ticketing.

Esta situación le fue trasladada al CEO, el cual, conocedor de la necesidad de mejorar la gestión interna y preocupado por la reciente cantidad de noticias que aparecen en los medios sobre ciberataques, **ha decidido implantar un SGSI basado en la norma ISO 27001.**

Igualmente, el CEO ha manifestado que una vez esté completada la adecuación, querrá **certificar** a la organización ya que le dará una ventaja competitiva con respecto al resto de empresas del sector, además de generar confianza en clientes y posibles patrocinadores.

Para poder empezar por un alcance abarcable, se ha decidido que en una primera fase el **alcance del SGSI** se limitará al "*Sistema de apuestas deportivas WEB*".

Una vez implantado el SGSI, en futuras revisiones del mismo, probablemente se ampliará el alcance, aunque inicialmente se ha dejado fuera los terminales físicos de apuestas y los servicios de administración de la empresa.

3 Objetivos de seguridad de la información

El principal objetivo del plan **es formalizar y mejorar la gestión interna de la seguridad de la información,** de manera que se mejore el nivel de seguridad general de la organización a la vez que se dispondrá de herramientas para medir, tanto la seguridad, como su evolución.

Adicionalmente, se ha planteado certificar el SGSI con el objetivo de **generar confianza en sus usuarios y futuros socios**, a la vez que conseguirá un **elemento diferencial que mejorará su competitividad frente a la competencia**.

De estas actuaciones es espera que se cumplan los siguientes objetivos específicos:

- Reducir en, al menos, un 5% los cortes de servicio relacionados con la ciberseguridad.
- Optimizar la gestión de la seguridad de forma que se reduzca un 10% la cantidad de horas dedicadas a las actuales tareas de seguridad (no se contabilizarán las nuevas que surjan con motivo de la adecuación).

- Reducir a 5 días el tiempo máximo de corrección de vulnerabilidades desde su publicación.

4 Análisis diferencial contra ISO 27001

Como paso previo a la implantación del SGSI, se ha hecho un análisis diferencial del cumplimiento de la norma ISO 27001 y de su "Anexo A" de medidas de seguridad.

Para ello, se ha recopilado información tanto técnica como organizativa de DivertiApuesta, la cual se ha contrastado uno a uno con cada punto de la norma.

Para evaluar el nivel de cumplimiento de forma objetiva, se ha utilizado el modelo de madurez CMMI, el cual establece los siguientes 5 niveles de madurez para la implantación de controles:

- **Nivel 0, o L0:** control inexistente.
- **Nivel 1, o L1:** control en fases iniciales de implantación.
- **Nivel 2, o L2:** se cumple con el control aunque de manera informal, pero repetible
- **Nivel 3, o L3:** el control se encuentra implantado y documentados
- **Nivel 4, o L4:** el control, además de estar implantado y documentado, se gestiona formalmente y se puede medir
- **Nivel 5, o L5:** el control, además de cumplir con L4, ha estado sometido a mejora continua y se encuentra optimizado.

A continuación se muestra el resumen de cumplimiento de los diferentes apartados de la norma. Puede consultarse el análisis completo en el documento anexo "*Anexo I - Detalle del análisis diferencial*":

N.º	Apartado	Estado
4	CONTEXTO DE LA ORGANIZACIÓN	30 %
5	LIDERAZGO	23 %
6	PLANIFICACIÓN	0 %
7	SOPORTE	40 %
8	OPERACIÓN	23 %
9	EVALUACIÓN DEL DESEMPEÑO	7 %
10	MEJORA	5 %
Anex 5	Políticas de seguridad	5 %
Anex 6	Organización de la seguridad de la información	42 %
Anex 7	Seguridad relativa a los RRHH	46 %
Anex 8	Gestión de activos	45 %
Anex 9	Control de acceso	59 %
Anex 10	Criptografía	25 %
Anex 11	Seguridad física y ambiental	68 %
Anex 12	Seguridad en la operativa	67 %
Anex 13	Seguridad en las telecomunicaciones	50 %
Anex 14	Adquisición, desarrollo y mantenimiento	83 %
Anex 15	Relación con proveedores	33 %
Anex 16	Gestión de incidentes de seguridad	89 %
Anex 17	Seguridad en la continuidad de negocio	5 %
Anex 18	Cumplimiento	52 %
	Cumplimiento General	38 %

Tabla 1: Resumen del análisis diferencial

De la presente tabla se desprende que en general el propio contenido de la norma (apartados del 4º al 10º) son los que presentan un menor nivel de cumplimiento, probablemente motivado por la falta de interés de la organización por la estandarización y procedimentación.

No obstante, al llegar al anexo A de la norma, los niveles de cumplimiento suben significativamente, debido principalmente los conocimientos del personal técnico y a la aplicación de buenas prácticas en su gestión diaria.

5 Esquema documental

Como parte del esquema documental del SGSI de DivertiApuesta, se han definido los siguientes documentos, cuyo contenido se encuentra en los anexos correspondientes:

Política de Seguridad: normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información.

Procedimiento de Auditorías Internas: documento que contiene la planificación de las auditorías que se llevarán a cabo, los requisitos que se establecerán a los auditores internos y la metodología a seguir.

Gestión de Indicadores: indicadores para medir la eficacia de los controles de seguridad implantados.

Procedimiento Revisión por Dirección: procedimiento por el cual la dirección revisa anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información.

Gestión de Roles y Responsabilidades: definición del equipo que se encarga de crear, mantener, supervisar y mejorar el sistema. Incluye responsabilidades de cada una de las figuras que intervienen en la operación del SGSI.

Metodología de Análisis de Riesgos: establece la sistemática para calcular el riesgo, incluyendo la identificación y valoración de los activos, amenazas y vulnerabilidades, así como el procedimiento para gestionar los riesgos detectados.

Declaración de Aplicabilidad: documento que incluye todos los controles de seguridad establecidos, con el detalle de su aplicabilidad, estado y documentación relacionada.

6 Análisis de riesgos

En el presente apartado abordaremos el análisis de riesgos del sistema de información. Para ello utilizaremos la metodología MAGERIT, desarrollada por el Consejo Superior de Administración Electrónica Español, y documentada en tres documentos de libre acceso conocidos como Libro I, II y III. La selección de esta metodología está motivada por ser de las más utilizada a nivel nacional.

Los pasos naturales de MAGERIT son: identificar y valorar activos, establecer sus dependencias, identificar y asignar amenazas a los activos, estimar la probabilidad y la degradación que pueda causar una amenaza, y por último, establecer las salvaguardas para reducir los niveles de riesgo en el sistema.

Para la realización de este análisis se ha seguido el documento "*Anexo VII - Metodología de análisis de riesgos*" apoyado en la herramienta PILAR.

6.1 Identificación de activos y dependencias

Para la identificación de activos, se ha utilizado la estructura de tipos de activos que sugiere PILAR:

- Capa de negocio
  - Servicios finales
  - Datos
- Equipamiento
  - Software
  - Hardware
    - Servidores
    - Hardware de red
  - Servicios de comunicaciones
  - Elementos auxiliares
- Proveedores
- Instalaciones
- Personal

En el más alto nivel (activos esenciales) se ha identificado el propio servicio de apuestas como principal activo a proteger, y tres unidades de información: información del servicio, información de gestión interna e información estratégica de negocio.

También se han identificado como activos TIC, los departamentos de personal, las instalaciones y los empleados, además de por supuesto, los activos hardware, software y similares:

Activos esenciales	Equipos HW
Servicio de apuestas	Máquinas físicas de apuestas
Información de la plataforma apuestas	Servidores desarrollo (4)
Información de gestión interna	Servidor VPN y de correo electrónico
Información estratégica de negocio	Equipos usuario
Servicios internos	Servidores WEB para apuestas 1y2
Servicio interno administración	Servidor gestión interna
Servicio interno sistemas	Robot de copias
Servicio interno desarrollo	Servidor BBDD
Servicio interno comercial	Servidor apuestas de terminales físicos
Servicio interno negocio	**Comunicaciones**
Servicio interno seguridad	Switch interno
Personal	Red de datos
Personal técnico	Firewall interno
Dirección, administración, comercial	Firewall externo
Aplicaciones	**Elementos auxiliares**
Web de apuestas de usuarios	Impresoras
Core del software de apuestas	**Servicios subcontratados**
Software de máquinas físicas de apuestas	Suministro eléctrico
Gestor documental	Servicio de limpieza
Gestor ticketing	Conexion WAN principal
Gestor de código fuente SVN	Conexion WAN backup
SW de gestión de la BBDD	**Instalaciones**
Base de datos de apuestas	Sede principal
SW administración	Sala de servidores
SW copias	Sistema de climatización
Sistema operativo servidores	Sistema de control de acceso
Sistema operativo usuarios	SAI y grupo electrógeno
Herramientas ofimáticas y SW común de usuarios	
Antivirus	

Tabla 2 Inventario de activos

Se añade una captura de cómo se muestra esta información en PILAR:

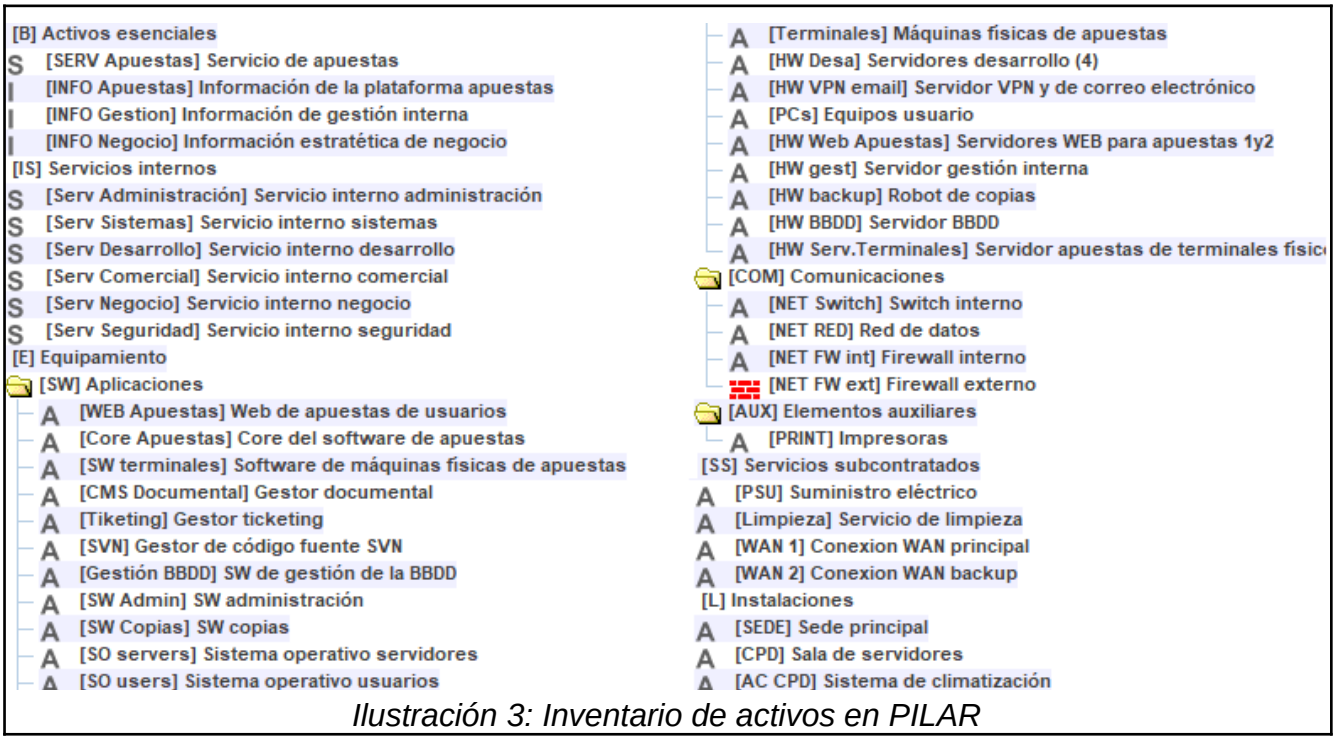


Ilustración 3: Inventario de activos en PILAR

El siguiente paso ha sido determinar las **dependencias** de los activos. Para ello se ha planteado que un activo A depende del activo B, cuando la disminución de la seguridad de cualquiera de las dimensiones de B, repercute en una reducción de la seguridad de A.

En la siguiente lista los activos y tipos de activos están marcados en negrita y las dependencias en texto normal.

Además se ha identificando el **porcentaje de dependencia** entre activos de modo que cuando la dependencia se acompañe de un 90% indicará que la dependencia es prácticamente total, mientras que porcentajes más pequeños indican menor porcentaje de dependencia:

Activos esenciales (B)

B - Servicio de apuestas-

-100% Información de la plataforma apuestas

-10% Información de gestión interna

-90% Información estratégica de negocio

-10% Servicio interno administración

-100% Servicio interno sistemas

-90% Servicio interno desarrollo

-10% Servicio interno comercial

-90% Servicio interno negocio

-90% Servicio interno seguridad

-100% Web de apuestas de usuarios

-100% Core del software de apuestas

-90% Software de máquinas físicas de apuestas

-100% Sistema operativo servidores

-90% Máquinas físicas de apuestas

-90% Servidor VPN y de correo electrónico

-100% Servidores WEB para apuestas 1y2

-100% Servidor BBDD

-90% Servidor apuestas de terminales físicos

-100% Red de datos

B - Información de la plataforma apuestas-

-50% Servicio interno sistemas

-10% Servicio interno desarrollo

-10% Servicio interno seguridad

B - Información de gestión interna-

-100% Servicio interno administración

-50% Servicio interno comercial

B - Información estratégica de negocio-

-100% Servicio interno negocio

Servicios internos (IS)

IS - Servicio interno administración-

-90% Gestor documental

-10% Gestor ticketing

-100% SW administración

-100% Sistema operativo usuarios

-100% Herramientas ofim y SW usuarios

-50% Antivirus

-100% Equipos usuario

-100% Servidor gestión interna

-100% Red de datos

-10% Impresoras

-100% Dirección, administración, comercial

IS - Servicio interno sistemas-

-100% Gestor documental

-100% Gestor ticketing

-50% Gestor de código fuente SVN

-100% SW de gestión de la BBDD

-100% Sistema operativo usuarios

-50% Herramientas ofim y SW usuarios

-50% Antivirus

-100% Equipos usuario

-10% Servidor gestión interna

-100% Red de datos

-100% Personal técnico

IS - Servicio interno desarrollo-

-10% Gestor documental

-50% Gestor ticketing

-100% Gestor de código fuente SVN

-100% Sistema operativo usuarios

-50% Herramientas ofim y SW usuarios

-50% Antivirus

-100% Servidores desarrollo (4)

-100% Equipos usuario

-10% Servidor gestión interna

-100% Red de datos

-100% Personal técnico

IS - Servicio interno comercial-

-100% Gestor documental

-10% Gestor ticketing

-100% Sistema operativo usuarios

-100% Herramientas ofim y SW usuarios

-50% Antivirus

-100% Equipos usuario

-50% Servidor gestión interna

-100% Red de datos

-10% Impresoras

-100% Dirección, administración, comercial

IS - Servicio interno negocio-

-100% Gestor documental

-90% Gestor ticketing

-100% Sistema operativo usuarios

-100% Herramientas ofim y SW usuarios

-50% Antivirus

-100% Equipos usuario

-90% Servidor gestión interna

-100% Red de datos

-10% Impresoras

-100% Dirección, administración, comercial

IS - Servicio interno seguridad-

-90% Gestor documental

-90% Gestor ticketing
-100% Sistema operativo usuarios
-50% Herramientas ofim y SW usuarios
-50% Antivirus
-100% Equipos usuario
-10% Servidor gestión interna
-100% Red de datos
-100% Personal técnico

Equipamiento (E)

E - Web de apuestas de usuarios-
-100% Gestor de código fuente SVN
-50% SW copias
-50% Robot de copias
-100% Red de datos
E - Core del software de apuestas-
-100% Gestor de código fuente SVN
-50% SW copias
-50% Robot de copias
-100% Red de datos
E - Software de máquinas físicas de apuestas-
-100% Gestor de código fuente SVN
-50% SW copias
-50% Robot de copias
-100% Red de datos
E - Gestor documental-
-50% SW copias
-50% Robot de copias
-100% Red de datos
E - Gestor ticketing-
-50% SW copias
-50% Robot de copias
-100% Red de datos

E - Gestor de código fuente SVN-
-50% SW copias
-50% Robot de copias
-100% Red de datos

E - SW de gestión de la BBDD-
-50% SW copias
-50% Robot de copias
-100% Red de datos
E - SW BBDD de apuestas
-50% SW copias
-50% Robot de copias
-100% Red de datos
E - SW administración-
-50% SW copias
-50% Robot de copias
-100% Red de datos
E - SW copias-
-100% Red de datos
E - Sistema operativo servidores-
E - Sistema operativo usuarios-
E - Herramientas ofim y SW usuarios-
E - Antivirus-
E - Máquinas físicas de apuestas-
E - Servidores desarrollo (4)-
-100% Sala de servidores
E - Servidor VPN y de correo electrónico-
-100% Sala de servidores
E - Equipos usuario-
-100% Sede principal
E - Servidores WEB para apuestas 1y2-
-100% Sala de servidores
E - Servidor gestión interna-
-100% Sala de servidores
E - Robot de copias-
-100% Sala de servidores
E - Servidor BBDD-
-100% Sala de servidores
E - Servidor apuestas de terminales físicos-
-100% Sala de servidores
E - Switch interno-
-100% Sala de servidores

E - Red de datos-

-100% Switch interno

-100% Firewall interno

-100% Firewall externo

-100% Conexion WAN principal

-10% Conexion WAN backup

E - Firewall interno-

-100% Sala de servidores

E - Firewall externo-

-100% Sala de servidores

E - Impresoras-

-100% Sede principal

Servicios subcontratados (SS)

SS - Suministro eléctrico-

SS - Servicio de limpieza-

SS - Conexion WAN principal-

SS - Conexion WAN backup-

Personal (P)

P - Personal técnico-

P - Dirección, administración, comercial-

Instalaciones (L)

L - Sede principal

-100% Suministro eléctrico

-50% Servicio de limpieza

-100% Sala de servidores

-90% Sistema de control de acceso

L - Sala de servidores-

-100% Sistema de climatización

-90% Sistema de control de acceso

-90% SAI y grupo electrógeno

L - Sistema de climatización-

L - Sistema de control de acceso-

L - SAI y grupo electrógeno-

A continuación se muestra una captura de cómo se representan las dependencias en PILAR, donde un activo depende de los activos anidados bajo él y son marcados con una letra "d" azul. También figura el porcentaje de dependencia, mientras que si no se muestra porcentaje significa que es dependencia total (100%):

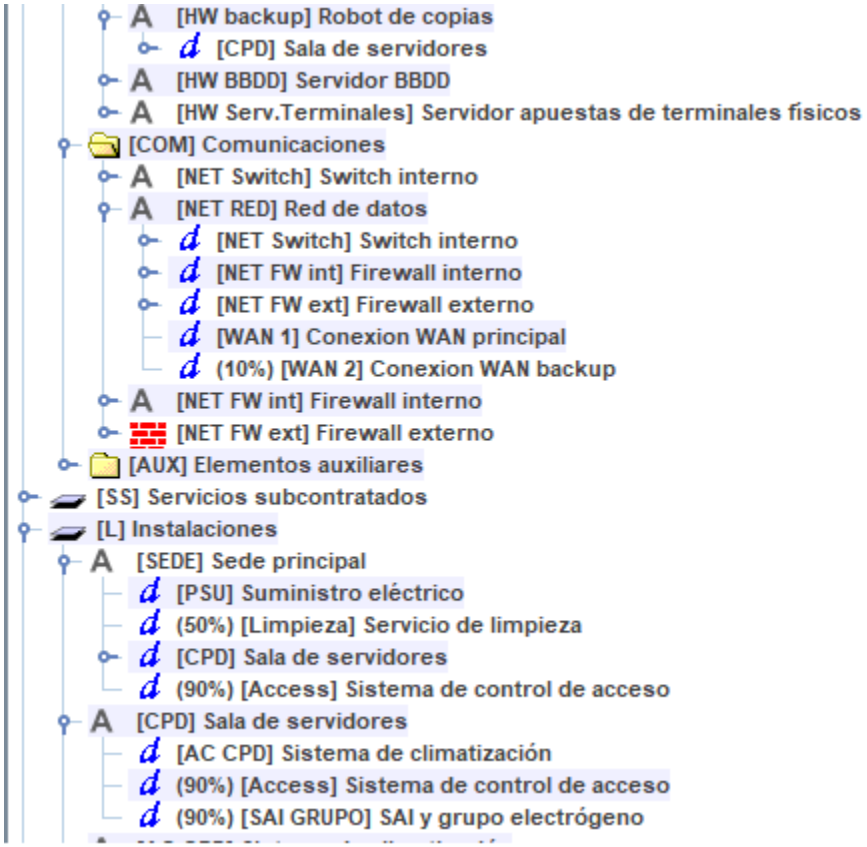


Ilustración 4: Dependencias de activos en PILAR

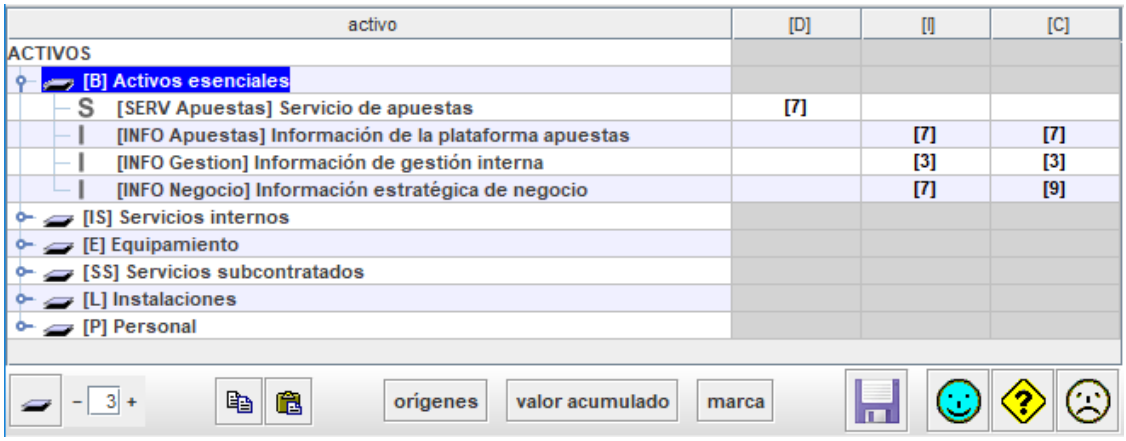
6.2 Valoración de activos y dimensiones

En esta fase del análisis se han valorado las diferentes dimensiones de la seguridad para los activos esenciales de la organización (servicios e información).

Una de las grandes ventajas de utilizar el modelo de dependencias de PILAR es que no es necesario valorar cada activo individualmente, ya que los activos inferiores heredarán la criticidad de los activos superiores a los que dan soporte en la medida en que estos sean críticos y el porcentaje de dependencia.

Así pues, no tendría sentido otorgar un cierto valor a un servidor que nada tiene que ver con el proceso de negocio y que no es necesario para la prestación del servicio.

Siguiendo las guías de uso de PILAR y las prácticas habituales del sector, para los servicios únicamente valoraremos la disponibilidad, y para las unidades de información el resto de dimensiones: esto se debe a que, por ejemplo, los servicios no son confidenciales ni tienen integridad ya que estas son cualidades de la información que el servicio maneja.



activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[SERV Apuestas] Servicio de apuestas	[7]		
[INFO Apuestas] Información de la plataforma apuestas		[7]	[7]
[INFO Gestion] Información de gestión interna		[3]	[3]
[INFO Negocio] Información estratégica de negocio		[7]	[9]
[IS] Servicios internos			
[E] Equipamiento			
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			

orígenes | valor acumulado | marca

Ilustración 5: Valoración de servicios e información

A continuación se muestran en verde los valores acumulados calculados por la aplicación:

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[SERV Apuestas] Servicio de apuestas	[7]		
[INFO Apuestas] Información de la plataforma apuestas	[7]	[7]	[7]
[INFO Gestion] Información de gestión interna	[4]	[3]	[3]
[INFO Negocio] Información estratégica de negocio	[7]	[7]	[9]
[IS] Servicios internos			
[Serv Administración] Servicio interno administración	[5]	[3]	[3]
[Serv Sistemas] Servicio interno sistemas	[7]	[6]	[6]
[Serv Desarrollo] Servicio interno desarrollo	[7]	[4]	[4]
[Serv Comercial] Servicio interno comercial	[5]	[2]	[2]
[Serv Negocio] Servicio interno negocio	[7]	[7]	[9]
[Serv Seguridad] Servicio interno seguridad	[7]	[4]	[4]
[E] Equipamiento			
[SW] Aplicaciones			
[WEB Apuestas] Web de apuestas de usuarios	[7]		
[Core Apuestas] Core del software de apuestas	[7]		
[SW terminales] Software de máquinas físicas de apuestas	[7]		
[CMS Documental] Gestor documental	[7]	[7]	[9]
[Tiketing] Gestor ticketing	[7]	[7]	[9]
[SVN] Gestor de código fuente SVN	[7]	[6]	[6]
[Gestión BBDD] SW de gestión de la BBDD	[7]	[6]	[6]
[BBDD apuestas] Base de datos de apuestas	[7]	[7]	[9]
[SW Admin] SW administración	[5]	[3]	[3]
[SW Copias] SW copias	[7]	[7]	[9]
[SO servers] Sistema operativo servidores	[7]		
[SO users] Sistema operativo usuarios	[7]	[7]	[9]
[APPs users] Herramientas ofimáticas y SW común de usu	[7]	[7]	[9]
[Antivirus] Antivirus	[7]	[6]	[8]

Ilustración 6: Valoración de activos heredada [1/2]

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[IS] Servicios internos			
[E] Equipamiento			
[SW] Aplicaciones			
[HW] Equipos			
[Terminales] Máquinas físicas de apuestas	[7]		
[HW Desa] Servidores desarrollo (4)	[7]	[4]	[4]
[HW VPN email] Servidor VPN y de correo electrónico	[7]		
[PCs] Equipos usuario	[7]	[7]	[9]
[HW Web Apuestas] Servidores WEB para apuestas 1y2	[7]		
[HW gest] Servidor gestión interna	[7]	[7]	[9]
[HW backup] Robot de copias	[7]	[7]	[9]
[HW BBDD] Servidor BBDD	[7]		
[HW Serv.Terminales] Servidor apuestas de terminales físic	[7]		
[COM] Comunicaciones			
[NET Switch] Switch interno	[7]	[7]	[9]
[NET RED] Red de datos	[7]	[7]	[9]
[NET FW int] Firewall interno	[7]	[7]	[9]
[NET FW ext] Firewall externo	[7]	[7]	[9]
[AUX] Elementos auxiliares			
[PRINT] Impresoras	[5]	[4]	[6]
[SS] Servicios subcontratados			
[PSU] Suministro eléctrico	[7]	[7]	[9]
[Limpieza] Servicio de limpieza	[7]	[6]	[8]
[WAN 1] Conexion WAN principal	[7]	[7]	[9]
[WAN 2] Conexion WAN backup	[7]	[6]	[8]
[L] Instalaciones			
[SEDE] Sede principal	[7]	[7]	[9]
[CPD] Sala de servidores	[7]	[7]	[9]
[AC CPD] Sistema de climatización	[7]		
[Access] Sistema de control de acceso	[7]	[7]	[9]
[SAI GRUPO] SAI y grupo electrógeno	[7]		
[P] Personal			
[Técnicos] Personal técnico	[7]	[6]	[6]
[Empl Genérico] Dirección, administración, comercial	[7]	[7]	[9]

Ilustración 7: Valoración de activos heredada [2/2]

A pesar de que pueda parecer que la tabla está incompleta, existe hardware y software que no tienen requisitos de integridad y confidencialidad ya que hemos desglosado por un lado los servicios y por otro la información, siendo estos activos solo necesarios para que el servicio esté disponible.

Evidentemente la información que esos activos almacenan, debe cumplir con requisitos de integridad y confidencialidad, pero estos se valoran en los activos que almacenan información, por ejemplo *"[BBDD Apuestas] Base de datos de apuestas"* a la que se puede apreciar que se auto-aplican los niveles disponibilidad, integridad y confidencialidad mayores.

6.3 Identificación y valoración de amenazas

Aunque no se ha mencionado, durante la fase de identificación de activos, además de añadirlos dentro de la capa correspondiente, para cada uno se ha indicado el tipo de activo que és, por ejemplo, una aplicación de desarrollo propio, un servidor de correo, una base de datos, un cortafuegos, o una unidad de negocio.

A continuación se muestran algunos ejemplos:

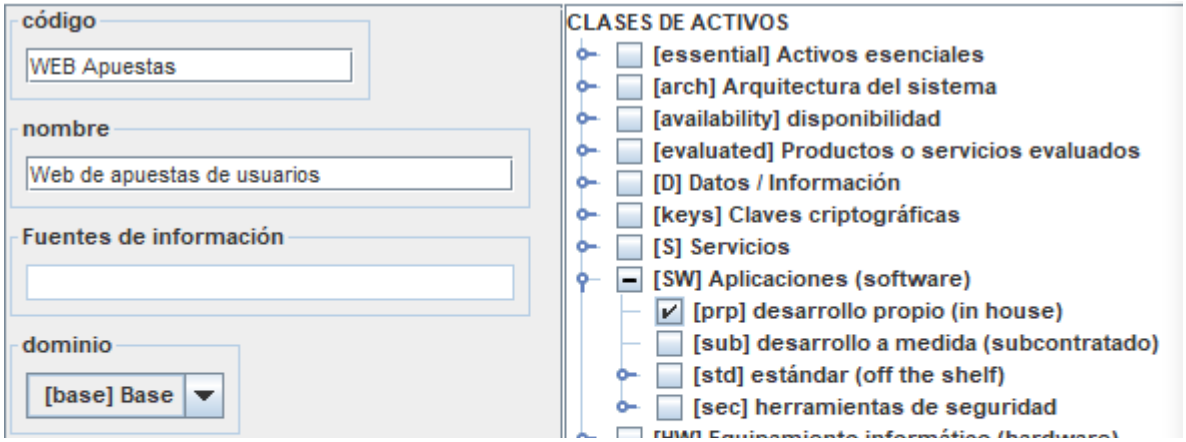


Ilustración 8: Clasificación activo WEB Apuestas

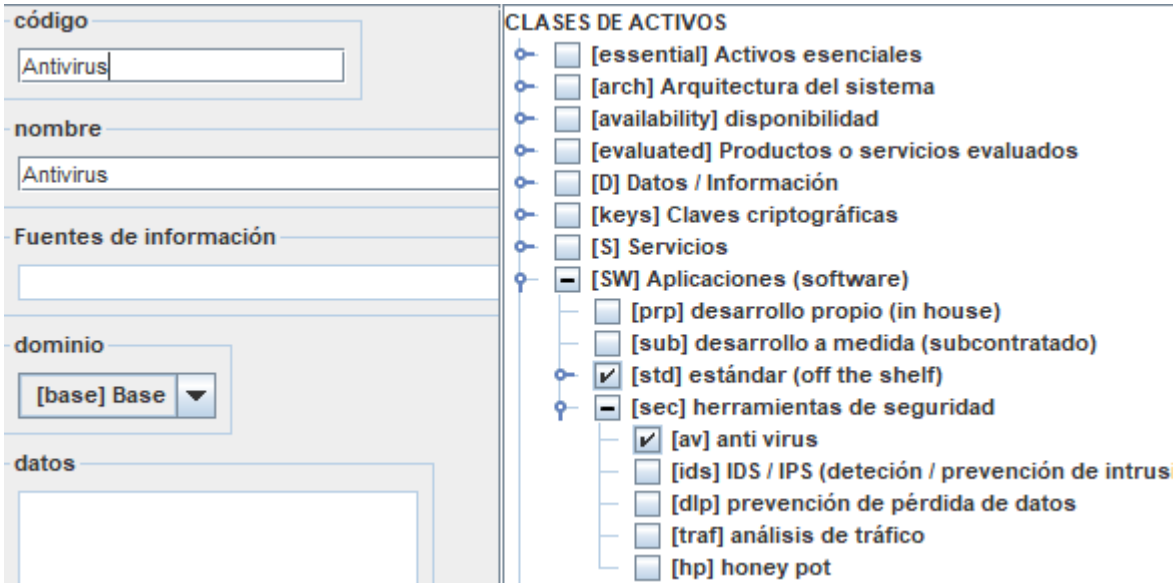


Ilustración 9: Clasificación activo Antivirus

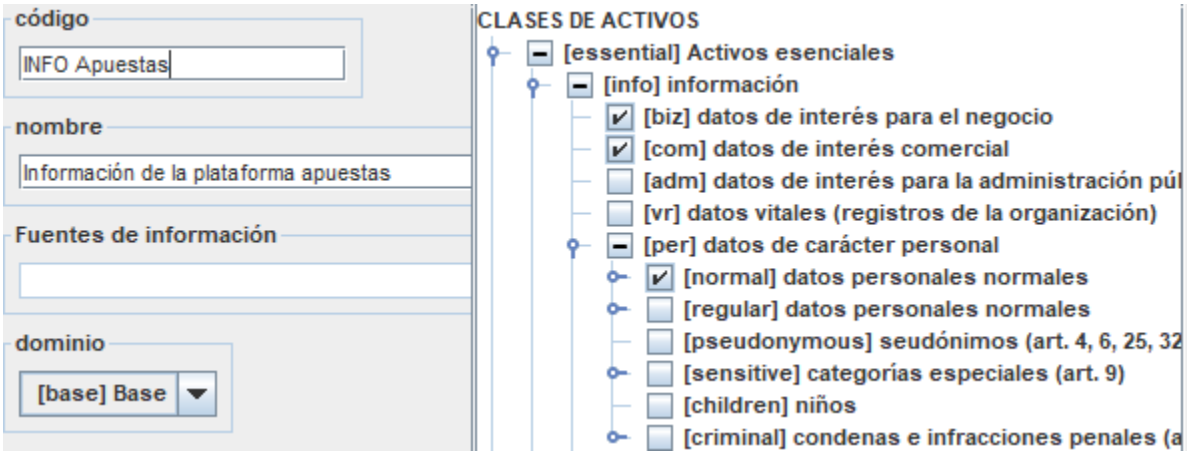


Ilustración 10: Clasificación activo Información de apuestas

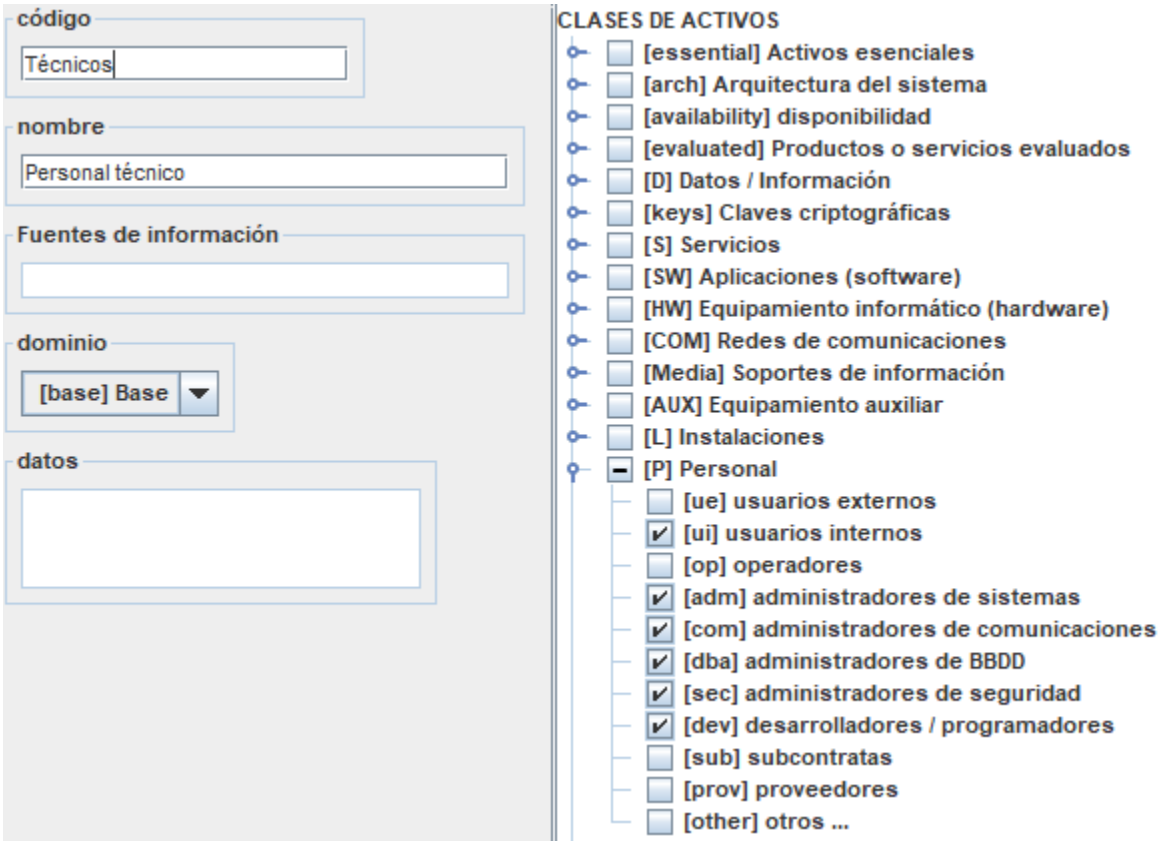


Ilustración 11: Clasificación activo Personal Técnico

Gracias a esta clasificación, PILAR asigna automáticamente aquellas amenazas que pueden afectar al activo según su tipología y características.

Si bien esta automatización facilita el proceso, se han repasado todas las amenazas para asegurarse de que no falta ninguna. Como resultado de la revisión se han añadido las siguientes amenazas:

- Amenazas al sistema de control de accesos, ya que debido a su tipificación no se le ha asignado ninguna automáticamente.
- Se asignan a mano salvaguardas a suministro eléctrico y al servicio de limpieza
- Se añade acceso no autorizado al CPD y edificio.

Adicionalmente, durante esta revisión se han detectado algunas amenazas muy poco probables que han sido eliminadas:

Para el hardware:

- Contaminación medioambiental
- Contaminación electromagnéticas
- Emanaciones electromagnéticas
- Ataque destructivo (salvo a los terminales físicos de apuestas)
- Desastres industriales (ya contemplado fuego y agua)
- Desastres naturales (ya contemplado fuego y agua)
- Fuego por desastres naturales (ya contemplado por motivos industriales)
- Manipulación de hardware (salvo a los terminales físicos de apuestas)

Para el hardware del CPD:

- Pérdida de equipos
- Robo de equipos
- Ataque destructivo

Otros:

- Destrucción de información para electrónica de red y servicios subcontratados sin acceso a información
- Ocupación enemiga para las instalaciones
- Se elimina el software dañino como error del usuario para los servidores ya que hay otro para ataques deliberados.

Ya que a continuación se enumerarán las amenazas con su valoración, no se adjunta el listado completo de amenazas identificadas, solo se muestra una captura del proceso de identificación:

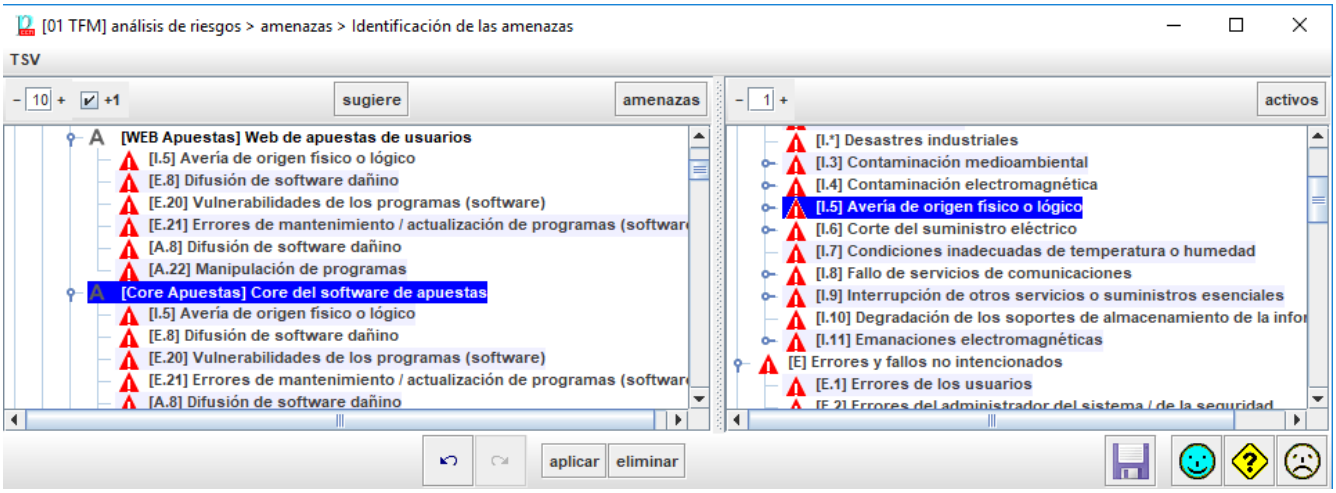


Ilustración 12: Asociación de salvaguardas a activos

En cuanto a la valoración de amenazas, PILAR también ofrece una estimación inicial en cuanto a la degradación que causaría la materialización de la amenaza sobre el activo en cada una de las dimensiones, además de la probabilidad de ocurrencia (se representa como frecuencia, siendo un entero que representa el número estimado de materializaciones de la amenaza durante un año natural).

Estas estimaciones sí que han sido ampliamente modificadas, tanto la probabilidad como el impacto, ya que no tienen en cuenta la existencia de salvaguardas ya implantadas, y son complicadas de estimar por la aplicación sin conocer el negocio.

Dada la extensión del listado, a continuación se muestra solo un extracto del mismo. Puede consultarse el listado completo en el fichero del análisis de riesgos adjunto (*Anexo X – AR inicial*).

activo		frec...	[D]	[I]	[C]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
A [WEB Apuestas] Web de apuestas de usuarios			A		
[I.5] Avería de origen físico o lógico		1	A		
[E.20] Vulnerabilidades de los programas (software)		2	M		
[E.21] Errores de mantenimiento / actualización de program		5	B		
[A.8] Difusión de software dañino		1	M		
[A.22] Manipulación de programas		0,2	A		
A [Core Apuestas] Core del software de apuestas			A		
[I.5] Avería de origen físico o lógico		1	A		
[E.20] Vulnerabilidades de los programas (software)		2	M		
[E.21] Errores de mantenimiento / actualización de program		5	B		
[A.8] Difusión de software dañino		1	M		
[A.22] Manipulación de programas		0,2	A		
A [SW terminales] Software de máquinas físicas de apuestas			A		
[I.5] Avería de origen físico o lógico		1	A		
[E.20] Vulnerabilidades de los programas (software)		2	B		
[E.21] Errores de mantenimiento / actualización de program		1	B		
[A.8] Difusión de software dañino		1	M		
[A.22] Manipulación de programas		0,2	A		
A [CMS Documental] Gestor documental			M	T	T
[I.5] Avería de origen físico o lógico		1	M		
[E.20] Vulnerabilidades de los programas (software)		1	B	M	M
[E.21] Errores de mantenimiento / actualización de program		5	B	B	
[A.8] Difusión de software dañino		1	M	B	M
[A.22] Manipulación de programas		0,2	M	T	T
A [Tiketing] Gestor ticketing			A	B	M
[I.5] Avería de origen físico o lógico		1	A		
[E.20] Vulnerabilidades de los programas (software)		1	B	B	B
[E.21] Errores de mantenimiento / actualización de program		2	B	B	
[A.8] Difusión de software dañino		1	M	B	M
[A.22] Manipulación de programas		0,2	M	B	B
A [SVN] Gestor de código fuente SVN			A	T	T
[I.5] Avería de origen físico o lógico		1	A		
[E.20] Vulnerabilidades de los programas (software)		1	B	B	M
[E.21] Errores de mantenimiento / actualización de program		2	B	B	
[A.8] Difusión de software dañino		1	M	B	M
[A.22] Manipulación de programas		0,2	M	T	T
A [Gestión BBDD] SW de gestión de la BBDD			M	B	B
[I.5] Avería de origen físico o lógico		1	M		
[E.20] Vulnerabilidades de los programas (software)		1	M	B	B
[E.21] Errores de mantenimiento / actualización de program		2	B	B	
[A.8] Difusión de software dañino		1	M	B	B
[A.22] Manipulación de programas		0,2	M	B	B

Ilustración 13: Valoración de amenazas

6.4 Riesgo potencial

Una vez introducidos en PILAR todos los datos necesarios, la aplicación calcula automáticamente los niveles de riesgo de la organización analizada.

Para ello, en el apartado informes dispone de diferentes representaciones donde podemos extraer información muy valiosa.

Empezando por la tabla de riesgo acumulado, podemos observar qué activos suponen un mayor riesgo para la organización. En la tabla pueden verse los niveles de riesgos según cada activo permitiendo identificar "zonas calientes" del inventario de activos donde radican la mayoría de riesgos:

potencial | current | target | PILAR

activo	[D]	[I]	[C]
ACTIVOS	{5,2}	{4,5}	{6,2}
[B] Activos esenciales			
[IS] Servicios internos			
[E] Equipamiento	{5,2}	{4,5}	{6,2}
[SW] Aplicaciones	{5,0}	{4,5}	{6,2}
[WEB Apuestas] Web de apuestas de usuarios	{4,5}		
[Core Apuestas] Core del software de apuestas	{4,5}		
[SW terminales] Software de máquinas físicas de	{4,5}		
[CMS Documental] Gestor documental	{3,8}	{4,5}	{5,6}
[Tiketing] Gestor ticketing	{4,5}	{1,7}	{4,9}
[SVN] Gestor de código fuente SVN	{4,5}	{3,6}	{3,6}
[Gestión BBDD] SW de gestión de la BBDD	{3,8}	{1,3}	{1,0}
[BBDD apuestas] Base de datos de apuestas	{4,8}	{3,8}	{6,2}
[SW Admin] SW administración	{2,6}	{1,6}	{2,2}
[SW Copias] SW copias	{4,5}	{3,9}	{5,1}
[SO servers] Sistema operativo servidores	{5,0}		
[SO users] Sistema operativo usuarios	{4,2}	{4,2}	{5,6}
[APPs users] Herramientas ofimáticas y SW com	{5,0}	{3,8}	{5,6}
[Antivirus] Antivirus	{3,8}	{2,7}	{3,9}
[HW] Equipos	{4,8}	{3,3}	{5,7}
[Terminales] Máquinas físicas de apuestas	{3,5}		
[HW Desa] Servidores desarrollo (4)	{3,2}	{1,5}	{2,8}
[HW VPN email] Servidor VPN y de correo electró	{4,7}		
[PCs] Equipos usuario	{4,5}	{3,3}	{5,7}
[HW Web Apuestas] Servidores WEB para apuesta	{4,8}		
[HW gest] Servidor gestión interna	{3,3}	{3,2}	{5,6}
[HW backup] Robot de copias	{3,6}	{3,3}	{5,7}
[HW BBDD] Servidor BBDD	{4,8}		
[HW Serv.Terminales] Servidor apuestas de term	{4,7}		
[COM] Comunicaciones	{5,2}	{3,9}	{5,1}
[NET Switch] Switch interno	{5,1}	{2,7}	{5,1}
[NET RED] Red de datos	{5,2}	{3,9}	{5,1}
[NET FW int] Firewall interno	{5,1}	{2,7}	{5,1}
[NET FW ext] Firewall externo	{5,2}	{3,9}	{5,1}
[AUX] Elementos auxiliares	{2,1}	{0,75}	{0,98}
[PRINT] Impresoras	{2,1}	{0,75}	{0,98}
[SS] Servicios subcontratados	{5,1}	{4,5}	{5,7}
[PSU] Suministro eléctrico	{5,1}		
[Limpieza] Servicio de limpieza	{2,2}	{2,8}	{4,0}

Ilustración 14: Riesgo acumulado potencial

Si bien la tabla anterior muestra el riesgo a nivel de activo, para una visión más ejecutiva, es interesante analizar de qué forma estos riesgos se trasladan a los servicios y la información del negocio, que al fin y al cabo, es lo que debe protegerse. Para ello disponemos de la vista "*riesgo repercutido*", donde vemos qué dimensión de qué activos esenciales corren un mayor riesgo:

potencial | current | target | PILAR

activo	[D]	[I]	[C]
ACTIVOS	{5,2}	{4,5}	{6,2}
[SERV Apuestas] Servicio de apuestas	{5,2}		
[D] disponibilidad	{5,2}		
[INFO Apuestas] Información de la plataforma apuestas		{4,5}	{5,1}
[I] integridad de los datos		{4,5}	
[C] confidencialidad de los datos			{5,1}
[INFO Gestion] Información de gestión interna		{2,2}	{2,7}
[I] integridad de los datos		{2,2}	
[C] confidencialidad de los datos			{2,7}
[INFO Negocio] Información estratégica de negocio		{4,5}	{6,2}
[I] integridad de los datos		{4,5}	
[C] confidencialidad de los datos			{6,2}

Ilustración 15: Riesgo repercutido

Continuando con las representaciones de los riesgos, a vista que mayor información nos ofrece para poder decidir qué medidas de seguridad debemos aplicar, es la llamada "*tabla*" que asocia activos de bajo nivel, con activos de alto nivel y el riesgo correspondiente:

padre	D	hijo	D	amenaza	V	D	I	F	R
[INFO Negocio] Información estra...	[C]	[BBDD apuestas] Base de datos ...	[C]	[A.8] Difusión de software dañino	[9]	T	[9]	1	{6,2}
[INFO Negocio] Información estra...	[C]	[PCs] Equipos usuario	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	1	{5,7}
[INFO Negocio] Información estra...	[C]	[WAN 1] Conexion WAN principal	[C]	[E.19] Fugas de información	[9]	A	[8]	1	{5,7}
[INFO Negocio] Información estra...	[C]	[HW backup] Robot de copias	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	1	{5,7}
[INFO Negocio] Información estra...	[C]	[BBDD apuestas] Base de datos ...	[C]	[A.22] Manipulación de programas	[9]	T	[9]	0,2	{5,6}
[INFO Negocio] Información estra...	[C]	[CMS Documental] Gestor docu...	[C]	[A.22] Manipulación de programas	[9]	T	[9]	0,2	{5,6}
[INFO Negocio] Información estra...	[C]	[HW gest] Servidor gestión inter...	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	1	{5,6}
[INFO Negocio] Información estra...	[C]	[SO users] Sistema operativo us...	[C]	[E.20] Vulnerabilidades de los pr...	[9]	M	[7]	5	{5,6}
[INFO Negocio] Información estra...	[C]	[APPs users] Herramientas ofim...	[C]	[A.8] Difusión de software dañino	[9]	M	[7]	5	{5,6}
[INFO Negocio] Información estra...	[C]	[Empl Genérico] Dirección, admi...	[C]	[A.29] Extorsión	[9]	T	[9]	0,1	{5,4}
[INFO Negocio] Información estra...	[C]	[SO users] Sistema operativo us...	[C]	[E.8] Difusión de software dañino	[9]	M	[6]	10	{5,4}
[INFO Negocio] Información estra...	[C]	[WAN 2] Conexion WAN backup	[C]	[E.19] Fugas de información	[9]	A	[7]	1	{5,2}
[SERV Apuestas] Servicio de apu...	[D]	[NET FW ext] Firewall externo	[D]	[E.24] Caída del sistema por agot...	[7]	A	[6]	5	{5,2}
[SERV Apuestas] Servicio de apu...	[D]	[NET FW ext] Firewall externo	[D]	[A.24] Denegación de servicio	[7]	A	[6]	5	{5,2}
[SERV Apuestas] Servicio de apu...	[D]	[NET RED] Red de datos	[D]	[E.24] Caída del sistema por agot...	[7]	A	[6]	5	{5,2}
[SERV Apuestas] Servicio de apu...	[D]	[NET RED] Red de datos	[D]	[A.24] Denegación de servicio	[7]	A	[6]	5	{5,2}
[INFO Negocio] Información estra...	[C]	[NET FW int] Firewall interno	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET RED] Red de datos	[C]	[A.5] Suplantación de la identidad	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET Switch] Switch interno	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[Empl Genérico] Dirección, admi...	[C]	[A.19] Revelación de información	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET FW ext] Firewall externo	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET RED] Red de datos	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[WAN 1] Conexion WAN principal	[C]	[A.19] Revelación de información	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET FW int] Firewall interno	[C]	[A.5] Suplantación de la identidad	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET Switch] Switch interno	[C]	[A.5] Suplantación de la identidad	[9]	A	[8]	0,2	{5,1}

Ilustración 16: Tabla riesgos de activos y repercusión en negocio

Si analizamos la primera línea de la tabla, se interpreta que el riesgo mayor para la organización es que por un ataque de software malicioso (columna "*amenaza*") contra la BBDD de apuestas (columna "*hijo*"), se comprometa la confidencialidad (columna "*D*") de la información estratégica (columna "*padre*").

A continuación se incluye la tabla de los riesgos más relevantes detectados:

[Puede consultarse la tabla completa en el fichero de PILAR adjunto]

padre	D	hijo	D	amenaza	V	D	I	F	R
[INFO Negocio] Información estra...	[C]	[BBDD apuestas] Base de datos ...	[C]	[A.8] Difusión de software dañino	[9]	T	[9]	1	{6,2}
[INFO Negocio] Información estra...	[C]	[PCs] Equipos usuario	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	1	{5,7}
[INFO Negocio] Información estra...	[C]	[WAN 1] Conexion WAN principal	[C]	[E.19] Fugas de información	[9]	A	[8]	1	{5,7}
[INFO Negocio] Información estra...	[C]	[HW backup] Robot de copias	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	1	{5,7}
[INFO Negocio] Información estra...	[C]	[BBDD apuestas] Base de datos ...	[C]	[A.22] Manipulación de programas	[9]	T	[9]	0,2	{5,6}
[INFO Negocio] Información estra...	[C]	[CMS Documental] Gestor docu...	[C]	[A.22] Manipulación de programas	[9]	T	[9]	0,2	{5,6}
[INFO Negocio] Información estra...	[C]	[HW gest] Servidor gestión inter...	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	1	{5,6}
[INFO Negocio] Información estra...	[C]	[SO users] Sistema operativo us...	[C]	[E.20] Vulnerabilidades de los pr...	[9]	M	[7]	5	{5,6}
[INFO Negocio] Información estra...	[C]	[APPs users] Herramientas ofim...	[C]	[A.8] Difusión de software dañino	[9]	M	[7]	5	{5,6}
[INFO Negocio] Información estra...	[C]	[Empl Genérico] Dirección, admi...	[C]	[A.29] Extorsión	[9]	T	[9]	0,1	{5,4}
[INFO Negocio] Información estra...	[C]	[SO users] Sistema operativo us...	[C]	[E.8] Difusión de software dañino	[9]	M	[6]	10	{5,4}
[INFO Negocio] Información estra...	[C]	[WAN 2] Conexion WAN backup	[C]	[E.19] Fugas de información	[9]	A	[7]	1	{5,2}
[SERV Apuestas] Servicio de apu...	[D]	[NET FW ext] Firewall externo	[D]	[E.24] Caída del sistema por agot...	[7]	A	[6]	5	{5,2}
[SERV Apuestas] Servicio de apu...	[D]	[NET FW ext] Firewall externo	[D]	[A.24] Denegación de servicio	[7]	A	[6]	5	{5,2}
[SERV Apuestas] Servicio de apu...	[D]	[NET RED] Red de datos	[D]	[E.24] Caída del sistema por agot...	[7]	A	[6]	5	{5,2}
[SERV Apuestas] Servicio de apu...	[D]	[NET RED] Red de datos	[D]	[A.24] Denegación de servicio	[7]	A	[6]	5	{5,2}
[INFO Negocio] Información estra...	[C]	[NET FW int] Firewall interno	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET RED] Red de datos	[C]	[A.5] Suplantación de la identidad	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET Switch] Switch interno	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[Empl Genérico] Dirección, admi...	[C]	[A.19] Revelación de información	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET FW ext] Firewall externo	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET RED] Red de datos	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[WAN 1] Conexion WAN principal	[C]	[A.19] Revelación de información	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET FW int] Firewall interno	[C]	[A.5] Suplantación de la identidad	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET Switch] Switch interno	[C]	[A.5] Suplantación de la identidad	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[CPD] Sala de servidores	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[WAN 1] Conexion WAN principal	[C]	[A.5] Suplantación de la identidad	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[NET FW ext] Firewall externo	[C]	[A.5] Suplantación de la identidad	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[SW Copias] SW copias	[C]	[A.8] Difusión de software dañino	[9]	A	[8]	0,2	{5,1}
[INFO Negocio] Información estra...	[C]	[SW Copias] SW copias	[C]	[A.22] Manipulación de programas	[9]	A	[8]	0,2	{5,1}
[SERV Apuestas] Servicio de apu...	[D]	[PSU] Suministro eléctrico	[D]	[I.6] Corte del suministro eléctrico	[7]	T	[7]	1	{5,1}
[SERV Apuestas] Servicio de apu...	[D]	[WAN 1] Conexion WAN principal	[D]	[I.8] Fallo de servicios de comuni...	[7]	T	[7]	1	{5,1}
[SERV Apuestas] Servicio de apu...	[D]	[NET FW int] Firewall interno	[D]	[I.8] Fallo de servicios de comuni...	[7]	T	[7]	1	{5,1}
[SERV Apuestas] Servicio de apu...	[D]	[NET Switch] Switch interno	[D]	[I.8] Fallo de servicios de comuni...	[7]	T	[7]	1	{5,1}
[SERV Apuestas] Servicio de apu...	[D]	[WAN 2] Conexion WAN backup	[D]	[I.8] Fallo de servicios de comuni...	[7]	T	[7]	1	{5,1}
[SERV Apuestas] Servicio de apu...	[D]	[NET FW ext] Firewall externo	[D]	[I.8] Fallo de servicios de comuni...	[7]	T	[7]	1	{5,1}
[SERV Apuestas] Servicio de apu...	[D]	[NET RED] Red de datos	[D]	[I.8] Fallo de servicios de comuni...	[7]	T	[7]	1	{5,1}
[INFO Apuestas] Información de l...	[C]	[BBDD apuestas] Base de datos ...	[C]	[A.8] Difusión de software dañino	[7]	T	[7]	1	{5,1}
[INFO Negocio] Información estra...	[C]	[Empl Genérico] Dirección, admi...	[C]	[A.30] Ingeniería social (picaresca)	[9]	M	[6]	5	{5,1}
[INFO Negocio] Información estra...	[C]	[CMS Documental] Gestor docu...	[C]	[E.20] Vulnerabilidades de los pr...	[9]	M	[7]	1	{5,0}
[INFO Negocio] Información estra...	[C]	[BBDD apuestas] Base de datos ...	[C]	[E.20] Vulnerabilidades de los pr...	[9]	M	[7]	1	{5,0}
[INFO Negocio] Información estra...	[C]	[APPs users] Herramientas ofim...	[C]	[A.22] Manipulación de programas	[9]	M	[7]	1	{5,0}
[INFO Negocio] Información estra...	[C]	[CMS Documental] Gestor docu...	[C]	[A.8] Difusión de software dañino	[9]	M	[7]	1	{5,0}
[SERV Apuestas] Servicio de apu...	[D]	[WAN 2] Conexion WAN backup	[D]	[A.24] Denegación de servicio	[7]	A	[6]	3	{5,0}
[SERV Apuestas] Servicio de apu...	[D]	[SO servers] Sistema operativo ...	[D]	[I.5] Avería de origen físico o lógi...	[7]	A	[6]	3	{5,0}
[SERV Apuestas] Servicio de apu...	[D]	[WAN 1] Conexion WAN principal	[D]	[A.24] Denegación de servicio	[7]	A	[6]	3	{5,0}
[SERV Apuestas] Servicio de apu...	[D]	[APPs users] Herramientas ofim...	[D]	[E.20] Vulnerabilidades de los pr...	[7]	M	[5]	20	{5,0}

Ilustración 17: Relación activos - riesgo

Además, al seleccionar un riesgo, la propia aplicación sugiere medidas de seguridad a implantar para rebajar estos niveles de riesgo. Para el ejemplo del software malicioso sobre la BBDD de apuestas, se muestran las siguientes salvaguardas marcadas en rojo: seguridad de las aplicaciones, herramientas antivirus, y gestión de incidentes entre otras.

salvaguarda	dud...	fue...	com...	rec...	
SALVAGUARDAS					
[IA] Identificación y autenticación					
[AC] Control de acceso lógico					
[D] Protección de la Información					
[K] Protección de claves criptográficas					
[S] Protección de los Servicios					
[SW] Protección de las Aplicaciones Informáticas (SW)				7	
[SW.1] Administración				3	
[SW.backup] Copias de seguridad (backup) (SW)				4	
[SW.start] Puesta en producción				3	
[SW.SC] Se aplican perfiles de seguridad				7	
[SW.op] Explotación / Producción				5	
[SW.CM] Cambios (actualizaciones y mantenimiento)					
[SW.end] Desmantelamiento				3	
[HW] Protección de los Equipos Informáticos (HW)					
[COM] Protección de las Comunicaciones					
[IP] Sistema de protección de frontera lógica					
[MP] Protección de los Soportes de Información					
[AUX] Elementos Auxiliares					
[HW_0049] Protección física del equipamiento					
[L] Protección de las Instalaciones					
[PPS] Protección del perímetro físico					
[PS] Gestión del Personal				6	
[PDS] Servicios potencialmente peligrosos					
[IR] Gestión de incidentes				6	
[IR.1] Se dispone de normativa de actuación para la gestión de incidentes				2	
[IR.2] Se dispone de procedimientos para la gestión de incidentes				4	
[IR.3] Contención del incidente				6	
[IR.4] Gestión del incidente				4	
[IR.5] Cooperación con otras organizaciones				3	
[IR.6] Comunicación de los incidentes de seguridad				3	
[IR.7] Comunicación de las deficiencias de seguridad				2	
[IR.8] Comunicación de los fallos del software					
[IR.9] Se dispone de un registro de incidentes					
[IR.a] Los fallos y las medidas correctoras se registran y se revisan				3	
[IR.b] Control formal del proceso de recuperación ante el incidente				3	
[IR.c] Formación y concienciación				3	
[IR.d] Se aprende de los incidentes				3	
[IR.e] Se toman medidas para prevenir la repetición				4	
[tools] Herramientas de seguridad				8	
[tools.AV] Herramienta contra código dañino				8	
[tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión					
[tools.conf] Herramienta de chequeo de configuración					
[tools.traffic] Herramienta de monitorización de tráfico					
[tools.DLP] DLP: Herramienta de monitorización de contenidos					
[tools.HP] Honey net / honey pot					
[tools.SFV] Verificación de las funciones de seguridad				6	
[V] Gestión de vulnerabilidades				5	

Ilustración 18: Salvaguardas sugeridas

5 Declaración de aplicabilidad

Durante el proceso de análisis de riesgos se identifican tanto los controles implantados en la organización, como aquellos que deberían implantarse.

La norma ISO 27001 exige que dichos controles, independientemente de que sean requeridos por la norma o no, sean recogidos en un documento llamado Declaración de Aplicabilidad, en el cual se expondrá la motivación de implantar el control como parte del SGSI. Además, una vez completado el listado, se deberán revisar los controles del anexo de la norma para asegurarse de que no se ha omitido ninguno por error, y se justificará la no-aplicabilidad de aquellos controles de la norma que se hayan descartado.

Llegados a este punto se ha evaluado uno a uno todos los controles de la norma indicando si aplica o no al SGSI de Divertiapuesta con la correspondiente justificación.

Puede consultarse el documento completo en el "*Anexo VIII - Declaración de aplicabilidad*".

7 Plan de tratamiento del riesgo

A cada uno de los riesgos identificados, tal y como indica el procedimiento de análisis de riesgos, se ha asignado un **propietario** formal, así como una **acción para tratarlo** (mitigarlo, transferirlo, asumirlo o evitarlo).

Las decisiones individuales sobre cada riesgo pueden consultarse en el documento adjunto "*Anexo XII – Tratamiento de riesgos*" (se muestra extracto):

Activo	Amenaza	Riesgo	Propietario	Opción de tratamiento	Proyecto que lo trata
Base de datos de apuestas	Difusión de software dañino	6,2	CISO	Reducir	3, 5 y 6
Equipos usuario	Acceso no autorizado	5,7	Cada usuario	Reducir	1
Conexion WAN principal	Fugas de información	5,7	Compañía de telecomu	Transferir	N/A
Robot de copias	Acceso no autorizado	5,7	CIO	Reducir	2 y 5
Base de datos de apuestas	Manipulación de programas	5,6	CISO	Reducir	3 y 4
Gestor documental	Manipulación de programas	5,6	CISO	Reducir	3 y 4
Servidor gestión interna	Acceso no autorizado	5,6	CIO	Reducir	2 y 3
Sistema operativo usuarios	Vulnerabilidades de los programas	5,6	CIO	Reducir	3 y 4
Herramientas ofimáticas y SW común	Difusión de software dañino	5,6	Cada usuario	Reducir	3 y 6
Dirección, administración, comercial	Extorsión	5,4	CEO	Reducir	1 y 5
Sistema operativo usuarios	Difusión de software dañino	5,4	Cada usuario	Reducir	3, 5 y 6
Conexion WAN backup	Fugas de información	5,2	Compañía de telecomu	Transferir	N/A
Firewall externo	Caída del sistema por agotamiento	5,2	CIO	Reducir	3 y 4
Firewall externo	Denegación de servicio	5,2	CISO	Reducir	6
Red de datos	Caída del sistema por agotamiento	5,2	CIO	Reducir	3 y 4
Red de datos	Denegación de servicio	5,2	CISO	Reducir	6
Firewall interno	Acceso no autorizado	5,1	CISO	Reducir	2 y 3

Ilustración 19: Extracto del documento de tratamiento de riesgos

Como parte de esas formas de tratamiento, se han definido una serie de tareas que reduzcan los niveles de riesgo a la vez que mejoren la seguridad de la información del sistema.

Estos proyectos buscan mejorar tanto la gestión diaria, la seguridad como el nivel progresivo de cumplimiento de cara a una futura certificación.

Cabe destacar que dado el bajo nivel de madurez en ciberseguridad de Divertiapuesta, serán necesarias varias iteraciones del ciclo PDCA hasta conseguir un nivel de cumplimiento certificable, por lo que en esta primera fase se ha optado por priorizar aquellas tareas que sentaran las bases para posibles mejoras, a la vez que supondrán un aumento significativo en los niveles de seguridad y concienciación sobre la misma.

La ejecución de los proyectos se plantea de forma secuencial, por lo que tras cada uno de los proyectos se mostrará tanto la mejora del cumplimiento normativo esperado, como en qué medida se espera que este afecte a los niveles de riesgo.

La tabla completa de niveles de cumplimiento se podrá consultar como documento anexo (*Anexo IX – Evolución de cumplimiento.ods*).

7.1 Proyecto 1 - Definir la política y normativas de seguridad de la organización

Motivación:	Antes de abordar cualquier otra iniciativa de seguridad, se ha considerado necesario establecer las bases que van a marcar la hoja de ruta de la seguridad en la organización y formalizar el compromiso público con esta, mediante la creación de la política y normativa de seguridad
Puntos de la norma ISO 27001 asociados:	Mejora el cumplimiento del punto 5.1 Mejora el cumplimiento del punto 5.2 Mejora el cumplimiento del punto A.5.1.1
Responsable:	Responsable de seguridad y dirección
Plazo de implantación:	Corto - 3 semanas vista
Coste económico:	Solo recursos propios. Ver detalle de planificación y multiplicar horas * coste persona
Planificación e hitos a cumplir:	Definición de los documentos (5 jornadas) Revisión y aprobación por dirección (2 jornadas) Publicación y difusión a las partes interesadas (1 jornada)

	APARTADO DE LA NORMA	% de cumplimiento INICIAL		% de cumpl. Tras PROYECTO	
5	LIDERAZGO	23%		63%	
5.1	Liderazgo y compromiso	1 Inicial	10 %	2 Intuitivo y repetible	50 %
5.2	Política	1 Inicial	10 %	3 Definido	90 %
5.3	Roles, responsabilidades y autoridades	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %

	APARTADO DEL ANEXO	% de cumplimiento INICIAL		% de cumpl. Tras PROYECTO	
5	POLITICAS DE SEGURIDAD	5%		25%	
5,1	Directrices de la Dirección en seguridad de la inform	5 %		25 %	
5.1.1	Conjunto de políticas para la seguridad de la informaci	1 Inicial	10 %	2 Intuitivo y repetible	50 %
5.1.2	Revisión de las políticas para la seguridad de la inform	0 No implementado	0 %	0 No implementado	0 %

Tabla 3: Mejora del cumplimiento P1

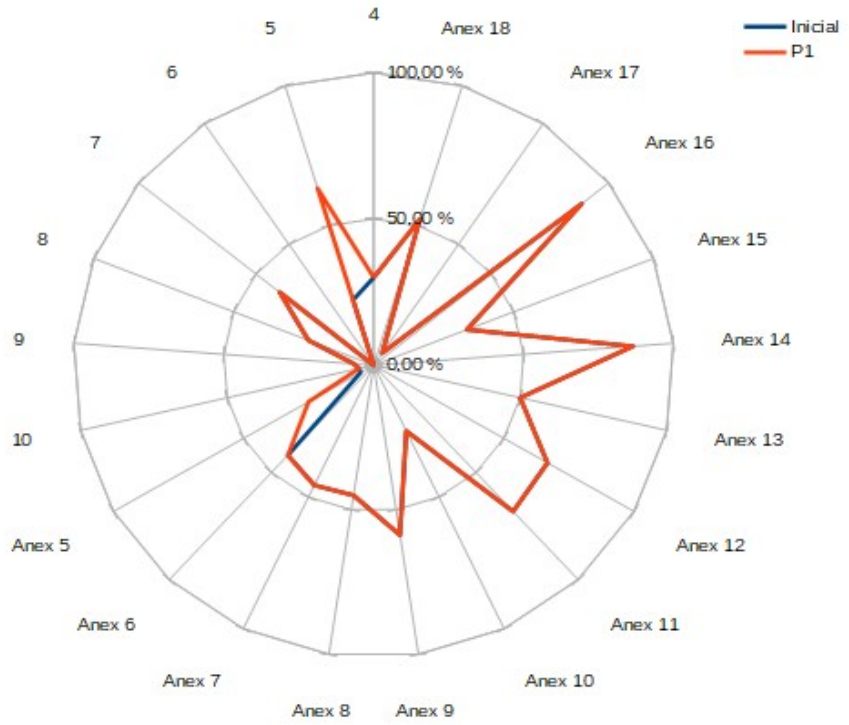


Ilustración 20: Mejora del cumplimiento P1

Como se puede observar, este proyecto es puramente normativo, por lo que el nivel de cumplimiento de dos apartados concretos del análisis diferencial se ven ampliamente mejorados, mientras que no afectan a otros componentes técnicos.

7.2 Proyecto 2 - Formalizar el proceso de acceso a la información, inventariarla y clasificarla

Motivación:	No existen criterios claros acerca de a qué información puede acceder cada usuario generando confusión a la hora de otorgar permisos, dificultando la eliminación de permisos ante cambios de departamentos o salidas de personal, y poniendo en peligro la confidencialidad de la información más sensible
Puntos de la norma ISO 27001 asociados:	Mejora el cumplimiento del punto 7.5 Mejora el cumplimiento del punto A.5.1.1 Mejora el cumplimiento del punto A.8.1.1 Mejora el cumplimiento del punto A.8.2 Mejora el cumplimiento del punto A.9.1.1 Mejora el cumplimiento del punto A.9.4.1
Responsable:	Responsable de seguridad y sistemas
Plazo de implantación:	Largo - 3 meses vista
Coste económico:	Solo recursos propios. Ver detalle de planificación y multiplicar horas * coste persona
Planificación e hitos a cumplir:	- Categorización y clasificación de la información (4 jornadas) - Creación y categorización de los roles que podrán acceder a los tipos de información (2 jornadas) - Documentación de las medidas de seguridad en el tratamiento de la información por los diferentes perfiles, teniendo en cuenta aspectos como preservación, control de accesos, seguridad en el almacenamiento o en las comunicaciones (4 jornadas) - Aprobación por dirección, comunicación y difusión a las partes interesadas (2 jornadas) - Implantación de las medidas técnicas necesarias para cumplir con la nueva normativa (20 jornadas)

	APARTADO DE LA NORMA	% cumpl. Tras PROYECTO1		% cumpl. Tras PROYECTO2	
7	SOPORTE	40%		56%	
7.1	Recursos	3 Definido	90 %	3 Definido	90 %
7.2	Competencia	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
7.3	Concienciación	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
7.4	Comunicación	0 No implementado	0 %	0 No implementado	0 %
7.5	Información documentada	1 Inicial	10 %	3 Definido	90 %

	APARTADO DEL ANEXO	% de cumpl. Tras PROYECTO		% de cumpl. Tras PROYECTO 2	
8	GESTION DE ACTIVOS	45%		73%	
8,2	Clasificacion de la Informacion	5%		90%	
8.2.1	Directrices de clasificación.	1 Inicial	10 %	3 Definido	90 %
8.2.2	Etiquetado y manipulado de la información.	0 No implementado	0 %	3 Definido	90 %
9	CONTROL DE ACCESO	59%		61%	
9,4	Control de acceso a sistemas y aplicaciones	60%		70%	
9.4.1	Restricción del acceso a la información.	2 Intuitivo y repetible	50 %	3 Definido	90 %
9.4.2	Procedimientos seguros de inicio de sesión.	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
9.4.3	Gestión de contraseñas de usuario.	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
9.4.4	Uso de herramientas de administración de sistemas.		N/A		N/A
9.4.5	Control de acceso al código fuente de los programas	3 Definido	90 %	3 Definido	90 %

Tabla 4: Mejora del cumplimiento P2

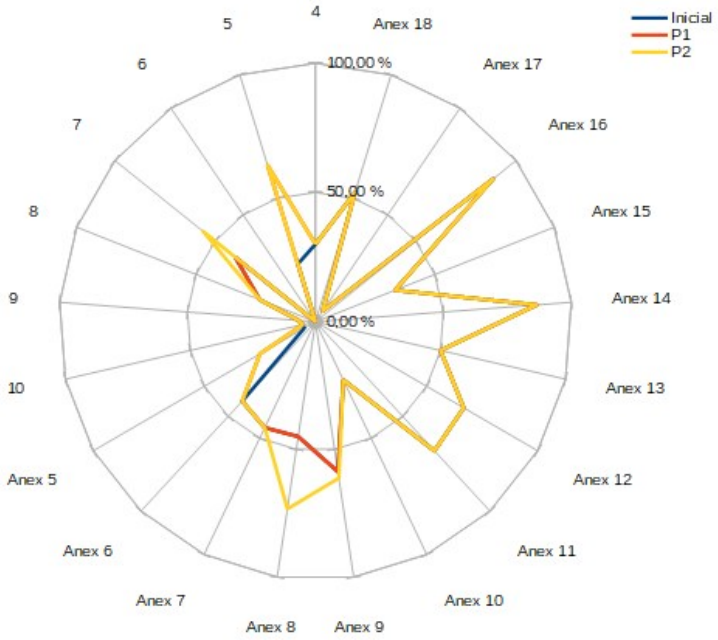


Ilustración 21: Mejora del cumplimiento P2

Como se puede observar, este proyecto mejora más apartados de cumplimiento que el P1, a pesar de que algunos niveles de cumplimiento no se han aumentado por no suponer una mejora suficiente para pasar a un nivel de madurez mayor (por ejemplo en el control A.5.1.1, el cual no se ha incluido tampoco en la tabla).

7.3 Proyecto 3 - Planificación, documentación y control de tareas periódicas

Motivación:	No existe una planificación sobre ciertas tareas asociadas a la seguridad de la información, como pueden ser la revisión de usuarios inactivos, los análisis de vulnerabilidades, la actualización de servidores, la prueba de las copias de seguridad o la comprobación del funcionamiento y actualización de los antivirus, lo que lleva a que se aborden de forma aleatoria según la disponibilidad del personal, y sin quedar trazabilidad de las mismas
Puntos de la norma ISO 27001 asociados:	Mejora el cumplimiento del punto 5.3 Mejora el cumplimiento del punto 8.1 Mejora el cumplimiento del punto 9.1 Mejora el cumplimiento del punto A.5 Mejora el cumplimiento del punto A.6.1.1 Mejora el cumplimiento del punto A.9.2.6 Mejora el cumplimiento del punto A.11.2.4 Mejora el cumplimiento del punto A.12 Mejora el cumplimiento del punto A.13.1 Mejora el cumplimiento del punto A.15.2.1 Mejora el cumplimiento del punto A.16.1 Mejora el cumplimiento del punto A.17.1.3 Mejora el cumplimiento del punto A.18
Responsable:	Departamento de seguridad
Plazo de implantación:	Corto - 3 semanas vista
Coste económico:	Solo recursos propios. Ver detalle de planificación y multiplicar horas * coste persona
Planificación e hitos a cumplir:	- Identificación y planificación de las tareas (4 jornadas) - Procedimentación de cada una de las tareas (10 jornadas) - Puesta en marcha de las tareas y formación al personal implicado (3 jornadas)

	APARTADO DE LA NORMA	% cumpl. Tras PROYECTO2		% cumpl. Tras PROYECTO3	
8	OPERACIÓN	23%		37%	
8.1	Planificación y control operacional	2 Intuitivo y repetible	50 %	3 Definido	90 %
8.2	Apreciación de los riesgos de seguridad de la inf.	1 Inicial	10 %	1 Inicial	10 %
8.3	Tratamiento de los riesgos de seguridad de la inf.	1 Inicial	10 %	1 Inicial	10 %
9	EVALUACIÓN DEL DESEMPEÑO	7%		20%	
9.1	Seguimiento, medición, análisis y evaluación	1 Inicial	10 %	2 Intuitivo y repetible	50 %
9.2	Auditoría Interna	0 No implementado	0 %	0 No implementado	0 %
9.3	Revisión por la dirección	1 Inicial	10 %	1 Inicial	10 %
10	MEJORA	5%		5%	
10.1	No conformidad y acciones correctivas	0 No implementado	0 %	0 No implementado	0 %
10.2	Comprensión de la organización	1 Inicial	10 %	1 Inicial	10 %

	APARTADO DEL ANEXO	% de cumpl. Tras PROYECTO 2		% de cumpl. Tras PROYECTO 3	
5	POLÍTICAS DE SEGURIDAD	25%		90%	
5,1	Directrices de la Dirección en seguridad de la informa	25 %		90 %	
5.1.1	Conjunto de políticas para la seguridad de la información	2 Intuitivo y repetible	50 %	3 Definido	90 %
5.1.2	Revisión de las políticas para la seguridad de la informaci	0 No implementado	0 %	3 Definido	90 %
12	SEGURIDAD EN LA OPERATIVA	67%		71%	
12.4	Registros y supervisión	30%		40%	
12.4.1	Registro de eventos	2 Intuitivo y repetible	50 %	3 Definido	90 %
12.4.2	Protección de la información de registro	1 Inicial	10 %	1 Inicial	10 %
12.4.3	Registros de administración y operación	1 Inicial	10 %	1 Inicial	10 %
12.4.4	Sincronización del reloj	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
12.6	Gestión de la vulnerabilidad técnica	70 %		90 %	
12.6.1	Gestión de las vulnerabilidades técnicas	3 Definido	90 %	3 Definido	90 %
12.6.2	Restricción en la instalación de software	2 Intuitivo y repetible	50 %	3 Definido	90 %
13	SEGURIDAD EN LAS TELECOMUNICACIONES	50%		57%	
13,1	Gestión de la seguridad en las redes.	50 %		63 %	
13.1.1	Controles de red.	3 Definido	90 %	3 Definido	90 %
13.1.2	Mecanismos de seguridad asociados a servicios en red.	1 Inicial	10 %	2 Intuitivo y repetible	50 %
13.1.3	Segregación de redes.	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
15	RELACIÓN CON PROVEEDORES	33%		43%	
15.2	Gestión de la provisión de servicios del proveedor	30 %		50 %	
15.2.1	Control y revisión de la provisión de servicios del proveed	2 Intuitivo y repetible	50 %	3 Definido	90 %
15.2.2	Gestión de cambios en la provisión del servicio del provee	1 Inicial	10 %	1 Inicial	10 %
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PA	5%		13%	
17.1	Continuidad de la seguridad de la información	0 %		17 %	
17.1.1	Planificación de la continuidad de la seguridad de la inform	0 No implementado	0 %	0 No implementado	0 %
17.1.2	Implementar la continuidad de la seguridad de la informaci	0 No implementado	0 %	0 No implementado	0 %
17.1.3	Verificación, revisión, y evaluación de la continuidad de la	0 No implementado	0 %	2 Intuitivo y repetible	50 %
17.2	Redundancias	10 %		10 %	
17.2.1	Disponibilidad de los recursos de tratamiento de la informa	1 Inicial	10 %	1 Inicial	10 %
18	CUMPLIMIENTO	52%		79%	
18.1	Cumplimiento de los requisitos legales y contractuales	71 %		81 %	
18.1.1	Identificación de la legislación aplicable y de los requisitos	2 Intuitivo y repetible	50 %	3 Definido	90 %
18.1.2	Derechos de propiedad intelectual (DPI)	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
18.1.3	Protección de los registros de la organización	3 Definido	90 %	3 Definido	90 %
18.1.4	Protección y privacidad de la información de carácter pers	4 Gestionado	95 %	4 Gestionado	95 %
18.1.5	Regulación de los controles criptográficos		N/A		N/A
18.2	Revisiones de la seguridad de la información	33 %		77 %	
18.2.1	Revisión independiente de la seguridad de la información	0 No implementado	0 %	2 Intuitivo y repetible	50 %
18.2.2	Cumplimiento de las políticas y normas de seguridad	2 Intuitivo y repetible	50 %	3 Definido	90 %
18.2.3	Comprobación del cumplimiento técnico	2 Intuitivo y repetible	50 %	3 Definido	90 %

Tabla 5: Mejora del cumplimiento P3

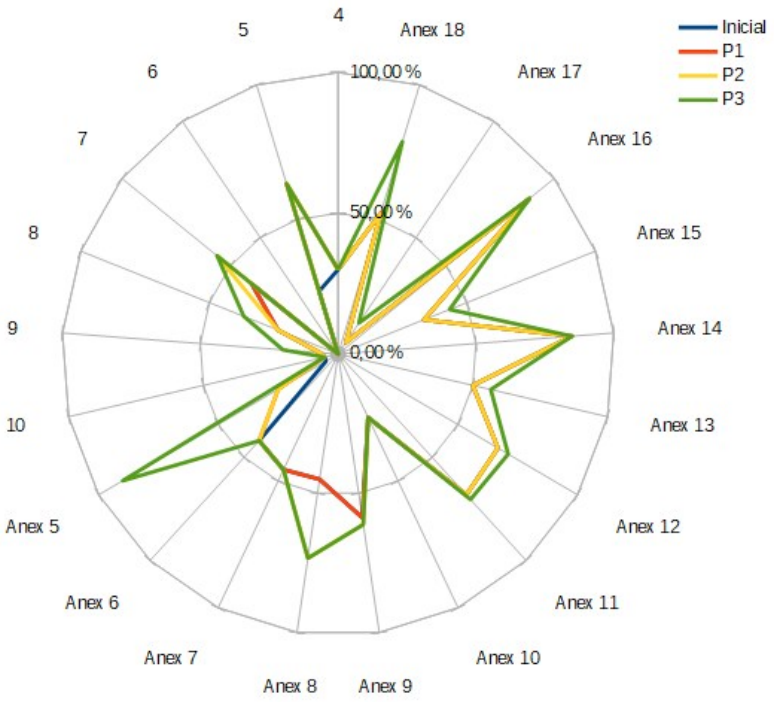


Tabla 6: Mejora cumplimiento P3

Como se puede apreciar esta formalización de tareas afecta significativamente a los niveles de seguridad en diferentes puntos de la norma, ya que muchas tareas que se hacían informalmente (L2 – 50%) pasan a un L3 que supone un 90% de cumplimiento.

7.4 Proyecto 4 - Implantar un control de cambios gestionado

Motivación:	El cada vez mayor volumen de negocio, hace necesaria la contratación de nuevo personal y montaje de nuevos sistemas, lo cual puede derivar en una situación de gestión caótica de los sistemas sin una adecuada gestión de cambios controlada
Puntos de la norma ISO 27001 asociados:	Mejora el cumplimiento del punto A.5.1.1 Mejora el cumplimiento del punto A.6.1.1 Mejora el cumplimiento del punto A.12.1 Mejora el cumplimiento del punto A.12.5 Mejora el cumplimiento del punto A.12.6 Mejora el cumplimiento del punto A.14.2.2 Mejora el cumplimiento del punto A.14.2.3
Responsable:	Departamento de sistemas
Plazo de implantación:	Corto - 3 semanas vista
Coste económico:	Solo recursos propios. Ver detalle de planificación y multiplicar horas * coste persona + herramientas de software libre
Planificación e hitos a cumplir:	- Diseño del procedimiento de gestión de cambios (6 jornadas) - Búsqueda, instalación y configuración de herramienta de seguimiento (4 jornadas) - Formación al personal afectado e implantación progresiva (5 jornadas)

	APARTADO DEL ANEXO	% de cumpl. Tras PROYECTO 3		% de cumpl. Tras PROYECTO 4	
12	SEGURIDAD EN LA OPERATIVA	67%		77%	
12.1	Procedimientos y responsabilidades operacionales	71%		81%	
12.1.1	Documentación de procedimientos de operación	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
12.1.2	Gestión de cambios	2 Intuitivo y repetible	50 %	3 Definido	90 %
12.1.3	Gestión de capacidades	3 Definido	90 %	3 Definido	90 %
12.1.4	Separación de los recursos de desarrollo, prueba y operac	4 Gestionado	95 %	4 Gestionado	95 %
12.5	Control de software en explotación	50 %		90 %	
12.5.1	Instalación del software en explotación	2 Intuitivo y repetible	50 %	3 Definido	90 %
12.6	Gestión de la vulnerabilidad técnica	70 %		90 %	
12.6.1	Gestión de las vulnerabilidades técnicas	3 Definido	90 %	3 Definido	90 %
12.6.2	Restricción en la instalación de software	2 Intuitivo y repetible	50 %	3 Definido	90 %
14	ADQUISICIÓN, DESARROLLO Y MANT	83%		86%	
14.2	Seguridad en el desarrollo y en los procesos de sopor	66 %		76 %	
14.2.1	Política de desarrollo seguro	3 Definido	90 %	3 Definido	90 %
14.2.2	Procedimientos de control de cambios en sistemas	2 Intuitivo y repetible	50 %	3 Definido	90 %
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios	2 Intuitivo y repetible	50 %	3 Definido	90 %
14.2.4	Restricciones a los cambios en los paquetes de software	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
14.2.5	Principios de ingeniería de sistemas seguros	3 Definido	90 %	3 Definido	90 %
14.2.6	Entorno de desarrollo seguro	4 Gestionado	95 %	4 Gestionado	95 %
14.2.7	Externalización del desarrollo de software		N/A		N/A
14.2.8	Pruebas funcionales de seguridad de sistemas	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
14.2.9	Pruebas de aceptación de sistemas	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %

Tabla 7: Mejora del cumplimiento P4

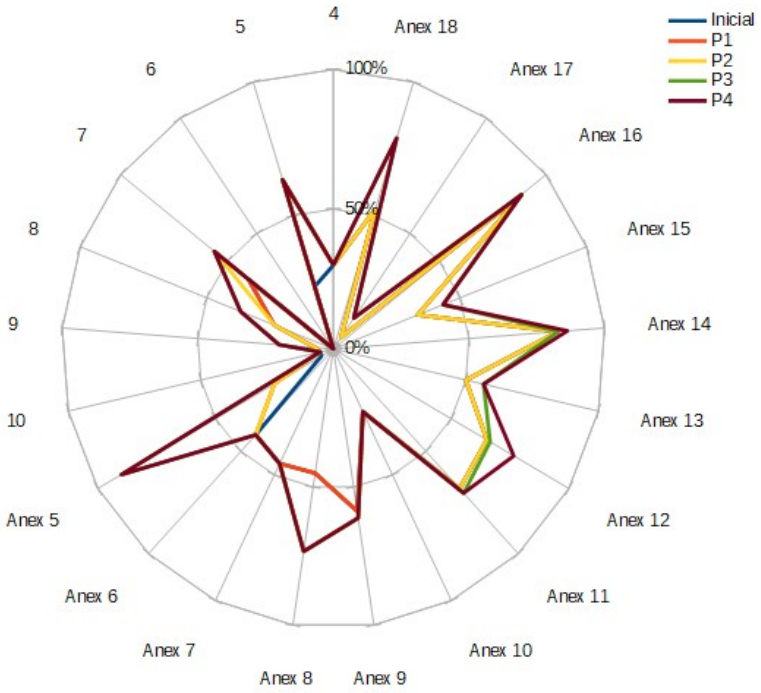


Ilustración 22: Mejora del cumplimiento P4

Como era de esperar, este proyecto no mejora sustancialmente el nivel global de cumplimiento, aunque junto con ciertos controles clave o estratégicos, la mejora en cuanto a la seguridad de la información es notable.

7.5 Proyecto 5 - Cifrado de la información sensible

Motivación:	Se dispone de información que debe ser protegida frente a accesos no autorizados de terceros y e incluso personal interno. Para evitar filtraciones, robos de información, o uso malicioso de información privilegiada, se decide cifrar las bases de datos de apuestas, de información estratégica y las correspondientes copias de seguridad
Puntos de la norma ISO 27001 asociados:	Mejora el cumplimiento del punto 7.5.3 Mejora el cumplimiento del punto A.8.2.2 Mejora el cumplimiento del punto A.9.1.1 Mejora el cumplimiento del punto A.9.4.1 Mejora el cumplimiento del punto A.10
Responsable:	Departamento de sistemas
Plazo de implantación:	Corto - 3 semanas vista
Coste económico:	Presupuesto de 3000€ anuales para licencia de software de cifrado. El resto de recursos serán propios. Ver detalle de planificación y multiplicar horas * coste persona
Planificación e hitos a cumplir:	- Análisis de diferentes soluciones (10 jornadas) - Realizar pruebas en entorno aislado (5 jornadas) - Despliegue progresivo en producción (5 jornadas)

	APARTADO DEL ANEXO	% de cumpl. Tras PROYECTO 4		% de cumpl. Tras PROYECTO 5	
9	CONTROL DE ACCESO	61%		67%	
9,1	Requisitos de negocio para el control de accesos	30 %		50 %	
9.1.1	Política de control de accesos.	2 Intuitivo y repetible	50 %	3 Definido	90 %
9.1.2	Control de acceso a las redes y servicios asociados.	1 Inicial	10 %	1 Inicial	10 %
9,4	Control de acceso a sistemas y aplicaciones	70%		71%	
9.4.1	Restricción del acceso a la información.	3 Definido	90 %	4 Gestionado	95 %
9.4.2	Procedimientos seguros de inicio de sesión.	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
9.4.3	Gestión de contraseñas de usuario.	2 Intuitivo y repetible	50 %	2 Intuitivo y repetible	50 %
9.4.4	Uso de herramientas de administración de sistemas.		N/A		N/A
9.4.5	Control de acceso al código fuente de los programas	3 Definido	90 %	3 Definido	90 %
10	CRIPTOGRAFÍA	25%		90%	
10,1	Directrices de la Dirección en seguridad de la informa	25 %		90 %	
10,1,1	Política de uso de controles criptográficos	0 No implementado	0 %	3 Definido	90 %
10,1,2	Gestión de claves	2 Intuitivo y repetible	50 %	3 Definido	90 %

Tabla 8: Mejora del cumplimiento P5

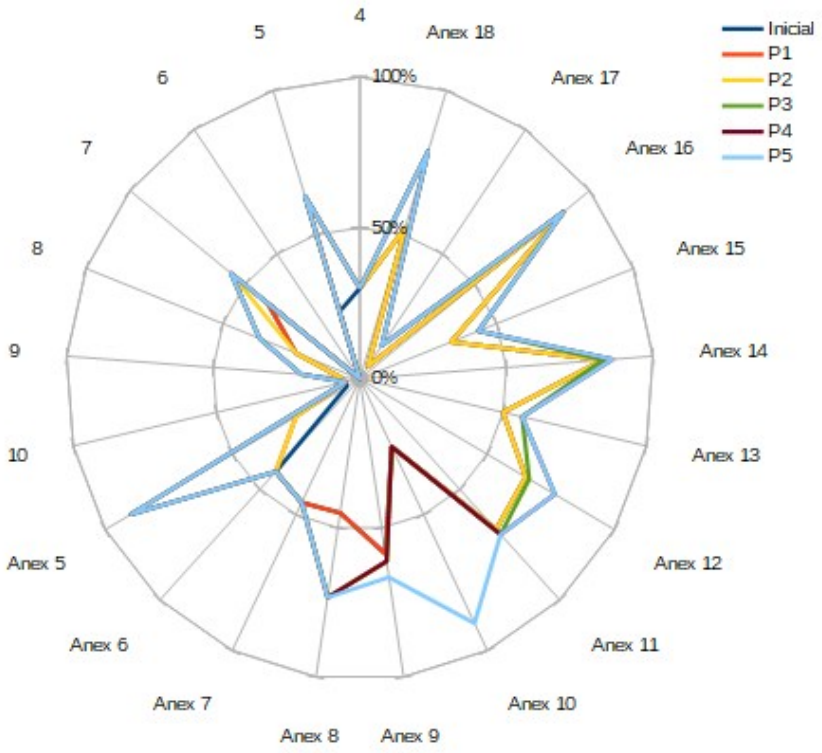


Ilustración 23: Mejora del cumplimiento P5

Tal y como era de esperar, el presente proyecto ha mejorado sustancialmente los niveles de cumplimiento del dominio de control 10 referente al uso de cifrado, sin afectar significativamente al resto de dominios.

7.6 Proyecto 6 – Aproximación a la continuidad de negocio

Motivación:	No se cuenta con equipos de respaldo para los principales servidores ni de la electrónica de red esencial para prestar el servicio en caso de contingencia. Se debería adquirir equipamiento para poder hacer frente a una situación de crisis en parte de la infraestructura TI, aunque no fuera con el 100% de los servicios o capacidad
Puntos de la norma ISO 27001 asociados:	Mejora el cumplimiento del punto A.5.1.1 Mejora el cumplimiento del punto A.17
Responsable:	Departamentos de dirección, seguridad y de sistemas
Plazo de implantación:	Largo - 6 meses vista
Coste económico:	Presupuesto de 15000€ para la compra de equipos de virtualización + electrónica de red + licencias que puedan soportar los procesos básicos de negocio. El resto de recursos serán propios. Ver detalle de planificación y multiplicar horas * coste persona
Planificación e hitos a cumplir:	- Identificación de los servicios e información críticos y los niveles mínimos de funcionamiento deseado (2 jornadas) - Identificación de la tecnología necesaria óptima y equipamiento necesario (7 jornadas) - Diseño del plan de continuidad con los futuros medios a adquirir (8 jornadas) - Compra y puesta en marcha de los nuevos sistemas (24 jornadas) - Pruebas de la nueva infraestructura y del plan de continuidad (4 jornadas)

	APARTADO DEL ANEXO	% de cumpl. Tras PROYECTO 5		% de cumpl. Tras PROYECTO 6	
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PA	13%		90%	
17.1	Continuidad de la seguridad de la información	17 %		90 %	
17.1.1	Planificación de la continuidad de la seguridad de la info	0 No implementado	0 %	3 Definido	90 %
17.1.2	Implementar la continuidad de la seguridad de la inform	0 No implementado	0 %	3 Definido	90 %
17.1.3	Verificación, revisión, y evaluación de la continuidad de	2 Intuitivo y repetible	50 %	3 Definido	90 %
17.2	Redundancias	10 %		90 %	
17.2.1	Disponibilidad de los recursos de tratamiento de la infor	1 Inicial	10 %	3 Definido	90 %

Tabla 9: Mejora del cumplimiento P6

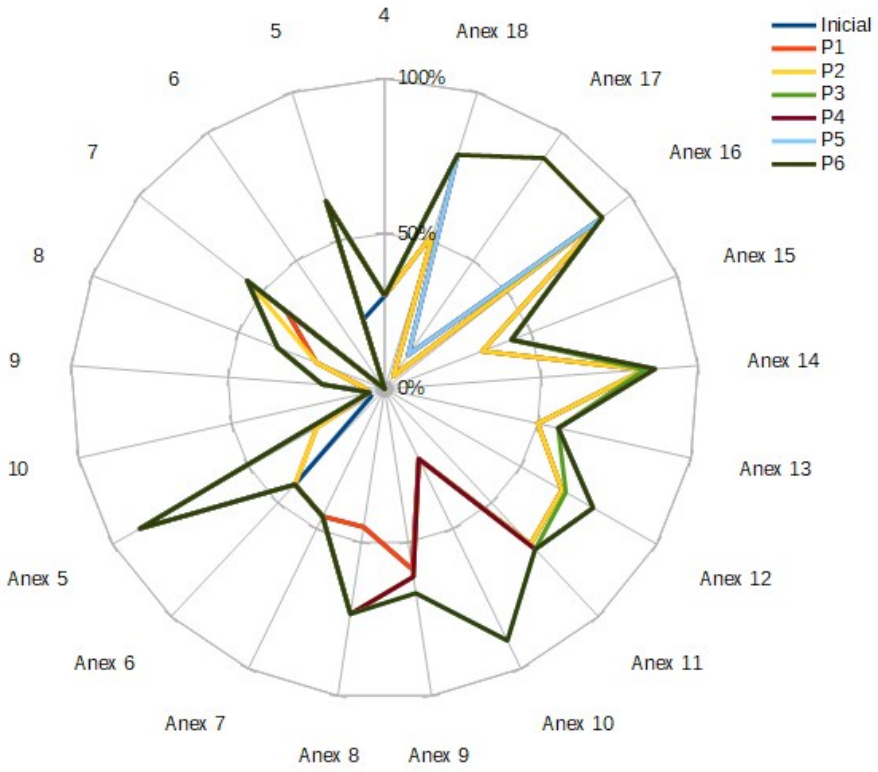


Ilustración 24: Mejora del cumplimiento P6

Si bien con este proyecto el proceso de continuidad ha pasado a estar definido, lo cual es un nivel de madurez adecuado, la infraestructura de respaldo continuará estando en el mismo edificio por lo que en futuras iteraciones del PDCA deberá considerarse continuar evolucionando el PCN para mejorar los niveles de resiliencia de Divertiapuesta.

7.7 Planificación

A continuación se muestra un diagrama resumen con la planificación de los diferentes proyectos en semanas.

Si bien varios se pueden abordar en paralelo, con el fin de evitar un impacto en la carga de trabajo del personal, se ha decidido abordarlos secuencialmente:

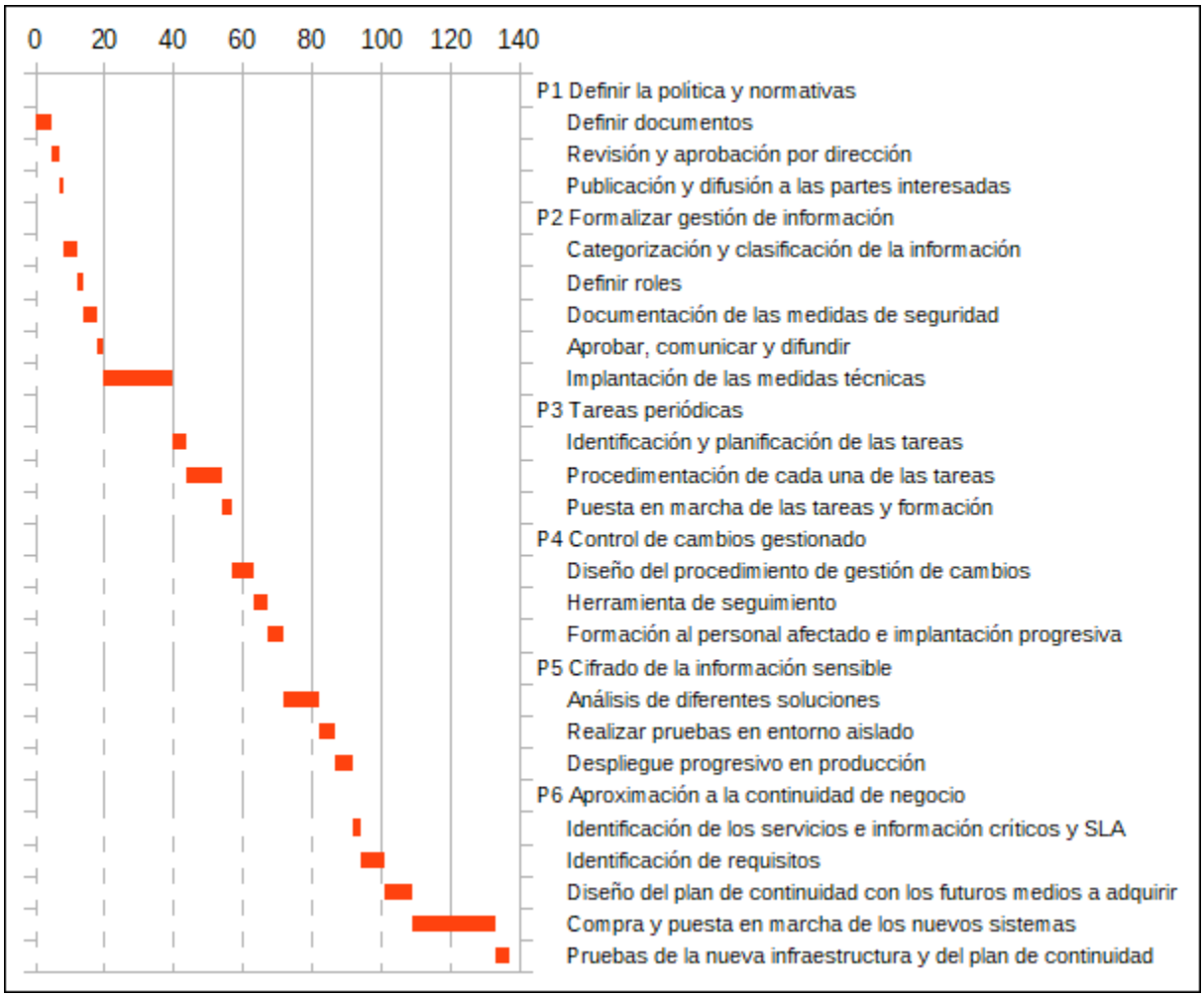


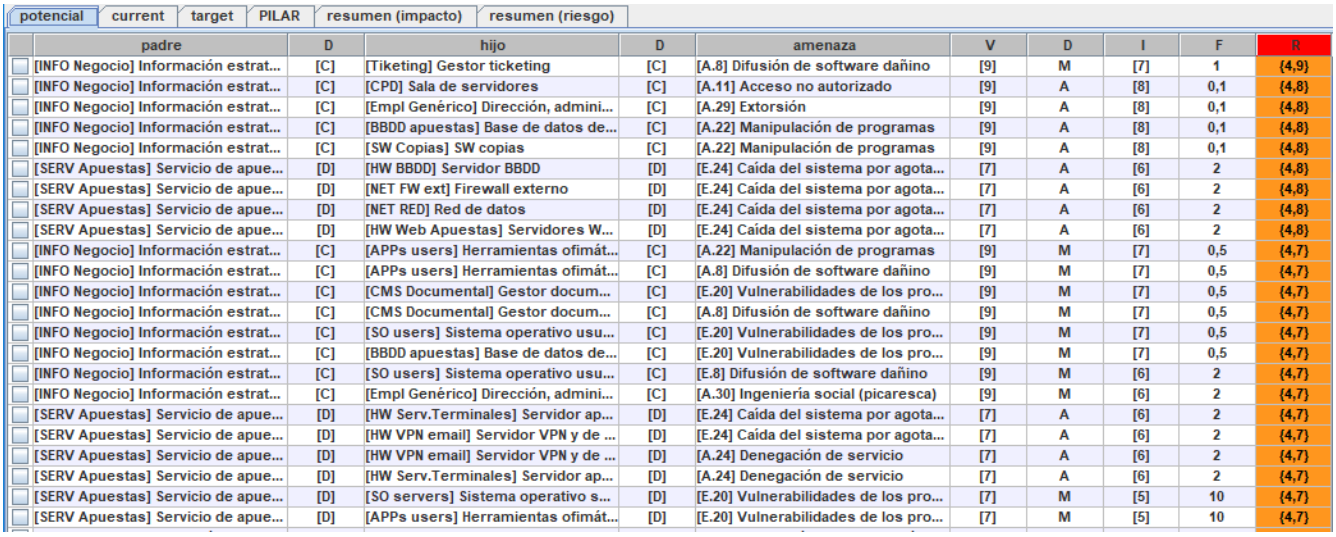
Ilustración 25: Planificación de proyectos en jornadas

7.8 Análisis del nivel de riesgo residual

Una vez estimados los beneficios que se conseguirán con las diferentes opciones de tratamiento de riesgo planteadas, se han actualizado los valores en la herramienta PILAR para obtener una estimación de los nuevos niveles de riesgo.

Para ello se han modificado los parámetros de probabilidad o impacto, según el tipo de medidas que se van a implantar, por ejemplo, para el mayor riesgo del análisis, que era difusión de software dañino en la base de datos de apuestas, los proyectos planteados harán que se revisen los antivirus periódicamente (se reduce la probabilidad de infección), y que se disponga de una copia de la base de datos para contingencia (reduciendo el impacto).

Ya que ambas tablas son muy voluminosas, se adjunta la versión del análisis con los nuevos valores, mostrando a continuación la parte alta de la tabla de riesgos donde se aprecia que se han reducido todos por debajo de 5, un buen umbral para plantear a la dirección que asuma:



potencial | current | target | PILAR | resumen (impacto) | resumen (riesgo)

padre	D	hijo	D	amenaza	V	D	I	F	R
[INFO Negocio] Información estrat...	[C]	[Tiketing] Gestor ticketing	[C]	[A.8] Difusión de software dañino	[9]	M	[7]	1	{4,9}
[INFO Negocio] Información estrat...	[C]	[CPD] Sala de servidores	[C]	[A.11] Acceso no autorizado	[9]	A	[8]	0,1	{4,8}
[INFO Negocio] Información estrat...	[C]	[Empl Genérico] Dirección, admini...	[C]	[A.29] Extorsión	[9]	A	[8]	0,1	{4,8}
[INFO Negocio] Información estrat...	[C]	[BBDD apuestas] Base de datos de...	[C]	[A.22] Manipulación de programas	[9]	A	[8]	0,1	{4,8}
[INFO Negocio] Información estrat...	[C]	[SW Copias] SW copias	[C]	[A.22] Manipulación de programas	[9]	A	[8]	0,1	{4,8}
[SERV Apuestas] Servicio de apue...	[D]	[HW BBDD] Servidor BBDD	[D]	[E.24] Caída del sistema por agota...	[7]	A	[6]	2	{4,8}
[SERV Apuestas] Servicio de apue...	[D]	[NET FW ext] Firewall externo	[D]	[E.24] Caída del sistema por agota...	[7]	A	[6]	2	{4,8}
[SERV Apuestas] Servicio de apue...	[D]	[NET RED] Red de datos	[D]	[E.24] Caída del sistema por agota...	[7]	A	[6]	2	{4,8}
[SERV Apuestas] Servicio de apue...	[D]	[HW Web Apuestas] Servidores W...	[D]	[E.24] Caída del sistema por agota...	[7]	A	[6]	2	{4,8}
[INFO Negocio] Información estrat...	[C]	[APPs users] Herramientas ofimát...	[C]	[A.22] Manipulación de programas	[9]	M	[7]	0,5	{4,7}
[INFO Negocio] Información estrat...	[C]	[APPs users] Herramientas ofimát...	[C]	[A.8] Difusión de software dañino	[9]	M	[7]	0,5	{4,7}
[INFO Negocio] Información estrat...	[C]	[CMS Documental] Gestor docum...	[C]	[E.20] Vulnerabilidades de los pro...	[9]	M	[7]	0,5	{4,7}
[INFO Negocio] Información estrat...	[C]	[CMS Documental] Gestor docum...	[C]	[A.8] Difusión de software dañino	[9]	M	[7]	0,5	{4,7}
[INFO Negocio] Información estrat...	[C]	[SO users] Sistema operativo usu...	[C]	[E.20] Vulnerabilidades de los pro...	[9]	M	[7]	0,5	{4,7}
[INFO Negocio] Información estrat...	[C]	[BBDD apuestas] Base de datos de...	[C]	[E.20] Vulnerabilidades de los pro...	[9]	M	[7]	0,5	{4,7}
[INFO Negocio] Información estrat...	[C]	[SO users] Sistema operativo usu...	[C]	[E.8] Difusión de software dañino	[9]	M	[6]	2	{4,7}
[INFO Negocio] Información estrat...	[C]	[Empl Genérico] Dirección, admini...	[C]	[A.30] Ingeniería social (picaresca)	[9]	M	[6]	2	{4,7}
[SERV Apuestas] Servicio de apue...	[D]	[HW Serv.Terminales] Servidor ap...	[D]	[E.24] Caída del sistema por agota...	[7]	A	[6]	2	{4,7}
[SERV Apuestas] Servicio de apue...	[D]	[HW VPN email] Servidor VPN y de ...	[D]	[E.24] Caída del sistema por agota...	[7]	A	[6]	2	{4,7}
[SERV Apuestas] Servicio de apue...	[D]	[HW VPN email] Servidor VPN y de ...	[D]	[A.24] Denegación de servicio	[7]	A	[6]	2	{4,7}
[SERV Apuestas] Servicio de apue...	[D]	[HW Serv.Terminales] Servidor ap...	[D]	[A.24] Denegación de servicio	[7]	A	[6]	2	{4,7}
[SERV Apuestas] Servicio de apue...	[D]	[SO servers] Sistema operativo s...	[D]	[E.20] Vulnerabilidades de los pro...	[7]	M	[5]	10	{4,7}
[SERV Apuestas] Servicio de apue...	[D]	[APPs users] Herramientas ofimát...	[D]	[E.20] Vulnerabilidades de los pro...	[7]	M	[5]	10	{4,7}

Tabla 10: Riesgo residual

8 Auditoría de cumplimiento

En el presente punto se ha llevado a cabo una auditoría de cumplimiento para conocer de forma independiente el nivel de cumplimiento del SGSI.

Esta auditoría, a pesar de haber sido realizada por un tercero, se ha hecho desde el contexto de una auditoría interna, la cual busca además de verificar el cumplimiento, tratar de aportar información sobre partes mejorables del sistema, más allá de lo que una auditoría de certificación reflejaría.

Es por ello que han aparecido numerosas oportunidades de mejora, y que se han documentado los hallazgos tanto para cumplimientos como incumplimientos, siendo estos últimos los únicos que aparecen en las auditorías de certificación.

Cabe destacar que los puntos marcados como “oportunidad de mejora” y “observaciones”, si bien no siempre reflejan una clara no conformidad, deberían ser abordados de forma similar a las *no conformidades*, ya que son susceptibles de evolucionar hasta *no conformidad*.

Puede encontrarse el análisis de cada uno de los controles revisados en el documento “*Anexo XIII - Auditoría de cumplimiento*”.

9 Anexo I – Listado de documentación adjunta

Listado de documentación anexa:

Anexo I - Detalle del análisis diferencial

Anexo II - Política de seguridad

Anexo III - Procedimiento de auditoría interna

Anexo IV - Gestión de indicadores

Anexo V - Procedimiento de revisión por dirección

Anexo VI – Roles y responsabilidades

Anexo VII - Metodología de análisis de riesgos

Anexo VIII - Declaración de aplicabilidad

Anexo IX – Evolución de cumplimiento

Anexo X – AR inicial

Anexo XI – AR tras proyectos

Anexo XII – Tratamiento de riesgos

Anexo XIII - Auditoría de cumplimiento

10 Bibliografía

Información genérica sobre normas ISO: http://es.wikipedia.org

Información genérica y ejemplos sobre documentación de la norma: www.iso27000.es

Ejemplo de política de seguridad: https://www.trevenque.es/wp-content/uploads/2017/03/POL%C3%8DTICA-DE -SEGURIDAD-DE -LA-INFORMACI%C3%93N.pdf

Ejemplo de política de seguridad: https://www.caroycuervo.gov.co/recursos/6.1.POLITICA_DE_SEGURIDAD_ICC_0.pdf

MAGERIT v3:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Manual aplicación PILAR: http://www.ar-tools.com/es/tools/pilar/v71/doc.html