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

Empresa de videojuegos móviles XXX

Adrian Belmonte Martín

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

Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio José Segovia Henares

Profesor responsable de la asignatura: Carles Garrigues Olivella

Centro: Universitat Oberta de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013*
Nombre del autor:	*Adrián Belmonte Martín*
Nombre del consultor/a:	*Antonio José Segovia*
Nombre del PRA:	--
Fecha de entrega (mm/aaaa):	06/06/2016
Titulación::	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Idioma del trabajo:	*Castellano*
Palabras clave	*ISO 27000, Activo, Riesgo, Auditoría cumplimiento*

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

El presente proyecto ha consistido en una elaboración de un plan de implementación de la normativa ISO 27001 en la empresa de videojuegos XXX.

Dicha empresa no contaba con ningún tipo de estudio previo. La auditoría se ha dividido en distintas fases>

La primera fase consistió en un análisis de la empresa en distintos aspectos (funcional, organizativo, técnico, procedimental, de riesgos, documentación, etc.).

Una vez recopilada toda esta información, se procedió a realizar un análisis diferencial con la norma ISO 27002 para saber exactamente nuestro punto de partida. Posteriormente se definió un sistema de gestión documental que incluye política de la seguridad, gestión de indicadores, responsabilidades, roles, procedimientos de revisión y declaración de aplicabilidad.

En la fase 3 se procedió a la definición y realización de un análisis de riesgos, siguiendo para ello la metodología MAGERIT, lo cual nos llevó al cálculo del impacto y el riesgo potencial para cada activo.

Como Fase 4, se plantean una serie de proyectos para, por un lado, mitigar los riesgos detectados en el análisis, y por el otro conseguir una mejora en el cumplimiento de la norma. Estos proyectos se encuentran desglosados y planificados tanto de recursos como económicamente.

Finalmente, se realiza una auditoría de cumplimiento, donde se puede observar cómo la organización mejora en los distintos dominios de la seguridad después de la implementación de los proyectos.

Índice

1. Orígenes de la ISO

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 - ahora ISO 9001
- 1992 Publicación BS 7750 - ahora ISO 14001
- 1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información. La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En el año 2004 se publicó la UNE 71502 titulada Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) y que fue elaborada por el comité técnico AEN/CTN 71. Es una adaptación nacional de la norma británica British Standard BS 7799-2:2002. Con la publicación de UNE-ISO/IEC 27001 (traducción al español del original inglés) dejó de estar vigente la UNE 71502 y las empresas nacionales certificadas en esta última están pasando progresivamente sus certificaciones a UNE-ISO/IEC 27001.

1.1 La serie ISO 27000

La seguridad de la información tiene asignada la serie 27000 dentro de los estándares ISO/IEC, los más interesantes para el desarrollo de este proyecto son los siguientes:

ISO 27000: Publicada en mayo de 2009. Contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman.

UNE-ISO/IEC 27001:2007 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Fecha de la de la versión española 29 noviembre de 2007. Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIs deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO 17799).

ISO/IEC 27002: (anteriormente denominada ISO 17799). Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles.

ISO/IEC 27003: En fase de desarrollo; probable publicación en 2009. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requisitos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004: Publicada en diciembre de 2009. Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados.

ISO 27005: Publicada en junio de 2008. Consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335.

ISO 27006: Publicada en febrero de 2007. Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

2. Contextualización

2.1 Selección de la empresa

Para la realización del TFM hemos seleccionado la startup de juegos móviles XXXX, a pesar de contar con sólo 3 años de vida, el lanzamiento de varios juegos con un gran impacto ha levantado el interés de varios inversores y compañías, por lo que se espera que en breve se inicie su expansión o incluso su posible compra por una gran desarrolladora.

Al estar ganando peso en la comunidad, la dirección se está preocupando cada vez más por la seguridad de la información, y ha decidido tomar cartas en el asunto de manera activa. Esto no es del todo casual, ya que, al estar cada vez mejor posicionado en el sector, el riesgo de poder sufrir un posible incidente de seguridad (cosa que ya ha ocurrido, pero ha sido silenciado) y que pueda tener un impacto negativo en la imagen de la empresa, como una denegación de servicio que impida a los

usuarios usar las aplicaciones o un robo del código por parte de terceros o empresas (espionaje industrial).

Por tanto, es necesario mitigar cualquier tipo de evento que pudiera dar al traste con cualquier negociación que se pudiera llevar a cabo en el futuro y poder vender una buena imagen ante los inversores.

Por otra parte, la implementación de un sistema de gestión de la seguridad de la información, ahora que la empresa no se encuentra en expansión, permitirá integrar la cultura de seguridad en la misma de una manera temprana y eficaz, haciendo que este sistema pueda crecer con la misma.

2.2 Descripción de la empresa

Las características más reseñables de la empresa, que son interesantes desde un punto de vista de seguridad son las siguientes:

- Actualmente cuenta con 30 empleados, entre los que se encuentran varios freelance, algunos de los cuales son requeridos puntualmente. Cada departamento tiene empleados en ambos lugares, por lo que es común la realización de videoconferencias y otros tipos de actividades en la red
- Las nóminas y las gestiones laborales las realiza una gestora.
- Dos oficinas: Una en Barcelona, la otra recientemente abierta en Copenhague. En Barcelona es donde se encuentran mayor cantidad de empleados (20). Ambas oficinas tienen similar estructura interna, a pesar de que la oficina de Barcelona es un poco mayor que la danesa

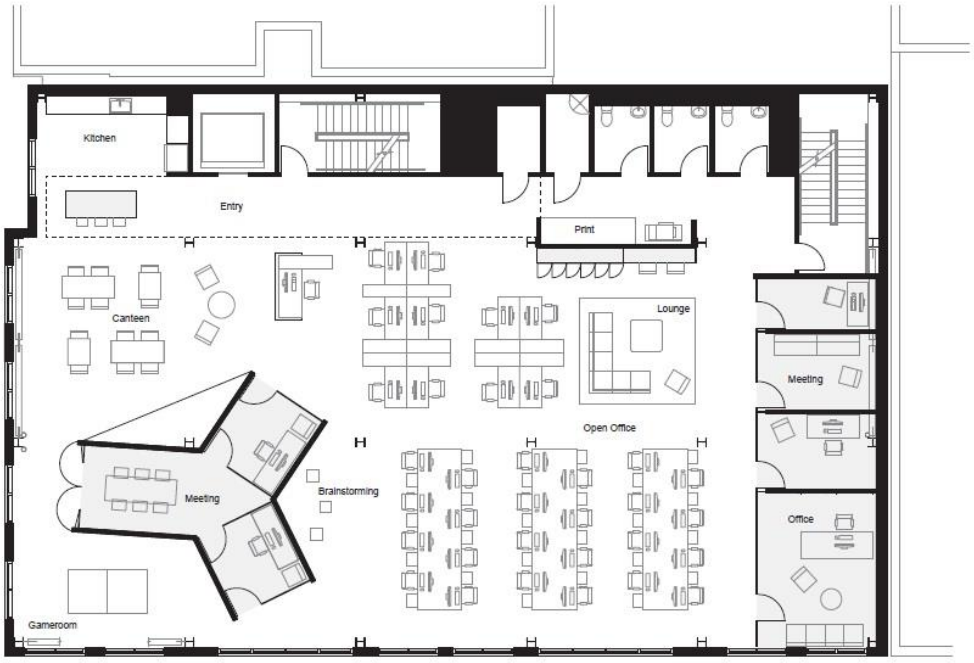

Ilustración 1 Plano de las oficinas

- Se promueve el trabajo desde casa, la compañía provee de ADSL en casa de los empleados, así como un dispositivos para la conexión 3G/4G.
- Dentro de la oficina no existe puesto fijo, cada puesto de trabajo tiene un puerto LAN y, si es necesario, es posible conectarse mediante WIFI.
- Se promueve el BYOD ("Bring your own device"), al entrar a cada empleado se le proporciona un presupuesto para que elija su propio equipo portatil, tablet y móvil, sin que existan demasiadas limitaciones en cuanto a las plataformas ya que todas las herramientas usadas se encuentran disponibles fácilmente para todas ellas.

2.3 Sistemas

Se intenta minimizar la cantidad de sistemas a mantener, es por ello que muchos sistemas se encuentran desplegados en la nube o usando servicios en la misma, sin embargo, se ha optado por mantener sistemas dentro de la organización. Así por ejemplo:

- Sistemas de integración continua y de pruebas unitarias: Desplegado en los sistemas de la empresa
- Repositorios de código (GitHub): En GitHub, acceso privado
- Servidores de correo: Uso de Gmail mediante google apps
- CRM: Desplegado en los sistemas de la empresa
- Nóminas y datos de negocio: Almacenados en servidores de la empresa
- Datos de clientes: Almacenados en servidores de la empresa
- Sistemas VPN para interconexión de oficinas: Desplegados en la empresa
- Gestores de tareas y gestión de equipo: Cloud

- Servidores Web: Desplegado como servicio Amazon
- Firewall: Desplegado localmente
- Sistemas perimetrales (IDS/IDS): Desplegados en la empresa
- Sistema de correlación de eventos
- Plataforma recolección y correlación de eventos: Desplegados en la empresa
- Almacenaje de información y documentación de trabajo: Cloud
- Almacenaje de imágenes (diseño gráfico): Cloud
- Paquetes de office (Libreoffice)
- Estadísticas de juego de los usuarios (comportamiento, horas de juego, etc…): Elastic Cloud Storage

2.4 Áreas de negocio

La empresa tiene una estructura bastante horizontal, la dirección (CEOs) a veces hace funciones de project manager e incluso se implica en el desarrollo de los distintos productos, aunque este hecho está cambiando últimamente debido al aumento de responsabilidades en los puestos de dirección.

2.4.1 Área de desarrollo de producto ("Core")

La coordinación del área de desarrollo de producto la realiza directamente la dirección (realmente son los Productores, Game director), se encuentra dividido en:

- Desarrollo: Liderados por un Technical Manager, y según la experiencia y la implicación varias categorías. Se encargan del desarrollo de la lógica de los distintos videojuegos
- Diseño: Diseño del producto y de las distintas fases del juego
- Arte: Encontramos aquí todo lo relacionado con el diseño gráfico del producto y la web, así como la realización de animaciones.
- QA / testing: Encargados de realizar y programar las pruebas al producto, así como realizar los controles de calidad pertinentes.

Ilustración 2 Estructura de área de desarrollo ("Core")

2.4.2 Área de sistemas e infraestructura

- Sistemas: Encargados de mantener y dar soporte a la infraestructura tanto en las oficinas (VPN, Cortafuegos, etc...) como en Cloud.
- Deployment y releases: Encargados de mantener y optimizar los sistemas de integración continua, integración de pruebas unitarias, etc...

2.5 Metodología de trabajo

La metodología de trabajo en esta empresa viene siguiendo una pauta cada vez más habitual en muchas nuevas empresas, con una mayor flexibilidad para el empleado y una mayor horizontalidad en la organización del trabajo, centrándose más en la responsabilidad de la ejecución de las tareas que en que el trabajador se encuentre en su sitio a una hora determinada.

Por tanto, ningún empleado tiene un horario definido, permitiendo y apoyando el trabajo desde casa quedando las oficinas para quien necesite realizar alguna reunión, trabajar en grupos, o por que prefiera estar en un entorno laboral. Todas las zonas de trabajo son abiertas. Las oficinas se encuentran abiertas de 8 de la mañana a 18 horas, se encuentran en un bloque de oficinas ambas y se encuentran vigiladas por la seguridad del edificio.

Se intenta que todos los documentos y el material de trabajo necesario se encuentren accesible para los empleados que lo necesiten. Para ello se ha intentado simplificar desde un principio la administración de sistemas propios intentando llevar cada vez más sistemas a la nube. A la hora de producir material (Documentos, gráficos, etc…) al tener cada usuario un sistema distinto se intenta que los formatos generados sean lo más abiertos posibles, a ser posible abiertos, lo que facilita el cruce de información entre plataformas y permite un considerable ahorro en licencias.

En ocasiones, se contrata personal freelance para trabajos puntuales, a los que, dependiendo de las necesidades, se les permite el acceso a repositorios y sistemas. Se intenta mantener un sistema de mínimo privilegio, cosa que no siempre se consigue.

En cuanto a la organización jerárquica, como hemos comentado, se intenta enfocar el trabajo en equipos más que personas concretas. Sin embargo, la dirección (las personas fundadoras de la empresa) tiene un rol bastante más relevante que el resto a la hora de toma de decisiones.

En cuanto al modelo de negocio, la empresa tiene desarrollados varios videojuegos de cierto éxito en plataformas IOS y Android. Hay tres tipos de Juegos:

- Free-to-Play: El juego se puede descargar e instalar sin realizar pago alguno. Durante el desarrollo del mismo se muestran anuncios que permiten monetizar el desarrollo
- Compra directa: Se paga una cantidad a la hora de descargar el juego. El usuario tiene posteriormente acceso completo a todas las características del juego
- Micropagos: Se permite la descarga del juego completo y funcionalidad completa, pero para ganar cierta ventaja en el mismo se deben realizar pagos de pequeña cantidad que permiten obtener recursos, mejoras o pasar de nivel.

Otro valor añadido de la empresa es el comportamiento de los usuarios, la empresa recopila información sobre ciertos patrones de comportamiento de los usuarios (horas de juego, tiempo, franja horaria, localización, pais, amigos de facebook…), cuya correlación pueden permitir tener una importante ventaja competitiva en un futuro.

Uno de los proyectos de la empresa pasa por el uso de estos datos, pero por el momento, se limitan a ser guardados en un proveedor en la nube (Elastic Cloud Storage).

2.6 Procesos de trabajo

El proceso general de trabajo es en grandes rasgos como se muestra en la siguiente ilustración.

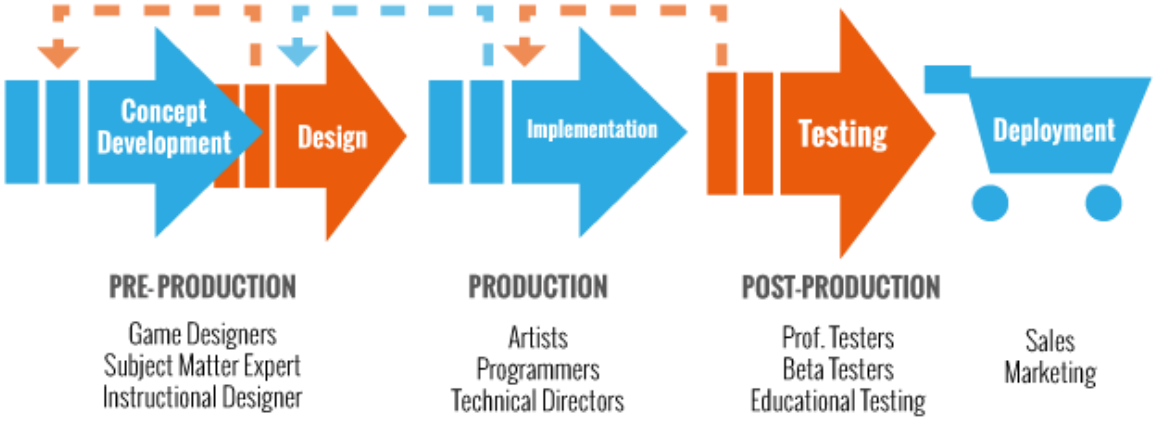

Ilustración 3 Proceso general de trabajo

El código fuente y los recursos se encuentran en un GitHub privado, a la hora de realizar una release se envía al sistema de integración continua, que integra los cambios, comprueba la consistencia de todos ellos y les realiza pruebas unitarias (entre las que se encuentran varias de seguridad). El sistema de integración se encuentra desplegado en las oficinas de Barcelona, aunque es accesible desde el exterior.

El despliegue se realiza en entornos de prueba, los betatesters se encargan de probar las nuevas versiones de los juegos. Si todo es correcto, se procede al lanzamiento en la "store" correspondiente.

Por su parte, la gestión de la documentación y del equipo (tareas) se realiza con varios servicios en la nube.

2.7 Estado general de la seguridad física de las oficinas

Los CPDs de las dos oficinas están situadas en una habitación separada dentro de las mismas con único método de acceso mediante llave, la cual está al resguardo del responsable de uno de los directivos Ambos CPDs disponen en la sala de un sistema de aire acondicionado para mantener un control de temperatura y humedad.

Las dos sedes de la empresa tienen contratada una línea de cable de alta velocidad. La conexión entre las dos oficinas se realiza mediante conexión VPN. La red no se encuentra segmentada de ninguna manera.

Como hemos indicado anteriormente, ambas oficinas se encuentran en un bloque de oficinas. No existe ningún tipo de control de acceso. La seguridad física corre a cargo del dueño del edificio y es parte del alquiler.

3. Alcance y Objetivos del plan director

Durante los últimos meses, la empresa ha venido desarrollando exitosamente un sistema de desarrollo de negocio, dentro del contexto de BPM (Business Process management) basado en Business Intelligence (BI).

Debido a diversas situaciones, políticas, inherentes al negocio y sociales, la dirección sabe que la seguridad va a ser un proceso vital durante los próximos años y, pretende, si todo va según lo planeado realizar una gran inversión en seguridad a medio plazo.

Es por ello que teniendo un BPM desarrollado a pequeña escala quieren integrar en ella la inteligencia de amenazas (Threat Intelligence) con el objetivo de tener a su alcance, en un futuro más información para poder invertir convenientemente en sistemas o procesos específicos.

A grandes rasgos, los objetivos del plan director a desarrollar son los siguientes:

- Identificar, calificar y hacer un tratamiento adecuado de los riesgos que puedan impactar negativamente la información, los procesos y la organización sobre las redes de telecomunicaciones y los servicios asociados al segmento de hogares, implementando las salvaguardas que permitan reducir el nivel de exposición frente a ataques informáticos.
- Implementación de un equipo de seguridad proactivo (Threat Intelligence) encargado de recolectar y modelar amenazas que afecten a la compañía, incidentes de seguridad mediante las distintas plataformas desplegadas y filtración de datos.
- Mitigar lo máximo posible cualquier incidente de seguridad. Dar el valor estratégico que la seguridad de la información tiene. La dirección teme que pueda ocurrir cualquier evento que pueda poner en peligro o afectar a la imagen de la compañía. Para ello los indicadores de respuesta a incidentes se van a modelar de la siguiente manera:
- Triage/categorización del incidente de seguridad: Máximo 12 horas
- Incidentes categorizados de nivel Alto: 12 horas
- Incidentes categorizados Medio: 24 horas
- Incidentes categorizados Bajo: 48 horas
- Proteger la empresa y la información que posee, para ello se debe implementar y probar un plan de continuidad de negocio. En caso de catástrofe, la empresa deberá estar capacitada para operar parcialmente en 72 horas máximo y estar recuperada completamente en una semana máximo.
- Dar cumplimiento a la normatividad y legislación vigente. Para ello, se propone como objetivo no tener denuncias por incumplimiento de normativa o legislación.
- Fomentar la cultura organizacional, la capacitación y toma de conciencia en seguridad informática mediante la implementación de cursos de formación que serán medidos a través de exámenes. Se propone como objetivo que al menos el 80% de los empleados superen correctamente los ejercicios.

El alcance del SGSI englobará todos los procesos de negocio y de desarrollo de la empresa, así como cualquier otra actividad que resulte de la aplicación de esta auditoría con el objetivo de mejorar la seguridad de la organización. Para ello se va a seguir una metodología PDCA:

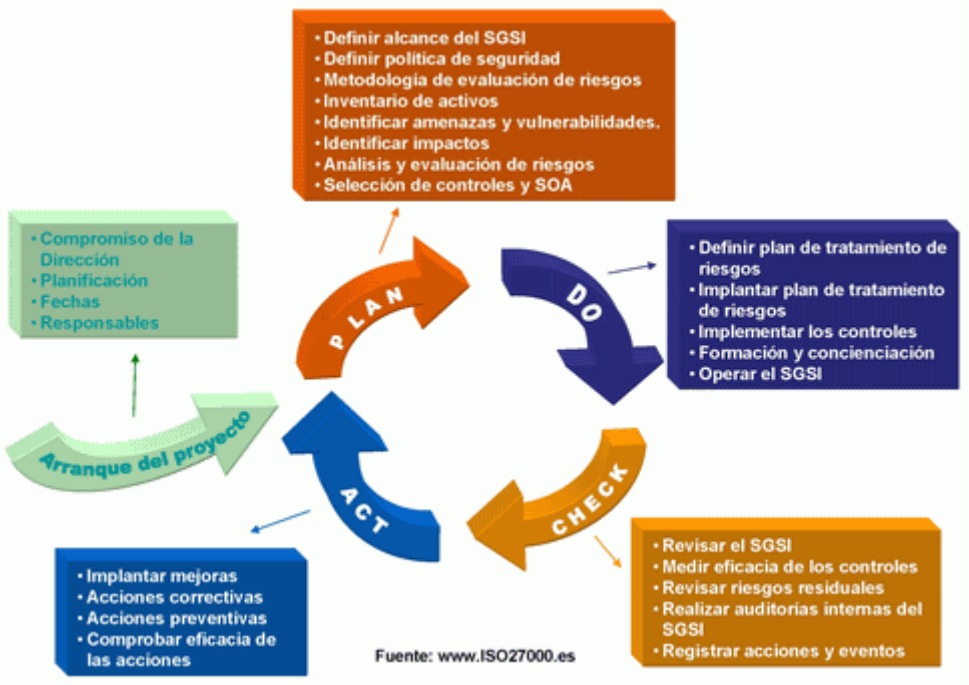

Ilustración 4 Ciclo Deming a aplicar

4. Análisis diferencial

Se realiza a continuación el análisis diferencial de la norma ISO27001 e ISO27002 con respecto al estado actual de la compañía.

Se van a definir los siguientes niveles de cumplimiento:

Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos
L6	N/A	No aplica	

Tabla 1 Niveles de cumplimiento

4.1 Análisis diferencial ISO 27001:2013

En la siguiente tabla se muestra el estado actual de la empresa con respecto a la norma:

Control 27001:2013	Requerimientos	Valoración
4	**Contexto de la organización**	
4,1	**Comprender la organización y su contexto**	
4,2	Comprender las necesidades y expectativas de las partes interesadas	L1
4.2 (a)	Las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información	L0
4.2 (b)	Los requisitos de estas partes interesadas pertinentes a la seguridad de la información.	L0
4,3	Determinación del alcance del sistema de gestión de seguridad de la información	L0
4,4	Información de sistema de gestión de la seguridad	L0
5	**Liderazgo**	
5,1	**Liderazgo y compromiso**	
5.1 (a)	Garantizar la política de seguridad de la información y de los objetivos de seguridad de la información se establecen y son compatibles con la dirección estratégica de la organización;	L0
5.1 (b)	Garantizar la integración de los requisitos del sistema de gestión de seguridad de la información en el los procesos de la organización;	L0
5.1 (c)	Velar por que los recursos necesarios para el sistema de gestión de seguridad de la información están disponibles;	L1
5.1 (d)	Comunicar la importancia de una gestión eficaz de seguridad de la información y de ajustarse a los requisitos del sistema de gestión de seguridad de la información;	L1
5.1 (e)	Garantizar que el sistema de gestión de seguridad de la información alcanza su resultado previsto	L0
5.1 (f)	La dirección y el apoyo a las personas a contribuir a la eficacia de la seguridad de la información sistema de gestión;	L0
5.1 (g)	La promoción de la mejora continua;	L0
5.1 (h)	El apoyo a otras funciones de gestión pertinentes para demostrar su liderazgo, ya que se aplica a su área de responsabilidad.	L0

5,2	La alta dirección debe establecer una política de seguridad de la información que:	L0
5.2 (a)	es apropiada para el propósito de la organización;	L0
5.2 (b)	incluye los objetivos de seguridad de la información (véase 6.2) o proporciona el marco para establecer la información objetivos de seguridad	L0
5.2 (c)	incluye un compromiso de cumplir con los requisitos aplicables relacionados con la seguridad de la información	L0
5.2 (d)	incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información	L0
5.2 (e)	La política de seguridad de la información deberá estará disponible como información documentada;	L0
5.2 (f)	La política de seguridad de la información deberá ser comunicada dentro de la organización;	L0
5.2 (g)	La política de seguridad de la información deberá estar disponible para las partes interesadas, según proceda.	L0
5,3	Funciones de organización, responsabilidades y autoridades	L0
5.3 (a)	garantizar que el sistema de gestión de seguridad de la información se ajusta a los requisitos de la presente Estándar Internacional	L0
5.3 (b)	Informar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.	L0
6	**Planificación**	
6,1	**Acciones para hacer frente a los riesgos y oportunidades**	
6.1.1	Generalidades	
6.1.1(a)	garantizar que el sistema de gestión de seguridad de la información puede alcanzar su resultado previsto (s);	L0
6.1.1 (b)	prevenir o reducir los efectos no deseados; y	L0
6.1.1 (c)	lograr la mejora continua.	L0
6.1.1 (d)	La organización debe planificar las acciones para hacer frente a estos riesgos y oportunidades	L0
6.1.1 (e1)	La organización debe planificar como integrar y poner en práctica las acciones en su sistema de gestión de seguridad de la información procesos	L0
6.1.1 (e2)	La organización debe planificar como evaluar la eficacia de estas acciones.	L0
6.1.2	Evaluación de riesgos de seguridad	
6.1.2 (a1)	establece y mantiene los criterios de riesgo de seguridad de información que incluyen los criterios de aceptación de riesgos	L0

6.1.2 (a2)	establece y mantiene los criterios de riesgo de seguridad de información que incluyen los criterios para la realización de las evaluaciones de riesgos de seguridad de la información;	L0
6.1.2 (b)	se asegura de que las evaluaciones de riesgos de seguridad de información repetidos producen consistente, válida y resultados comparables	L0
6.1.2 (c1)	aplicar el proceso de evaluación de riesgos de seguridad de información para identificar los riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad de la información en el ámbito de la información sistema de gestión de la seguridad	L1
6.1.2 (c2)	identificar a los propietarios de riesgo	L0
6.1.2 (d1)	evaluar las posibles consecuencias que se derivarían si los riesgos identificados en 6.1.2 (c1) fueron a materializarse	L1
6.1.2 (d2)	evaluar la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 (c1)	L0
6.1.2 (d3)	determinar los niveles de riesgo;	L0
6.1.2 (e1)	comparar los resultados de análisis de riesgos con los criterios de riesgo establecidos en 6.1.2 a); y	L0
6.1.2 (e2)	dar prioridad a los riesgos analizados para el tratamiento del riesgo.	L0
6.1.3	Información de tratamiento de riesgos de seguridad	
6.1.3 (a)	seleccionar las opciones de tratamiento de riesgos de seguridad de información adecuados y teniendo en cuenta el riesgo resultados de la evaluación;	L0
6.1.3 (b)	determinar todos los controles que sean necesarios para implementar el tratamiento de los riesgos de seguridad de información opción (s) elegido;	L0
6.1.3 (c)	comparar los controles determinados en 6.1.3 b) anterior con los del Anexo A y comprobar que no es necesario los controles se han omitido;	L0
6.1.3 (d)	producir una Declaración de aplicabilidad que contiene los controles necesarios (véase 6.1.3 b) yc)) y justificación de inclusiones, si están implementadas o no, y la justificación de las exclusiones de los controles del Anexo A;	L0
6.1.3 (e)	formular un plan de información sobre el tratamiento de riesgos de seguridad; y	L0
6.1.3 (f)	obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los propietarios de riesgo ' los riesgos de seguridad de información residuales	L0
6,2	Objetivos de seguridad de la Información y la planificación para alcanzarlos	
6.2 (a)	ser coherente con la política de seguridad de la información;	L0
6.2 (b)	ser medibles (si es posible);	L0

6.2 (c)	tener en cuenta los requisitos de seguridad de la información es aplicable, y los resultados de la evaluación de riesgos y tratamiento de riesgos	L0
6.2 (d)	ser comunicada; y	L0
6.2 (e)	se actualizará según corresponda.	L0
6.2 (f)	lo que será hecho	L0
6.2 (g)	qué recursos serán necesarios;	L0
6.2 (h)	que será responsable;	L0
6.2 (i)	cuando se completará; y	L0
6.2 (j)	Cómo se evaluarán los resultados.	
7	**Soporte**	
7,1	**Recursos**	
7,2	Competencia	
7.2 (a)	determinar la competencia necesaria de la persona (s) que hace el trabajo bajo su control que afecta su rendimiento de seguridad de la información	L1
7.2 (b)	asegurarse de que estas personas son competentes sobre la base de una educación adecuada, capacitación o experiencia	L1
7.2 (c)	en su caso, tomar acciones para adquirir la competencia necesaria, y evaluar la eficacia de las acciones realizadas	L1
7.2 (d)	Retener la información documentada apropiada como evidencia de la competencia.	L1
7,3	Conciencia	
7.3 (a)	la política de seguridad de la información;	L0
7.3 (b)	su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de rendimiento de seguridad mejorada de la información	L0
7.3 (c)	Las consecuencias de que no se ajusten a los requisitos del sistema de gestión de seguridad de la información.	L0
7,4	Comunicación	
7.4 (a)	en el qué comunicar;	L1
7.4 (b)	cuando para comunicarse;	L1
7.4 (c)	con quien comunicarse;	L1
7.4 (d)	quien comunicará;	L1
7.4 (e)	Los procesos mediante los cuales se efectúa la comunicación.	L1
7,5	Información documentada	
7.5.1	General	L1

7.5.1 (a)	La información requerida por esta Norma Internacional documentado; y	L0
7.5.1 (b)	información documentada determinada por la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.	L0
7.5.2	Creación y actualización	L0
7.5.2 (a)	Identificación y descripción (por ejemplo, un título, fecha, autor, o el número de referencia);	L1
7.5.2 (b)	Formato (por ejemplo, el idioma, la versión de software, gráficos) y medios de comunicación (por ejemplo, papel, electrónico);	L1
7.5.2 (c)	La revisión y aprobación de idoneidad y adecuación.	L2
7.5.3	Control de la información documentada	L1
7.5.3 (a)	Asegurar está disponible y adecuado para su uso, donde y cuando sea necesario; y	L1
7.5.3 (b)	Asegurar que está protegido de manera adecuada (por ejemplo, de la pérdida de confidencialidad, uso indebido o pérdida de integridad).	L1
7.5.3 (c)	Asegurar la distribución, acceso, recuperación y uso	L1
7.5.3 (d)	Asegurar almacenamiento y conservación, incluyendo la preservación de la legibilidad	L1
7.5.3 (e)	Asegurar el control de cambios (por ejemplo, control de versiones);	L2
7.5.3 (f)	Asegurar la retención y disposición.	L3
8	**Funcionamiento**	
8,1	**Planificación y control operacional**	
8,2	Evaluación del riesgo de seguridad	L0
8,3	Información de tratamiento de riesgos de seguridad	L0
9	**Evaluación de Rendimiento**	
9,1	Monitoreo, medición, análisis y evaluación	
9.1 (a)	lo que necesita ser monitoreado y medido, incluidos los procesos y controles de seguridad de la información;	L0
9.1 (b)	Determinar los métodos de vigilancia, medición, análisis y evaluación, en su caso, para garantizar resultados válidos	L1
9.1 (c)	Determinar cuándo se llevarán a cabo el seguimiento y medición	L0
9.1 (d)	Determinar que hará un seguimiento y medir	L0
9.1 (e)	Determinar cuándo se analizan y evalúan los resultados del seguimiento y medición	L0
9.1 (f)	Determinar que deberá analizar y evaluar los resultados	L0
9,2	La auditoría interna	

9.2 (a1)	cumple requisitos propios de la organización de su sistema de gestión de seguridad de la información	L0
9.2 (a2)	Cumple los requisitos de esta norma internacional;	L0
9.2 (b)	se ha implementado y se mantiene de manera eficaz.	L0
9.2 (c)	planificar, establecer, implementar y mantener un programa (s) de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación y presentación de informes. El programa (s) de auditoría tendrá en cuenta la importancia de los procesos de que se trate y los resultados de auditorías anteriores;	L0
9.2 (d)	definir los criterios de auditoría y el alcance de cada auditoría;	L0
9.2 (e)	seleccionar auditores y realizar auditorías que garanticen la objetividad y la imparcialidad del proceso de auditoría;	L0
9.2 (f)	asegurarse de que los resultados de las auditorías se reportan a la gestión pertinente; y	L0
9.2 (g)	conservar la información documentada como prueba del programa (s) de auditoría y los resultados de la auditoría.	L0
9,3	Revisión de la Gestión	
9.3 (a)	el estado de las acciones de las revisiones por la dirección previas;	L0
9.3 (b)	los cambios en los problemas externos e internos que son relevantes para la gestión de seguridad de la información sistema	L0
9.3 (c1)	la retroalimentación sobre el desempeño de seguridad de la información, incluyendo las tendencias en no conformidades y acciones correctivas	L0
9.3 (c2)	la retroalimentación sobre el desempeño de seguridad de la información, incluyendo las tendencias en seguimiento y medición de resultados;	L0
9.3 (c3)	la retroalimentación sobre el desempeño de seguridad de la información, incluyendo las tendencias en resultados de la auditoría; y	L0
9.3 (c4)	la retroalimentación sobre el desempeño de seguridad de la información, incluyendo las tendencias en el cumplimiento de los objetivos de seguridad de la información;	L0
9.3 (d)	la retroalimentación de las partes interesadas;	L0
9.3 (e)	los resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos; y	L0
9.3 (f)	Oportunidades de mejora continua.	L0
10	**Proceso de mejora**	
10,1	No conformidad y acciones correctivas	
10.1 (a1)	reaccionan a la no conformidad, y según sea el caso tomar medidas para controlar y corregirlo	L0

10.1 (a2)	reaccionan a la no conformidad, y según sea el caso hacer frente a las consecuencias;	L0
10.1 (b1)	evaluar la necesidad de adoptar medidas para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o producirse en otros lugares, por la revisión de la no conformidad	L0
10.1 (b2)	evaluar la necesidad de adoptar medidas para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o producirse en otros lugares, por determinar las causas de la no conformidad	L0
10.1 (b3)	evaluar la necesidad de adoptar medidas para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o producirse en otros lugares, por determinar si existen no conformidades similares, o podrían producirse;	L0
10.1 (c)	implementar cualquier acción necesaria;	L0
10.1 (d)	revisar la eficacia de las medidas correctivas adoptadas; y	L0
10.1 (e)	Realizar cambios en el sistema de gestión de seguridad de la información, si es necesario.	L0
10.1 (f)	la naturaleza de las no conformidades y de cualquier acción tomada posteriormente, y	L0
10.1 (g)	Los resultados de cualquier acción correctiva.	L0
10,2	Mejora continua	L0

Tabla 2 Estado actual de la empresa con respecto a la norma

	Dominio	% de conformidad	# NC mayores	# NC menores	# NC OK
4	**Contexto de la organización**	5%	5	0	0
5	**Liderazgo**	1%	14	0	0
6	**Planificación**	0%	31	0	0
7	**Soporte**	10%	14	3	0
8	**Funcionamiento**	0%	3	0	0
9	**Evaluación de Rendimiento**	5%	23	0	0
10	**Proceso de mejora**	0%	11	0	0

Tabla 3 Conformidades

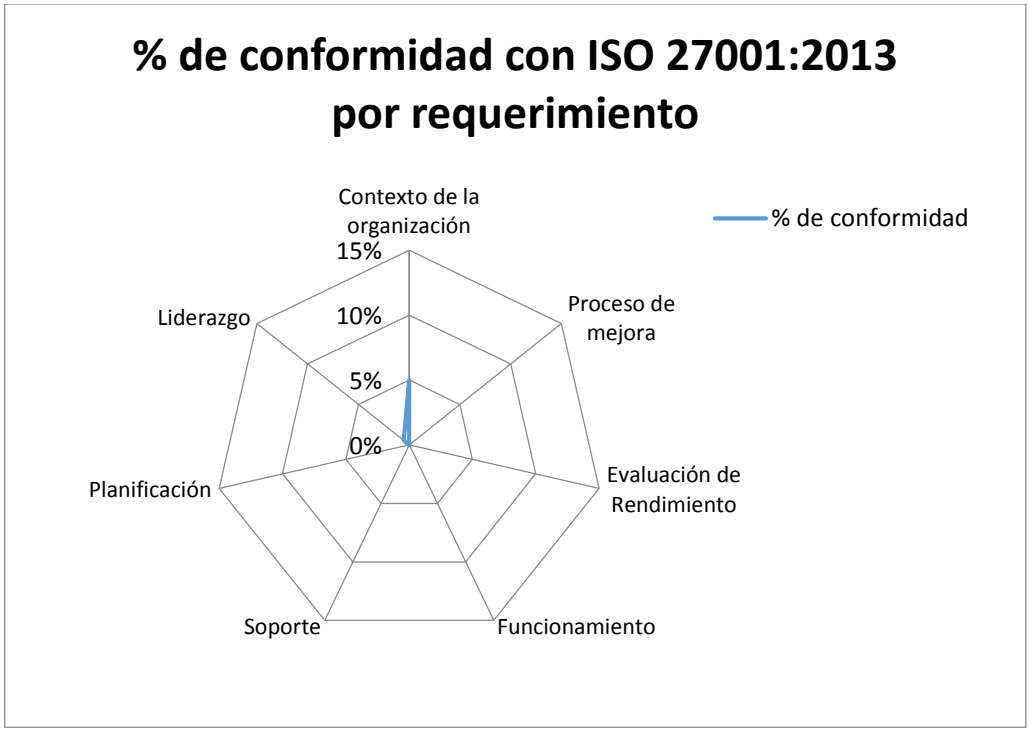

Ilustración 5 Niveles de conformidad ISO 27001

4.2 Análisis diferencial ISO 27002:2013

El análisis diferencial nos será útil para comparar el estado actual de la organización con la norma y para, posteriormente, comparar el nivel de implementación de la misma.

A.5	Política de Seguridad	Cumplimiento	Observaciones
A5.1	**Directrices de la Dirección en seguridad de la información**		
A.5.1.1	Conjunto de políticas para la seguridad de la información.	L0	No se dispone de unas directrices en seguridad de la información
A.5.1.2	Revisión de las políticas para la seguridad de la información	L0	No se dispone de unas directrices en seguridad de la información
A.6	**Aspectos organizativos de la seguridad de la información**		
A.6.1	**Organización Interna**		
A.6.1.1	Asignación de responsabilidades para la segur. de la información.	L2	Algunas tareas si se encuentran definidas, pero no de una manera documentada y procesada
A.6.1.2	Segregación de tareas.	L2	Algunas tareas si se encuentran definidas, pero no de una manera documentada y procesada
A.6.1.3	Contacto con las autoridades.	L0	
A.6.1.4	Contacto con grupos de interés especial.	L0	
A.6.1.5	Seguridad de la información en la gestión de proyectos.	L0	
A.6.2	**Dispositivos para movilidad y teletrabajo.**		
A.6.2.1	Política de uso de dispositivos para movilidad	L0	A pesar de utilizar dispositivos en movilidad constantemente, no existe una política clara al respecto
A.6.2.2	Teletrabajo	L0	A pesar de utilizar dispositivos en movilidad constantemente, no existe una política clara al respecto
A.7	**La seguridad ligada a los recursos humanos**		
A.7.1	**Antes de la contratación**		
A.7.1.1	Investigación de antecedentes	L0	
A.7.1.2	Términos y condiciones de contratación	L2	Se realiza de manera parcial

A.7.2	**Durante la contratación**		
A.7.2.1	Responsabilidades de gestión	L1	
A.7.2.2	Concienciación, educación y capacitación en segur. de la informac.	L2	Se realizan algunos cursos internos, pero sin una estructura ni finalidad clara
A.7.2.3	Proceso Disciplinario	L0	
A.7.3	**Cese o cambio de puesto de trabajo.**		
A.7.3.1	Cese o cambio de puesto de trabajo.	L0	
A.8	**Gestión de Activos**		
A.8.1	**La responsabilidad de los activos**		
A.8.1.1	Inventarios de Activos	L0	
A.8.1.2	Propiedad de Activos	L0	La propiedad de los activos es de los usuarios finales (se los deja en propiedad)
A.8.1.3	Uso aceptables de los activos	N/A	
A.8.1.4	Devolución de activos	N/A	
A.8.2	**Clasificación de la información**		
A.8.2.1	Directrices de clasificación	L0	
A.8.2.2	Etiquetado de la información y la manipulación	L0	
A.8.2.3	Manipulación de activos	L0	
A.8.3	**Manejo de los soportes de almacenamiento**		
A.8.3.1	Gestión de soportes extraíbles.	L0	
A.8.3.2	Eliminación de soportes	L0	No se tiene una política clara al respecto a pesar de que ha sido necesario varias veces.
A.8.3.3	Soportes físicos en tránsito	L0	
A9	**Control de Acceso**		
A9.1	**Requerimiento de negocio de control de acceso**		
A9.1.1	Política de control de acceso	L1	Los guardias del edificio pueden controlar si entra alguien ajeno, pero no llevan un control exhaustivo

A9.1.2	Control de acceso a las redes y servicios asociados.	L0	
A9.2	**Gestión de acceso de los usuarios**		
A9.2.1	Gestión de altas/bajas en el registro de usuarios.	L1	Se gestiona según vaya siendo necesario. No existe ningún procedimiento estandarizado ni se encuentra documentado
A9.2.2	Gestión de los derechos de acceso asignados a usuarios.	L1	
A9.2.3	Gestión de los derechos de acceso con privilegios especiales	L1	
A9.2.4	Gestión de información confidencial de autenticación de usuarios	L1	
A9.2.5	Revisión de los derechos de acceso de los usuarios	L1	Se modifican o eliminan usuarios de freelance según se vea que es necesario, pero no existe ningún procedimiento estandarizado ni se encuentra documentado
A9.2.6	Retirada o adaptación de los derechos de acceso	L1	Se modifican o eliminan usuarios de freelance según se vea que es necesario, pero no existe ningún procedimiento estandarizado ni se encuentra documentado
A9.3	**Responsabilidades de los usuarios**		
A9.3.1	Uso de información confidencial para la autenticación.	L0	
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	L1	
A9.4.2	Procedimientos seguros de inicio de sesión	L0	
A9.4.3	Gestión de contraseñas de usuario	L2	Solo en servidores de la empresa
A9.4.4	Uso de herramientas de administración de sistemas.	L2	
A9.4.5	Control de acceso al código fuente de los programas	L3	
A10	**Cifrado**		
A10.1	**Controles criptográficos.**		
A10.1.1	Política de uso de los controles criptográficos	L0	

A10.1.2	Gestión de claves	L0	
A.11	**Seguridad Fisica y ambiental**		
A11.1	**Areas Seguras**		
A11.1.1	Perímetro de seguridad física	L0	
A11.1.2	Controles de entradas físicas	L0	
A11.1.3	Seguridad de oficinas, despachos y recursos.	L2	
A11.1.4	Protección contra las amenazas externas y ambientales.	L2	Solo en sala de servidores
A11.1.5	El trabajo en áreas seguras.	N/A	
A11.1.6	Zonas de acceso público, de entrega y de carga	N/A	
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	L2	Solo en sala de servidores
A11.2.2	Instalaciones de suministro	L0	Solo en sala de servidores
A11.2.3	Seguridad del cableado	L4	
A11.2.4	Mantenimiento de los equipos	L4	
A11.2.5	Salida de activos fuera de las dependencias de la empresa	L0	No se tiene controlado
A11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	L0	Depende del usuario. No existe una política común para esto
A11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	L0	No se tiene un procedimiento definido para la retirada o reutilización segura
A11.2.8	Equipo informático de usuario desatendido.	L0	
A11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	L0	No hay política común para esto
A12	**Seguridad en la operativa**		
A12.1	**Responsabilidades y procedimientos de operación**		
A12.1.1	Documentación de procedimientos de operación	L4	Los procedimientos de operación se encuentran definidos

A12.1.2	Gestión del Cambio	L1	La gestión de cambio se encuentra definida, pero no documentada
A12.1.3	Gestión de capacidades	L4	
A12.1.4	Separación de entornos de desarrollo, prueba y producción.	L4	Se encuentra correctamente separado los entornos
A12.2	**Protección contra código malicioso**		
A12.2.1	Controles contra el código malicioso	L2	Sólo en servidores de la empresa
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	L3	Solo en servidores de la empresa. Los usuarios no están obligado a hacer copias de sus datos
A12.4	**Registro de actividad y supervisión**		
A12.4.1	Registro y gestión de eventos de actividad	L1	Se encuentra activado. No existe procedimiento estándar de revisión y actuación
A12.4.2	Protección de los registros de información	L2	
A12.4.3	Registros de actividad del administrador y operador del sistema	L1	
A12.4.4	Sincronización de relojes	L2	Sólo en servidores se comprueba fehacientemente.
A12.5	**Control del software en explotación.**		
A12.5.1	Instalación del software en sistemas en producción	L4	
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	L0	
A12.6.2	Restricciones en la instalación de software.	L2	Sólo en servidores
A12.7	**Consideraciones de las auditorías de los sistemas de información**		
A12.7.1	Controles de auditoría de los sistemas de información	L0	
A13	Seguridad en las telecomunicaciones		
A13.1	**Gestión de la seguridad en las redes**		

A13.1.1	Controles de red.	L2	Varios controles en la red
A13.1.2	Mecanismos de seguridad asociados a servicios en red	L1	
A13.1.3	Segregación de redes	L0	
A13.2	**Intercambio de información con partes externas**		
A13.2.1	Políticas y procedimientos de intercambio de información	L0	
A13.2.2	Acuerdos de intercambio	L0	
A13.2.3	Mensajería electrónica.	L0	
A13.2.4	Acuerdos de confidencialidad y secreto	L0	
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de infor.**		
A14.1	**Requisitos de seguridad de los sistemas de información**		
A14.1.1	Análisis y especificación de los requisitos de seguridad	L0	
A14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes	L3	Sólo donde es requerido por cumplimiento de terceros
A14.1.3	Protección de las transacciones por redes telemáticas	L3	Sólo donde es requerido por cumplimiento de terceros
A14.2	**Seguridad en los procesos de desarrollo y soporte**		
A14.2.1	Política de desarrollo seguro de software	L2	Se realizan pruebas de seguridad durante el despliegue, pero no están estandarizadas ni documentadas
A14.2.2	Procedimientos de control de cambios en los sistemas	L3	Se lleva un control de los cambios en el Software
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el S.O	L2	Sólo en los servidores
A14.2.4	Restricciones a los cambios en los paquetes de software	L0	
A14.2.5	Uso de principios de ingeniería en protección de sistemas	L2	
A14.2.6	Seguridad en entornos de desarrollo	L2	Depende mucho del sistema del usuario final

A14.2.7	Externalización del desarrollo de software	L4	
A14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	L3	
A14.2.9	Pruebas de aceptación	L3	
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos utilizados en pruebas	L4	Se realiza una copia de los datos en las pruebas
A15	**Relaciones con los suministradores**		
A15.1	**Seguridad de la información en las relaciones con suministradores**		
A15.1.1	Política de seguridad de la información para suministradores	L0	
A15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	L0	
A15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	L0	
A15.2	**Gestión de la prestación del servicio por suministradores**		
A15.2.1	Supervisión y revisión de los servicios prestados por terceros	L4	Cumplimientos de SLA de proveedores en cloud
A15.2.2	Gestión de cambios en los servicios prestados por terceros	L2	
A16	**Gestión de incidentes en la seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras.**		
A16.1.1	Responsabilidades y procedimientos	L0	
A16.1.2	Notificación de los eventos de seguridad de la información	L0	
A16.1.3	Notificación de puntos débiles de la seguridad	L0	
A16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	L0	

A16.1.5	Respuesta a los incidentes de seguridad	L0	
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	L0	
A16.1.7	Recopilación de evidencias	L0	
A17	**Aspectos de seguridad de la información en la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	L0	No existe un plan adecuado que garantice la continuidad del negocio
A17.1.2	Implantación de la continuidad de la seguridad de la información	L0	
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad	L0	
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	L0	
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales.**		
A18.1.1	Identificación de la legislación aplicable	L4	En temas de legislación y protección de datos se cumplen los requisitos
A18.1.2	Derechos de propiedad intelectual (DPI)	L4	Se cumple, sin embargo, no según los criterios ISO
A18.1.3	Protección de los registros de la organización.	L4	
A18.1.4	Protección de datos y privacidad de la información personal	L4	
A18.1.5	Regulación de los controles criptográficos	L4	
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	L0	

A18.2.2	Cumplimiento de las políticas y normas de seguridad	L3	
A18.2.3	Comprobación del cumplimiento	L0	

Tabla 4 Análisis diferencial ISO 27002

	Dominio	% de conformidad	# NC baja efectividad	# NC alta efectividad	# NC OK
A.5	POLÍTICAS DE SEGURIDAD	0%	2	0	0
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	10%	5	2	0
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	15%	4	2	0
A.8	GESTIÓN DE ACTIVOS.	0%	8	0	0
A.9	CONTROL DE ACCESOS.	14%	11	3	0
A.10	CIFRADO.	0%	2	0	0
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	26%	8	3	2
A.12	SEGURIDAD EN LA OPERATIVA.	62%	5	5	4
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	10%	6	1	0
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	73%	2	9	2
A.15	RELACIONES CON SUMINISTRADORES.	36%	3	1	1
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	0%	7	0	0
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	0%	4	0	0
A.18	CUMPLIMIENTO.	63%	2	1	5

Tabla 5 Conformidades

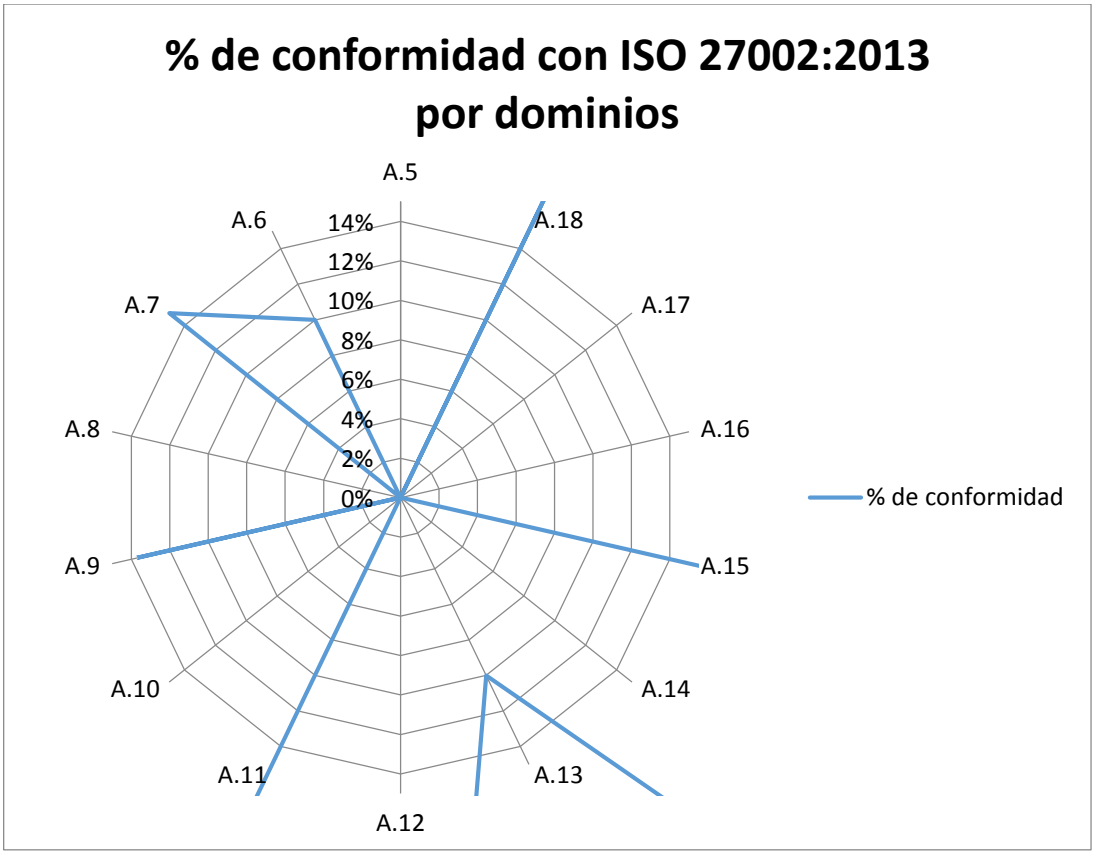

Ilustración 6 Porcentaje de conformidad por dominios

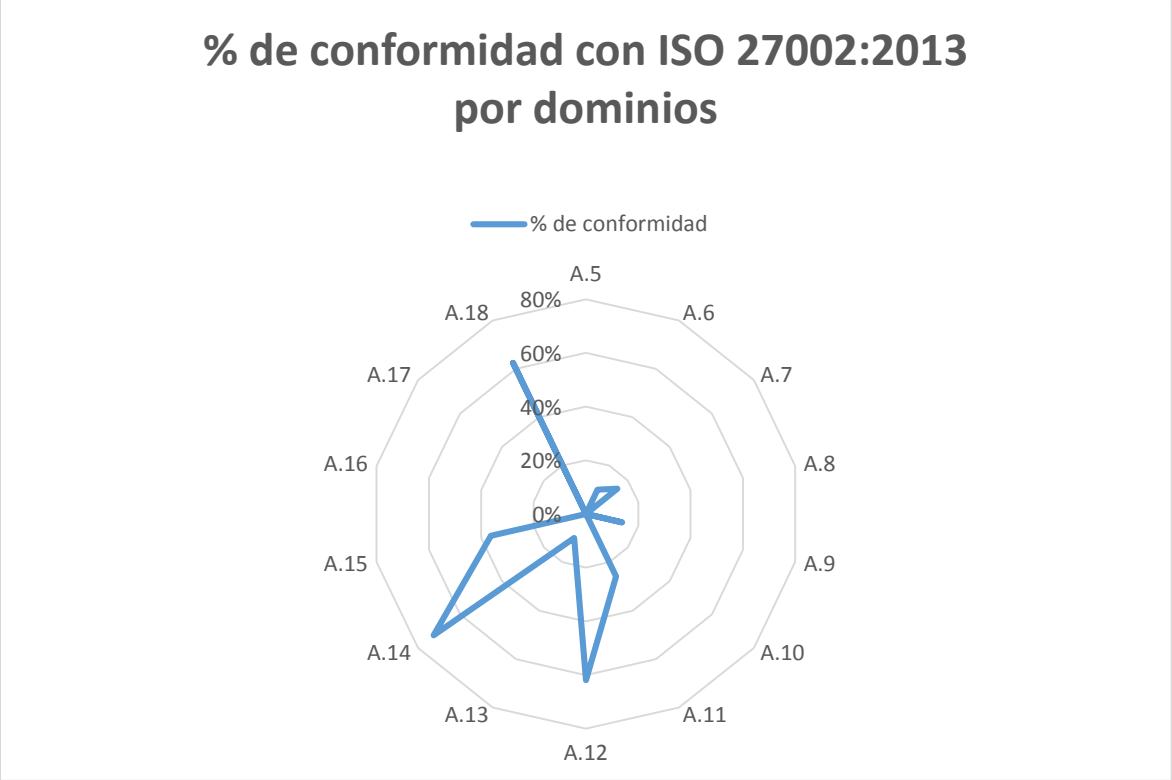

Ilustración 7 Porcentaje de conformidad por dominios (Completo)

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	57
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	13
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	19
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	8
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	14
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	0
L6	N/A	No aplica		3

Tabla 6 Recuento Total de Controles de la norma ISO27002 en base a CMM

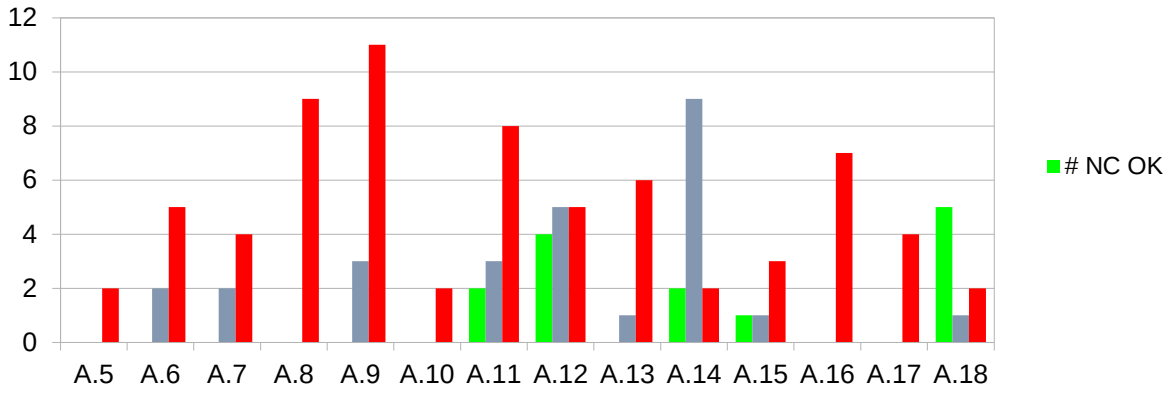

Tabla 7 Conformidades por dominio

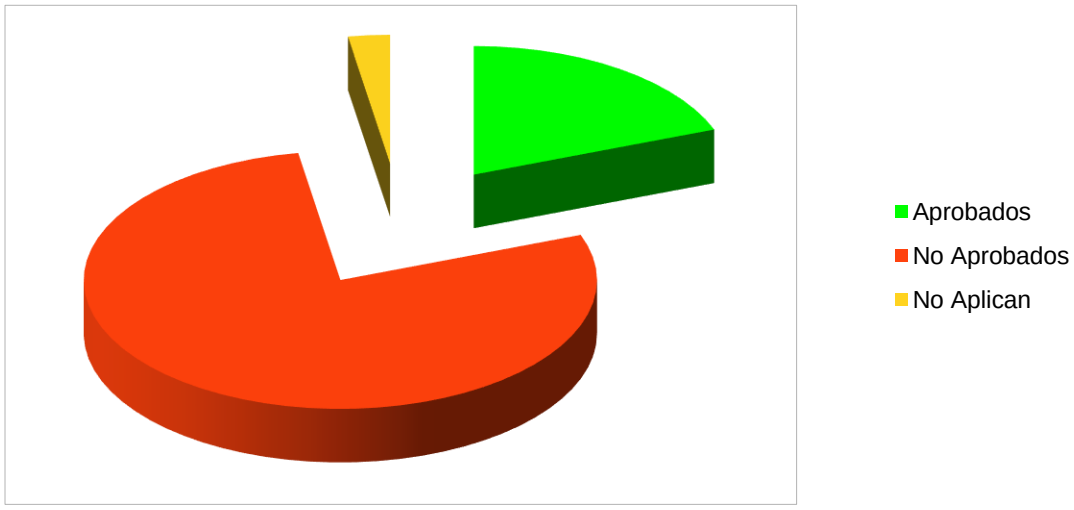

Ilustración 8 Porcentaje de aprobados sobre el total

5. Política de seguridad

La empresa tiene el compromiso de realizar una política de seguridad en donde se establece la estrategia de la empresa y la implicación de la alta dirección respecto a la definición, desarrollo, mantenimiento y mejora de un SGSI, así como la definición e implementación de políticas específicas que la dirección considere de obligado cumplimiento por todos los trabajadores o colaboradores de la misma.

5.1 Objetivo de la política de seguridad

La política de seguridad es una declaración ética, responsables y de estricto cumplimiento en toda la organización, la cual se desarrolla y concreta en políticas, normas, guías y estándares de segundo nivel. Como constituyente del primer nivel de la pirámide jerárquica en seguridad de la información, se establecen las directrices en seguridad de la información, alineadas con los objetivos del negocio y la legislación aplicable, todo ello refrendado y con el compromiso de la Dirección de la compañía.

Los objetivos de la política de seguridad son los siguientes:

- Entender que la información en toda la organización debe ser protegida, manteniendo los niveles óptimos de seguridad, permitiendo velar porque dicha información (sea propia y/o de terceros) se le conserve los tres pilares básicos de la seguridad de la información: confidencialidad, integridad y disponibilidad.
- La empresa proveerá de las medidas técnicas y organizativas necesarias orientadas a detectar y corregir las vulnerabilidades de seguridad que se detecten e intentar garantizar un entorno seguro en el tratamiento de la información, así como todas las medidas para difundir y promover la seguridad de la información en todos sus dominios
- Los trabajadores deben incluir la cultura de seguridad como parte de sus funciones diarias, ya que sin la implicación de los mismo, no será posible un correcto funcionamiento del SGSI, así mismo, los trabajadores deberán ser proactivos en el mantenimiento y mejora del SGSI, de tal que forma que propongan las mejoras que estimen oportunas y pongan en conocimiento del responsable de seguridad o del SGSI cualquier incidente de seguridad que observen.
- Las normas definidas en la política de seguridad serán de obligado cumplimiento por cualquiera que trate con la información de la organización, se definirán controles para que los distintos colaboradores y empleados respeten el deber de secreto de la información.
- Todos los trabajadores y personal que trate con la información deberán conocer y aceptar la política de seguridad de la empresa.
- La empresa tomará las medidas y acciones que considere oportunas para hacer cumplir con la política de seguridad.

5.2 Alcance de la política de seguridad

La Política de Seguridad es de aplicación a todos los activos de la empresa, ya sean en formato papel, informático o audiovisual y debe ser conocida y aceptada por todo el personal que trate con información de la empresa ya sea interno o externo.

Debido al tamaño de la empresa, el alcance se aplica a todos los procesos de la misma, sin embargo, debe entenderse como un proceso continuo de maduración y mejora.

5.3 Estructura organizacional

Como reflejo del compromiso de la dirección con la seguridad, se acuerda que dentro del área de infraestructura y sistemas (y bajo las órdenes del responsable del área correspondiente) se cree un área de seguridad cuya principales responsabilidades serán:

- Liderar la implementación y mantenimiento del SGSI.
- Llevar a cabo las auditorias del SGSI de manera periódica.
- Generar las respectivas acciones preventivas, correctivas y de mejora sobre el sistema.
- Despliegue y mantenimiento de plataformas de seguridad: Firewalls, IDS, SIEM y plataformas de Threat Intelligence.
- Revisión de incidencias y correlación de logs para determinar posibles incidentes de seguridad.
- Participar de las capacitaciones programadas.
- Verificar los informes de la auditoría.
- Crear, ajustar e implementar los planes de toma de conciencia y capacitación sobre seguridad.
- Utilizar todos los medios técnicos y profesionales a su alcance para implementar y mantener el SGSI.
- Realizar análisis de riesgos de seguridad de la información.
- Gestionar, realizar y/o liderar pruebas de instrucción y Ethical hacking.
- Convocar a las reuniones/comités de seguimientos.
- Respuesta a incidentes de seguridad.
- Liderar los planes de auditoría, retroalimentando al comité de seguridad.
- Ejecutar las acciones con ética, respeto, transparencia, independencia e imparcialidad.

Este área contará con un responsable de seguridad propio y será dotada de personal y recursos suficientes para la realización de sus actividades y ser encargado de coordinar el equipo de trabajo (equipo de seguridad), recibir y asignar funciones y tareas a los miembros del equipo de seguridad, coordinar y gestionar las capacitaciones en seguridad, gestionar elementos contractuales, con proveedores y el presupuesto.

5.4 Gestión de Roles y responsabilidades

Se procede a definir los siguientes roles y comités:

5.4.1 El Comité de Dirección de la compañía

En primer lugar se deberá crear un Comité de Dirección con los altos cargos de la compañía. En este caso, estará formado por los socios fundadores de la empresa, cualquier decisión tomada por este comité en materia de seguridad deberá quedar recogida en un acta de reunión.

Las funciones en materia de seguridad de la información del Comité de Dirección de la compañía son las siguientes:

- Hacer de la seguridad de la información un punto de la agenda del Comité de Dirección de la compañía.
- Nombrar a los miembros de un Comité de Seguridad de la Información y darles soporte, dotarlo de los recursos necesarios y establecer sus directrices de trabajo.
- Aprobar la política, normas y responsabilidades generales en materia de seguridad de la información.
- Determinar el umbral de riesgo aceptable en materia de seguridad.
- Analizar posibles riesgos introducidos por cambios en las funciones o funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas.
- Aprobar el Plan de seguridad de la información, que recoge los principales proyectos e iniciativas en la materia.
- Realizar el seguimiento del cuadro de mando de la seguridad de la información.

5.4.2 El Comité de Seguridad de la Información (CSI)

Es nombrado por el comité de dirección. Las decisiones en materia de seguridad de la información son tomadas de forma consensuada por un grupo formado por diferentes responsables dentro de la compañía.

En este caso particular estará formado por cuatro miembros permanentes:

- Un miembro del comité de dirección (Socio fundador de la empresa)
- Responsable de área de desarrollo
- Responsable del área de sistemas e infraestructuras
- Responsable del área de seguridad

En principio, al no contar con dichos departamentos, los responsables jurídicos y de RRHH, no son llamados como miembros permanentes, sin embargo es posible que puedan ser llamados en caso de necesidad a los responsables de las empresas contratadas o contratar un consultor externo.

En cualquier caso, si el crecimiento de la empresa es el esperado, está planificado que se cuente con gabinetes de RRHH y jurídico propio, por lo que los responsables de cada área, pasarían a engrosar el CSI.

Las funciones en materia de seguridad de la información del Comité de Seguridad de la Información son las siguientes:

- Implantar las directrices del Comité de Dirección.
- Asignar roles y funciones en materia de seguridad.

- Presentar a aprobación al Comité de Dirección las políticas, normas y responsabilidades en materia de seguridad de la información.
- Validar el mapa de riesgos y las acciones de mitigación propuestas por el responsable de seguridad de la información (RSI).
- Validar el Plan de seguridad de la información o Plan director de seguridad de la información y presentarlo a aprobación al Comité de Dirección. Supervisar y hacer el seguimiento de su implantación.
- Supervisar y aprobar el desarrollo y mantenimiento del Plan de continuidad de negocio.
- Velar por el cumplimiento de la legislación que en materia de seguridad sea de aplicación.
- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.
- Revisar las incidencias más destacadas.
- Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

5.4.3 Responsable de seguridad de la información (RSI)

La designación de un responsable de seguridad de la información (RSI) es la única vía para avanzar de forma organizada y paulatina en seguridad de la información, ya que garantiza que hay alguien para quien la seguridad de la información es una prioridad.

Las funciones en materia de seguridad de la información de los RSI son coordinar las acciones orientadas a garantizar la seguridad de la información en cualquiera de sus formas (digital, óptica, papel...) y en todo su ciclo de vida (creación, mantenimiento, distribución, almacenaje y destrucción), para protegerla en términos de confidencialidad, privacidad, integridad, disponibilidad, autenticidad y trazabilidad.

El RSI será, para este caso en concreto el responsable del área de seguridad, pudiendo delegar tareas si lo ve necesario, pero no la responsabilidad de las acciones

Las funciones del RSI se concretan en:

- Implantar las directrices del Comité de Seguridad de la Información de la compañía.
- Elaborar, promover y mantener una política de seguridad de la información, y proponer anualmente objetivos en materia de seguridad de la información.
- Desarrollar y mantener el documento de Organización de la seguridad de la información en colaboración con el área de Organización/RR. HH., en el cual se recogerá quién asume cada una de las responsabilidades en seguridad, así como una descripción detallada de funciones y dependencias.
- Desarrollar, con el soporte de las unidades correspondientes, el marco normativo de seguridad y controlar su cumplimiento.
- Actuar como punto focal en materia de seguridad de la información dentro de la compañía, lo cual incluye la coordinación con otras unidades y funciones (seguridad física, prevención, emergencias, relaciones con la prensa...), a fin de gestionar la seguridad de la información de forma global.
- Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo, de

acuerdo con el umbral aceptable definido por el Comité de Dirección. Elevar el mapa de riesgos y el Plan de seguridad de la información al CSI.

- Controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de aplicaciones.
- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas. Esta revisión ha de permitir proponer o actualizar el Plan de seguridad de la información, incorporando todas las acciones preventivas, correctivas y de mejora que se hayan ido detectando. Una vez aprobado dicho plan y el presupuesto por el CSI, el RSI deberá gestionar el presupuesto asignado y la contratación de recursos cuando sea necesario.
- Coordinar acciones con las áreas de negocio para elaborar y gestionar un Plan de continuidad de negocio de la compañía, basado en el análisis de riesgo y la criticidad de los procesos de negocio, y la determinación del impacto en caso de materialización del riesgo.
- Velar por el cumplimiento legal coordinando las actuaciones necesarias con las unidades responsables.
- Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad a nivel tecnológico (gestión de trazas, vulnerabilidades, cambios...), hacer el seguimiento de los incidentes de seguridad y escalarlos al CSI si corresponde.
- Elaborar y mantener un plan de concienciación y formación en seguridad de la información del personal, en colaboración con la unidad responsable de la formación en la compañía.
- Hacer seguimiento y revisar los incidentes de seguridad, escalándolos al CSI si corresponde.
- Coordinar la implantación de herramientas y controles de seguridad de la información y definir el cuadro de mando de la seguridad. El RSI debe analizar y mantener actualizado dicho cuadro de mando, presentándolo al CSI con la periodicidad que se establezca.

5.5 Responsabilidades generales

5.5.1 Nivel dirección

El compromiso de la dirección es vital para el correcto desarrollo e implementación del SGSI, ya que debe dotar de recursos personales y económicos de la actividad y controlar actividades de manera que las decisiones y proyectos que se definan cuenten con su aval y sean acordes a los objetivos estratégicos del negocio.

Es el grupo encargado de definir la estrategia de seguridad y continuidad de la información para la compañía, definir y aprobar las políticas de seguridad de la información, elaborar y presentar los proyectos de seguridad, establecer las prioridades para su desarrollo, y revisar la implantación y la efectividad de las medidas adoptadas. La Alta Dirección demostrará su compromiso a través de:

- La revisión y aprobación de las Políticas de seguridad de la información.
- La promoción activa de una cultura de seguridad dentro de la compañía.
- Facilitar la divulgación de este manual a todos los funcionarios de la compañía.
- El aseguramiento de los recursos adecuados para implantar y mantener las Políticas y el SGSI

5.5.2 Nivel técnico operativo

Tienen las funciones siguientes:

- Cumplir con las políticas, normas y procedimientos en materia de seguridad de la información.
- Colaborar con el RSI en su definición.
- Implantar en los sistemas de información los controles de seguridad prescritos, las acciones correctoras establecidas y gestionar las vulnerabilidades detectadas.
- Requerir la participación del RSI en nuevos proyectos de desarrollo o adaptación/implantación de productos de mercado, especialmente cuando puedan ser críticos en términos de confidencialidad, privacidad, integridad, continuidad, autenticidad, no repudio y trazabilidad, o puedan tener un impacto mediático importante.
- Requerir la participación del RSI en la implantación o gestión de los cambios de hardware y software.
- Garantizar la inclusión de la seguridad en todo el ciclo de vida de los datos: creación, mantenimiento, conservación y destrucción, y en los procesos de gestión de hardware y software.
- Adoptar medidas para proteger la información según su clasificación por parte del responsable de la información.
- Colaborar con el RSI en la identificación de riesgos y la propuesta de soluciones, y colaborar en las revisiones o auditorías de seguridad que se lleven a cabo.

5.5.3 Nivel de usuario

Son los usuarios de la información y por tal razón son los responsables de cumplir el modelo, políticas y definiciones establecidas para la compañía. Todo el personal interno o externo con acceso a la información de la compañía (trabajadores, proveedores en prestación de servicios), tiene la obligación de:

- Mantener la confidencialidad de la información.
- Hacer un buen uso de los equipos y de la información a la cual tienen acceso y protegerla de accesos no autorizados.
- Respetar las normas y procedimientos vigentes en materia de seguridad de la información, y velar por que terceras partes en prestación de servicios también la respeten.
- Utilizar adecuadamente las credenciales de acceso a los sistemas de información.
- Respetar la legislación vigente en materia de protección de datos de carácter personal y cualquier otra que sea de aplicación.
- Notificar, por la vía establecida, insuficiencias, anomalías o incidentes de seguridad y situaciones sospechosas que pudieran poner en peligro la seguridad de la información.

6. Definición del Sistema de gestión documental

Nos encontramos que la empresa XXX no tiene definido correctamente un sistema de gestión documental que permita integrar correctamente el SGSi.

Un aspecto tan básico como la terminología es una cuestión a resolver en primera instancia, puesto que facilitará que los diferentes tipos de documentos que se vayan creando se clasifiquen correctamente desde el primer momento,

Vamos a utilizar la siguiente jerarquía de documentos:

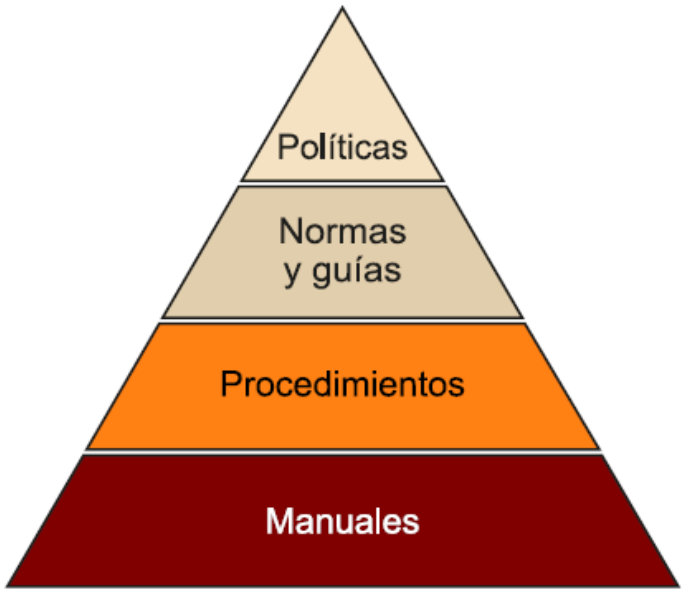

Ilustración 9 Jerarquía de documentos

Cuanto más arriba en la pirámide, más directrices generales y/o estratégicas y menor nivel de concreción. Asimismo, mayor estabilidad, es decir, poca variación en los documentos, y necesidad de aprobación por parte de la Dirección.

Por el contrario, cuanto más abajo en la pirámide, mayor nivel de detalle, orientación a personal más especializado, mucha necesidad de actualización de la documentación y aprobación a niveles inferiores.

Por norma general, un documento de nivel superior se desarrolla en documentos de nivel inferior.

A continuación se recogen y describen los distintos tipos de documentos que vamos a usar:

	Definición	Obligatoriedad	Aprobado por	Divulgación
Políticas	Recogen directrices estratégicas, de alto nivel, bajo las cuales se amparará cualquier acción en materia de seguridad de la información. Todo documento de nivel inferior debiera	Las políticas son de obligado cumplimiento y deben ser aprobadas por la dirección	La dirección de la compañía	Todo el personal y colaboradores

	desarrollar en base a una política			
Normas	Desarrollan la política a un nivel concreto y específico	De obligado cumplimiento por todo el personal y colaborador	Dirección	A quien se indique en la guía como objetivo de la misma
Guías	Proporciona una solución a un problema determinado	Buenas prácticas. No obligado cumplimiento, pero sí altamente recomendado	Comité asignado	A quien se indique en la guía como objetivo de la misma
Procedimiento	Presentan un conjunto de acciones a llevar a cabo para conseguir un determinado objetivo	De obligado cumplimiento por todo el personal y colaborador	Persona responsable del procedimiento	A quien se indique en el procedimiento como objetivo de la misma
Manuales (técnicos y de usuario)	Son listas de tareas o instrucciones detalladas para realizar determinadas acciones o utilizar herramientas concretas, se dividirán en manuales orientados a técnicos o a usuarios finales	Recomendado	Responsable	Persona que lleva a cabo la acción descrita en el manual

Tabla 8 Tipos de documentos definidos para la organización

6 .1 Nomenclatura de la documentación

Los documentos van a seguir el siguiente formato SGSI-XX-Título.

XX: Tipo de documento. Siendo:

- PO: Politica
- NO:Norma
- GU: Guia
- PR: Procedimiento
- MU: Manual de Usuario
- MT: Manual Técnico

Título: Titulo del documento.

6. 2 Acceso y registro de documentos

Aún sin una nomenclatura clara, la empresa realizaba el almacenamiento de la documentación de trabajo a través de una plataforma cloud de gestión documental, que llevaba automáticamente las versiones y modificaciones de los distintos archivos.

Debido a que se va a seguir usando esta plataforma, al poder consultar versiones anteriores de todos los documentos, no se incluye una versión del documento en el nombre.

Sin embargo si se hace necesario definir el ciclo de vida de los documentos y la definición de una estructura documental común, en el que sí vendrá recogido en número de la versión., esto se realizará en la política correspondiente.

6. 3 Documentos relacionados con políticas de seguridad

Una vez definido el sistema de gestión documental que vamos a definir para la organización y para dar soporte a las líneas generales antes descritas, la empresa ha definido las siguientes políticas:

Política de Seguridad de alto nivel. Este documento formará parte del documento de políticas de seguridad de la organización y además tendrá un código de documento independiente denominado SGSI-PO-Politica_de_Seguridad.

Este documento será aprobado y firmado por la dirección y estará disponible y accesible públicamente.

El resto de documentos que se describen a continuación, formarán parte del documento de Política de Seguridad y deberán ser igualmente aprobados y refrendados por la dirección

- Política de clasificación de la información.
- Política de control de acceso.
- Política de uso adecuado de los recursos de la empresa.
- Política de acceso remoto o teletrabajo.
- Política de comunicación de información.
- Política de gestión de activos
- Política de gestión de la continuidad
- Política de gestión de incidentes
- Política de cifrado
- Política en seguridad operativa
- Política de Recursos Humanos
- Política de seguridad física y ambiental.
- Política de adquisición, desarrollo y mantenimiento de los sistemas
- Política de relación con los suministradores

7. Procedimientos de auditorías internas

7.1 Definición

Las auditorías internas son el instrumento que se nos proporciona para comprobar que nuestro SGSI se encuentre correctamente actualizado con respecto a la norma ISO 27001:2013. Mediante estas auditorías se realiza un control periódico del estado de implementación de la norma ISO. La fiscalización de la auditoría, se presentará un informe con los resultados y una serie de acciones correctoras sobre las desviaciones detectadas.

El procedimiento tendrá los siguientes puntos:

- Objetivos
- Alcance
- Calendario
- Equipo
- Procedimiento de actuación

7.2 Objetivos

El objetivo de la auditoria interna es comprobar la evolución en el cumplimiento de la norma ISO 27001 en la empresa XXX, así como detectar e implementar mejoras que se consideren necesarias para el cumplimiento de la misma.

7.3 Alcance

El alcance de la auditoría interna es el mismo que el definido en el SGSI. Las auditorías internas se realizaran de un requerimiento cada vez de la norma ISO27001:2013. El listado de los principales requerimientos incluidos en la norma es el siguiente.

- Contexto de la organización
- Liderazgo
- Planificación
- Soporte
- Funcionamiento
- Evaluación de Rendimiento
- Proceso de mejora

7.4 Calendario

Una vez al año se realizará una auditoría interna, de manera obligatoria en los siguientes ámbitos:

- Conformidad con la norma ISO 27001:2013
- Funcionamiento de los controles de seguridad lógica
- Funcionamiento de los controles de seguridad física
- Revisión del plan de continuidad, contingencia y pruebas asociadas

7.5 Equipo

El equipo estará compuesto por miembros de la empresa y de una empresa externa auditada. El equipo será elegido en última instancia por el RSI y aprobado por el CSI.

- Responsable de auditoría: Encargado de llevar a cabo la auditoría. Encargado de garantizar la independencia y transparencia de la auditoría.
- Equipo Externo: Sin ninguna relación directa con la compañía ni con ninguno de sus procedimientos. Debe rotar cada dos años. Contará al menos con los siguientes perfiles
    - Auditor Jefe: Al menos 5 años de experiencia demostrables en auditoría. Certificado CISA o CISSP al menos.
    - Responsable técnico: Al menos 3 años de experiencia demostrables en auditoría
- Personal interno: Técnico asignado por el RSI para dar soporte a las actividades

7.6 Procedimiento

Entrada:

- Requerimiento de la auditoria interna
- Ámbitos afectados
- Informe con cambios organizacionales que afecten a dichos ámbitos
- Informes anteriores relacionados

Proceso:

1. Desde dirección se aprueba de la realización de la auditoria interna correspondiente de acuerdo con el plan de auditorías de la empresa o un requerimiento.

2. Se procede a la búsqueda y asignación de equipo auditor que no debe tener ninguna relación con el departamento a auditar. Se puede recurrir a auditores externos, pero deberán cumplir los Requisitos Auditor, definidos por el responsable de seguridad.

3. Se procede a la comunicación formal de la auditoria a todo el personal afectado con una antelación mínima de una semana.

4. Realización de la auditoria, que constara como mínimo de los siguientes pasos:

    - Reunión inicial
    - Revisión documentación
    - Verificación “in situ”
    - Cuestionario ad-oc de auditoria
    - Reunión final

5. Realización del informe de auditoría que será entregado al Responsable de Seguridad de la Información (RSI), que a su vez lo presentará a la dirección de la empresa.

	6. Se presentara además un informe de NO CONFORMIDADES que será entregado al RSI que será utilizado para realizar el seguimiento de dichos defectos detectados, así como de las medidas correctoras a aplicar.
Salida	Informe de auditoria.

El informe de auditoría se ajustará a la nomenclatura indicada en el SGSI.

Así mismo el informe deberá contener, al menos:

- Fecha de la auditoría
- Nombre de los auditores y empresas
- Alcance
- Ámbito y objetivos (Controles auditados)
- Conformidades con la norma o porcentaje de implementación
- No conformidades detectadas
- Informe ejecutivo
- Informe técnico con actuaciones de mejoras

8. Gestión de Indicadores

8.1 Definición

Un indicador de seguridad es un valor mediante el cual se puede comprobar el comportamiento y la eficacia de los controles de seguridad implantados dentro de un tiempo específico. Para ello se utilizan métricas de seguridad, que definen las reglas para poder medir de forma real el nivel de seguridad de la compañía.

8.2 Objetivos

El objetivo de los indicadores es comprobar de una manera objetiva la evolución en el cumplimiento de la norma ISO 27001 en la empresa XXX, así como proporcionar herramientas que permitan una medición eficaz de los efectos que la implementación de la norma tiene en la organización.

8.3 Alcance

El alcance es el SGSI y sus procesos asociados. Se tendrán en cuenta todos los dominios de la norma por separado.

8.4 Definición de indicadores

Los indicadores se actualizarán y revisarán una vez al año, se realizará una auditoría para comprobar la eficacia de cada uno de ellos y finalmente se realizará un informe que se enviará a dirección para su evaluación.

Control	Indicadores
A.5- Política de Seguridad	A5-I01: Grado de adopción de las políticas de la organización mediante revisiones por parte de la dirección, auditorías u otras autoevaluaciones A5-I02: Número de políticas modificadas o creadas en el último periodo A5-I03: Porcentaje de los controles de la ISO/IEC 27001 aplicables, para los cuales se ha escrito, aprobado y comunicado políticas A5-I04: Número de revisiones realizadas a la política de seguridad
A.6 - Aspectos organizativos de la seguridad de la información	A6-I01: Tareas realizadas y cerradas por el RSI y por cada responsable de realizarlas A6-I02: Tiempo de respuesta en el contacto con las autoridades y grupos de especial interés A6-I03: Número de grupos de especial interés contactados A6-I04: Número y porcentaje de proyectos de seguridad implementados y completados
A.7 - La seguridad ligada a los recursos humanos	A7-I01: Porcentaje de personal nuevo, que ha sido investigado y han pasado las pruebas de acuerdo a las políticas de la compañía antes de empezar a trabajar A7-I02: Tiempo medio de retirada de los derechos de acceso a un trabajador cesado o que cambia de puesto de trabajo

	A7-I03: Número de incidencias causadas por los empleados durante el empleo A7-I04: Número de activos no devueltos por los empleados que cambian de puesto de trabajo o cesan del empleo A7-I05: Número de cursos de formación, concienciación o capacitación en seguridad de la información impartidos a los empleados A7-I06: Número de dispositivos perdidos fuera de la oficina
A.8 - Gestión de Activos	A8-I01: Porcentaje de activos inventariados y etiquetados A8-I02: Grado de despliegue del inventario de activos A8-I03: Porcentaje de los activos identificados como críticos para los que se tienen desarrollados planes de tratamiento de riesgos y se mantienen dentro de un rango aceptable establecido. A8-I04: Clasificación de los datos sensibles por su distribución en los sistemas
A9 - Control de Acceso	A9-I01: Existencia, revisión y adecuación de políticas de control de accesos A9-I02: Porcentaje de trabajadores cuyas responsabilidades en seguridad de la información se encuentran aceptadas A9-I03: Evaluación de logs y estadísticas del software y hardware, relacionando vulnerabilidades aprovechadas e intentos de acceso a programas, plataformas y edificios A9-I04: Existencia y efectividad de controles de acceso a los sistemas operativos de las plataformas informáticas

	A9-I05: Tiempo medio de retirada de los derechos de acceso a un trabajador cesado o que cambia de puesto de trabajo A9-I06: Número de incidencias reportadas por fallos en el control de acceso
A10 - Cifrado	A10-I01: Numero de claves de usuario débiles
A.11 - Seguridad Física y ambiental	A11-I01: Número de revisiones periódicas de seguridad física de las instalaciones A11-I02: Número de mantenimientos a los equipos de la compañía A11-I03: Número de material retirado de la compañía A11-I04: Número de incidentes por parte del equipo de seguridad A11-I05: Numero de reportes por parte de la seguridad física
A12 - Seguridad en la operativa	A12-I01: Número de no conformidades en auditoría técnica A12-I02: Número de cambios realizados y su gestión A12-I03: Número de copias de seguridad realizadas A12-I04: Número de incidencias en las que se ha tenido que restaurar sistemas o datos A12-I05: Numero de eventos de seguridad A12-I06: Triage, tipos de eventos y tiempo de resolución de incidentes de seguridad A12-I07: Número de vulnerabilidades técnicas, reportadas, evaluadas y solucionadas.

A13 - Seguridad en las telecomunicaciones	A13-I01: Número de controles de red A13-I02: Número de acuerdos de intercambio de información vigente
A14 - Adquisición, desarrollo y mantenimiento de los sistemas de infor.	A14-I01: Número y evolución de requisitos de seguridad en hardware y software A14-I02: Número de vulnerabilidades descubiertas y reportadas en desarrollo A14-I03: Tiempo de implementación en el cambio de software tras notificación de fallo o vulnerabilidad A14-I04: Porcentaje de tipos de fallos A14-I05: Numero de pruebas funcionales al código A14-I06: Porcentaje de sistemas en los que los controles de validación de datos han sido vulnerados A14-I07: Porcentaje de procesos de cambios realizados conforme a la normativa existente al respecto, en relación al total de cambios solicitados y realizados
A15 - Relaciones con los suministradores	A15-I01: Numero de suministradores y porcentaje de cumplimiento conforme a requerimientos A15-I02: Número de incidencias de incumplimiento por parte de los proveedores A15-I03: Porcentaje de cambios suministrados por terceros A15-I04: Número y porcentaje sobre el total de fallos sobre código suministrados por terceros.
A16 - Gestión de incidentes en la seguridad de la información	A16-I01: Número de incidentes de seguridad A16-I02: Total de incidentes gestionados y porcentajes de cada tipo

	A16-I03: Incidentes de seguridad notificados externamente A16-I04: Incidentes de seguridad notificados a terceros A16-I05: Tiempo de resolución de incidentes de seguridad A16-I06: Número de fuentes de consulta de vulnerabilidades y notificaciones técnicas A16-I07: Tiempo de implementación de información obtenida por CTI A16-I08: Número de peticiones de soporte en temas relacionados con la seguridad de la información P A16-I09: Porcentaje de incidentes de seguridad que generaron costes superiores al umbral aceptable
A17 - Aspectos de seguridad de la información en la gestión de la continuidad de negocio	A17-I01: Efectividad en la implementación de los planes de continuidad de negocio A17-I02: Grado de despliegue de los planes de continuidad del negocio A17-I03: Tiempo de recuperación de sistemas en pruebas A17-I04: Número de actuaciones de recuperación de datos o de continuidad del negocio
A18 - Cumplimiento	A18-I01: Número de requerimientos legales agrupados y analizados por estado y nivel de riesgo A18-I02: Porcentaje de requisitos externos claves cumplidos a través de auditorias A18-I03: Efectividad de las auditorías o revisiones normativas A18-I04: Número de recomendaciones de auditoría agrupadas y analizadas A18-I05: Porcentaje de hallazgos de auditoría que han sido resueltos y cerrados respecto del total que se abrió en el mismo período

	A18-I06: Plazos de tiempo en resolver las recomendaciones A18-I07: Grado de despliegue del análisis de riesgos A18-I08: Tendencia en el número de riesgos relacionados con la seguridad de información según nivel de severidad A18-I09: Gastos de la seguridad de la información respecto al presupuesto asignado

9. Procedimiento de revisión por dirección

9.1 Definición

El procedimiento de revisión de dirección consiste en controlar el correcto funcionamiento del SGSI una vez este implantado. En caso de detectar problema, este control llevara como resultado acciones correctoras

9.2 Objetivos

El objetivo es múltiple:

- Informar y mantener informada a la dirección de las actividades realizadas en relación con el SGSI
- Informar de nuevos riesgos o necesidades que pudieran haber surgido con el paso del tiempo, reestructurando recursos según las necesidades.

9.3 Alcance

El alcance es el SGSI y sus procesos asociados. Este procedimiento se realizará anualmente.

9.4 Composición

La composición de la revisión por dirección se compondrá de los siguientes miembros:

- Comité de dirección
- CSI

- RSI
- Si así se requiere, es posible, puntualmente invitar a un asesor jurídico o técnico.

La convocatoria se realizará, con al menos tres meses de antelación, se requerirá confirmación de asistencia. Así mismo se proveerá:

- Listado completo de asistentes
- Fecha, hora y lugar
- Orden del día de puntos a tratar
- Informes a revisar

9.5 Procedimiento

Entrada:	Resultado de las Auditorías realizadas (internas/externas), y sus revisiones. Se añadirán los comentarios oportunos. Problemas y/o incidencias reportadas. Soluciones o técnicas, con sus procedimientos para mejorar el SGSI. Las vulnerabilidades y amenazas reportadas que son recurrentes sin aparente solución todavía. Cuantificadores de la efectividad dada sobre el SGSI. Relación de cambios o actualizaciones mayores que puedan desestabilizar el SI. Valores arrojados por los indicadores sobre los diversos servicios departamentales. Informes relevantes sobre monitorización de servicios hospitalarios y sus sistemas de información. Acciones correctivas tomadas. Estado del seguimiento de los objetivos Si procede o no revisiones de la Política de Seguridad y Análisis de Riesgos. Actas de las reuniones precedentes. Propuestas de mejora. Recomendaciones e ideas aportadas.
Proceso:	1. Evaluación y análisis ● El responsable de seguridad presentara cada uno de los informes a dirección y serán discutidos en común. ● Una serie de decisiones serán consensuadas entre ambos. 2. Toma de decisiones

	• Dirección, en base a la documentación aportada y consensuado junto con el responsable de seguridad, aprueba las acciones a tomar, plazos y personas responsables para cada acción. • Se decide una fecha para la siguiente revisión y se plantean seguimientos parciales si las disconformidades fueron demasiadas.
Salida	Planificación de acciones a tomar. Valores objetivos de los indicadores. Evaluación de deficiencia de recursos y sus necesidades.

10. Declaración de aplicabilidad

A.5	Política de Seguridad	Aplica	Justificación
A5.1	**Directrices de la Dirección en seguridad de la información**		
A.5.1.1	Conjunto de políticas para la seguridad de la información.	SI	La dirección se encuentra interesada en la definición
A.5.1.2	Revisión de las políticas para la seguridad de la información	SI	La dirección se encuentra interesada en las posteriores revisiones
A.6	**Aspectos organizativos de la seguridad de la información**		
A.6.1	**Organización Interna**		
A.6.1.1	Asignación de responsabilidades para la segur. de la información.	SI	Se encuentra definido un mecanismo de asignación de responsabilidades
A.6.1.2	Segregación de tareas.	SI	Se encuentra definido un mecanismo de segregación de responsabilidades
A.6.1.3	Contacto con las autoridades.	SI	Es necesario establecer contacto con las autoridades competentes
A.6.1.4	Contacto con grupos de interés especial.	SI	Es necesario establecer contacto con las los grupos correspondientes (CSIRT)
A.6.1.5	Seguridad de la información en la gestión de proyectos.	SI	Se hace necesario implementar este control
A.6.2	**Dispositivos para movilidad y teletrabajo.**		
A.6.2.1	Política de uso de dispositivos para movilidad	SI	Política BYOD

A.6.2.2	Teletrabajo	SI	Se teletrabaja de manera frecuente
A.7	**La seguridad ligada a los recursos humanos**		
A.7.1	**Antes de la contratación**		
A.7.1.1	Investigación de antecedentes	SI	No penales. Se contactará con anteriores empleadores para consolidar lo indicado en su CV
A.7.1.2	Términos y condiciones de contratación	SI	Necesario informar de términos y condiciones previos a la contratación
A.7.2	**Durante la contratación**		
A.7.2.1	Responsabilidades de gestión	SI	Se debe ajustar a la política de seguridad
A.7.2.2	Concienciación, educación y capacitación en segur. de la informac.	SI	Es un objetivo dentro de la implementación de SGSI
A.7.2.3	Proceso Disciplinario	SI	Es necesario definir en caso de incumplir políticas o normativas
A.7.3	**Cese o cambio de puesto de trabajo.**		
A.7.3.1	Cese o cambio de puesto de trabajo.	SI	Implementar procedimientos necesarios
A.8	**Gestión de Activos**		
A.8.1	**La responsabilidad de los activos**		
A.8.1.1	Inventarios de Activos	SI	Necesario, a implementar
A.8.1.2	Propiedad de Activos	SI	Es necesario controlar la propiedad de activos
A.8.1.3	Uso aceptables de los activos	SI	Si, sobre todo en equipos de uso de empresa
A.8.1.4	Devolución de activos	SI	En el caso de que sea de la empresa y no haya sido cedido a empleado
A.8.2	**Clasificación de la información**		
A.8.2.1	Directrices de clasificación	SI	Aplicable a todos los documentos
A.8.2.2	Etiquetado de la información y la manipulación	SI	Aplicable a todos los documentos
A.8.2.3	Manipulación de activos	SI	Necesario que sea definido
A.8.3	**Manejo de los soportes de almacenamiento**		
A.8.3.1	Gestión de soportes extraíbles.	SI	Para los pertenecientes a la empresa y buenas prácticas para los pertenecientes a los usuarios
A.8.3.2	Eliminación de soportes	SI	Es necesario definir tanto en local como en cloud (mediante SLA)
A.8.3.3	Soportes físicos en tránsito	SI	Se hace necesario definir el tratamiento en este caso

A9	**Control de Acceso**		
A9.1	**Requerimiento de negocio de control de acceso**		
A9.1.1	Política de control de acceso	SI	Necesario implementar controles técnicos para el acceso
A9.1.2	Control de acceso a las redes y servicios asociados.	SI	Necesario implementar controles técnicos para el acceso a redes internas
A9.2	**Gestión de acceso de los usuarios**		
A9.2.1	Gestión de altas/bajas en el registro de usuarios.	SI	Necesario definir procedimiento
A9.2.2	Gestión de los derechos de acceso asignados a usuarios.	SI	Necesario definir procedimiento
A9.2.3	Gestión de los derechos de acceso con privilegios especiales	SI	Necesario definir procedimiento
A9.2.4	Gestión de información confidencial de autenticación de usuarios	SI	Necesario definir procedimiento
A9.2.5	Revisión de los derechos de acceso de los usuarios	SI	Necesario definir procedimiento
A9.2.6	Retirada o adaptación de los derechos de acceso	SI	Necesario definir procedimiento
A9.3	**Responsabilidades de los usuarios**		
A9.3.1	Uso de información confidencial para la autenticación.	SI	Aplicado parcialmente
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	SI	Aplicado parcialmente
A9.4.2	Procedimientos seguros de inicio de sesión	SI	Buenas prácticas en usuario, normas en equipo de empresa
A9.4.3	Gestión de contraseñas de usuario	SI	Formación, concienciación y herramientas
A9.4.4	Uso de herramientas de administración de sistemas.	SI	Se realizar parcialmente
A9.4.5	Control de acceso al código fuente de los programas	SI	Se realizar parcialmente
A10	**Cifrado**		
A10.1	**Controles criptográficos.**		
A10.1.1	Política de uso de los controles criptográficos	SI	Necesario definir
A10.1.2	Gestión de claves	SI	Necesario Definir

A.11	**Seguridad Física y ambiental**		
A11.1	**Areas Seguras**		
A11.1.1	Perímetro de seguridad física	NO	Aplica para CPD. Implementado parcialmente
A11.1.2	Controles de entradas fisicas	NO	Externo, no depende de la empresa
A11.1.3	Seguridad de oficinas, despachos y recursos.	SI	Implementado parcialmente
A11.1.4	Protección contra las amenazas externas y ambientales.	SI	Implementado parcialmente
A11.1.5	El trabajo en áreas seguras.	SI	En CPD
A11.1.6	Zonas de acceso público, de entrega y de carga	NO	No implementado. La empresa no tiene un proceso definido para entrega/carga
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	SI	Implementado parcialmente
A11.2.2	Instalaciones de suministro	SI	Implementado parcialmente
A11.2.3	Seguridad del cableado	SI	Implementado parcialmente
A11.2.4	Mantenimiento de los equipos	SI	Implementado parcialmente. Sin un procedimiento específico
A11.2.5	Salida de activos fuera de las dependencias de la empresa	SI	Necesario que aplique a casos especiales
A11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	SI	Necesario que aplique a casos especiales
A11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	SI	Buenas prácticas y concienciación de usuarios
A11.2.8	Equipo informático de usuario desatendido.	SI	Buenas prácticas y concienciación de usuarios
A11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	SI	Buenas prácticas y concienciación de usuarios
A12	**Seguridad en la operativa**		
A12.1	**Responsabilidades y procedimientos de operación**		
A12.1.1	Documentación de procedimientos de operación	SI	Necesario definir
A12.1.2	Gestión del Cambio	SI	Necesario definir
A12.1.3	Gestión de capacidades	SI	Necesario definir por crecimiento inminente
A12.1.4	Separación de entornos de desarrollo, prueba y producción.	SI	Implementado parcialmente
A12.2	**Protección contra código malicioso**		

A12.2.1	Controles contra el código malicioso	SI	Necesario en equipos de usuario y sistemas de la compañía
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	SI	Implementado parcialmente. En parte viene por acuerdos por terceros (SLAs)
A12.4	**Registro de actividad y supervisión**		
A12.4.1	Registro y gestión de eventos de actividad	SI	Implementado parcialmente
A12.4.2	Protección de los registros de información	SI	Necesario definir
A12.4.3	Registros de actividad del administrador y operador del sistema	SI	Necesario definir
A12.4.4	Sincronización de relojes	SI	Aplica actualmente
A12.5	**Control del software en explotación.**		
A12.5.1	Instalación del software en sistemas en producción	SI	Necesario definir procedimiento
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	SI	Objetivo principal
A12.6.2	Restricciones en la instalación de software.	SI	Sólo en equipos de la compañía. Los usuarios pueden instalar lo que quieran en sus equipos
A12.7	**Consideraciones de las auditorías de los sistemas de información**		
A12.7.1	Controles de auditoría de los sistemas de información	SI	Necesario definir e implementar
A13	Seguridad en las telecomunicaciones		
A13.1	**Gestión de la seguridad en las redes**		
A13.1.1	Controles de red.	SI	Necesario definir e implementar
A13.1.2	Mecanismos de seguridad asociados a servicios en red	SI	Implementado parcialmente
A13.1.3	Segregación de redes	SI	Necesario definir e implementar
A13.2	**Intercambio de información con partes externas**		
A13.2.1	Políticas y procedimientos de intercambio de información	SI	Necesario definir con partes interesadas
A13.2.2	Acuerdos de intercambio	SI	Necesario definir con partes interesadas

A13.2.3	Mensajería electrónica.	SI	Cuando sea necesario, como parte de canal de comunicación.
A13.2.4	Acuerdos de confidencialidad y secreto	SI	Cuando sea necesario por niveles de confidencialidad.
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de infor.**		
A14.1	**Requisitos de seguridad de los sistemas de información**		
A14.1.1	Análisis y especificación de los requisitos de seguridad	SI	Necesario definir
A14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes	SI	Implementado parcialmente. Necesario definir procedimiento
A14.1.3	Protección de las transacciones por redes telemáticas	SI	Compras por partes de usuarios
A14.2	**Seguridad en los procesos de desarrollo y soporte**		
A14.2.1	Política de desarrollo seguro de software	SI	Sin política o guía común definida. Necesario formar a desarrolladores.
A14.2.2	Procedimientos de control de cambios en los sistemas	SI	Implementado parcialmente. Necesario definir
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el S.O	SI	Implementado parcialmente. Necesario definir
A14.2.4	Restricciones a los cambios en los paquetes de software	SI	Aplicable a sistemas de la organización.
A14.2.5	Uso de principios de ingeniería en protección de sistemas	SI	Sin política o guía común definida. Necesario formar a desarrolladores.
A14.2.6	Seguridad en entornos de desarrollo	SI	Necesario concienciar y buenas prácticas
A14.2.7	Externalización del desarrollo de software	NO	No aplica. No existe outsourcing de este tipo.
A14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	SI	Sin política o guía común definida. Necesario formar a desarrolladores.
A14.2.9	Pruebas de aceptación	SI	Necesario definir
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos utilizados en pruebas	SI	Necesario definir procedimiento y concienciación de usuarios
A15	**Relaciones con los suministradores**		
A15.1	**Seguridad de la información en las relaciones con suministradores**		
A15.1.1	Política de seguridad de la información para suministradores	SI	Definir y proporcionar cuando corresponda

A15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	SI	Definir y proporcionar o exigir cuando corresponda
A15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	SI	Definir y proporcionar o exigir cuando corresponda
A15.2	**Gestión de la prestación del servicio por suministradores**		
A15.2.1	Supervisión y revisión de los servicios prestados por terceros	SI	Necesario definir
A15.2.2	Gestión de cambios en los servicios prestados por terceros	NO	No aplica en este momento
A16	**Gestión de incidentes en la seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras.**		
A16.1.1	Responsabilidades y procedimientos	SI	Necesario definir responsabilidades y procedimientos de gestión de incidentes
A16.1.2	Notificación de los eventos de seguridad de la información	SI	Necesario definir procedimientos de escalado para mejorar la toma de decisiones
A16.1.3	Notificación de puntos débiles de la seguridad	SI	Necesario definir procedimientos de notificación
A16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	SI	Necesario definir procedimientos de escalado para mejorar la toma de decisiones
A16.1.5	Respuesta a los incidentes de seguridad	SI	Necesario definir procedimientos y crear equipo de seguridad
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	Necesario definir procedimientos de escalado para mejorar la toma de decisiones
A16.1.7	Recopilación de evidencias	SI	Bien por el equipo de seguridad o externamente según sea necesario
A17	**Aspectos de seguridad de la información en la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Necesario realizar y probar plan de contingencia
A17.1.2	Implantación de la continuidad de la seguridad de la información	SI	Necesario implantar
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad	SI	Necesario verificar y revisar periódicamente
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	NO	No está planeado que haya ninguna redundancia de instalaciones. Parte del procesamiento se realiza en cloud
A18	**Cumplimiento**		

A18.1	**Cumplimiento de los requisitos legales y contractuales.**		
A18.1.1	Identificación de la legislación aplicable	SI	Necesario identificar y determinar
A18.1.2	Derechos de propiedad intelectual (DPI)	SI	Necesario gestionar
A18.1.3	Protección de los registros de la organización.	SI	Implementado parcialmente. Necesario definir procesos
A18.1.4	Protección de datos y privacidad de la información personal	SI	Implementado parcialmente. Necesario definir procesos
A18.1.5	Regulación de los controles criptográficos	SI	Implementado parcialmente. Necesario definir procesos
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	SI	Está planificado auditorías externas e independientes
A18.2.2	Cumplimiento de las políticas y normas de seguridad	SI	Necesario en las revisiones.
A18.2.3	Comprobación del cumplimiento	SI	En última instancia, responsabilidad de dirección

Tabla 9 Declaración de aplicabilidad

11. Análisis y evaluación de riesgos

11.1 Definición de la metodología

El análisis de riesgos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
- Determinar a qué amenazas están expuestos aquellos activos
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

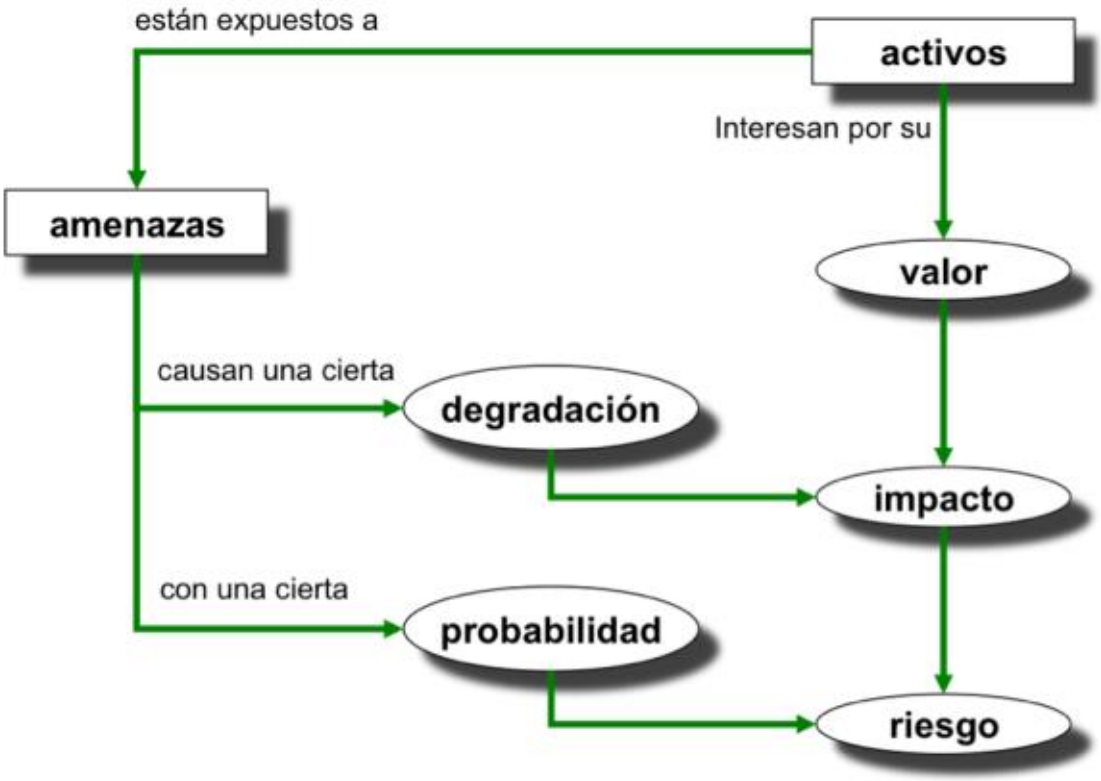

Ilustración 10 Diagrama de relaciones

La evaluación del riesgo, de manera general, incluye las siguientes actividades y acciones:

- Identificación de los activos.
- Identificación de los requisitos legales y de negocio que son relevantes para la identificación de los activos.
- Valoración de los activos identificados, teniendo en cuenta los requisitos legales y de negocio identificados anteriormente, y el impacto de una pérdida de confidencialidad, integridad y disponibilidad.
- Identificación de las amenazas y vulnerabilidades importantes para los activos identificados.
- Evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir.
- Cálculo del riesgo.
- Evaluación de los riesgos frente a una escala de riesgos preestablecidos.

Concretamente, la aplicación de la metodología MAGERIT nos permite diferenciar 10 pasos en la realización del análisis de riesgos.

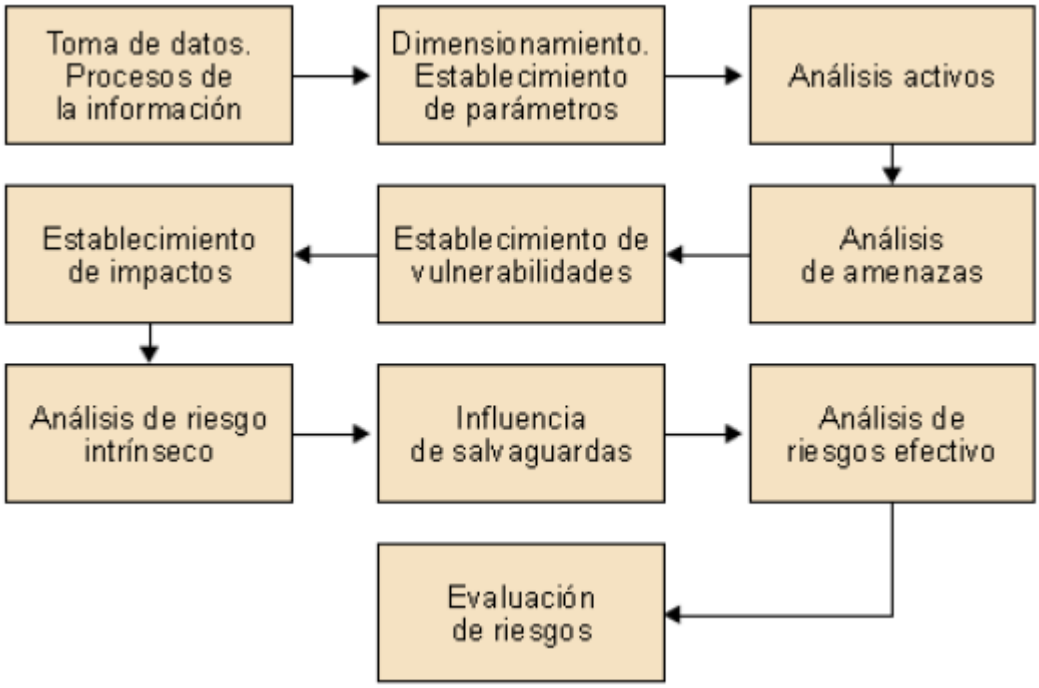

Ilustración 11 Metodología de análisis de riesgos

11.1.1 Toma de datos y proceso de información

En esta fase debe definirse el alcance que se ha de estudiar o analizar, ya que, dependiendo de éste, será más o menos costoso el proceso. A mayor alcance, mayor es el número de riesgos analizables.

Para este caso en particular el alcance va a ser:

- Seguridad física y lógica de las dos oficinas
- Hardware, software, interfaces de sistemas, datos de información en dichas localizaciones.
- Infraestructuras desplegadas en las localización (P.e: CDP)
- Personal contratado
- Sistemas y plataformas en la nube
- Activos Intangibles

11.1.2 Establecimiento de parámetros

En esta fase se procederá a establecer los parámetros que se usarán durante el proceso de análisis de riesgo.

Los parámetros que vamos identificar son los siguientes:

- Valor de los activos
- Vulnerabilidad
- Impacto
- Efectividad del control de seguridad

Así mismo se realizará una tipificación de los mismos, esto nos permitirá su identificación posterior mediante agrupaciones por tipo de activo. Esta agrupación nos ayudara también a la identificación de amenazas potenciales y la elección de salvaguardas apropiadas para cada uno de los tipos. A continuación se presentan los distintos tipos de activo considerados junto con la abreviatura utilizada para cada uno (basado en el Libro II de MAGERIT, apart 2).

Tipo	Abreviatura
Instalaciones	[L]
Hardware	[HW]
Software	[SW]
Datos/Información	[D]
Redes de comunicaciones	[COM]
Equipamiento Auxiliar	[AUX]
Personal	[P]
Soporte de información	[MEDIA]

Tabla 10 Tipos de activos según Magerit v3.0

Valor de los activos

Este parámetro tiene el objeto de asignar una valoración económica a todos los activos de una organización que se pretenden analizar. Para realizar una correcta valoración de los activos, se debe tener presente tanto el valor de uso del activo como el valor de configuración y de reposición. Para el caso de la empresa se definen los siguientes valores.

Valoración	Rango	Valor
Muy alto	> 250.001 Euros	300.000 Euros
Alto	Entre 100.001 y 250.000 Euros	175.000 Euros
Medio	Entre 15.001 y 100.000 Euros	60.000 Euros

Bajo	Entre 5001 y 15000 Euros	10.000 Euros
Muy bajo	<5000 Euros	2500 Euros

Tabla 11 Criterios de valoración de activos

Vulnerabilidad

Las vulnerabilidades se entienden como una frecuencia de ocurrencia de una amenaza; es decir, la frecuencia con la que puede una organización sufrir alguna amenaza en concreto. Se van a clasificar de la siguiente manera:

Probabilidad	Frecuencia	Valor
Muy Alta	Probabilidades de ocurrencia 1 vez al día	1
Alta	Probabilidades de ocurrencia 1 vez cada 2 semanas	26/365=0,071233
Media	Probabilidades de ocurrencia 1 vez cada 2 meses	6/365=0,016438
Baja	Probabilidades de ocurrencia 1 vez cada 6 meses	2/365=0,005479
Remota	Probabilidades de ocurrencia 1 vez al año	1/365=0,002739

Tabla 12 Frecuencia de ocurrencias

Impacto

El impacto se define como el tanto por ciento del valor del activo que se pierde en el caso de que suceda un incidente sobre él, describiendo la degradación que el activo sufre en términos de integridad, disponibilidad y confidencialidad

Valor	Criterio	Descripción
10	Daño muy grave a la organización	La explotación de la vulnerabilidad puede resultar en altas pérdidas financieras por: daño de activos o recursos tangibles, impedimento del logro de los objetivos de la organización, deterioro de la reputación e intereses. Mayor de 500.001 Euros
7-9	Daño grave a la organización	Pérdida financiera significativa, amenaza con pérdida de imagen de la Organización.

		Hasta 500.000
4-6	Daño importante a la organización	Pérdida financiera moderada, no amenaza la imagen y confianza de la Organización Hasta 250.000 Euros
1-3	Daño menor a la organización	Pérdida financiera menor. Hasta 50.000 Euros
0	Irrelevante para la organización	Costos asociados bajos. Menor de 5.000 Euros

Tabla 13 Definición de indicadores de impacto

Efectividad del control de seguridad

Este parámetro medirá la influencia que las medidas de protección tendrán en la organización. Dicho de otro modo: Cómo las diferentes medidas que podamos implementar pueden reducir el riesgo

A la hora de reducir un riesgo, hay que tener en cuenta que las medidas de seguridad tienen dos modos de actuar contra él: o bien reducen la vulnerabilidad (la frecuencia de ocurrencia), o bien reducen el impacto que provoca dicho riesgo.

Para este parámetro, también debe realizarse una clasificación de niveles válida para todo el estudio.

Variación impacto/vulnerabilidad	**Valor**
Muy alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

Tabla 14 Variación immpacto/vulnerabilidad

11.2 Identificación y valoración de activos

Un activo es cualquier elemento de la empresa que tiene un valor y es necesario proteger.

El objetivo de este apartado es caracterizar los elementos, sus relaciones con otros activos y determinar en qué dimensiones de seguridad son importantes y valorados
En este apartado se procederá a identificar y valorar los activos de la empresa, siendo activos, por ejemplo:

- Los equipos informáticos que permiten hospedar datos, aplicaciones y servicios.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los servicios que se pueden prestar gracias a aquellos datos,
- Los servicios que se necesitan para poder gestionar dichos datos
- Los dispositivos de soporte para el almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

En cuanto a la valoración, esta depende de los atributos que hacen valioso el activo (Ej.:
Autenticidad, integridad, confidencialidad, disponibilidad, trazabilidad). Una dimensión es una faceta o aspecto en particular (confidencialidad) y puede ser usada para valorar el activo de forma independiente de lo que ocurra con otras dimensiones.
Para valorar los activos es muy importante usar una escala común o criterio homogéneo que permita comparar análisis realizados en ejercicios previos, para ello vamos a hacer uso del patrón ACIDA, en el cual se valora el activo en las distintas dimensiones de seguridad y ponderando cuál de ellas resulta más crítica e importante para cada activo. Esta ponderación nos ayudará a identificar qué dimensión deberá ser mejor protegida. Las dimensiones ACIDA son las siguientes:

Propiedad	Definición
[A] Authenticity	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]
[C] Confidentiality	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[I] Integrity	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[D] Disponibility	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[A] Accountability	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

Tabla 15 Dimensiones ACIDA

Para la realización de este apartado hemos dividido los activos en las dos oficinas y hemos creado un apartado para los recursos híbridos y los sistemas en la nube.

Oficina Barcelona

Ámbito	Activo	ID	Valor	Aspectos críticos				
				A	C	I	D	A
L	Rack principal (CPD)	[L1]	10	8	9	10	10	8
L	Archivo	[L2]	8	9	9	7	8	7
AUX	Aire acondicionado oficina	[AUX1]	2	-	-	-	7	-
AUX	Aire acondicionado CPD	[AUX2]	5	-	-	-	8	-
AUX	UPS Rack	[AUX3]	5	-	-	-	8	-
AUX	Cableado LAN	[AUX4]	7	-	-	-	9	-
AUX	Cableado Eléctrico	[AUX5]	7	-	-	-	9	-
HW	Punto de acceso WIFI	[AUX6]	5	2	7	3	6	5
HW	Switch	[AUX7]	5	4	5	7	7	5
COM	Router fibra une las sedes y da conexión a Internet	[COM1]	6	5	6	8	8	6
HW	Firewall	[HW1]	6	7	6	8	9	8
HW	Centralita IP	[HW2]	7	3	6	6	9	8
HW	FAX	[HW3]	4	2	3	3	5	3
HW	3 impresoras/Escaner red Laser	[HW4]	3	2	2	4	5	5
HW	Servidor Sistema de integración continua (linux)	[HW5]	9	9	7	9	9	7
HW	Servidor VPN	[HW6]	9	9	9	9	9	8
DATOS	Servidores CRM: Nóminas, datos de cliente y negocio	[DATOS 1]	8	9	10	10	9	6
HW	IDS	[HW7]	5	6	7	6	7	8
HW	SIEM	[HW8]	6	6	6	6	8	8
HW	Servidores de Logs	[HW9]	6	9	9	9	10	8
DATOS	Servidor Backup	[DATOS 2]	9	9	9	9	10	7
P	20 empleados	[P1]	8	-	-	-	6	-
HW	20 Portátiles empleados	[HW10]	9	6	8	7	9	4
HW	2 Portátiles para el uso interno en CPD y similar	[HW11]	7	6	7	7	7	5
HW	20 Móviles empleados	[HW12]	6	5	8	6	6	7
HW	10 tablets Android	[HW13]	6	5	8	3	3	3
HW	20 Dispositivos conexión 3G/4G	[HW14]	5	5	6	2	5	5
SW	20 Libreoffice	[SW1]	4	2	3	2	3	3
SW	20 Cliente programa VPN	[SW2]	2	8	6	7	7	6
SW	5 Photoshop	[SW3]	2	2	2	2	4	3
SW	IDE Desarrollo	[SW4]	2	3	3	3	5	6
Datos	Imágenes corporativas	[Datos3]	8	-	-	6	8	5
Datos	Recursos artísticos	[Datos4]	8	-	-	7	7	5

Tabla 16 Activos Oficina Barcelona

Oficina Copenhagen

Ámbito	Activo	ID	Valor	Aspectos críticos				
				A	C	I	D	A
L	Rack principal (CPD)	[L3]	10	8	9	10	10	8
L	Archivo	[L4]	8	9	9	7	8	7
AUX	Aire acondicionado oficina	[AUX8]	2	-	-	-	7	-
AUX	Aire acondicionado CPD	[AUX9]	5	-	-	-	8	-
AUX	UPS Rack	[AUX10]	5	-	-	-	8	-
AUX	Cableado LAN	[AUX11]	7	-	-	-	9	-
AUX	Cableado Electrico	[AUX12]	7	-	-	-	9	-
HW	Punto de acceso WIFI	[HW15]	5	2	7	3	6	5
HW	1 Switch	[HW16]	5	4	5	7	7	5
COM	Router fibra une las sedes y de conexión a Internet	[COM2]	6	5	6	8	8	6
HW	Firewall	[HW17]	6	7	6	8	9	8
HW	Centralita IP	[HW18]	7	3	6	6	9	8
HW	FAX	[HW19]	4	2	3	3	5	3
HW	2 impresoras/Escaner red Laser	[HW20]	3	2	2	4	5	5
P	10 empleados	[P2]	-	-	-	-	6	-
HW	10 Portatiles empleados	[HW21]	9	6	8	7	9	4
HW	1 Portátiles para el uso interno en CPD y similar	[HW22]	7	6	7	7	7	5
HW	10 Móviles empleados	[HW23]	6	5	8	6	6	7
HW	10 tablets Android	[HW24]	6	5	8	3	3	3
HW	10 Dispositivos conexión 3G/4G	[HW25]	5	5	6	2	5	5
SW	10 Libreoffice	[SW5]	4	2	3	2	3	3
SW	10 Cliente programa VPN	[SW6]	2	8	6	7	7	6
SW	IDE Desarrollo	[SW7]	2	3	3	3	5	6

Tabla 17 Activos Oficina Copenhagen

Recursos y servicios Híbridos o en la nube

Ámbito	Activo	ID	Valor	Aspectos críticos				
				A	C	I	D	A
DATOS	Estadísticas Juego Usuario (Amazon)	[DATOS 5]	9	8	10	9	9	8
DATOS	Servidor de almacenaje de código (externo)	[DATOS 6]	10	10	10	10	10	9
DATOS	Servidor de recursos y documentación (externo)	[DATOS 7]	9	8	8	9	9	8
DATOS	Servidor de correo (Externo)	[DATOS 8]	8	8	9	9	9	9
DATOS	Servidor de recursos y documentación (externo)	[DATOS 9]	8	7	7	8	9	

Tabla 18 Activos en la nube

11.3 Identificación de amenazas

De acuerdo con la metodología MAGERIT v3, vamos a considerar las siguiente posibles amenazas extraídas del Libro II, punto 5, "Catalogo de Elementos". Estas son:

[N] Desastres naturales. Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

- [N.1] Fuego
- N.2] Daños por agua
- [N.*] Desastres naturales

[I] De origen industrial. Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada. Origen: Natural (accidental)

- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte de suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios y suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados. Fallos no intencionales causados por las personas. Origen: Humano (accidental)

- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización
- [E.4] Errores de configuración
- [E.8] Difusión de SW dañino
- [E.9] Errores de [re]-encaminamiento
- [E.10] Errores de secuencia
- [E.15] Alteración accidental de la información
- [E.18] Destrucción de la información
- [E.19] Fugas de información
- [E.20] Vulnerabilidades de los programas (SW)
- [E.21] Errores de mantenimiento / actualización de programas (SW)
- [E.23] Errores de mantenimiento / actualización de equipos (HW)

- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques intencionados. Fallos deliberados causados por las personas. Origen: Humano (deliberado)

- [A.3]Manipulación de los registros de actividad (log)
- [A.4]Manipulación de la configuración
- [A.5]Suplantación de la identidad del usuario
- [A.6]Abuso de privilegios de acceso
- [A.7]Uso no previsto
- [A.8]Difusión de software dañino
- [A.9] [Re-]encaminamiento de mensajes
- [A.10]Alteración de secuencia
- [A.11]Acceso no autorizado
- [A.12]Análisis de tráfico
- [A.13]Repudio
- [A.14]Interceptación de información (escucha)
- [A.15]Modificación deliberada de la información
- [A.18]Destrucción de información
- [A.19]Divulgación de información
- [A.22]Manipulación de programas
- [A.23]Manipulación de los equipos
- [A.24]Denegación de servicio
- [A.25]Robo
- [A.26]Ataque destructivo
- [A.27]Ocupación enemiga
- [A.28]Indisponibilidad del personal
- [A.29]Extorsión
- [A.30]Ingeniería social (picaresca)

Procedemos a continuación a realizar la identificación de amenazas para cada grupo de activos.

ACTIVOS [HW]	Frecuencia	A	C	I	D	A
[HW1]Firewall	Media		100,00%	50,00%	100,00%	
[HW2]Centralita IP	Media		100,00%	50,00%	100,00%	
[HW3]FAX	Media		100,00%	50,00%	100,00%	
[HW4]3 impresoras/Escaner red Laser	Media		100,00%	50,00%	100,00%	
[HW5]Servidor Sistema de integración continua (linux)	Media		100,00%	50,00%	100,00%	
[HW6]Servidor VPN	Media		100,00%	50,00%	100,00%	
[HW7]IDS	Media		100,00%	50,00%	100,00%	
[HW8]SIEM	Media		100,00%	50,00%	100,00%	
[HW9]Servidores de Logs	Media		100,00%	50,00%	100,00%	
[HW10]20 Portatiles empleados	Media		100,00%	50,00%	100,00%	
[HW11]2 Portátiles para el uso interno en CPD y similar	Media		100,00%	50,00%	100,00%	
[HW12]20 Móviles empleados	Media		100,00%	50,00%	100,00%	
[HW13]10 tablets android	Media		100,00%	50,00%	100,00%	
[HW14]20 Dispositivos conexión 3G/4G	Media		100,00%	50,00%	100,00%	
[HW15]Punto de acceso WIFI	Media		100,00%	50,00%	100,00%	
[HW16]1 Switch	Media		100,00%	50,00%	100,00%	
[HW17]Firewall	Media		100,00%	50,00%	100,00%	
[HW18]Centralita IP	Media		100,00%	50,00%	100,00%	
[HW19]FAX	Media		100,00%	50,00%	100,00%	
[HW20]2 impresoras/Escaner red Laser	Media		100,00%	50,00%	100,00%	
[HW21]10 Portatiles empleados	Media		100,00%	50,00%	100,00%	
[HW22]1 Portátiles para el uso interno en CPD y similar	Media		100,00%	50,00%	100,00%	
[HW23]10 Móviles empleados	Media		100,00%	50,00%	100,00%	
[HW24]10 tablets android	Media		100,00%	50,00%	100,00%	
[HW25]10 Dispositivos conexión 3G/4G	Media		100,00%	50,00%	100,00%	
LISTA DE AMENAZAS						
[N.1] Fuego	Remota				100,00%	
[N.2] Daños por agua	Remota				50,00%	
[N.*] Desastres naturales	Remota				50,00%	
[I.1] Fuego	Remota				100,00%	
[I.2] Daños por agua	Remota				50,00%	
[I.*] Desastres industriales	Remota				50,00%	
[I.3] Contaminación mecánica	Remota				50,00%	
[I.4] Contaminación electromagnética	Remota				50,00%	
[I.5] Avería de origen físico o lógico	Remota				50,00%	
[I.6] Corte del suministro eléctrico	Baja				100,00%	
[I.7] Condiciones inadecuadas de temperatura o humedad	Baja				50,00%	
[I.11] Emanaciones electromagnéticas	Remota				25,00%	
[E.2] Errores del administrador	Baja		50,00%	50,00%	50,00%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Baja		25,00%	50,00%	75,00%	
[E.24] Caída del sistema por agotamiento de recursos	Baja			10,00%	50,00%	
[E.25] Pérdida de equipos	Media		100,00%		100,00%	
[A.6] Abuso de privilegios de acceso	Remota		100,00%	50,00%		
[A.7] Uso no previsto	Baja		100,00%	50,00%		
[A.11] Acceso no autorizado	Media		100,00%	50,00%		
[A.23] Manipulación de los equipos	Media		100,00%		50,00%	
[A.24] Denegación de servicio	Baja				75,00%	
[A.25] Robo	Remota		100,00%		100,00%	
[A.26] Ataque destructivo	Remota				100,00%	

Tabla 19 Identificación de amenazas para activos HW

ACTIVOS [SW]	Frecuencia	[A]	[C]	[I]	[D]	[A]
[SW1] 20 Libreoffice	Alta	100,00%	100,00%	100,00%	100,00%	
[SW2] 20 Cliente programa VPN	Alta	100,00%	100,00%	100,00%	100,00%	
[SW3] 5 Phtoshop	Alta	100,00%	100,00%	100,00%	100,00%	
[SW4] IDE Desarrollo	Alta	100,00%	100,00%	100,00%	100,00%	
[SW5] 10 Libreoffice	Alta	100,00%	100,00%	100,00%	100,00%	
[SW6] 10 Cliente programa VPN	Alta	100,00%	100,00%	100,00%	100,00%	
[SW7] IDE Desarrollo	Alta	100,00%	100,00%	100,00%	100,00%	
LISTA DE AMENAZAS						
[I.5] Avería de origen físico o lógico	Baja				75,00%	
[E.1] Errores de los usuarios	Baja		10,00%	20,00%	10,00%	
[E.2] Errores del administrador	Remota		25,00%	20,00%	25,00%	
[E.8] Difusión de software dañino	Baja		30,00%	20,00%	50,00%	
[E.9] Errores de [re-]encaminamiento	Remota		10,00%			
[E.10] Errores de secuencia	Remota			10,00%		
[E.15] Alteración accidental de la información	Remota			10,00%		
[E.18] Destrucción de información	Baja				50,00%	
[E.19] Fugas de información	Baja		15,00%			
[E.20] Vulnerabilidades de los programas (software)	Baja		30,00%	30,00%	25,00%	
[E.21] Errores de mantenimiento / actualización de programas (software)	Alta			50,00%	30,00%	
[A.5] Suplantación de la identidad del usuario	Media	100,00%	50,00%	100,00%		
[A.6] Abuso de privilegios de acceso	Baja		50,00%	25,00%	25,00%	
[A.7] Uso no previsto	Remota		50,00%	10,00%	50,00%	
[A.8] Difusión de software dañino	Media		80,00%	80,00%	80,00%	
[A.9] [Re-]encaminamiento de mensajes	Remota		50,00%			
[A.10] Alteración de secuencia	Remota			25,00%		
[A.11] Acceso no autorizado	Remota		50,00%	25,00%		
[A.15] Modificación deliberada de la información	Remota			50,00%		
[A.18] Destrucción de información	Baja				20,00%	
[A.19] Divulgación de información	Media		50,00%			
[A.22] Manipulación de programas	Baja		100,00%	100,00%	100,00%	

Tabla 20 Identificación de amenazas para activos SW

ACTIVOS [DATOS]	Frecuencia	[A]	[C]	[I]	[D]	[A]
[DATOS1] Servidores CRM: Nóminas, datos de cliente y negocio	Alta	100,00%	100,00%	75,00%	100,00%	
[DATOS2] Servidor Backup	Alta	100,00%	100,00%	75,00%	100,00%	
[DATOS3] Imagenes corporativas	Alta	100,00%	100,00%	75,00%	100,00%	
[DATOS4] Recursos artisticos	Alta	100,00%	100,00%	75,00%	100,00%	
[DATOS5] Estadísticas Juego Usuario (Amazon)	Alta	100,00%	100,00%	75,00%	100,00%	
[DATOS6] Servidor de almacenaje de código (externo)	Alta	100,00%	100,00%	75,00%	100,00%	
[DATOS7] Servidor de recursos y documentación (externo)	Alta	100,00%	100,00%	75,00%	100,00%	
[DATOS8] Servidor de correo (Externo)	Alta	100,00%	100,00%	75,00%	100,00%	
LISTA DE AMENAZAS						
E.1] Errores de los usuarios	Alta		25,00%	25,00%	25,00%	
[E.2] Errores del administrador	Baja		30,00%	50,00%	30,00%	
[E.15] Alteración accidental de la información	Baja			20,00%		
[E.18] Destrucción de información	Baja			25,00%		
E.19] Fugas de información	Media			25,00%		
[A.5] Suplantación de la identidad del usuario	Baja	100,00%	50,00%	50,00%		
[A.6] Abuso de privilegios de acceso	Baja		100,00%	50,00%	100,00%	
[A.11] Acceso no autorizado	Baja			75,00%		
[A.15] Modificación deliberada de la información	Baja			50,00%		
[A.18] Destrucción de información	Remota				100,00%	
[A.19] Divulgación de información	Remota		100,00%			

Tabla 21 Identificación de amenazas para activos DATOS

ACTIVOS [AUX]	Frecuencia	[A]	[C]	[I]	[D]	[A]
[AUX1] Aire acondicionado oficina	Baja		100,00%	25,00%	100,00%	
[AUX2] Aire acondicionado CPD	Baja		100,00%	25,00%	100,00%	
[AUX3] UPS Rack	Baja		100,00%	25,00%	100,00%	
[AUX4] Cableado LAN	Baja		100,00%	25,00%	100,00%	
[AUX5] Cableado Electrico	Baja		100,00%	25,00%	100,00%	
[AUX6] Punto de acceso WIFI	Baja		100,00%	25,00%	100,00%	
[AUX7] Switch	Baja		100,00%	25,00%	100,00%	
[AUX8] Aire acondicionado oficina	Baja		100,00%	25,00%	100,00%	
[AUX9] Aire acondicionado CPD	Baja		100,00%	25,00%	100,00%	
[AUX10] UPS Rack	Baja		100,00%	25,00%	100,00%	
[AUX11] Cableado LAN	Baja		100,00%	25,00%	100,00%	
[AUX12] Cableado Electrico	Baja		100,00%	25,00%	100,00%	
LISTA DE AMENAZAS						
[N.1] Fuego	Remota				100,00%	
[N.2] Daños por agua	Remota				100,00%	
[N.*] Desastres naturales	Remota				100,00%	
[I.1] Fuego	Remota				100,00%	
[I.2] Daños por agua	Remota				100,00%	
[I.*] Desastres industriales	Remota				100,00%	
[I.3] Contaminación mecánica	Remota				100,00%	
[I.4] Contaminación electromagnética	Remota				100,00%	
[I.5] Avería de origen físico o lógico	Remota				100,00%	
[I.6] Corte del suministro eléctrico	Remota				100,00%	
[I.7] Condiciones inadecuadas de temperatura o humedad	Remota				100,00%	
[I.9] Interrupción de otros servicios y suministros esenciales	Remota				100,00%	
[I.11] Emanaciones electromagnéticas – NO APLICA -	Remota				100,00%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Baja				100,00%	
[E.25] Pérdida de equipos	Remota		30,00%		100,00%	
[A.7] Uso no previsto	Baja		20,00%	20,00%	100,00%	
[A.11] Acceso no autorizado	Baja		50,00%	25,00%		
[A.23] Manipulación de los equipos	Baja		30,00%		100,00%	
[A.25] Robo	Baja		100,00%		100,00%	
[A.26] Ataque destructivo	Remota				100,00%	

Tabla 22 Identificación de amenazas para activos AUX

ACTIVOS [L]	Frecuencia	[A]	[C]	[I]	[D]	[A]
[L1] Rack principal (CPD)	Baja		100,00%	50,00%	100,00%	
[L2] Archivo	Baja		100,00%	50,00%	100,00%	
[L3] Rack principal (CPD)	Baja		100,00%	50,00%	100,00%	
[L4] Archivo	Baja		100,00%	50,00%	100,00%	
LISTA DE AMENAZAS						
[N.1] Fuego	Remota				100,00%	
[N.2] Daños por agua	Remota				100,00%	
[N.*] Desastres naturales	Remota				100,00%	
[I.1] Fuego	Remota				100,00%	
[I.2] Daños por agua	Remota				100,00%	
[I.*] Desastres industriales	Remota				100,00%	
[I.11] Emanaciones electromagnéticas	Remota					
[E.15] Alteración accidental de la información	Baja			30,00%		
[E.18] Destrucción de información	Remota				50,00%	
[E.19] Fugas de información	Baja		25,00%			
[A.7] Uso no previsto	Baja		50,00%	50,00%	50,00%	
[A.11] Acceso no autorizado	Remota		60,00%	50,00%		
[A.15] Modificación deliberada de la información	Remota			50,00%		
[A.18] Destrucción de información	Remota				75,00%	
[A.19] Divulgación de información	Remota		80,00%			
[A.26] Ataque destructivo	Remota				100,00%	
[A.27] Ocupación enemiga	Remota		100,00%		100,00%	

Tabla 23Identificación de amenazas para activos L

ACTIVOS [P]	Frecuencia	[A]	[C]	[I]	[D]	[A]
[P1] 20 empleados	Baja		75,00%	50,00%	80,00%	
[P2] 10 empleados	Baja		75,00%	50,00%	80,00%	
LISTA DE AMENAZAS						
[E.19] Fugas de información	Baja		75,00%			
[E.28] Indisponibilidad del personal	Baja				25,00%	
[A.28] Indisponibilidad del personal	Baja				80,00%	
[A.29] Extorsión	Remota		50,00%	50,00%	50,00%	
[A.30] Ingeniería social (picaresca)	Baja		25,00%	25,00%	25,00%	

Tabla 24 Identificación de amenazas para activos P

ACTIVOS [COM]	Frecuencia	[A]	[C]	[I]	[D]	[A]
[COM1] Router fibra une las sedes y da conexión a Internet	Baja	100,00%	50,00%	50,00%	80,00%	
LISTA DE AMENAZAS						
[I.8] Fallo de servicios de comunicaciones	Baja				50,00%	
[E.2] Errores del administrador	Baja		30,00%	25,00%	30,00%	
[E.9] Errores de [re-]encaminamiento	Remota		15,00%			
[E.10] Errores de secuencia	Remota			15,00%		
[E.15] Alteración accidental de la información	Remota			25,00%		
[E.18] Destrucción de información	Remota				25,00%	
[E.19] Fugas de información	Remota		15,00%			
[E.24] Caída del sistema por agotamiento de recursos	Remota				50,00%	
[A.5] Suplantación de la identidad del usuario	Remota	100,00%	50,00%	30,00%		
[A.6] Abuso de privilegios de acceso	Remota		25,00%	15,00%	40,00%	
[A.7] Uso no previsto	Baja		20,00%	15,00%	75,00%	
[A.9] [Re-]encaminamiento de mensajes	Remota		20,00%			
[A.10] Alteración de secuencia	Remota			10,00%		
[A.11] Acceso no autorizado	Remota		50,00%	25,00%		
[A.12] Análisis de tráfico	Remota		25,00%			
[A.14] Interceptación de información (escucha)	Remota		50,00%			
[A.15] Modificación deliberada de la información	Remota			50,00%		
[A.19] Divulgación de información	Remota		50,00%			
[A.24] Denegación de servicio	Remota				80,00%	

Tabla 25 Identificación de amenazas para activos COM

11.4 Evaluación del impacto en los activos

Se denomina impacto a la medida de daño sobre el activo derivado de la materialización de una amenaza. Una vez que conocemos los activos, el valor de los mismos en distintas dimensiones ACIDA, el impacto potencial va a ser calculado para cada una de las dimensiones del activo mediante la siguiente fórmula:

Impacto Potencial = Valor Activo X Porcentaje de Impacto

Por tanto, vamos a proceder a calcular el valor del impacto para los distintos activos.

		Criticidad					% Impacto					Impacto Potencial				
TIPO	ID	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
HW	[HW1]	7	6	8	9	8		100,00 %	50,00 %	100,00 %		0	6	4	9	0
	[HW2]	3	6	6	9	8		100,00 %	50,00 %	100,00 %		0	6	3	9	0
	[HW3]	2	3	3	5	3		100,00 %	50,00 %	100,00 %		0	3	1,5	5	0
	[HW4]	2	2	4	5	5		100,00 %	50,00 %	100,00 %		0	2	2	5	0
	[HW5]	9	7	9	9	7		100,00 %	50,00 %	100,00 %		0	7	4,5	9	0
	[HW6]	9	9	9	9	8		100,00 %	50,00 %	100,00 %		0	9	4,5	9	0
	[HW7]	6	7	6	7	8		100,00 %	50,00 %	100,00 %		0	7	3	7	0
	[HW8]	6	6	6	8	8		100,00 %	50,00 %	100,00 %		0	6	3	8	0
	[HW9]	9	9	9	10	8		100,00 %	50,00 %	100,00 %		0	9	4,5	10	0
	[HW10]	6	8	7	9	4		100,00 %	50,00 %	100,00 %		0	8	3,5	9	0
	[HW11]	6	7	7	7	5		100,00 %	50,00 %	100,00 %		0	7	3,5	7	0
	[HW12]	5	8	6	6	7		100,00 %	50,00 %	100,00 %		0	8	3	6	0
	[HW13]	5	8	3	3	3		100,00 %	50,00 %	100,00 %		0	8	1,5	3	0
	[HW14]	5	6	2	5	5		100,00 %	50,00 %	100,00 %		0	6	1	5	0
	[HW15]	2	7	3	6	5		100,00 %	50,00 %	100,00 %		0	7	1,5	6	0
	[HW16]	4	5	7	7	5		100,00 %	50,00 %	100,00 %		0	5	3,5	7	0
	[HW17]	7	6	8	9	8		100,00 %	50,00 %	100,00 %		0	6	4	9	0
	[HW18]	3	6	6	9	8		100,00 %	50,00 %	100,00 %		0	6	3	9	0
	[HW19]	2	3	3	5	3		100,00 %	50,00 %	100,00 %		0	3	1,5	5	0
	[HW20]	2	2	4	5	5		100,00 %	50,00 %	100,00 %		0	2	2	5	0
	[HW21]	6	8	7	9	4		100,00 %	50,00 %	100,00 %		0	8	3,5	9	0
	[HW22]	6	7	7	7	5		100,00 %	50,00 %	100,00 %		0	7	3,5	7	0
	[HW23]	5	8	6	6	7		100,00 %	50,00 %	100,00 %		0	8	3	6	0
	[HW24]	5	8	3	3	3		100,00 %	50,00 %	100,00 %		0	8	1,5	3	0
	[HW25]	5	6	2	5	5		100,00 %	50,00 %	100,00 %		0	6	1	5	0
L	[L1]	8	9	10	10	8		100,00 %	50,00 %	100,00 %		0	9	5	10	0
	[L2]	9	9	7	8	7		100,00 %	50,00 %	100,00 %		0	9	3,5	8	0
	[L3]	8	9	10	10	8		100,00 %	50,00 %	100,00 %		0	9	5	10	0

	[L4]	9	9	7	8	7		100,00 %	50,00 %	100,00 %		0	9	3,5	8	0
AUX	[AUX1]	-	-	-	7	-		100,00 %	25,00 %	100,00 %		0	0	0	7	0
	[AUX2]	-	-	-	8	-		100,00 %	25,00 %	100,00 %		0	0	0	8	0
	[AUX3]	-	-	-	8	-		100,00 %	25,00 %	100,00 %		0	0	0	8	0
	[AUX4]	-	-	-	9	-		100,00 %	25,00 %	100,00 %		0	0	0	9	0
	[AUX5]	-	-	-	9	-		100,00 %	25,00 %	100,00 %		0	0	0	9	0
	[AUX6]	2	7	3	6	5		100,00 %	25,00 %	100,00 %		0	7	0,75	6	0
	[AUX7]	4	5	7	7	5		100,00 %	25,00 %	100,00 %		0	5	1,75	7	0
	[AUX8]	-	-	-	7	-		100,00 %	25,00 %	100,00 %		0	0	0	7	0
	[AUX9]	-	-	-	8	-		100,00 %	25,00 %	100,00 %		0	0	0	8	0
	[AUX10]	-	-	-	8	-		100,00 %	25,00 %	100,00 %		0	0	0	8	0
	[AUX11]	-	-	-	9	-		100,00 %	25,00 %	100,00 %		0	0	0	9	0
	[AUX12]	-	-	-	9	-		100,00 %	25,00 %	100,00 %		0	0	0	9	0
COM	[COM1]	5	6	8	8	6	100,00 %	50,00 %	50,00 %	80,00 %		5	3	4	6,4	0
Dat	[DATOS1]	9	10	10	9	6	100,00 %	100,00 %	75,00 %	100,00 %		9	10	7,5	9	0
	[DATOS2]	9	9	9	10	7	100,00 %	100,00 %	75,00 %	100,00 %		9	9	6,75	10	0
	[DATOS3]	-	-	6	8	5	100,00 %	100,00 %	75,00 %	100,00 %		0	0	4,5	8	0
	[DATOS4]	-	-	7	7	5	100,00 %	100,00 %	75,00 %	100,00 %		0	0	5,25	7	0
	[DATOS5]	8	10	9	9	8	100,00 %	100,00 %	75,00 %	100,00 %		8	10	6,75	9	0
	[DATOS6]	10	10	10	10	9	100,00 %	100,00 %	75,00 %	100,00 %		10	10	7,5	10	0
	[DATOS7]	8	8	9	9	8	100,00 %	100,00 %	75,00 %	100,00 %		8	8	6,75	9	0
	[DATOS8]	8	9	9	9	9	100,00 %	100,00 %	75,00 %	100,00 %		8	9	6,75	9	0
P	[P1]	-	-	-	6	-		75,00 %	50,00 %	80,00 %		0	0	0	4,8	0
	[P2]	-	-	-	6	-		75,00 %	50,00 %	80,00 %		0	0	0	4,8	0
SW	[SW1]	2	3	2	3	3	100,00 %	100,00 %	100,00 %	100,00 %		2	3	2	3	0
	[SW2]	8	6	7	7	6	100,00 %	100,00 %	100,00 %	100,00 %		8	6	7	7	0
	[SW3]	2	2	2	4	3	100,00 %	100,00 %	100,00 %	100,00 %		2	2	2	4	0
	[SW4]	3	3	3	5	6	100,00 %	100,00 %	100,00 %	100,00 %		3	3	3	5	0
	[SW5]	2	3	2	3	3	100,00 %	100,00 %	100,00 %	100,00 %		2	3	2	3	0
	[SW6]	8	6	7	7	6	100,00 %	100,00 %	100,00 %	100,00 %		8	6	7	7	0
	[SW7]	3	3	3	5	6	100,00 %	100,00 %	100,00 %	100,00 %		3	3	3	5	0

Tabla 26 Evaluación del impacto

11.5 Evaluación del riesgo potencial

Una vez obtenido el impacto potencial vamos a proceder a realizar el cálculo del riesgo potencial. Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. Este riesgo es calculado para cada activo en cada dimensión mediante la siguiente formula:

Riesgo = Frecuencia X Impacto Potencial

Para facilitar la lectura, se multiplica cada valor por cien.

				Impacto Potencial				Riesgo					
TIPO	ID	Frecuencia	Valor Frec	A	C	I	D	A	A	C	I	D	A
	[HW1]	Media	0,016438	0	6	4	9	0	0	9,8628	6,5752	14,7942	0
	[HW2]	Media	0,016438	0	6	3	9	0	0	9,8628	4,9314	14,7942	0
	[HW3]	Media	0,016438	0	3	1,5	5	0	0	4,9314	2,4657	8,219	0
	[HW4]	Media	0,016438	0	2	2	5	0	0	3,2876	3,2876	8,219	0
	[HW5]	Media	0,016438	0	7	4,5	9	0	0	11,5066	7,3971	14,7942	0
	[HW6]	Media	0,016438	0	9	4,5	9	0	0	14,7942	7,3971	14,7942	0
	[HW7]	Media	0,016438	0	7	3	7	0	0	11,5066	4,9314	11,5066	0
	[HW8]	Media	0,016438	0	6	3	8	0	0	9,8628	4,9314	13,1504	0
	[HW9]	Media	0,016438	0	9	4,5	10	0	0	14,7942	7,3971	16,438	0
	[HW10]	Media	0,016438	0	8	3,5	9	0	0	13,1504	5,7533	14,7942	0
	[HW11]	Media	0,016438	0	7	3,5	7	0	0	11,5066	5,7533	11,5066	0
	[HW12]	Media	0,016438	0	8	3	6	0	0	13,1504	4,9314	9,8628	0
	[HW13]	Media	0,016438	0	8	1,5	3	0	0	13,1504	2,4657	4,9314	0
	[HW14]	Media	0,016438	0	6	1	5	0	0	9,8628	1,6438	8,219	0
	[HW15]	Media	0,016438	0	7	1,5	6	0	0	11,5066	2,4657	9,8628	0
	[HW16]	Media	0,016438	0	5	3,5	7	0	0	8,219	5,7533	11,5066	0
	[HW17]	Media	0,016438	0	6	4	9	0	0	9,8628	6,5752	14,7942	0
	[HW18]	Media	0,016438	0	6	3	9	0	0	9,8628	4,9314	14,7942	0
	[HW19]	Media	0,016438	0	3	1,5	5	0	0	4,9314	2,4657	8,219	0
	[HW20]	Media	0,016438	0	2	2	5	0	0	3,2876	3,2876	8,219	0
	[HW21]	Media	0,016438	0	8	3,5	9	0	0	13,1504	5,7533	14,7942	0
	[HW22]	Media	0,016438	0	7	3,5	7	0	0	11,5066	5,7533	11,5066	0
	[HW23]	Media	0,016438	0	8	3	6	0	0	13,1504	4,9314	9,8628	0
	[HW24]	Media	0,016438	0	8	1,5	3	0	0	13,1504	2,4657	4,9314	0
	[HW25]	Media	0,016438	0	6	1	5	0	0	9,8628	1,6438	8,219	0
	[L1]	Baja	0,005479	0	9	5	10	0	0	4,9311	2,7395	5,479	0
	[L2]	Baja	0,005479	0	9	3,5	8	0	0	4,9311	1,91765	4,3832	0
	[L3]	Baja	0,005479	0	9	5	10	0	0	4,9311	2,7395	5,479	0
	[L4]	Baja	0,005479	0	9	3,5	8	0	0	4,9311	1,91765	4,3832	0
	[AUX1]	Baja	0,005479	0	0	0	7	0	0	0	0	3,8353	0
	[AUX2]	Baja	0,005479	0	0	0	8	0	0	0	0	4,3832	0
	[AUX3]	Baja	0,005479	0	0	0	8	0	0	0	0	4,3832	0
	[AUX4]	Baja	0,005479	0	0	0	9	0	0	0	0	4,9311	0

	[AUX5]	Baja	0,005479	0	0	0	9	0	0	0	0	4,9311	0
	[AUX6]	Baja	0,005479	0	7	0,75	6	0	0	3,8353	0,410925	3,2874	0
	[AUX7]	Baja	0,005479	0	5	1,75	7	0	0	2,7395	0,958825	3,8353	0
	[AUX8]	Baja	0,005479	0	0	0	7	0	0	0	0	3,8353	0
	[AUX9]	Baja	0,005479	0	0	0	8	0	0	0	0	4,3832	0
	[AUX10]	Baja	0,005479	0	0	0	8	0	0	0	0	4,3832	0
	[AUX11]	Baja	0,005479	0	0	0	9	0	0	0	0	4,9311	0
	[AUX12]	Baja	0,005479	0	0	0	9	0	0	0	0	4,9311	0
	[COM1]	Baja	0,005479	5	3	4	6,4	0	2,7395	1,6437	2,1916	3,50656	0
	[DATOS1]	Alta	0,071233	9	10	7,5	9	0	64,1097	71,233	53,42475	64,1097	0
	[DATOS2]	Alta	0,071233	9	9	6,75	10	0	64,1097	64,1097	48,082275	71,233	0
	[DATOS3]	Alta	0,071233	0	0	4,5	8	0	0	0	32,05485	56,9864	0
	[DATOS4]	Alta	0,071233	0	0	5,25	7	0	0	0	37,397325	49,8631	0
	[DATOS5]	Alta	0,071233	8	10	6,75	9	0	56,9864	71,233	48,082275	64,1097	0
	[DATOS6]	Alta	0,071233	10	10	7,5	10	0	71,233	71,233	53,42475	71,233	0
	[DATOS7]	Alta	0,071233	8	8	6,75	9	0	56,9864	56,9864	48,082275	64,1097	0
	[DATOS8]	Alta	0,071233	8	9	6,75	9	0	56,9864	64,1097	48,082275	64,1097	0
	[P1]	Baja	0,005479	0	0	0	4,8	0	0	0	0	2,62992	0
	[P2]	Baja	0,005479	0	0	0	4,8	0	0	0	0	2,62992	0
	[SW1]	Alta	0,071233	2	3	2	3	0	14,2466	21,3699	14,2466	21,3699	0
	[SW2]	Alta	0,071233	8	6	7	7	0	56,9864	42,7398	49,8631	49,8631	0
	[SW3]	Alta	0,071233	2	2	2	4	0	14,2466	14,2466	14,2466	28,4932	0
	[SW4]	Alta	0,071233	3	3	3	5	0	21,3699	21,3699	21,3699	35,6165	0
	[SW5]	Alta	0,071233	2	3	2	3	0	14,2466	21,3699	14,2466	21,3699	0
	[SW6]	Alta	0,071233	8	6	7	7	0	56,9864	42,7398	49,8631	49,8631	0
	[SW7]	Alta	0,071233	3	3	3	5	0	21,3699	21,3699	21,3699	35,6165	0

Tabla 27 Evaluación del riesgo potencial

El nivel de riesgo aceptable ha sido definido y aprobado por Dirección en valores iguales o menores a 50. En la tabla anterior de riesgo se ha procedido a marcar en amarillo aquellos valores de riesgo superiores a dicho umbral y que deberán ser tratados con la implantación de controles con el objetivo de reducir su riesgo por debajo del límite establecido por Dirección.

11.6 Conclusiones

En el siguiente gráfico observamos la media que se le dan en las distintas dimensiones a los distintos grupos de activos.

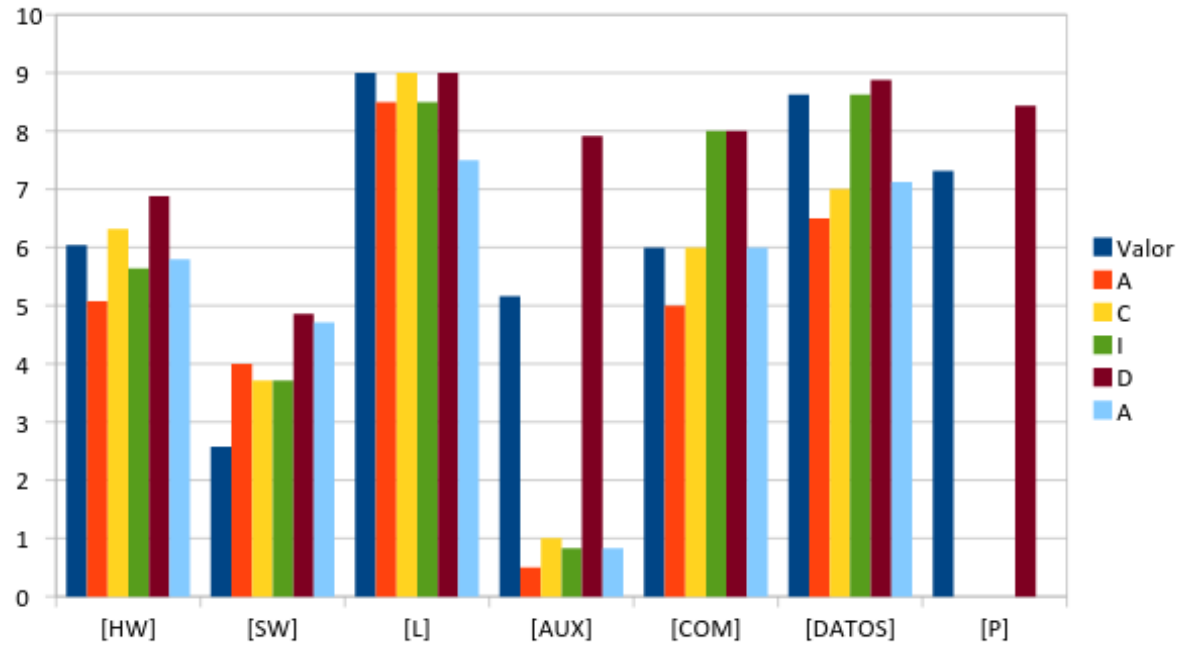

Ilustración 12 Media del valor por grupos

A continuación podemos observar el impacto medio para cada dimensión y para grupo de activos.

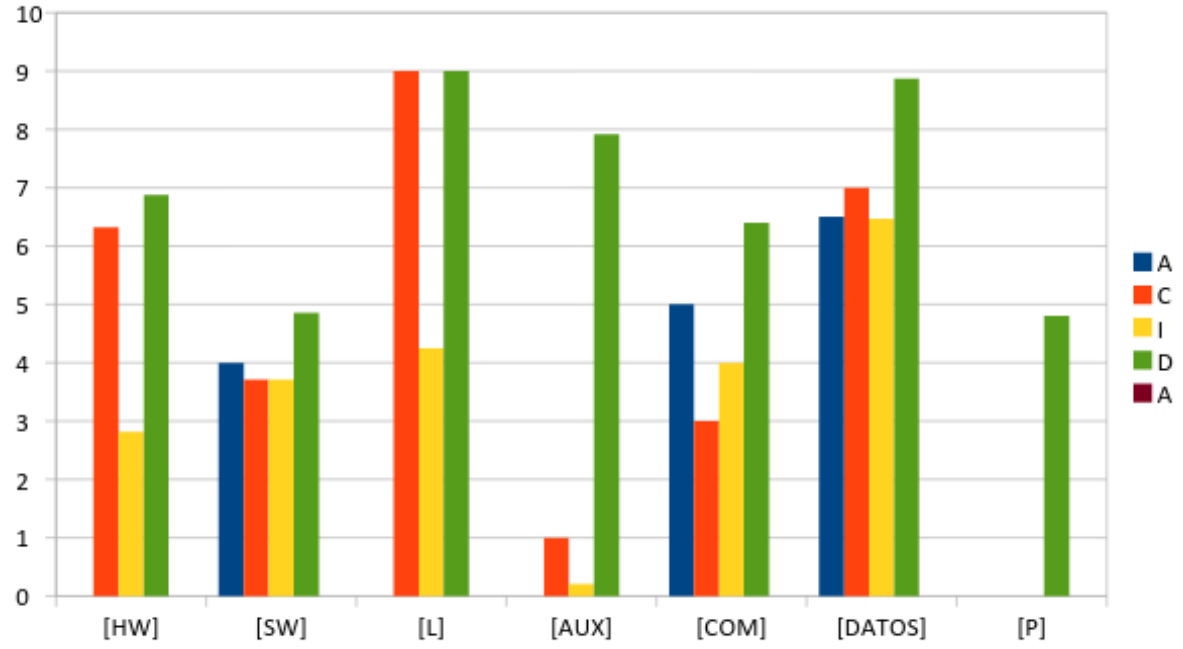

Ilustración 13 Impacto medio para cada dimensión

Finalmente obtenemos lo mismo para el riesgo:

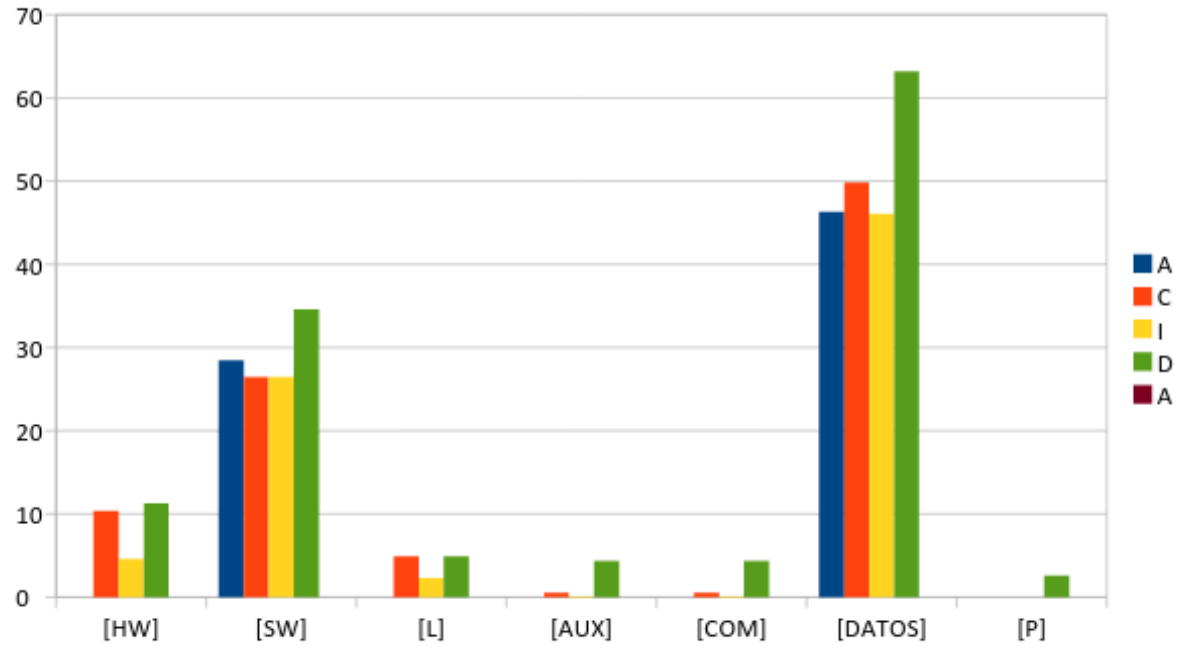

Ilustración 14 Riesgo medio para cada dimensión

Por tanto, tras observar los gráficos y basándonos en ellos podemos obtener como conclusión los siguientes puntos:

- De las distintas reuniones con la dirección y los distintos departamentos se puede observar que se obtiene una valoración alta en las instalaciones, y en algunos dominios de los datos y hardware.
- La media del impacto obtenido se denota que la disponibilidad tiene un gran impacto en todos los grupos de activos
- De la media del riesgo podemos observar qué grupos poseen una mayor exposición al riego.
- Finalmente, de la tabla del análisis de riesgo hemos obtenido una imagen clara sobre qué puntos hay que mejorar para tratar el mismo en concordancia con lo acordado con la dirección.

12. Propuesta de proyectos

Evaluación de proyectos que debe llevar a cabo la Organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de los mismos.

12.1 Introducción

En este apartado se procederá a establecer y definir una serie de proyectos que deberán acometerse en la organización para alinearse con los objetivos planteados en el plan director.

Esto es realizado conforme a las necesidades detectadas en el análisis de riesgos y los objetivos definidor por la dirección.

La finalidad de este apartado es, una vez identificados los activos más vulnerables, proponer proyectos con el objetivo de mitigar los riesgos detectados más importantes.

12.2 Propuesta de mejora

Se han propuesto 13 proyectos diferentes que engloban distintos ámbitos o dominios de la seguridad de la información

Las distintas propuestas tienen el objetivo principal de mitigar riesgos que se encuentren por encima del umbral de riesgo tolerado por dirección (>50), aunque también, como efecto colateral, se mitigaran otros riesgos (no críticos) relacionados.

Para la ejecución de este proyecto va a ser necesario contratar personal experto en algunos casos o necesitar soporte de auditores externos en otro

- PR01 – COPIAS DE SEGURIDAD
- PR02 - ORGANIZACIÓN Y CLASIFICACION DE LA INFORMACION
- PR03 - DEFINICION DE UN BASELINE EN SOFTWARE y HARDWARE
- PR04 - PLAN DE CONTINUIDAD DE NEGOCIO
- PR05 - POLITICA DE SEGURIDAD DE LA INFORMACION
- PR06 - POLITICA DE CONTROL DE ACCESO
- PR07 - DEFINICION DE POLITICAS DE ACTUALIZACION
- PR08 - PROGRAMA DE FORMACION CONTINUA
- PR09 - RRHH
- PR10 - GESTION DE INCIDENTES DE SEGURIDAD , INTEGRACIÓN SIEM Y LOGS E INTELIGENCIA DE AMENAZAS
- PR11 – PLAN DE GESTION DE ACTIVOS DE EMPRESA Y EMPLEADOS
- PR12 – GESTION DE PROVEEDORES
- PR13 – CUMPLIMIENTO DE LEGISLACION Y PROPIEDAD INTELECTUAL

12.3 Planificación temporal y económica

La ejecución del plan se llevará a cabo a través de 24 meses (Dos años) en total comenzará el 1 de Septiembre de 2016 y finalizará el 1 de Septiembre de 2018.

Para la determinación del coste y el presupuesto, la hora de trabajo de un Jefe de Proyecto será de 100 Euros, mientras que la de un técnico será de 60 Euros.

1 Person day (PD) será el equivalente a 8 horas de trabajo lectivas.

Por tanto:

- 1 PD de un JP= 800 Euros
- 1 PD de un técnico= 480 Euros

<table>
<tr><td>Proyecto</td><td colspan="3">PR01 – COPIAS DE SEGURIDAD</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td colspan="2">Fin</td></tr>
<tr><td>8 Semanas</td><td>1/09/2016</td><td colspan="2">26/10/2016</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td>Recursos</td><td colspan="3">1 JP
1 Técnico de sistemas</td></tr>
<tr><td>PD</td><td colspan="3"><table>
<tr><td>Puesto</td><td>PD</td><td>PD SubTotal</td><td rowspan="3">4640 €</td></tr>
<tr><td>JP</td><td>1PD</td><td>800 €</td></tr>
<tr><td>Técnico</td><td>8PD</td><td>3840 €</td></tr>
</table></td></tr>
<tr><td>Presupuesto</td><td colspan="3"><table>
<tr><td>Concepto</td><td>Precio</td><td rowspan="3">34640 €</td></tr>
<tr><td>Personal</td><td>4640 €</td></tr>
<tr><td>Material (Cintas, USB, HD y Armarios):</td><td>30000 €</td></tr>
</table></td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="3"><table>
<tr><td>Concepto</td><td>Subtotal</td><td rowspan="4">10440€</td></tr>
<tr><td>JP -2PD</td><td>1600 €</td></tr>
<tr><td>Técnico -8PD</td><td>3840 €</td></tr>
<tr><td>Material</td><td>5000 €</td></tr>
</table></td></tr>
<tr><td>Objetivo</td><td colspan="3">Definición de una política de copias de seguridad que garantice la integridad y disponibilidad de la información en caso de desastre.</td></tr>
<tr><td>Descripción</td><td colspan="3">Para la protección de los activos más importantes de la empresa, los datos, se hace necesario establecer claramente un procedimiento de copias de seguridad que los proteja ante cualquier desastre.

Se divide en:

1. <u>Copias de seguridad de datos en organización (servidores/backup)</u>

Es necesario realizar una copia de seguridad de todos los datos del servidor y de los distintos servicios, incluyendo datos, sistema operativo y configuraciones
La política deberá incluir un procedimiento escrito de restauración de los datos
La copia se debe realizar en cinta y almacenada en un armario ignifugo en una localización distinta a la del servidor.

2. <u>Copias de seguridad en proveedores Cloud</u>

Se deberá realizar una comprobación de los SLA de backup de los distintos proveedores de servicio, para comprobar que estos cumplen con la política de copias de seguridad. Esta se realizará una vez cada 18 meses
En caso de contratar un nuevo servicio, el SLA de copias de seguridad deberá ser aprobado por el RSI</td></tr>
</table>

	3. <u>Copias de seguridad de datos de usuario en equipos</u> Se deberá hacer énfasis (y para ello se realizarán cursos de formación) en que el usuario es responsable de mantener copias de seguridad de los datos almacenados en su equipo, los datos de trabajo y documentos deben ser salvados en los proveedores o plataformas habilitadas a tal efecto. Se deberá revisar la ejecución y validez de este procedimiento una vez cada tres meses sin prejuicio de cualquier actividad individual.
Beneficios	• Asegura la integridad y disponibilidad de los datos. • Asegura la restauración de sistemas y servicios. • Disminuye el tiempo de inactividad por perdida de datos. • Minimiza las pérdidas de información y productividad en caso de desastre
Relaciones	• Revisión SLA con proveedores cloud • Continuidad de negocio • Formación de usuarios

<table>
<tr><td>Proyecto</td><td colspan="2">PR02 - ORGANIZACIÓN Y CLASIFICACION DE LA INFORMACION</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>8 Semanas</td><td>15/09/2016</td><td>09/11/2016</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1 JP
1 Técnico</td></tr>
<tr><td>PD</td><td colspan="2">
<table>
<tr><th>Puesto</th><th>PD</th><th>SubTotal</th><th rowspan="3">2480€</th></tr>
<tr><td>JP</td><td>1 PD</td><td>800 €</td></tr>
<tr><td>Técnico</td><td>3,5 PD</td><td>1680€</td></tr>
</table>
</td></tr>
<tr><td>Presupuesto</td><td colspan="2">2480€</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2">
<table>
<tr><th>Puesto</th><th>PD</th><th>SubTotal</th><th rowspan="3">4000€</th></tr>
<tr><td>JP</td><td>2 PD</td><td>1600 €</td></tr>
<tr><td>Técnico</td><td>5 PD</td><td>2400€</td></tr>
</table>
</td></tr>
<tr><td>Objetivo</td><td colspan="2">Realizar una reorganización y reclasificación de qué y cómo se almacenan los distintos documentos y recursos en la empresa.</td></tr>
<tr><td>Descripción</td><td colspan="2">Tras el análisis completo realizado se procede a redefinir la política central de seguridad de la empresa.
Esto incluirá la redefinición de la nomenclatura de los documentos, siguiendo la política definido para ello, así como la inclusión de cierta información en los documentos.
Una vez documentada debidamente, se debe aprobar por dirección y debe ser comunicada adecuadamente tanto a la totalidad de los empleados como a toda empresa externa.
Esta política debe ser revisada anualmente así como todos los sistemas técnicos desplegados con el fin de asegurar el cumplimiento de la misma.</td></tr>
<tr><td>Beneficios</td><td colspan="2">• Definición de roles y responsabilidades en materia de seguridad.
• Implementación de cambios organizacionales en concordancia con las directrices de seguridad
• Reducción de riesgos y amenazas debido a una mejor definición de la política.
• Documentación consistente y actualizada
• Refuerzo de la seguridad con terceras partes</td></tr>
</table>

Relaciones	Con todos los procesos de seguridad de la empresa

<table>
<tr><td>Proyecto</td><td colspan="3">PR03 - DEFINICION DE UN BASELINE EN SOFTWARE Y HARDWARE</td></tr>
<tr><td>Duración</td><td colspan="2">Comienzo</td><td>Fin</td></tr>
<tr><td>12 Semanas</td><td colspan="2">15/11/2016</td><td>06/02/2016</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td>Recursos</td><td colspan="3">1 JP
2 Técnicos</td></tr>
<tr><td>PD</td><td colspan="3"><table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">4640 €</td></tr>
<tr><td>JP</td><td>1PD</td><td>800 €</td></tr>
<tr><td>Técnico</td><td>8 PD</td><td>3840€</td></tr>
</table></td></tr>
<tr><td>Presupuesto</td><td colspan="3">4640 €</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="3"><table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">6400 €</td></tr>
<tr><td>JP</td><td>2PD</td><td>1600 €</td></tr>
<tr><td>Técnico</td><td>10 PD</td><td>4800 €</td></tr>
</table></td></tr>
<tr><td>Objetivo</td><td colspan="3">Se debe realizar una auditoría de todo el software usado y necesario para la correcta operación de la organización
Por otra parte, se debe establecer una configuración estándar tanto para los clientes como para los servidores, tanto de software como de hardware. El software debe ser uniforme y debe poseer una licencia valida cuando será necesario, además de estar actualizado con los últimos parches de seguridad.
Las líneas bases deben incluir por defecto una serie de medidas de seguridad de serie</td></tr>
<tr><td>Descripción</td><td colspan="3">Es necesario definir y disponer de una línea base actualizada de todo el SW y HW, esto ayudará a definir las necesidades tanto de los programas y de hardware necesario incluyendo versiones mínimas para el funcionamiento de los mismos como requerimientos mínimos de hardware
Esta configuración de referencia debe incluir una serie de políticas de seguridad mínimas (como el bloqueo automático de pantalla en equipos desatendidos, des habilitación del autoarranque en dispositivos USB, solo permitir la ejecución de aplicación en ciertas rutas del sistema de archivos,...) que serán comunes y obligatorias en todas las instalaciones.</td></tr>
<tr><td>Beneficios</td><td colspan="3">Simplificación de la gestión y procedimientos de la organización
Incremento de la seguridad al homogeneizar las plataformas
Menor curva de aprendizaje para nuevas incorporaciones</td></tr>
</table>

	Aumento de la productividad al poder realizar instrucciones técnicas precisas y por evitar problemas de distintas versiones de Hardware o Software
Relaciones	Plan de continuidad de negocio

<table>
<tr><td>Proyecto</td><td colspan="2">PR04 - PLAN DE CONTINUIDAD DE NEGOCIO</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>24 Semanas</td><td>15/02/2017</td><td>01/08/2017</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1 JP
2 Técnicos</td></tr>
<tr><td>PD</td><td colspan="2">
<table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">16000€</td></tr>
<tr><td>JP</td><td>8 PD</td><td>6400 €</td></tr>
<tr><td>Técnico</td><td>20PD</td><td>9600 €</td></tr>
</table>
</td></tr>
<tr><td>Presupuesto</td><td colspan="2">16000€</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2">
<table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">7200€</td></tr>
<tr><td>JP</td><td>3 PD</td><td>2400€</td></tr>
<tr><td>Técnico</td><td>10 PD</td><td>4800€</td></tr>
</table>
</td></tr>
<tr><td>Objetivo</td><td colspan="2">Definir un plan de actuación que asegure la continuidad del negocio ante un eventual desastre, con el objetivo de reducir al mínimo el tiempo necesario para la recuperación de los servicios esenciales.</td></tr>
<tr><td>Descripción</td><td colspan="2">Se deberán evaluar los riesgos analizados en el presente plan y junto con el comité de SI, elaborar un documento donde se detallen los pasos a tomar en caso de desastre total dentro de la empresa. Se deberá incluir toda la información de contacto de proveedores, necesidades de hardware y software y proceso de recuperación de la información. Este plan deberá ser revisado anualmente en función de los resultados de las auditorías internas que se practiquen en un futuro.
El plan de continuidad de negocio debe ser probado (mediante un simulacro) y actualizado al menos una vez al año.</td></tr>
<tr><td>Beneficios</td><td colspan="2">• Asegura la continuidad del negocio con una interrupción mínima del mismo.
• Reduce los costes por inactividad en el negocio.
• Personal formado y preparado para reaccionar en caso de desastre grave.</td></tr>
</table>

	• Tras su elaboración detallada, se dispone de un conocimiento mayor de todos los agentes involucrados la organización.
Relaciones	-

<table>
<tr><td>Proyecto</td><td colspan="2">PR05 - POLITICA DE SEGURIDAD DE LA INFORMACION</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>10 Semanas</td><td>01/12/2016</td><td>08/02/2017</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1 JP
1 Técnico</td></tr>
<tr><td>PD</td><td colspan="2"><table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">4560 €</td></tr>
<tr><td>JP</td><td>1,5 PD</td><td>1200 €</td></tr>
<tr><td>Técnico</td><td>7 PD</td><td>3360 €</td></tr>
</table></td></tr>
<tr><td>Presupuesto</td><td colspan="2">4560 €</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2"><table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">9600 €</td></tr>
<tr><td>JP</td><td>6PD</td><td>4800</td></tr>
<tr><td>Técnico</td><td>10PD</td><td>4800</td></tr>
</table></td></tr>
<tr><td>Objetivo</td><td colspan="2">Redefinición y mejora de la política de seguridad de la empresa definida inicialmente para adecuarlo y actualizarlo al nuevo marco a implementar.</td></tr>
<tr><td>Descripción</td><td colspan="2">Tras el análisis completo realizado de la empresa se procede a redefinir la política central de seguridad de la empresa. Una vez documentada debidamente, se debe aprobar por dirección y debe ser comunicada adecuadamente tanto a la totalidad de los empleados
Esta política debe ser revisada anualmente así como todos los sistemas técnicos desplegados con el fin de asegurar el cumplimiento de la misma.</td></tr>
<tr><td>Beneficios</td><td colspan="2">• Definición de roles y responsabilidades en materia de seguridad.
• Reducción de riesgos y amenazas debido a una mejor definición de la política.
• Reducción en costes derivados de estos riesgos y amenazas.
• Refuerzo de la seguridad con terceras partes.</td></tr>
<tr><td>Relaciones</td><td colspan="2">Plan de formación</td></tr>
</table>

<table>
<tr><td>Proyecto</td><td colspan="2">PR06 - POLITICA DE CONTROL DE ACCESO</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>20 Semanas</td><td>01/05/2017</td><td>15/09/2017</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1 JP
2 Técnicos</td></tr>
<tr><td>PD</td><td colspan="2">
<table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">11200 €</td></tr>
<tr><td>JP</td><td>5PD</td><td>4000€</td></tr>
<tr><td>Técnico</td><td>15PD</td><td>7200€</td></tr>
</table>
</td></tr>
<tr><td>Presupuesto</td><td colspan="2">
<table>
<tr><td>Concepto</td><td>Subtotal</td><td rowspan="3">36200€</td></tr>
<tr><td>Personal</td><td>11200 €</td></tr>
<tr><td>Material y dispositivos:</td><td>25000 €</td></tr>
</table>
</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2">
<table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">6240€</td></tr>
<tr><td>JP</td><td>3PD</td><td>2400 €</td></tr>
<tr><td>Técnico</td><td>8PD</td><td>3840 €</td></tr>
</table>
</td></tr>
<tr><td>Objetivo</td><td colspan="2">

Definición de quien puede acceder a qué información.
Mantenimiento de la política del mínimo acceso
Definición de acceso a las premisas, oficinas y CPD

</td></tr>
<tr><td>Descripción</td><td colspan="2">Es necesario realizar:

Una auditoria completa de los usuarios de todos los sistemas, permisos y a qué información debe acceder para que realicen sus funciones
Identificar recursos y crear checklist que serán usados durante la creación, modificación y eliminación de usuarios
Proporcionar pautas a la seguridad del edificio para el control de acceso al mismo (control de entradas y salidas, control de identidad, etc.)
Establecer los dispositivos necesarios en la entrada a la oficina y a aquellos sitios identificados como sensibles
La política debe incluir también una política de creación segura de contraseña
Para los equipos de los usuarios es necesario dar pautas en la formación sobre la creación y uso de contraseñas seguras y de políticas de usuario en su equipo

</td></tr>
<tr><td>Beneficios</td><td colspan="2">

Reducción de posibles errores de usuario

</td></tr>
</table>

	• Mayor control de acceso a la información evitando posibles fugas de información. • Análisis de riesgos más fiables dentro de la empresa
Relaciones	Organización y clasificación de la información

<table>
<tr><td>Proyecto</td><td colspan="2">PR07 - DEFINICION DE POLITICAS DE ACTUALIZACION</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>4 Semanas</td><td>15/02/2017</td><td>14/03/2017</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1 JP
1 Técnico</td></tr>
<tr><td>PD</td><td colspan="2">
<table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">3200 €</td></tr>
<tr><td>JP</td><td>1 PD</td><td>800 €</td></tr>
<tr><td>Técnico</td><td>5 PD</td><td>2400 €</td></tr>
</table>
</td></tr>
<tr><td>Presupuesto</td><td colspan="2">3200 €</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2">
<table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">4640€</td></tr>
<tr><td>JP</td><td>1 PD</td><td>800 €</td></tr>
<tr><td>Técnico</td><td>8 PD</td><td>3840€</td></tr>
</table>
</td></tr>
<tr><td>Objetivo</td><td colspan="2">Establecer una política para llevar a cabo de manera correcta las actualizaciones de los distintos sistemas, con especial cuidado en los sistemas críticos, con el objetivo de que todos los sistemas y su software se encuentren siempre a la última versión.
La política también incluirá un apartado que controlará el ciclo de vida de los dispositivos, incluyendo la retirada y la eliminación segura de los datos.</td></tr>
<tr><td>Descripción</td><td colspan="2">El proyecto debe incluir la creación de un entorno de pruebas donde poder actualizar los sistemas sin miedo a interrumpir el servicio en la empresa. Se deberán definir una batería de pruebas que se ejecutaran cada vez que se realicen las actualizaciones y una vez comprobado que no se producen errores, se procederá a aprobar la actualización de los sistemas de producción. Los sistemas clientes deberían poder actualizarse sin intervención de los usuarios mientras que los servidores se actualizarán manualmente, una vez sean validadas las actualizaciones en el entorno de prueba
Dentro del programa de formación habrá un apartado dedicado a este proyecto.</td></tr>
</table>

Beneficios	• Reducción del riesgo de ataque debido a un menos número de bugs en los sistemas. • Mayor productividad de los usuarios al utilizar programas más actualizados y en teoría, con menos errores. • Ayuda a mantener un inventario completo del software de la empresa. • Evita fuga de datos al controlar la salida y eliminación de datos en los dispositivos
Relaciones	Definición de Base line

<table>
<tr><td>Proyecto</td><td colspan="2">PR08 - PROGRAMA DE FORMACION CONTINUA</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>8 Semanas</td><td>01/03/2017</td><td>25/04/2017</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1 JP
2 Técnicos (formación interna)
1 Empresa Externa</td></tr>
<tr><td>PD</td><td colspan="2">
<table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">9280 €</td></tr>
<tr><td>JP</td><td>2PD</td><td>1600 €</td></tr>
<tr><td>Técnico</td><td>16 PD</td><td>7680 €</td></tr>
</table>
</td></tr>
<tr><td>Presupuesto</td><td colspan="2">
<table>
<tr><td>Concepto</td><td>Subtotal</td><td rowspan="4">27280 €</td></tr>
<tr><td>Personal</td><td>9280 €</td></tr>
<tr><td>Empresa Externa</td><td>8000 €</td></tr>
<tr><td>Certificaciones</td><td>10000 €</td></tr>
</table>
</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2">N/A (será repetido anualmente)</td></tr>
<tr><td>Objetivo</td><td colspan="2">Conseguir la concienciación de los usuarios en materia de seguridad</td></tr>
<tr><td>Descripción</td><td colspan="2">

Se establece un calendario de formación y concienciación en materia de seguridad anual
Para los técnicos en sistemas y en seguridad se ofrece la posibilidad de certificación en cursos de seguridad y relacionados
Para los desarrolladores se impartirán cursos específicos en programación segura
Existe la posibilidad de los mismos técnicos certificados puedan impartir formación interna en materias de seguridad y concienciación
Los cursos deberán ser actualizados con los nuevos controles implementados, así como cualquier novedad que se introduzca en la organización.

</td></tr>
<tr><td>Beneficios</td><td colspan="2">

Una mayor concienciación de los usuarios reduce el riesgo de amenazas.

</td></tr>
</table>

	• Mejora la imagen de empresa con los clientes, transmitiendo seguridad y profesionalidad. • Mejora la productividad e interacción entre los trabajadores que ahora saben mejor sus roles y responsabilidades. • Mejor calidad de código y actuaciones del personal
Relaciones	

<table>
<tr><td>Proyecto</td><td colspan="2">PR09 – RRHH</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>8 Semanas</td><td>02/10/2017</td><td>24/11/2017</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1JP
1Tecnico</td></tr>
<tr><td>PD</td><td colspan="2"><table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">3200 €</td></tr>
<tr><td>JP</td><td>1PD</td><td>800 €</td></tr>
<tr><td>Técnico</td><td>5PD</td><td>2400 €</td></tr>
</table></td></tr>
<tr><td>Presupuesto</td><td colspan="2">3200 €</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2"><table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">4800 €</td></tr>
<tr><td>JP</td><td>0PD</td><td>0 €</td></tr>
<tr><td>Técnico</td><td>10PD</td><td>4800 €</td></tr>
</table></td></tr>
<tr><td>Objetivo</td><td colspan="2">Crear, almacenar y proteger toda la información relativa al ciclo de vida de los empleados. Debe abarcar todo lo referente a su contratación, modificaciones, finalización de contratos o incidentes que pudieran ocurrir durante su paso por la empresa así como la salida de la misma.</td></tr>
<tr><td>Descripción</td><td colspan="2">En toda contratación se deberá proceder a una verificación del historial del potencial trabajador. Además, una vez contratado, el trabajador debe ser informado de los distintos roles dentro de la empresa, responsabilidades, cláusulas de confidencialidad, posibles procesos disciplinarios y políticas de seguridad. Todo deberá estar por escrito, firmado por ambas partes y archivado adecuadamente. Se incluye aquí la necesidad de definir y asignar en el organigrama de la empresa el rol de responsables de seguridad, así como sus responsabilidades específicas. Se debe analizar si se producen conflictos de responsabilidades o intereses, en especial con personal de apoyo externo, evitando así accesos no autorizados o malintencionados.</td></tr>
<tr><td>Beneficios</td><td colspan="2">• Mejora de procedimientos de RRHH</td></tr>
</table>

	• Asegurar cumplimiento de LOPD • Establecer normas y disciplina en los trabajadores. • Definición clara de roles y responsables
Relaciones	Política de control de acceso

<table>
<tr><td>Proyecto</td><td colspan="2">PR10 - GESTION DE INCIDENTES DE SEGURIDAD , INTEGRACIÓN SIEM Y LOGS E INTELIGENCIA DE AMENAZAS</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>60 Semanas</td><td>03/04/2017</td><td>25/05/2018</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1 JP
3 Técnicos</td></tr>
<tr><td>PD</td><td colspan="2">
<table>
<tr><th>Puesto</th><th>PD</th><th>SubTotal</th><th rowspan="3">56000 €</th></tr>
<tr><td>JP</td><td>10 PD</td><td>8000 €</td></tr>
<tr><td>Técnico</td><td>100 PD</td><td>48000 €</td></tr>
</table>
</td></tr>
<tr><td>Presupuesto</td><td colspan="2">
<table>
<tr><th>Concepto</th><th>Subtotal</th><th rowspan="6">251000 €</th></tr>
<tr><td>Personal</td><td>56000 €</td></tr>
<tr><td>Licencias</td><td>50000 €</td></tr>
<tr><td>Hardware</td><td>70000 €</td></tr>
<tr><td>Software</td><td>50000 €</td></tr>
<tr><td>Formación especifica</td><td>25000 €</td></tr>
</table>
</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2">
<table>
<tr><th>Puesto</th><th>PD</th><th>SubTotal</th><th rowspan="3">69600€</th></tr>
<tr><td>JP</td><td>15 PD</td><td>12000€</td></tr>
<tr><td>Técnico</td><td>120 PD</td><td>57600€</td></tr>
</table>
</td></tr>
<tr><td>Objetivo</td><td colspan="2">Se debe disponer de un sistema capaz de recibir las notificaciones de seguridad y un procedimiento definido de actuación frente a los incidentes de seguridad.</td></tr>
<tr><td>Descripción</td><td colspan="2">Para ello se va a establecer:
• Integración de las distintas plataformas de monitorización, detección de intrusos y log
• Procedimiento para la monitorización y correlado de eventos</td></tr>
</table>

	• Procedimiento de gestión de incidentes de seguridad reactivos y proactivos • Sistema de gestión de la inteligencia de amenazas e integración con otros procesos de negocio. • Plataforma de almacenamiento del conocimiento y la información para análisis y usos posteriores • Los distintos procedimientos se actualizarán constantemente, pero será auditado en completo, al menos, una vez cada seis meses.
Beneficios	• Procedimientos claramente definidos ayudan a una mejor y más rápida respuesta a los problemas. • Se identifican las responsabilidades y roles que se ven afectados por una incidencia de seguridad. • Aprendizaje en base a incidencias previas registradas. • Los registros pueden servir como evidencias legales. • Esta gestión de incidentes produce un ciclo de mejoras del tipo PDCA.
Relaciones	-

<table>
<tr><td>Proyecto</td><td colspan="2">PR11 – PLAN DE GESTION DE ACTIVOS DE EMPRESA Y EMPLEADOS</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>20 Semanas</td><td>01/03/2017</td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1 JP
1 Técnico</td></tr>
<tr><td>PD</td><td colspan="2"><table><tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">9600 €</td></tr><tr><td>JP</td><td>3 PD</td><td>2400 €</td></tr><tr><td>Técnico</td><td>15PD</td><td>7200€</td></tr></table></td></tr>
<tr><td>Presupuesto</td><td colspan="2">9600 €</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2"><table><tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">8800 €</td></tr><tr><td>JP</td><td>5PD</td><td>4000 €</td></tr><tr><td>Técnico</td><td>10 PD</td><td>4800 €</td></tr></table></td></tr>
<tr><td>Objetivo</td><td colspan="2">La identificación, clasificación y asignación de todos los activos de la empresa. Se deben establecer políticas de seguridad tanto en su localización, uso, acceso, mantenimiento y la desclasificación de los mismos.
Así mismo, debe tenerse un listado de los activos de los empleados (BYOD) que se usen con motivos laborales</td></tr>
<tr><td>Descripción</td><td colspan="2">El proyecto deberá definir políticas de seguridad que cubran toda la vida útil de cada activo incluyendo equipos, cableado, impresoras, escáneres y servidores. Se deberá estudiar y definir la vida útil de cada equipamiento, incluyendo su mantenimiento y el procedimiento de reasignación. Además se deberá planificar la protección de todos ellos, como subidas de tensión, y definir una política de renovación del parque tecnológico para evitar futuros incidentes debido al envejecimiento de los mismos.
Se debe recordar que la asignación de un activo a un trabajador debe incluir la responsabilidad de este último del correcto uso del mismo. Es muy importante considerar la protección física de activos de procesamiento de información tales como los servidores de la empresa: su ubicación, acceso físico a ellos o la protección contra amenazas ambientales.</td></tr>
</table>

Beneficios	• Inventario actualizado • Políticas definidas de control de activos permiten conocer mejor el inmovilizado de la empresa y sus necesidades a futuro. • Definición de responsables de cada activo.
Relaciones	Definición de Baseline Política de seguridad de la información

<table>
<tr><td>Proyecto</td><td colspan="2">PR12 – GESTION DE PROVEEDORES</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>12 Semanas</td><td>01/05/2018</td><td>23/07/2018</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1JP
1Tecnico</td></tr>
<tr><td>PD</td><td colspan="2"><table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">7360 €</td></tr>
<tr><td>JP</td><td>5PD</td><td>4000 €</td></tr>
<tr><td>Técnico</td><td>7PD</td><td>3360 €</td></tr>
</table></td></tr>
<tr><td>Presupuesto</td><td colspan="2">7360 €</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2"><table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">6400 €</td></tr>
<tr><td>JP</td><td>2PD</td><td>1600€</td></tr>
<tr><td>Técnico</td><td>10 PD</td><td>4800€</td></tr>
</table></td></tr>
<tr><td>Objetivo</td><td colspan="2">Estableces un procedimiento para los requerimientos necesarios para el trato con los distintos proveedores de servicio, incluyendo:
Servicios legales y de RRHH
Proveedores de Hardware y Software
Proveedores de servicios Cloud</td></tr>
<tr><td>Descripción</td><td colspan="2">En este proyecto se van a establecer cuáles son los requisitos legales, funcionales y de seguridad mínimos a la hora de contratar o establecer relaciones con cualquier tipo de proveedor. Esto incluirá, acuerdos de servicio (SLA), soporte técnico y cualquier otro tipo de requerimiento que se crea necesario</td></tr>
<tr><td>Beneficios</td><td colspan="2">Mayor control sobre los proveedores, mejor servicio.
Aumento de nuestro conocimiento acerca de las partes subcontratadas de la empresa.
Aumento del control del presupuesto y de las necesidades del negocio</td></tr>
</table>

Relaciones	• Establecimiento de baseline de hardware y software • Continuidad del negocio

<table>
<tr><td>Proyecto</td><td colspan="2">PR14 – CUMPLIMIENTO DE LEGISLACION Y PROPIEDAD INTELECTUAL</td></tr>
<tr><td>Duración</td><td>Comienzo</td><td>Fin</td></tr>
<tr><td>4 Semanas</td><td>02/05/2017</td><td>29/05/2017</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Recursos</td><td colspan="2">1JP
1 Auditor legal externo</td></tr>
<tr><td>PD</td><td colspan="2">
<table>
<tr><td>Puesto</td><td>PD</td><td>SubTotal</td><td rowspan="3">1600€</td></tr>
<tr><td>JP</td><td>2 PD</td><td>1600€</td></tr>
<tr><td>Técnico</td><td>-</td><td>-</td></tr>
</table>
</td></tr>
<tr><td>Presupuesto</td><td colspan="2">
<table>
<tr><td>Concepto</td><td>Subtotal</td><td rowspan="3">6600€</td></tr>
<tr><td>Personal</td><td>1600 €</td></tr>
<tr><td>Auditor externo</td><td>5000 €</td></tr>
</table>
</td></tr>
<tr><td>Mantenimiento(Euros/año)</td><td colspan="2">N/A (será realizada anualmente)</td></tr>
<tr><td>Objetivo</td><td colspan="2">Comprobar que todos los procesos e información se encuentra correctamente encuadrada en el entorno legislativo y de propiedad intelectual</td></tr>
<tr><td>Descripción</td><td colspan="2">Mediante un experto externo se realizará una auditoría

Se realizará anualmente.</td></tr>
<tr><td>Beneficios</td><td colspan="2">• Adecuación al marco normativo actual
• Comprobación de la propiedad intelectual</td></tr>
<tr><td>Relaciones</td><td colspan="2">-</td></tr>
</table>

12.4 Planificación de ejecución

A continuación se presenta el diagrama de Gantt donde se puede observar detalladamente la planificación de la ejecución de los distintos proyectos, así como sus relaciones.

ID	Task Name	Start	Finish	Duration
1	PR01 - COPIAS DE SEGURIDAD	01/09/2016	26/10/2016	8w
2	PR02 - ORGANIZACIÓN Y CLASIFICACION DE LA INFORMACION	15/09/2016	09/11/2016	8w
3	PR03 - DEFINICION DE UN BASELINE EN SOFTWARE y HARDWARE	15/11/2016	06/02/2017	12w
4	PR04 - PLAN DE CONTINUIDAD DE NEGOCIO	15/02/2017	01/08/2017	24w
5	PR05 - POLITICA DE SEGURIDAD DE LA INFORMACION	01/12/2016	08/02/2017	10w
6	PR06 - POLITICA DE CONTROL DE ACCESO	01/05/2017	15/09/2017	20w
7	PR07 - DEFINICION DE POLITICAS DE ACTUALIZACION	15/02/2017	14/03/2017	4w
8	PR08 - PROGRAMA DE FORMACION CONTINUA	01/09/2016	26/10/2016	8w
9	PR09 - RRHH	02/10/2017	24/11/2017	8w
10	PR10 - GESTION DE INCIDENTES DE SEGURIDAD , INTEGRACIÓN SIEM Y LOGS E INTELIGENCIA DE AMENAZAS	03/04/2017	25/05/2018	60w
11	PR11 – PLAN DE GESTION DE ACTIVOS DE EMPRESA Y EMPLEADOS	01/03/2017	18/07/2017	20w
12	PR12 – GESTION DE PROVEEDORES	01/05/2018	23/07/2018	12w
13	PR13 – CUMPLIMIENTO DE LEGISLACION Y PROPIEDAD INTELECTUAL	02/05/2017	29/05/2017	4w

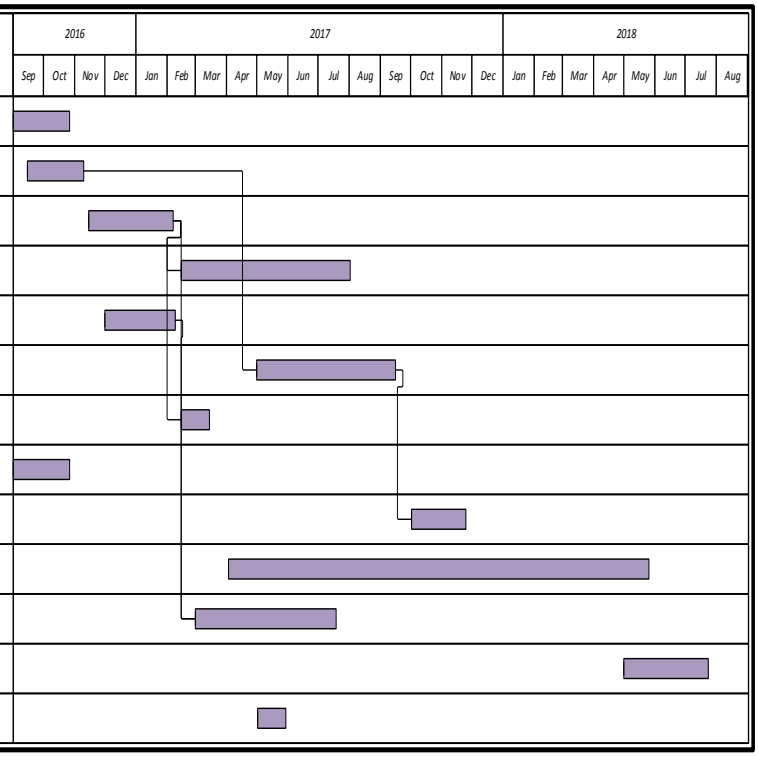

Ilustración 15 Diagrama de Gantt de la ejecución de los proyectos

12.5 Planificación económica de los proyectos

A continuación detallamos el coste de los distintos proyectos, así como el coste del mantenimiento de los mismos.

Proyecto	Coste Implementación	Coste Mantenimiento
PR01 – COPIAS DE SEGURIDAD	34.640 €	10.440 €
PR02 - ORGANIZACIÓN Y CLASIFICACION DE LA INFORMACION	2.480 €	4.000 €
PR03 - DEFINICION DE UN BASELINE EN SOFTWARE y HARDWARE	4.640 €	6.400 €
PR04 - PLAN DE CONTINUIDAD DE NEGOCIO	16.000 €	7.200 €
PR05 - POLITICA DE SEGURIDAD DE LA INFORMACION	4.560 €	9.600 €
PR06 - POLITICA DE CONTROL DE ACCESO	36.200 €	6.240 €
PR07 - DEFINICION DE POLITICAS DE ACTUALIZACION	3.200 €	4.640 €
PR08 - PROGRAMA DE FORMACION CONTINUA	27.280 €	27.280 €
PR09 – RRHH	3.200 €	4.800 €
PR10 - GESTION DE INCIDENTES DE SEGURIDAD , INTEGRACIÓN SIEM Y LOGS E INTELIGENCIA DE AMENAZAS	251.000 €	69.600 €
PR11 – PLAN DE GESTION DE ACTIVOS DE EMPRESA Y EMPLEADOS	9.600 €	8.800 €
PR12 – GESTION DE PROVEEDORES	7.360 €	6.400 €
PR13 – CUMPLIMIENTO DE LEGISLACION Y PROPIEDAD INTELECTUAL	1.600 €	1.600 €
Total	**401.760 €**	**167.000 €**

Tabla 28 Desglose de costes de implementación y mantenimiento

12.6 Evolución del riesgo tras implantación

A continuación se presenta el cálculo del impacto y del riesgo tras la implantación de los distintos proyectos, tal como hicimos en los puntos anteriores, el nivel restante de riesgo después de su tratamiento se denomina riesgo residual.

ACTIVOS [HW]	Frecuencia	A	C	I	D	A
[HW1]Firewall	Media		70,00%	50,00%	90,00%	
[HW2]Centralita IP	Media		70,00%	50,00%	90,00%	
[HW3]FAX	Media		70,00%	50,00%	90,00%	
[HW4]3 impresoras/Escaner red Laser	Media		70,00%	50,00%	90,00%	
[HW5]Servidor Sistema de integración continua (linux)	Media		70,00%	50,00%	90,00%	
[HW6]Servidor VPN	Media		70,00%	50,00%	90,00%	
[HW7]IDS	Media		70,00%	50,00%	90,00%	
[HW8]SIEM	Media		70,00%	50,00%	90,00%	
[HW9]Servidores de Logs	Media		70,00%	50,00%	90,00%	
[HW10]20 Portatiles empleados	Media		70,00%	50,00%	90,00%	
[HW11]2 Portátiles para el uso interno en CPD y similar	Media		70,00%	50,00%	90,00%	
[HW12]20 Móviles empleados	Media		70,00%	50,00%	90,00%	
[HW13]10 tablets android	Media		70,00%	50,00%	90,00%	
[HW14]20 Dispositivos conexión 3G/4G	Media		70,00%	50,00%	90,00%	
[HW15]Punto de acceso WIFI	Media		70,00%	50,00%	90,00%	
[HW16]1 Switch	Media		70,00%	50,00%	90,00%	
[HW17]Firewall	Media		70,00%	50,00%	90,00%	
[HW18]Centralita IP	Media		70,00%	50,00%	90,00%	
[HW19]FAX	Media		70,00%	50,00%	90,00%	
[HW20]2 impresoras/Escaner red Laser	Media		70,00%	50,00%	90,00%	
[HW21]10 Portatiles empleados	Media		70,00%	50,00%	90,00%	
[HW22]1 Portátiles para el uso interno en CPD y similar	Media		70,00%	50,00%	90,00%	
[HW23]10 Móviles empleados	Media		70,00%	50,00%	90,00%	
[HW24]10 tablets android	Media		70,00%	50,00%	90,00%	
[HW25]10 Dispositivos conexión 3G/4G	Media		70,00%	50,00%	90,00%	
LISTA DE AMENAZAS						
[N.1] Fuego	Remota				80,00%	
[N.2] Daños por agua	Remota				30,00%	
[N.*] Desastres naturales	Remota				50,00%	
[I.1] Fuego	Remota				90,00%	
[I.2] Daños por agua	Remota				30,00%	
[I.*] Desastres industriales	Remota				50,00%	
[I.3] Contaminación mecánica	Remota				40,00%	
[I.4] Contaminación electromagnética	Remota				30,00%	
[I.5] Avería de origen físico o lógico	Remota				50,00%	
[I.6] Corte del suministro eléctrico	Baja				60,00%	
[I.7] Condiciones inadecuadas de temperatura o humedad	Baja				50,00%	
[I.11] Emanaciones electromagnéticas	Remota				25,00%	
[E.2] Errores del administrador	Baja		10,00%	10,00%	25,00%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Baja		10,00%	20,00%	55,00%	

[E.24] Caída del sistema por agotamiento de recursos	Baja			10,00%	50,00%	
[E.25] Pérdida de equipos	Media		60,00%		70,00%	
[A.6] Abuso de privilegios de acceso	Remota		70,00%	50,00%		
[A.7] Uso no previsto	Baja		60,00%	50,00%		
[A.11] Acceso no autorizado	Media		70,00%	50,00%		
[A.23] Manipulación de los equipos	Media		70,00%		30,00%	
[A.24] Denegación de servicio	Baja				35,00%	
[A.25] Robo	Remota		60,00%		60,00%	
[A.26] Ataque destructivo	Remota				60,00%	

Tabla 29 Evolución del riesgo en activos HW

ACTIVOS [SW]	**Frecuencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[A]**
[SW1] 20 Libreoffice	Alta	70,00%	80,00%	80,00%	80,00%	
[SW2] 20 Cliente programa VPN	Alta	70,00%	80,00%	80,00%	80,00%	
[SW3] 5 Phtoshop	Alta	70,00%	80,00%	80,00%	80,00%	
[SW4] IDE Desarrollo	Alta	70,00%	80,00%	80,00%	80,00%	
[SW5] 10 Libreoffice	Alta	70,00%	80,00%	80,00%	80,00%	
[SW6] 10 Cliente programa VPN	Alta	70,00%	80,00%	80,00%	80,00%	
[SW7] IDE Desarrollo	Alta	70,00%	80,00%	80,00%	80,00%	
LISTA DE AMENAZAS						
[I.5] Avería de origen físico o lógico	Baja				55,00%	
[E.1] Errores de los usuarios	Baja		5,00%	10,00%	10,00%	
[E.2] Errores del administrador	Remota		25,00%	10,00%	25,00%	
[E.8] Difusión de software dañino	Baja		10,00%	20,00%	50,00%	
[E.9] Errores de [re-]encaminamiento	Remota		10,00%			
[E.10] Errores de secuencia	Remota			10,00%		
[E.15] Alteración accidental de la información	Remota			10,00%		
[E.18] Destrucción de información	Baja				50,00%	
[E.19] Fugas de información	Baja		15,00%			
[E.20] Vulnerabilidades de los programas (software)	Baja		30,00%	30,00%	25,00%	
[E.21] Errores de mantenimiento / actualización de programas (software)	Alta			40,00%	30,00%	
[A.5] Suplantación de la identidad del usuario	Media	70,00%	50,00%	70,00%		
[A.6] Abuso de privilegios de acceso	Baja		50,00%	25,00%	25,00%	
[A.7] Uso no previsto	Remota		50,00%	10,00%	50,00%	
[A.8] Difusión de software dañino	Media		80,00%	80,00%	80,00%	
[A.9] [Re-]encaminamiento de mensajes	Remota		30,00%			
[A.10] Alteración de secuencia	Remota			25,00%		
[A.11] Acceso no autorizado	Remota		25,00%	25,00%		
[A.15] Modificación deliberada de la información	Remota			50,00%		
[A.18] Destrucción de información	Baja				10,00%	
[A.19] Divulgación de información	Media		50,00%			
[A.22] Manipulación de programas	Baja		60,00%	60,00%	80,00%	

Tabla 30 Evolución del riesgo en activos SW

ACTIVOS [DATOS]	**Frecuencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[A]**
[DATOS1] Servidores CRM: Nóminas, datos de cliente y negocio	Alta	70,00%	70,00%	65,00%	65,00%	
[DATOS2] Servidor Backup	Alta	70,00%	70,00%	65,00%	65,00%	

[DATOS3] Imagenes corporativas	Alta	70,00%	70,00%	65,00%	65,00%	
[DATOS4] Recursos artisticos	Alta	70,00%	70,00%	65,00%	65,00%	
[DATOS5] Estadísticas Juego Usuario (Amazon)	Alta	70,00%	70,00%	65,00%	65,00%	
[DATOS6] Servidor de almacenaje de código (externo)	Alta	70,00%	70,00%	65,00%	65,00%	
[DATOS7] Servidor de recursos y documentación (externo)	Alta	70,00%	70,00%	65,00%	65,00%	
[DATOS8] Servidor de correo (Externo)	Alta	70,00%	70,00%	65,00%	65,00%	
LISTA DE AMENAZAS						
E.1] Errores de los usuarios	Alta		15,00%	5,00%	15,00%	
[E.2] Errores del administrador	Baja		10,00%	40,00%	20,00%	
[E.15] Alteración accidental de la información	Baja			20,00%		
[E.18] Destrucción de información	Baja			15,00%		
E.19] Fugas de información	Media			25,00%		
[A.5] Suplantación de la identidad del usuario	Baja	70,00%	20,00%	30,00%		
[A.6] Abuso de privilegios de acceso	Baja		70,00%	50,00%	60,00%	
[A.11] Acceso no autorizado	Baja			65,00%		
[A.15] Modificación deliberada de la información	Baja			50,00%		
[A.18] Destrucción de información	Remota				65,00%	
[A.19] Divulgación de información	Remota		60,00%			

Tabla 31 Evolución del riesgo en activos DATOS

ACTIVOS [AUX]	**Frecuencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[A]**
[AUX1] Aire acondicionado oficina	Baja		70,00%	15,00%	75,00%	
[AUX2] Aire acondicionado CPD	Baja		70,00%	15,00%	75,00%	
[AUX3] UPS Rack	Baja		70,00%	15,00%	75,00%	
[AUX4] Cableado LAN	Baja		70,00%	15,00%	75,00%	
[AUX5] Cableado Electrico	Baja		70,00%	15,00%	75,00%	
[AUX6] Punto de acceso WIFI	Baja		70,00%	15,00%	75,00%	
[AUX7] Switch	Baja		70,00%	15,00%	75,00%	
[AUX8] Aire acondicionado oficina	Baja		70,00%	15,00%	75,00%	
[AUX9] Aire acondicionado CPD	Baja		70,00%	15,00%	75,00%	
[AUX10] UPS Rack	Baja		70,00%	15,00%	75,00%	
[AUX11] Cableado LAN	Baja		70,00%	15,00%	75,00%	
[AUX12] Cableado Electrico	Baja		70,00%	15,00%	75,00%	
LISTA DE AMENAZAS						
[N.1] Fuego	Remota				70,00%	
[N.2] Daños por agua	Remota				60,00%	
[N.*] Desastres naturales	Remota				60,00%	
[I.1] Fuego	Remota				75,00%	
[I.2] Daños por agua	Remota				75,00%	
[I.*] Desastres industriales	Remota				60,00%	
[I.3] Contaminación mecánica	Remota				70,00%	
[I.4] Contaminación electromagnética	Remota				70,00%	
[I.5] Avería de origen físico o lógico	Remota				60,00%	
[I.6] Corte del suministro eléctrico	Remota				70,00%	
[I.7] Condiciones inadecuadas de temperatura o humedad	Remota				75,00%	
[I.9] Interrupción de otros servicios y suministros esenciales	Remota				75,00%	

[I.11] Emanaciones electromagnéticas – NO APLICA -	Remota				60,00%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Baja				70,00%	
[E.25] Pérdida de equipos	Remota		15,00%		75,00%	
[A.7] Uso no previsto	Baja		10,00%	10,00%	60,00%	
[A.11] Acceso no autorizado	Baja		30,00%	15,00%		
[A.23] Manipulación de los equipos	Baja		10,00%		70,00%	
[A.25] Robo	Baja		70,00%		70,00%	
[A.26] Ataque destructivo	Remota				75,00%	

Tabla 32 Evolución del riesgo en activos AUX

ACTIVOS [L]	**Frecuencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[A]**
[L1] Rack principal (CPD)	Baja		80,00%	50,00%	80,00%	
[L2] Archivo	Baja		80,00%	50,00%	80,00%	
[L3] Rack principal (CPD)	Baja		80,00%	50,00%	80,00%	
[L4] Archivo	Baja		80,00%	50,00%	80,00%	
LISTA DE AMENAZAS						
[N.1] Fuego	Remota				75,00%	
[N.2] Daños por agua	Remota				75,00%	
[N.*] Desastres naturales	Remota				75,00%	
[I.1] Fuego	Remota				70,00%	
[I.2] Daños por agua	Remota				75,00%	
[I.*] Desastres industriales	Remota				70,00%	
[I.11] Emanaciones electromagnéticas	Remota					
[E.15] Alteración accidental de la información	Baja			30,00%		
[E.18] Destrucción de información	Remota				30,00%	
[E.19] Fugas de información	Baja		25,00%			
[A.7] Uso no previsto	Baja		50,00%	50,00%	30,00%	
[A.11] Acceso no autorizado	Remota		60,00%	50,00%		
[A.15] Modificación deliberada de la información	Remota			50,00%		
[A.18] Destrucción de información	Remota				55,00%	
[A.19] Divulgación de información	Remota		80,00%			
[A.26] Ataque destructivo	Remota				60,00%	
[A.27] Ocupación enemiga	Remota		80,00%		80,00%	

Tabla 33 Evolución del riesgo en activos L

ACTIVOS [P]	**Frecuencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[A]**
[P1] 20 empleados	Baja		55,00%	40,00%	60,00%	
[P2] 10 empleados	Baja		55,00%	40,00%	60,00%	
LISTA DE AMENAZAS						
[E.19] Fugas de información	Baja		55,00%			
[E.28] Indisponibilidad del personal	Baja				15,00%	
[A.28] Indisponibilidad del personal	Baja				60,00%	
[A.29] Extorsión	Remota		30,00%	40,00%	30,00%	
[A.30] Ingeniería social (picaresca)	Baja		15,00%	15,00%	15,00%	

Tabla 34 Evolución del riesgo en activos P

ACTIVOS [COM]	Frecuencia	[A]	[C]	[I]	[D]	[A]
[COM1] Router fibra une las sedes y da conexión a Internet	Baja	80,00%	40,00%	30,00%	60,00%	
LISTA DE AMENAZAS						
[I.8] Fallo de servicios de comunicaciones	Baja				30,00%	
[E.2] Errores del administrador	Baja		20,00%	25,00%	20,00%	
[E.9] Errores de [re-]encaminamiento	Remota		15,00%			
[E.10] Errores de secuencia	Remota			15,00%		
[E.15] Alteración accidental de la información	Remota			25,00%		
[E.18] Destrucción de información	Remota				15,00%	
[E.19] Fugas de información	Remota		15,00%			
[E.24] Caída del sistema por agotamiento de recursos	Remota				30,00%	
[A.5] Suplantación de la identidad del usuario	Remota	80,00%	40,00%	30,00%		
[A.6] Abuso de privilegios de acceso	Remota		25,00%	10,00%	30,00%	
[A.7] Uso no previsto	Baja		20,00%	15,00%	60,00%	
[A.9] [Re-]encaminamiento de mensajes	Remota		20,00%			
[A.10] Alteración de secuencia	Remota			10,00%		
[A.11] Acceso no autorizado	Remota		20,00%	15,00%		
[A.12] Análisis de tráfico	Remota		25,00%			
[A.14] Interceptación de información (escucha)	Remota		40,00%			
[A.15] Modificación deliberada de la información	Remota			30,00%		
[A.19] Divulgación de información	Remota		30,00%			
[A.24] Denegación de servicio	Remota				60,00%	

Tabla 35 Evolución del riesgo en activos COM

		Criticidad					% Impacto				Impacto Potencial					
TIPO	ID	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
HW	[HW 1]	7	6	8	9	8		70,00%	50,00%	90,00%		0	4,2	4	8,1	0
	[HW 2]	3	6	6	9	8		70,00%	50,00%	90,00%		0	4,2	3	8,1	0
	[HW 3]	2	3	3	5	3		70,00%	50,00%	90,00%		0	2,1	1,5	4,5	0
	[HW 4]	2	2	4	5	5		70,00%	50,00%	90,00%		0	1,4	2	4,5	0
	[HW 5]	9	7	9	9	7		70,00%	50,00%	90,00%		0	4,9	4,5	8,1	0
	[HW 6]	9	9	9	9	8		70,00%	50,00%	90,00%		0	6,3	4,5	8,1	0
	[HW 7]	6	7	6	7	8		70,00%	50,00%	90,00%		0	4,9	3	6,3	0
	[HW 8]	6	6	6	8	8		70,00%	50,00%	90,00%		0	4,2	3	7,2	0
	[HW 9]	9	9	9	10	8		70,00%	50,00%	90,00%		0	6,3	4,5	9	0
	[HW 10]	6	8	7	9	4		70,00%	50,00%	90,00%		0	5,6	3,5	8,1	0
	[HW 11]	6	7	7	7	5		70,00%	50,00%	90,00%		0	4,9	3,5	6,3	0

	[HW 12]	5	8	6	6	7		70,00%	50,00%	90,00%		0	5,6	3	5,4	0
	[HW 13]	5	8	3	3	3		70,00%	50,00%	90,00%		0	5,6	1,5	2,7	0
	[HW 14]	5	6	2	5	5		70,00%	50,00%	90,00%		0	4,2	1	4,5	0
	[HW 15]	2	7	3	6	5		70,00%	50,00%	90,00%		0	4,9	1,5	5,4	0
	[HW 16]	4	5	7	7	5		70,00%	50,00%	90,00%		0	3,5	3,5	6,3	0
	[HW 17]	7	6	8	9	8		70,00%	50,00%	90,00%		0	4,2	4	8,1	0
	[HW 18]	3	6	6	9	8		70,00%	50,00%	90,00%		0	4,2	3	8,1	0
	[HW 19]	2	3	3	5	3		70,00%	50,00%	90,00%		0	2,1	1,5	4,5	0
	[HW 20]	2	2	4	5	5		70,00%	50,00%	90,00%		0	1,4	2	4,5	0
	[HW 21]	6	8	7	9	4		70,00%	50,00%	90,00%		0	5,6	3,5	8,1	0
	[HW 22]	6	7	7	7	5		70,00%	50,00%	90,00%		0	4,9	3,5	6,3	0
	[HW 23]	5	8	6	6	7		70,00%	50,00%	90,00%		0	5,6	3	5,4	0
	[HW 24]	5	8	3	3	3		70,00%	50,00%	90,00%		0	5,6	1,5	2,7	0
	[HW 25]	5	6	2	5	5		70,00%	50,00%	90,00%		0	4,2	1	4,5	0
L	[L1]	8	9	10	10	8		80,00%	50,00%	80,00%		0	7,2	5	8	0
	[L2]	9	9	7	8	7		80,00%	50,00%	80,00%		0	7,2	3,5	6,4	0
	[L3]	8	9	10	10	8		80,00%	50,00%	80,00%		0	7,2	5	8	0
	[L4]	9	9	7	8	7		80,00%	50,00%	80,00%		0	7,2	3,5	6,4	0
AUX	[AUX 1]	-	-	-	7	-		70,00%	15,00%	75,00%		0	0	0	5,25	0
	[AUX 2]	-	-	-	8	-		70,00%	15,00%	75,00%		0	0	0	6	0
	[AUX 3]	-	-	-	8	-		70,00%	15,00%	75,00%		0	0	0	6	0
	[AUX 4]	-	-	-	9	-		70,00%	15,00%	75,00%		0	0	0	6,75	0
	[AUX 5]	-	-	-	9	-		70,00%	15,00%	75,00%		0	0	0	6,75	0
	[AUX 6]	2	7	3	6	5		70,00%	15,00%	75,00%		0	4,9	0,45	4,5	0
	[AUX 7]	4	5	7	7	5		70,00%	15,00%	75,00%		0	3,5	1,05	5,25	0
	[AUX 8]	-	-	-	7	-		70,00%	15,00%	75,00%		0	0	0	5,25	0
	[AUX 9]	-	-	-	8	-		70,00%	15,00%	75,00%		0	0	0	6	0
	[AUX 10]	-	-	-	8	-		70,00%	15,00%	75,00%		0	0	0	6	0
	[AUX 11]	-	-	-	9	-		70,00%	15,00%	75,00%		0	0	0	6,75	0
	[AUX 12]	-	-	-	9	-		70,00%	15,00%	75,00%		0	0	0	6,75	0
COM	[COM1]	5	6	8	8	6	80,00%	40,00%	30,00%	60,00%		4	2,4	2,4	4,8	0
Dat	[DATOS1]	9	10	10	9	6	70,00%	70,00%	65,00%	65,00%		6,3	7	6,5	5,85	0
	[DATOS2]	9	9	9	10	7	70,00%	70,00%	65,00%	65,00%		6,3	6,3	5,85	6,5	0

	[DATOS3]	-	-	6	8	5	70,00%	70,00%	65,00%	65,00%		0	0	3,9	5,2	0
	[DATOS4]	-	-	7	7	5	70,00%	70,00%	65,00%	65,00%		0	0	4,55	4,55	0
	[DATOS5]	8	10	9	9	8	70,00%	70,00%	65,00%	65,00%		5,6	7	5,85	5,85	0
	[DATOS6]	10	10	10	10	9	70,00%	70,00%	65,00%	65,00%		7	7	6,5	6,5	0
	[DATOS7]	8	8	9	9	8	70,00%	70,00%	65,00%	65,00%		5,6	5,6	5,85	5,85	0
	[DATOS8]	8	9	9	9	9	70,00%	70,00%	65,00%	65,00%		5,6	6,3	5,85	5,85	0
P	[P1]	-	-	-	6	-		55,00%	40,00%	60,00%		0	0	0	3,6	0
	[P2]	-	-	-	6	-		55,00%	40,00%	60,00%		0	0	0	3,6	0
SW	[SW1]	2	3	2	3	3	70,00%	80,00%	80,00%	80,00%		1,4	2,4	1,6	2,4	0
	[SW2]	8	6	7	7	6	70,00%	80,00%	80,00%	80,00%		5,6	4,8	5,6	5,6	0
	[SW3]	2	2	2	4	3	70,00%	80,00%	80,00%	80,00%		1,4	1,6	1,6	3,2	0
	[SW4]	3	3	3	5	6	70,00%	80,00%	80,00%	80,00%		2,1	2,4	2,4	4	0
	[SW5]	2	3	2	3	3	70,00%	80,00%	80,00%	80,00%		1,4	2,4	1,6	2,4	0
	[SW6]	8	6	7	7	6	70,00%	80,00%	80,00%	80,00%		5,6	4,8	5,6	5,6	0
	[SW7]	3	3	3	5	6	70,00%	80,00%	80,00%	80,00%		2,1	2,4	2,4	4	0

Tabla 36 Evolución del Impacto Potencial

				Impacto Potencial				Riesgo					
TIPO	ID	Frecuencia	Valor Frec	A	C	I	D	A	A	C	I	D	A
	[HW1]	Media	0,016438	0	4,2	4	8,1	0	0	6,90396	6,5752	13,3148	0
	[HW2]	Media	0,016438	0	4,2	3	8,1	0	0	6,90396	4,9314	13,3148	0
	[HW3]	Media	0,016438	0	2,1	1,5	4,5	0	0	3,45198	2,4657	7,3971	0
	[HW4]	Media	0,016438	0	1,4	2	4,5	0	0	2,30132	3,2876	7,3971	0
	[HW5]	Media	0,016438	0	4,9	4,5	8,1	0	0	8,05462	7,3971	13,3148	0
	[HW6]	Media	0,016438	0	6,3	4,5	8,1	0	0	10,3559	7,3971	13,3148	0
	[HW7]	Media	0,016438	0	4,9	3	6,3	0	0	8,05462	4,9314	10,3559	0
	[HW8]	Media	0,016438	0	4,2	3	7,2	0	0	6,90396	4,9314	11,8354	0
	[HW9]	Media	0,016438	0	6,3	4,5	9	0	0	10,3559	7,3971	14,7942	0
	[HW10]	Media	0,016438	0	5,6	3,5	8,1	0	0	9,20528	5,7533	13,3148	0
	[HW11]	Media	0,016438	0	4,9	3,5	6,3	0	0	8,05462	5,7533	10,3559	0
	[HW12]	Media	0,016438	0	5,6	3	5,4	0	0	9,20528	4,9314	8,87652	0
	[HW13]	Media	0,016438	0	5,6	1,5	2,7	0	0	9,20528	2,4657	4,43826	0
	[HW14]	Media	0,016438	0	4,2	1	4,5	0	0	6,90396	1,6438	7,3971	0
	[HW15]	Media	0,016438	0	4,9	1,5	5,4	0	0	8,05462	2,4657	8,87652	0
	[HW16]	Media	0,016438	0	3,5	3,5	6,3	0	0	5,7533	5,7533	10,3559	0
	[HW17]	Media	0,016438	0	4,2	4	8,1	0	0	6,90396	6,5752	13,3148	0
	[HW18]	Media	0,016438	0	4,2	3	8,1	0	0	6,90396	4,9314	13,3148	0
	[HW19]	Media	0,016438	0	2,1	1,5	4,5	0	0	3,45198	2,4657	7,3971	0
	[HW20]	Media	0,016438	0	1,4	2	4,5	0	0	2,30132	3,2876	7,3971	0
	[HW21]	Media	0,016438	0	5,6	3,5	8,1	0	0	9,20528	5,7533	13,3148	0
	[HW22]	Media	0,016438	0	4,9	3,5	6,3	0	0	8,05462	5,7533	10,3559	0
	[HW23]	Media	0,016438	0	5,6	3	5,4	0	0	9,20528	4,9314	8,87652	0
	[HW24]	Media	0,016438	0	5,6	1,5	2,7	0	0	9,20528	2,4657	4,43826	0
	[HW25]	Media	0,016438	0	4,2	1	4,5	0	0	6,90396	1,6438	7,3971	0
	[L1]	Baja	0,005479	0	7,2	5	8	0	0	3,94488	2,7395	4,3832	0
	[L2]	Baja	0,005479	0	7,2	3,5	6,4	0	0	3,94488	1,91765	3,50656	0
	[L3]	Baja	0,005479	0	7,2	5	8	0	0	3,94488	2,7395	4,3832	0
	[L4]	Baja	0,005479	0	7,2	3,5	6,4	0	0	3,94488	1,91765	3,50656	0
	[AUX1]	Baja	0,005479	0	0	0	5,25	0	0	0	0	2,87648	0
	[AUX2]	Baja	0,005479	0	0	0	6	0	0	0	0	3,2874	0

	[AUX3]	Baja	0,005479	0	0	0	6	0	0	0	0	3,2874	0
	[AUX4]	Baja	0,005479	0	0	0	6,75	0	0	0	0	3,69833	0
	[AUX5]	Baja	0,005479	0	0	0	6,75	0	0	0	0	3,69833	0
	[AUX6]	Baja	0,005479	0	4,9	0,45	4,5	0	0	2,68471	0,24656	2,46555	0
	[AUX7]	Baja	0,005479	0	3,5	1,05	5,25	0	0	1,91765	0,5753	2,87648	0
	[AUX8]	Baja	0,005479	0	0	0	5,25	0	0	0	0	2,87648	0
	[AUX9]	Baja	0,005479	0	0	0	6	0	0	0	0	3,2874	0
	[AUX10]	Baja	0,005479	0	0	0	6	0	0	0	0	3,2874	0
	[AUX11]	Baja	0,005479	0	0	0	6,75	0	0	0	0	3,69833	0
	[AUX12]	Baja	0,005479	0	0	0	6,75	0	0	0	0	3,69833	0
	[COM1]	Baja	0,005479	4	2,4	2,4	4,8	0	2,1916	1,31496	1,31496	2,62992	0
	[DATOS1]	Alta	0,071233	6,3	7	6,5	5,85	0	44,8768	49,8631	46,3015	41,6713	0
	[DATOS2]	Alta	0,071233	6,3	6,3	5,85	6,5	0	44,8768	44,8768	41,6713	46,3015	0
	[DATOS3]	Alta	0,071233	0	0	3,9	5,2	0	0	0	27,7809	37,0412	0
	[DATOS4]	Alta	0,071233	0	0	4,55	4,55	0	0	0	32,411	32,411	0
	[DATOS5]	Alta	0,071233	5,6	7	5,85	5,85	0	39,8905	49,8631	41,6713	41,6713	0
	[DATOS6]	Alta	0,071233	7	7	6,5	6,5	0	49,8631	49,8631	46,3015	46,3015	0
	[DATOS7]	Alta	0,071233	5,6	5,6	5,85	5,85	0	39,8905	39,8905	41,6713	41,6713	0
	[DATOS8]	Alta	0,071233	5,6	6,3	5,85	5,85	0	39,8905	44,8768	41,6713	41,6713	0
	[P1]	Baja	0,005479	0	0	0	3,6	0	0	0	0	1,97244	0
	[P2]	Baja	0,005479	0	0	0	3,6	0	0	0	0	1,97244	0
	[SW1]	Alta	0,071233	1,4	2,4	1,6	2,4	0	9,97262	17,0959	11,3973	17,0959	0
	[SW2]	Alta	0,071233	5,6	4,8	5,6	5,6	0	39,8905	34,1918	39,8905	39,8905	0
	[SW3]	Alta	0,071233	1,4	1,6	1,6	3,2	0	9,97262	11,3973	11,3973	22,7946	0
	[SW4]	Alta	0,071233	2,1	2,4	2,4	4	0	14,9589	17,0959	17,0959	28,4932	0
	[SW5]	Alta	0,071233	1,4	2,4	1,6	2,4	0	9,97262	17,0959	11,3973	17,0959	0
	[SW6]	Alta	0,071233	5,6	4,8	5,6	5,6	0	39,8905	34,1918	39,8905	39,8905	0
	[SW7]	Alta	0,071233	2,1	2,4	2,4	4	0	14,9589	17,0959	17,0959	28,4932	0

Tabla 37 Evolución del riesgo y riesgo residual

En la tabla anterior se puede observar el riesgo residual obtenido tras el cálculo resultante del riesgo de los diferentes proyectos.

Como es posible comprobar, ya no existe ningún valor por encima del valor definido por la dirección.

12.7 Nivel de cumplimiento de la norma

En este apartado vamos a ver la correspondencia entre los distintos controles de los dominios de la ISO 27002:2013 y los proyectos definidos anteriormente.

Dominio ISO 27002:2013	Controles	Proyecto
A.5 Políticas de la Seguridad de la Información	5.1	PR05
A.6 Organización de la seguridad de la Información	6.1 6.2	PR02 PR09 PR10 PR11
A.7 Seguridad de RRHH	7.1 7.2	PR09 PR08
A.8 Gestión de activos	8.2 8.3	PR01 PR02
A.9 Control acceso	9.1 9.2 9.3 9.4	PR02 PR05 PR06 PR11
A.10 Criptografía		
A.11 Seguridad física y ambiental	11.1 11.2	PR08 PR11
A.12 Operaciones de seguridad	12.3 12.2 12.4 12.5 A.12.6 12.7	PR01 PR03 PR07 PR10
A.13 Seguridad de las comunicaciones	13.1 13.2	PR10
A.14 Adquisición, desarrollo y mantenimiento de sistemas	14.1 14.2	PR03 PR08
A.15 Relaciones con proveedores	15.1 15.2	PR11 PR12
A.16 Gestión de Incidentes de Seguridad de la información	16.1	PR10
A.17 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio	17.1	PR03 PR04
A.18 Cumplimiento	18.1 18.2	PR02 PR13

Tabla 38 Cumplimiento de la norma

13. Auditoría de cumplimiento

13.1 Objetivo

El objetivo de la auditoría del cumplimiento es comprobar el nivel de madurez de la seguridad en la empresa después de la puesta en marcha del plan de actuaciones en materia de seguridad. Tomamos como referencia los 14 dominios y los 114 controles de la norma 27002:2013.

Es importante destacar que esta auditoría se realiza partiendo del supuesto que todos los proyectos presentados han sido realizados y completados con éxito.

13.2 Alcance

El alcance de la auditoría de cumplimiento engloba todos los dominios y controles que se han implementado en la organización a través de los distintos proyectos.

13.3 Evolución del análisis diferencial

A continuación se muestra el resultado de las valoraciones de cumplimiento para cada uno de los dominios de la norma en cada uno de sus controles. Para una mejor comprensión, en la siguiente tabla se muestra, a modo de resumen, las valoraciones obtenidas de todos los dominios agrupando todos sus controles. Se ha procedido a comparar el estado inicial con el estado una vez implementados todos los proyectos recomendados.

A.5	**Política de Seguridad**	**Cumplimiento antes de auditoría**	**Cumplimiento tras auditoría**
A5.1	**Directrices de la Dirección en seguridad de la información**		
A.5.1.1	Conjunto de políticas para la seguridad de la información.	L0	L4
A.5.1.2	Revisión de las políticas para la seguridad de la información	L0	L4
A.6	**Aspectos organizativos de la seguridad de la información**		
A.6.1	**Organización Interna**		
A.6.1.1	Asignación de responsabilidades para la segur. de la información.	L2	L4

A.6.1.2	Segregación de tareas.	L2	L4
A.6.1.3	Contacto con las autoridades.	L0	L3
A.6.1.4	Contacto con grupos de interés especial.	L0	L3
A.6.1.5	Seguridad de la información en la gestión de proyectos.	L0	L4
A.6.2	**Dispositivos para movilidad y teletrabajo.**		
A.6.2.1	Política de uso de dispositivos para movilidad	L0	L3
A.6.2.2	Teletrabajo	L0	L3
A.7	**La seguridad ligada a los recursos humanos**		
A.7.1	**Antes de la contratación**		
A.7.1.1	Investigación de antecedentes	L0	L3
A.7.1.2	Términos y condiciones de contratación	L2	L4
A.7.2	**Durante la contratación**		
A.7.2.1	Responsabilidades de gestión	L1	L4
A.7.2.2	Concienciación, educación y capacitación en segur. de la informac.	L2	L4
A.7.2.3	Proceso Disciplinario	L0	L4
A.7.3	**Cese o cambio de puesto de trabajo.**		
A.7.3.1	Cese o cambio de puesto de trabajo.	L0	L5
A.8	**Gestión de Activos**		
A.8.1	**La responsabilidad de los activos**		
A.8.1.1	Inventarios de Activos	L0	L5
A.8.1.2	Propiedad de Activos	L0	L4

A.8.1.3	Uso aceptables de los activos	N/A	
A.8.1.4	Devolución de activos	N/A	
A.8.2	**Clasificación de la información**		
A.8.2.1	Directrices de clasificación	L0	L4
A.8.2.2	Etiquetado de la información y la manipulación	L0	L4
A.8.2.3	Manipulación de activos	L0	L4
A.8.3	**Manejo de los soportes de almacenamiento**		
A.8.3.1	Gestión de soportes extraíbles.	L0	L3
A.8.3.2	Eliminación de soportes	L0	L3
A.8.3.3	Soportes físicos en tránsito	L0	L2
A9	**Control de Acceso**		
A9.1	**Requerimiento de negocio de control de acceso**		
A9.1.1	Política de control de acceso	L1	L3
A9.1.2	Control de acceso a las redes y servicios asociados.	L0	L3
A9.2	**Gestión de acceso de los usuarios**		
A9.2.1	Gestión de altas/bajas en el registro de usuarios.	L1	L4
A9.2.2	Gestión de los derechos de acceso asignados a usuarios.	L1	L4
A9.2.3	Gestión de los derechos de acceso con privilegios especiales	L1	L4
A9.2.4	Gestión de información confidencial de autenticación de usuarios	L1	L4
A9.2.5	Revisión de los derechos de acceso de los usuarios	L1	L4
A9.2.6	Retirada o adaptación de los derechos de acceso	L1	L4

A9.3	**Responsabilidades de los usuarios**		
A9.3.1	Uso de información confidencial para la autenticación.	L0	L4
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	L1	L4
A9.4.2	Procedimientos seguros de inicio de sesión	L0	L3
A9.4.3	Gestión de contraseñas de usuario	L2	L3
A9.4.4	Uso de herramientas de administración de sistemas.	L2	L3
A9.4.5	Control de acceso al código fuente de los programas	L3	L5
A10	**Cifrado**		
A10.1	**Controles criptográficos.**		
A10.1.1	Política de uso de los controles criptográficos	L0	L3
A10.1.2	Gestión de claves	L0	L3
A.11	**Seguridad Fisica y ambiental**		
A11.1	**Areas Seguras**		
A11.1.1	Perímetro de seguridad física	L0	L4
A11.1.2	Controles de entradas físicas	L0	L4
A11.1.3	Seguridad de oficinas, despachos y recursos.	L2	L4
A11.1.4	Protección contra las amenazas externas y ambientales.	L2	L4
A11.1.5	El trabajo en áreas seguras.	N/A	N/A
A11.1.6	Zonas de acceso público, de entrega y de carga	N/A	N/A
A11.2	**Seguridad de los equipos**		

A11.2.1	Emplazamiento y protección de equipos	L2	L3
A11.2.2	Instalaciones de suministro	L0	L3
A11.2.3	Seguridad del cableado	L4	L5
A11.2.4	Mantenimiento de los equipos	L4	L3
A11.2.5	Salida de activos fuera de las dependencias de la empresa	L0	L4
A11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	L0	L3
A11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	L0	L4
A11.2.8	Equipo informático de usuario desatendido.	L0	L3
A11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	L0	L3
A12	**Seguridad en la operativa**		
A12.1	**Responsabilidades y procedimientos de operación**		
A12.1.1	Documentación de procedimientos de operación	L4	L5
A12.1.2	Gestión del Cambio	L1	L5
A12.1.3	Gestión de capacidades	L4	L5
A12.1.4	Separación de entornos de desarrollo, prueba y producción.	L4	L5
A12.2	**Protección contra código malicioso**		
A12.2.1	Controles contra el código malicioso	L2	L4
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	L3	L5
A12.4	**Registro de actividad y supervisión**		

A12.4.1	Registro y gestión de eventos de actividad	L1	L5
A12.4.2	Protección de los registros de información	L2	L5
A12.4.3	Registros de actividad del administrador y operador del sistema	L1	L5
A12.4.4	Sincronización de relojes	L2	L5
A12.5	**Control del software en explotación.**		
A12.5.1	Instalación del software en sistemas en producción	L4	L4
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	L0	L5
A12.6.2	Restricciones en la instalación de software.	L2	L3
A12.7	**Consideraciones de las auditorías de los sistemas de información**		
A12.7.1	Controles de auditoría de los sistemas de información	L0	L4
A13	**Seguridad en las telecomunicaciones**		
A13.1	**Gestión de la seguridad en las redes**		
A13.1.1	Controles de red.	L2	L4
A13.1.2	Mecanismos de seguridad asociados a servicios en red	L1	L4
A13.1.3	Segregación de redes	L0	L4
A13.2	**Intercambio de información con partes externas**		
A13.2.1	Políticas y procedimientos de intercambio de información	L0	L4
A13.2.2	Acuerdos de intercambio	L0	L4
A13.2.3	Mensajería electrónica.	L0	L3
A13.2.4	Acuerdos de confidencialidad y secreto	L0	L3

A14	**Adquisición, desarrollo y mantenimiento de los sistemas de infor.**		
A14.1	**Requisitos de seguridad de los sistemas de información**		
A14.1.1	Análisis y especificación de los requisitos de seguridad	L0	L4
A14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes	L3	L4
A14.1.3	Protección de las transacciones por redes telemáticas	L3	L4
A14.2	**Seguridad en los procesos de desarrollo y soporte**		
A14.2.1	Política de desarrollo seguro de software	L2	L5
A14.2.2	Procedimientos de control de cambios en los sistemas	L3	L4
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el S.O	L2	L4
A14.2.4	Restricciones a los cambios en los paquetes de software	L0	L4
A14.2.5	Uso de principios de ingeniería en protección de sistemas	L2	L5
A14.2.6	Seguridad en entornos de desarrollo	L2	L4
A14.2.7	Externalización del desarrollo de software	L4	L5
A14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	L3	L5
A14.2.9	Pruebas de aceptación	L3	L5
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos utilizados en pruebas	L4	L4
A15	**Relaciones con los suministradores**		
A15.1	**Seguridad de la información en las**		

	relaciones con suministradores		
A15.1.1	Política de seguridad de la información para suministradores	L0	L4
A15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	L0	L4
A15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	L0	L4
A15.2	**Gestión de la prestación del servicio por suministradores**		
A15.2.1	Supervisión y revisión de los servicios prestados por terceros	L4	L4
A15.2.2	Gestión de cambios en los servicios prestados por terceros	L2	L4
A16	**Gestión de incidentes en la seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras.**		
A16.1.1	Responsabilidades y procedimientos	L0	L5
A16.1.2	Notificación de los eventos de seguridad de la información	L0	L5
A16.1.3	Notificación de puntos débiles de la seguridad	L0	L5
A16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	L0	L5
A16.1.5	Respuesta a los incidentes de seguridad	L0	L5
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	L0	L4
A16.1.7	Recopilación de evidencias	L0	L5
A17	**Aspectos de seguridad de la información en la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		

A17.1.1	Planificación de la continuidad de la seguridad de la información	L0	L4
A17.1.2	Implantación de la continuidad de la seguridad de la información	L0	L4
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad	L0	L4
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	L0	L3
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los requisitos legales y contractuales.**		
A18.1.1	Identificación de la legislación aplicable	L4	L5
A18.1.2	Derechos de propiedad intelectual (DPI)	L4	L5
A18.1.3	Protección de los registros de la organización.	L4	L4
A18.1.4	Protección de datos y privacidad de la información personal	L4	L4
A18.1.5	Regulación de los controles criptográficos	L4	L4
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	L0	L4
A18.2.2	Cumplimiento de las políticas y normas de seguridad	L3	L4
A18.2.3	Comprobación del cumplimiento	L0	L4

Tabla 39 Auditoría del cumplimiento

13.4 Fichas de no conformidades

A continuación se presenta la fichas de las conformidades tras las medidas adoptadas.

	Dominio	% de conformidad	# NC baja efectividad	# NC alta efectividad	# NC OK
A.5	POLÍTICAS DE SEGURIDAD	95%	0	0	2
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	92%	0	4	3
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	96%	0	1	5
A.8	GESTIÓN DE ACTIVOS.	74%	1	3	5
A.9	CONTROL DE ACCESOS.	89%	1	4	9
A.10	CIFRADO.	0%	0	2	0
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	94%	0	6	7
A.12	SEGURIDAD EN LA OPERATIVA.	98%	0	1	13
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	95%	0	2	5
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	96%	0	0	13
A.15	RELACIONES CON SUMINISTRADORES.	95%	0	0	5
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	100%	0	0	7
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	93%	0	1	3
A.18	CUMPLIMIENTO.	96%	0	0	8

Tabla 40 Ficha de no conformidades (NC)

	Dominio	% de conformidad	# NC baja efectividad	Descripción NC
A.5	POLÍTICAS DE SEGURIDAD	95%	0	-
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	92%	0	-
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	96%	0	-
A.8	GESTIÓN DE ACTIVOS.	74%	1	Existen problemas a la hora de gestionar los activos de los empleados (en propiedad), sobre todo a la hora de que cumplan ciertas políticas comunes.
A.9	CONTROL DE ACCESOS.	89%	1	Es necesario mejorar el aspecto de control de accesos Físico, así como el control de las instalaciones
A.10	CIFRADO.	0%	0	-
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	94%	0	-
A.12	SEGURIDAD EN LA OPERATIVA.	98%	0	-
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	95%	0	-
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	96%	0	-
A.15	RELACIONES CON SUMINISTRADORES.	95%	0	-
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	100%	0	-
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	93%	0	-
A.18	CUMPLIMIENTO.	96%	0	-

Tabla 41 Descripción de No Conformidades (NC)

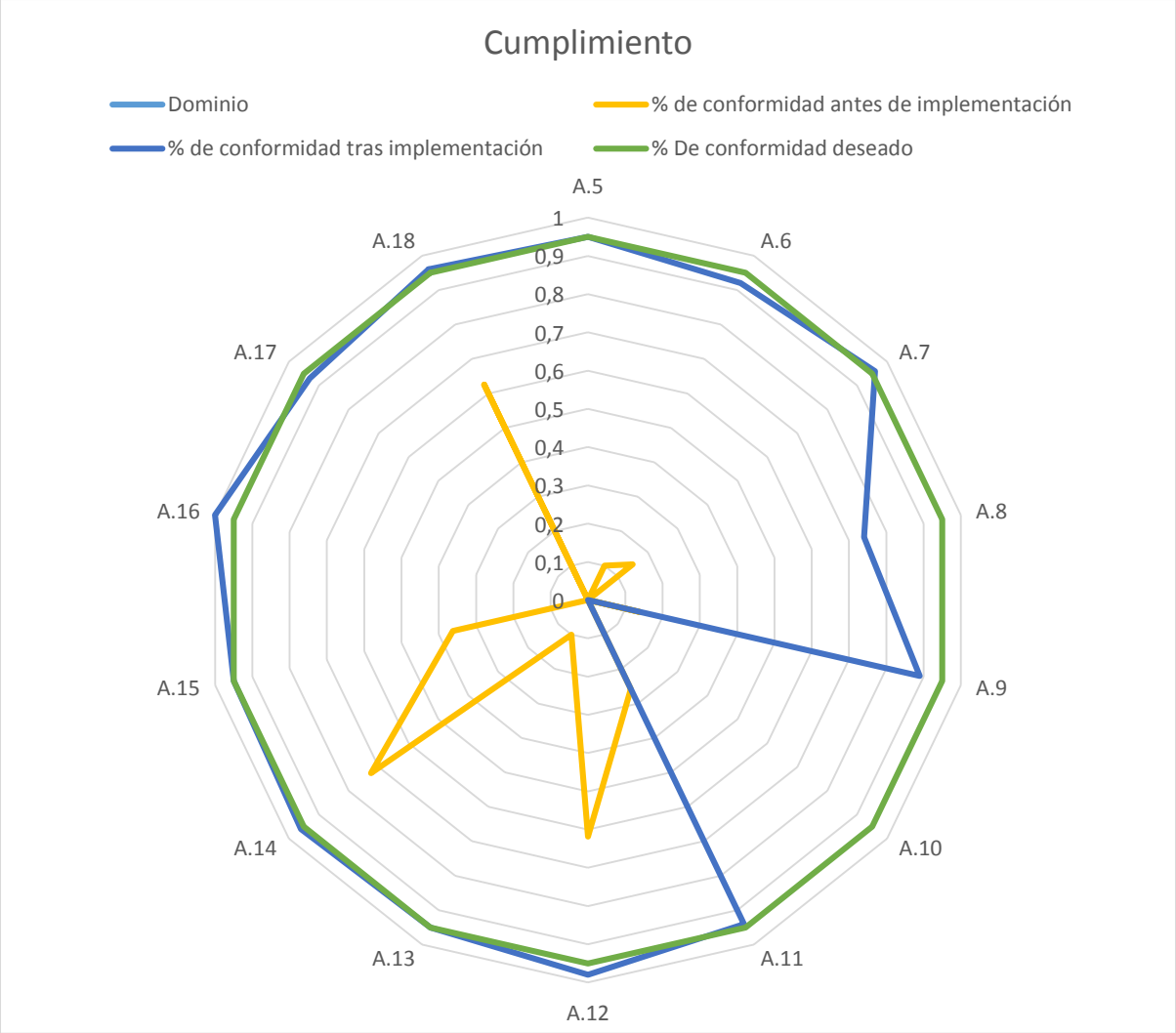

Ilustración 16 Cumplimiento antes y después de la auditoria

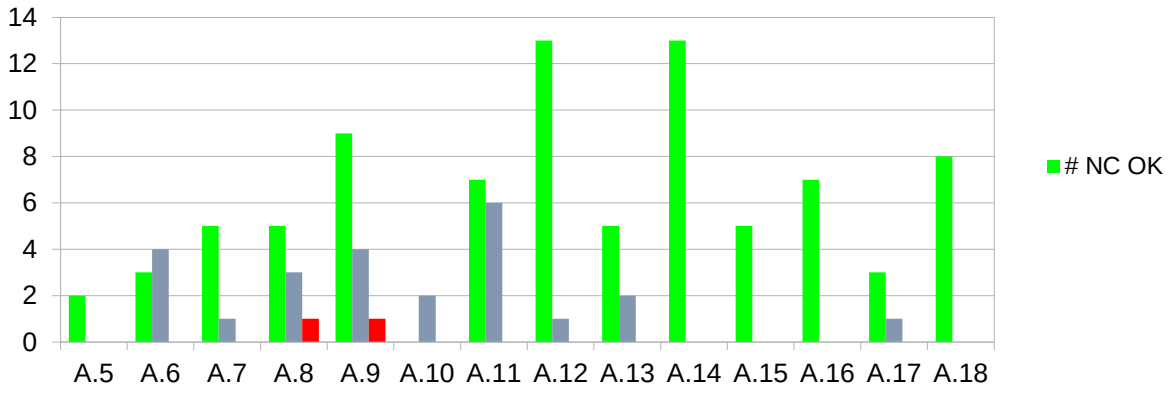

Ilustración 17 NC por dominios

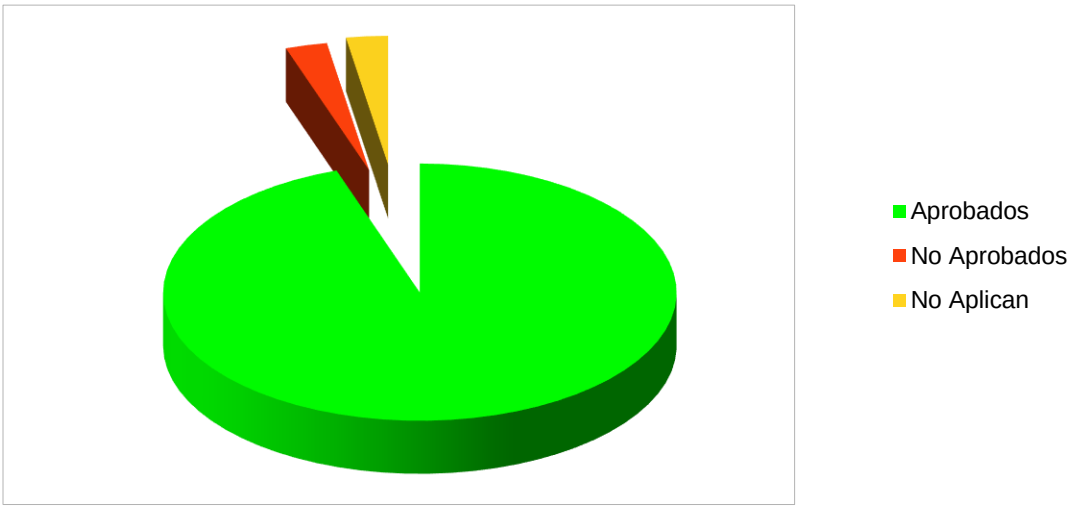

Ilustración 18 Conformidades

13.5 Resumen

Como se puede observar, con las medidas aplicadas se incrementa significativamente el cumplimiento en todos los dominios de la norma, sin embargo, es necesario incidir en los dos áreas donde se han encontrado más no conformidades (Gestión de activos y control de accesos), donde se tendrá, en un futuro, que desarrollar acciones para mejorar la seguridad en estos ámbitos.

14. Conclusiones

Estado previo

- Se detectaron múltiples carencias en cuanto al estado general de la seguridad en la organización, sin embargo, la dirección se encontraba desde un principio, plenamente comprometida con la implementación del plan director de seguridad en la organización. Este compromiso facilitó la tarea enormemente a los auditores
- La existencia de ciertos procesos y el uso de servicios en la nube, facilitó igualmente la auditoría y la implementación de ciertos controles
- Se procedió a un análisis profundo de la empresa obteniendo un listado detallado de activos críticos, sus riesgos y amenazas. A continuación se estudiaron las posibles soluciones que fueron reflejadas en proyectos con la finalidad de mitigar el riesgo a niveles aceptables definidos por la empresa

Objetivos conseguidos

- Se comprueba que tras la ejecución de este plan director, se produce una mejoría sustancial en la seguridad de la información en la organización. Este nivel de cumplimiento, supone una gran mejoría en términos generales en todos los aspectos de la empresa. Pudiendo permitir a la organización poder empezar afrontar la certificación si así lo desea
- Se comprueba una mayor concienciación de los trabajadores con la seguridad de la información. La formación planteada periódicamente ayudara a un mejor desempeño no solo en tareas de seguridad, sino de organización y funcionales. Esto es debido a la implementación de distintos cursos de formación y a las campañas de concienciación.
- La implementación de un equipo de respuesta a incidentes de seguridad y la futura integración de CTI (Cyber Threat Intelligence) en otros procesos de la inteligencia de negocio, permitirá medir el riesgo y las amenazas futuras de una manera eficiente.
- La identificación de activos y amenazas ha ayudado a la organización a ser consciente de qué posee y de qué tratamiento debe aplicar a cada uno

Proyectos y su impacto

- La propuesta de 13 proyectos diferentes, durante los dos años que están planificados, permitirá a la organización mitigar riesgos que se encuentren por encima del umbral de riesgo tolerado por dirección, aunque también, como efecto colateral, se mitigaran otros riesgos
- Todos los proyectos se encuentran definidos y planificados acorde a las necesidades acordadas con la dirección y se encuentran definidos acorde a la línea de actuación definida por la misma
- Se encuentran detallados en tiempo y presupuesto, los distintos proyectos a acometer. A la finalización de los mismos, la organización se encontrará suficientemente madura en materia de seguridad como para poder afrontar una certificación ISO

Proyectos futuros

- Una vez sea finalizada la implantación del SGSI en la empresa, y que todos los proyectos propuestos hayan concluido satisfactoriamente, la dirección podrá plantear la elaboración de un segundo plan director de seguridad que le permita medir el nivel real de implantación final, así como detectar nuevas necesidades y completar algunos dominios que no se hayan podido cubrir en el primero
- Como se indica en el propio plan director, deberán ser realizadas periódicamente diversas auditorías internas, por lo menos una vez al año.
- En cualquier caso, como se hace notar en el informe, existen algunos dominios donde la organización, por su propio “Status Quo” establecido no llega al nivel necesario. Se hace necesaria, en siguientes auditorias, encontrar una manera para solucionar estos puntos.
- En cualquier caso, es necesario hacer notar que la seguridad en una organización es un proceso en continua mejora.

Glosario de términos

Activo de Información: Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa información y tiene valor para la organización, como bases de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la empresa. La información, como activo corporativo, puede existir de muchas formas:

- Impresa
- Almacenada electrónicamente
- Transmitida por medios electrónicos
- Mostrada en videos
- Suministrada en una conversación
- Conocimiento de las personas

Alcance de la auditoría: Extensión y límites de una auditoría.

Amenazas: Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.

Análisis de Riesgos: Método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permiten determinar la extensión en que se cumplen los criterios definidos para la auditoría interna.

Auditado: Organización o Dependencia a la cual se le va a realizar una auditoría.

Auditor: Persona con la competencia para llevar a cabo una auditoría.

Auditor en seguridad de la información: Persona con la competencia para efectuar auditorías internas de seguridad de la información

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la organización. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Conclusiones de auditoría: Resultado de una auditoría, proporcionada por el equipo auditor después de la consideración de los objetivos de la auditoría y de todos los hallazgos de auditoría.

Conformidad: cumplimiento de un requisito.

Control: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

Criterios de auditoría: Conjunto de políticas, procedimientos o requisitos utilizados como una referencia frente a la cual se compara la evidencia de la auditoría.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante nuestros clientes.

Efectividad: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.

Eficacia: Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

Eficiencia: Relación entre el resultado alcanzado y los recursos utilizados.

Equipo auditor: Uno o más auditores que llevan a cabo una auditoría con el apoyo, si es necesario, de expertos técnicos.

Estimación del riesgo: Proceso de asignación de valores a la probabilidad e impacto de un riesgo.

Evento de seguridad de la información: Presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc.), asociada a una posible violación de la política de seguridad de la información, falla en controles y contramedidas, o que implica una situación desconocida que puede ser pertinente a la seguridad de la información.

Evidencia de auditoría: Registros, declaraciones de hechos o cualquier otra información que son relevantes para los criterios de auditoría y que son verificables. La evidencia de la auditoría puede ser cuantitativa o cualitativa.

Evitar el riesgo: Decisión de la organización de no involucrarse en una situación de riesgo o tomar acciones para retirarse de dicha situación.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

Hallazgo de auditoría: Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de la auditoría.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo asociados a la seguridad de la información.

Impacto: Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos del negocio.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

Integridad: La información debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la Empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas financieras.

La Dirección: Es la encargada de combinar los recursos humanos y técnicos lo mejor posible para conseguir los objetivos de la empresa; está conformada por la presidencia y directivos, quienes se encargarán de desarrollar los planes a largo plazo de la empresa.

No conformidad: El no cumplimiento de un requisito especificado. También puede denominarse no conformidad real.

No conformidad mayor: El no cumplimiento de un requisito debido a la falta frecuente o deliberada de cumplimiento de un requisito documentado en el sistema, incumplimiento de requisitos legales o reglamentarios, múltiples no conformidades menores dentro del mismo requisito de la Norma o la falta deliberada en corregir No Conformidades.

No conformidad menor: El no cumplimiento de un requisito sin que exista una amenaza relevante o significativa para el Sistema de Gestión de Calidad o cuando sea una instancia aislada de incumplimiento.

No conformidad potencial: Evento en el cual no hubo No Conformidad, pero en caso de repetirse pudiera serlo, por la existencia de un riesgo. Una acción preventiva pudiera ser tomada para evitar su ocurrencia.

Observación: Apartado del informe de auditoría en el que el auditor deja constancia de las oportunidades de mejora, de los riesgos para la calidad o de cualquier otro detalle que haya observado y le parece relevante registrar.

Observador: Integrante del equipo auditor que se encuentra en proceso de entrenamiento y su objetivo es adquirir competencia mediante la observación. Algunas veces apoya al equipo auditor tomando notas de los hallazgos de la auditoría en las listas de chequeo.

Plan de auditoría: Descripción de las actividades en el sitio y arreglos para una auditoría.

Probabilidad: Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Proceso: conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.

Programa de auditoría: Conjunto de una o más auditorías planificadas para un período de tiempo específico y dirigido hacia un propósito específico.

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.

Responsabilidades: Compromisos u obligaciones del personal o grupo de trabajo.

Riesgo: Consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la información en los activos de una empresa.

Riesgo Inherente: Es aquel riesgo que por su naturaleza no se puede separar de la situación donde se presenta. Es propio de las actividades que conlleva el proceso relacionado.

Riesgo Residual: Nivel restante de riesgo después de su tratamiento.

Riesgo en la seguridad de la información: Es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño a la organización.

Seguridad de la información: preservación de la integridad, la confidencialidad, y la disponibilidad de la información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. (Fuente: NTC-ISO/IEC 27001:2005).

S.G.S.I: Sistema de Gestión de Seguridad de la Información.

Transferencia del riesgo: Compartir con otra de las partes la pérdida (consecuencias negativas) de un riesgo.

Tratamiento de la Información: Desarrollo de las siguientes actividades sobre la información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo.

Vulnerabilidades: Debilidad de un activo de información frente a una amenaza.

Referencias

Wikipedia: Análisis de riesgo informático :
https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

Documentación MAGERIT:

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vwd4eEZjIqI

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vwd4eEZjIqI

Materiales del curso MISTIC, correspondientes a las siguientes asignaturas:

- Sistemas de Gestión de la Seguridad

- Auditoría Técnica

- Instituto nacional de Ciberseguridad (https://www.incibe.es/)

Sistema de Gestión de Seguridad de la Información en una Organización:

https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/index.html

Fases de Implantación de un SGSI en la empresa:
https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

Portal de ISO 27001 en Ingles:

http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Portal de ISO 27001 en español:

http://www.iso27000.es/sgsi.html

The Free ISO27k Toolkit:

http://www.iso27001security.com/html/iso27k_toolkit.html