Certificación de una empresa de Informática y telecomunicaciones en ISO/IEC 27001:2013

Nom Estudiant: Alejandro Rodríguez Pubill

Programa: Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Nom Consultor: Arsenio Tortajada Gallego

Centre: <UOC/DealSpain>

Data Lliurament: 12 de Diciembre de 2014

C) Copyright

FITXA DEL TREBALL FINAL

Titulo del Trabajo:	Certificación de una empresa de informática y telecomunicaciones en ISO/IEC 27001
Nombre del autor:	*Alejandro Rodríguez Pubill*
Nombre del consultor:	*Arsenio Tortajada Gallego*
Fecha de entrega (mm/aaaa):	*12/2014*
Àrea del Trabajo final:	*SGSI*
Titulación:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Resumen del Trabajo (Máximo 250 palabras):

Este trabajo corresponde a la parte final del Master Interuniversitario de Seguridad de las Tecnologías de la Informacion y Comunicaciones de la UOC, en el cual se plantea la creacion, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información de una empresa privada basándome en la norma ISO/IEC 27001:2013 y su anexo a la ISO 27002.

La actualización de la norma ISO 27001 hace que la estructura fundamental haya sufrido novedas y que los requisitos actuales hagan necesario el avance en esta materia para proteger el negocio.

La informacion es posiblemente el activo mas valioso para una organización y mantener su integridad, confidencialidad y disponibilidad para alcanzar los objetivos del negocio es una misión complicada, pero alcanzable. Para ello, se establecen una serie de medidas o normas que intentan cumplir con tal objetivo. Estas normas, se agrutinan en un SGSI.

En este trabajo, he enfocado la creación de un SGSI para una empresa dedicada a la venta online en un ambito específico heredando bastantes aspectos de su matriz en Alemania.

Abstract (in English, 250 words or less):

This work corresponds to the end of the Interuniversity Master Security Information Technologies and Communications of the UOC, in which the creation, maintenance and improvement of a management system for information security of a private company arises based ISO / IEC 27001: 2013 and ISO 27002 Annex.

Updating the ISO 27001 makes the fundamental structure has suffered NEWS & that current requirements necessitate progress in this area to protect the business.

The information is possibly the most valuable asset for an organization and maintain its integrity, confidentiality and availability to meet business objectives is a difficult but achievable mission. To this end, a series of measures or standards that attempt to meet this objective are set. These standards, agrutinan in an SGSI.

In this paper, I have focused the creation of an SGSI for a company dedicated to online sales on a specific scope inheriting many aspects of its parent company in Germany.

Paraules clau (entre 4 i 8):

SGSI, ISO, 27001, Riesgo, Normativa, Organización, Venta Online.

Índice

1. CONTEXTUALIZACIÓN Y DOCUMENTACIÓN: ANÁLISIS DE LA EMPRESA.

Segun la norma ISO/IEC 27001, un SGSI se define como "Un sistema de gestión que comprende la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Este sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.). Este sistema proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización."

“La información es poder” – Con esta cita anonima las empresas, tanto públicas como privadas, se hacen eco de la importancia que supone hoy en dia proteger su activo más valioso, la información. Ésta, aparece en las empresas en muchisimas formas, desde información contenida en un papel en un sobre hasta unos datos enviados por correo electronico.

Por este motivo, la información debe ser valorada en consecuencia y protegida a tal efecto.

Para tal efecto, la norma aceptada actualmente para este menester es la norma UNE-ISO/IEC 27001:2013 que son un conjunto de normas y estándares que proporcionan un marco de gestión de la seguridad de la información aplicable a cualquier organización. En las organizaciones grandes, medianas o pequeñas, públicas o privadas necesitan establecer medidas que aseguran sus activos más importantes que es la información para hacerlas más competitivas.

Estas normas no son de obligado cumplimientos pero si unas normas de buenas practicas que acreditan a las empresas que la informacion que manejan se hace de manera correcta y siguiendo unos controles exhaustivos. Economicamente, esta adecuación a la norma conlleva un precio, el cual nunca puede superar el del activo que se quiere proteger, por lo que tiene que haber un equilibrio entre el coste de la seguridad y el valor del activo a proteger.

En este trabajo, me centrare en la adecuación a la norma 27001:2013 para su posible certificación certificación en el futuro ya que la actualización a la 2013 todavía no es una UNE(Una Norma Española) y por lo tanto es imposible certificarse en españa en la 27001:2013.

1.1 Contexto y justificación

Las organizaciones que actualmente se encuentren certificadas en ISO/IEC 27001:2005 disponen de un periodo de transición estimado para adaptarse al nuevo estándar de 2 a 3 años. De la misma forma, existirá un notable impacto relacionado con la actualización de controles del anexo A / ISO27002, que implicará la adecuación de las herramientas de gestión y tratamiento de riesgos.

Para aquellas organizaciones que estén implantando un SGSI y cuyo proceso de implantación se encuentre lo suficiente maduro, cumpliéndose con la mayoría de los requisitos formales y disponiéndose de los correspondientes procedimientos, se recomienda la certificación contra la versión anterior de 2005 a corto plazo e ir planificando la migración a la versión 2013, siendo posible la certificación contra la versión 2005 durante aproximadamente un año.

ISO/IEC 27001:2013 ha sido desarrollado con base en el anexo SL de ISO/IEC del "Suplemento Consolidado de las Directivas ISO/IEC" (anteriormente publicado como "Guía ISO:83″), en el cual se proporciona un formato y un conjunto de lineamientos a seguir para el desarrollo documental de un sistema de gestión sin importar su enfoque empresarial, alineando bajo una misma estructura todos los documentos relacionados con los sistemas de gestión y evitando así problemas de integración con otros marcos de referencia.

- Descripción de la empresa:

El proyecto en concreto es la puesta en marcha en España de una compañía de una multinacional con sede en Alemania(GermanDeal GmbH**)** pero con nueva apertura de la misma en España, donde operarían sus servicios centrales(CPD). La empresa, ***SpainDeal S.A***, se dedica a la venta de productos relacionados con la informatica y las telecomunicaciones a través de su pagina web. En su plan de desarrollo y expansión se ha elegido a España para su nueva puesta en marcha en la península Ibérica.

Productos que ofrece:

- Telefonía voz IP
- Modems y cable modems
- Hardware & Software (Servidores)
- Venta Formación
- Satelites
- Redes WIFI Y WIMAX
- Cableado
- Distribución TV Digital (Canal + España)

En España, esta empresa replicara su estructura de su sede central, por lo que se hará una reproducción una estructura similar, siendo su responsable en españa, dependiente de la cupula en Alemania. La empresa se ubica en Madrid, y toda su infraestructura se ubica en un mismo edificio, donde están todos los departamentos, junto al centro logístico y también sus servidores donde se alojan todas las aplicaciones relacionadas con la página web.

Esta empresa dispone de una serie de controles previos heredado de su empresa padre, pero se realizara un SGSI de la seccion Técnica de la empresa, la cual, al tener una dinámica diferente a la matriz, se realizara el sgsi propio debido a la casuistica propia de la empresa ya que difiere de la Alemana.

El número de los trabajadores actualmente es entorno a los 200 empleados, unos 50 proveedores y mas de 100.000 clientes finales, incluidas empresas y personas físicas.

La estructura de la empresa se define de la siguiente manera:

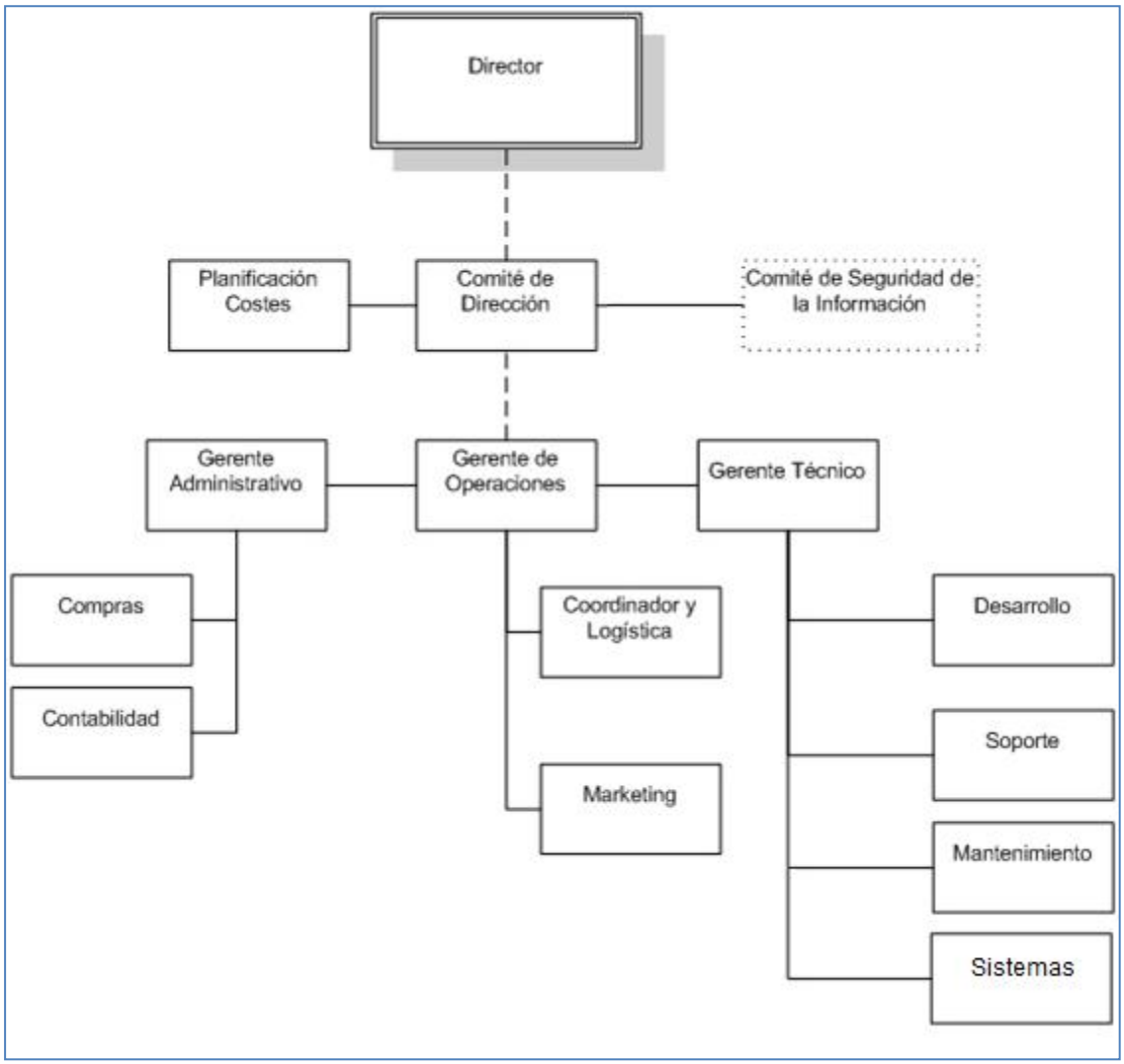

Ilustración 1 Estructura de la empresa

La empresa la forma:

-El director: máximo responsable el cual establece la estrategia corporativa junto con el comite de dirección. De él dependen:

- Planificación de costes

- Comite de dirección del cual dependen:

  - Gerente administrativo(Compras y Contabilidad)
  - Gerente de operaciones(Coordinador y Logistica y Marketing)
  - Gerente Técnico(Mantenimiento, Desarrollo, Soporte y Sistemas)

La misión principal de cada área es:

- Director: máximo responsable el cual establece la estrategia corporativa junto con el comite de dirección del cual dependen el resto de empleados.
- Comite de dirección:

- Garantizar la viabilidad del negocio: el Comité debe ser el principal garante de que se toman decisiones que son viables para el negocio (ya sea a corto, medio o largo plazo). A menudo, se han tomado muchas decisiones sin hacerse la pregunta de si ese negocio es sostenible y puede ser desarrollado por la empresa con garantías.
- Buscar el crecimiento: siempre teniendo en cuenta que el negocio debe ser viable y sobrevivir, a partir de aquí, el Comité debe buscar fórmulas y caminos de crecimiento del negocio de forma continuada.
- Asegurar la supervivencia del negocio: los miembros del Comité tienen que obsesionarse con hacer que el negocio sobreviva más allá de su tiempo como directivos y miembros de dicho Comité.
- Fijar el marco estratégico y asegurar su comprensión en toda la organización: el Comité debe fijar claramente el marco estratégico de la empresa (su misión, visión, valores, filosofía, clima, cultura y líneas estratégicas) y asegurar que toda la empresa toma sus decisiones siendo coherente con ese marco.
- Crear una organización efectiva y eficiente
- Desarrollar el talento y el liderazgo

Dependiendo directamente del Comite, se encuentra el gerente de operaciones, el cual es el responsable directo de sus secciones de logística y marketing y asu vez es el coordinador de las otras 2 secciones, la administrativa y la técnica.

- Planificación de costes : Este departamento se encarga de instrumentar y operar las políticas, normas, sistemas y procedimientos necesarios para garantizar la exactitud y seguridad en la captación y registro de las operaciones financieras, presupuestales y de consecución de metas de la entidad, a efecto de suministrar información que influye a la toma de decisiones, a promover la eficiencia y eficacia del control de gestión, a la evaluación de las actividades y facilite la fiscalización de sus operaciones, cuidando que dicha contabilización se realice con documentos comprobatorios y justificativos originales, y vigilando la debida observancia de las leyes, normas y reglamentos aplicables.

- Se creara un Comite de seguridad de la información que no existe actualmente. Será un cuerpo integrado por representantes de las distintas áreas de la empresa, destinado a garantizar el apoyo de las autoridades a las iniciativas de seguridad para lograr un trabajo eficaz y seguro. La creación del Comité responde a la necesidad de asegurar que la información que circule a través de los sistemas informáticos y se adecue a las premisas de confidencialidad, integridad y disponibilidad, para garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que así lo requieran.

Los departamentos de Desarrollo, Soporte, Mantenimiento y Sistemas se encuentran dentro de la gerencia técnica. Como veremos más adelante, este, será el objetivo del TFM, dontandole de un SGSI a esta sección para una posterior certificación en la ISO/IEC 27001:2013.

- Desarrollo: Este es el departamento que desarrolla los productos de software para la empresa, y su posterior producción. Esta compuesto por diferentes empleados, desde un Jefe de proyectos, programadores Senior, programadores Junior y analistas.

- Soporte: El departamento se encargara del soporte al cliente, realizando funciones de call center para todo tipo de problematica en el proceso compra de cualquier producto.
- Mantenimiento: Departamento encargado de la infraestructura y las comunicaciones(redes,cableado....)
- Sistemas: Departamento encargado de llevar a produccion los sistemas que se hayan desarrollado.

1.2 Objetivos

El objetivo por tanto, es realizar un plan de implementación de la ISO 27001:2013 en la sección técnica de una empresa que se dedica a la venta de multiproductos a traves de su pagina web para su certificación en ISO 27001:2013 durante los 6 meses posteriores a la publicación de la norma, ya que se recomienda usar ese marco de referencia en el caso de que no haber empezado el proceso de implantacion o encontrarse en las fases iniciales del proceso de implantación de un SGSI.

Se empezara el proyecto realizando una auditoria pasando los controles de la ISO/IEC 27002:2013 para ver en que situación partimos para posteriormente realizar el SGSI en base al resultado de la misma.

Esta certificación se quiere adquirir en el futuro, para que el cliente vea el compromiso de la empresa para tratar la información y que pueda confiar en ella al hacer cualquier compra a traves de ella.

1.3 Enfoque

El análisis de riesgos de una empresa es uno de los pilares básicos del SGSI. Una vez analicemos los activos, las amenazas que les pueden afectar y el coste que conllevara su protección o restitución, se crea el Analisis de Riesgos. En base a este Analisis de Riesgos se estableceran los recursos para eliminar, minimizar o aceptar las amenazas a las que se exponen los activos.

Al contrario de lo que se puede pensar, este Analisis no es exclusivo del valor economico del activo sino que va mas alla, siendo activos intangibles tambien los factores a valorar. Los activos intangibles tienen su origen en los conocimientos, habilidades, valores y actitudes de las personas, a estos activos intangibles se les denomina Capital Intelectual. Son activos intangibles las capacidades que se generan en la organización, cuando los recursos empiezan a trabajar en grupo.

Para la realización del Análisis de Riesgos hay distintas metodologias, pero para este proyecto me declino por la metodología MAGERIT, la cual es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. Actualizada en 2012 en su versión 3

Toda la información se puede obtener aqui:

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VC68mPl_u2E

1.4 Definición del Alcance

La norma ISO 27001:2013 en el punto 4.3 Alcance del SGSI establece los requisitos para su definición:

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance. Cuando se determina este alcance la organización debe considerar:

a) Entendimiento de la organización y su contexto (contexto de la organización, punto 4.1)

b) Expectativas de las partes interesadas (punto 4.2)

c) las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones

El alcance debe estar disponible como información documentada.

Para este proyecto, el alcance se limita al **departamento técnico** y a todos los procesos que ocurren cuando un cliente realiza una compra online junto con todos los servicios y sistemas que lo forman incluyendo servidores, aplicaciones y material humano. Este alcance esta delimitado por la declaración de aplicabilidad y la implementación de controles del presupuesto aprobado.

1.5 Análisis

En la nueva versión ISO/IEC 27001:2013 se da gran importancia a la adecuación a una estructura de alto nivel, siendo más sencillo la implementación y la homologación con otras normas de sistemas de gestión. Por otro lado, la ISO/IEC 27002:2013 se ve modificada quitando unos dominios y añadiendo otros, pasando de 11 dominios a 14 y quitando 20 controles, quedando en solo 113 de los 133 anteriores.

Numeral	Dominio
A.5	A.5 Políticas de seguridad de la información
A.6	A.6 Organización de la seguridad de la Información
A.7	A.7 Seguridad de los recursos humanos
A.8	A.8 Gestión de activos
A.9	A.9 Control de acceso
A.10	A.10 Criptografía
A.11	A.11 Seguridad física y del entorno
A.12	A.12 Seguridad de las operaciones
A.13	A.13 Seguridad de las comunicaciones
A.14	A.14 Adquisición, desarrollo y mantenimiento de sistemas
A.15	A.15 Relaciones con los proveedores
A.16	A.16 Gestión de incidentes de seguridad de la información
A.17	A.17 Aspectos de seguridad de la información de la gestión de continuidad del negocio
A.18	A.18 Cumplimiento

A pesar de haberse definido el alcance del SGSI, se considera necesario por el equipo de seguridad de la información, definir un alcance más acertado con la realidad o estado actual de la empresa, por tanto se hace necesario que el equipo de trabajo verifique el estado actual, a través de la realización de un análisis diferencial.

Porcentaje de implementación	Descripción
0%	Sin implementar
25%	Inicialmente implementado o en proceso de hacerlo.
50%	Parcialmente implementado pero no está aprobado
100%	Implementado y aprobado

El análisis diferencial es la identificación previa al proyecto de implantación del SGSI en una empresa, sobre las medidas de seguridad y verificación de aplicaciones de la normativa implementada en relación a la Seguridad de la Información. Este análisis diferencial se realizará con respecto a la ISO/IEC 27001 e ISO/IEC 27002. El análisis diferencial permite conocer de primera mano, el estado general de la empresa entorno a la seguridad de la información permitiendo la definición del alcance.

Una primera toma de contacto mostrada en el Anexo 1 para las 2 normas:

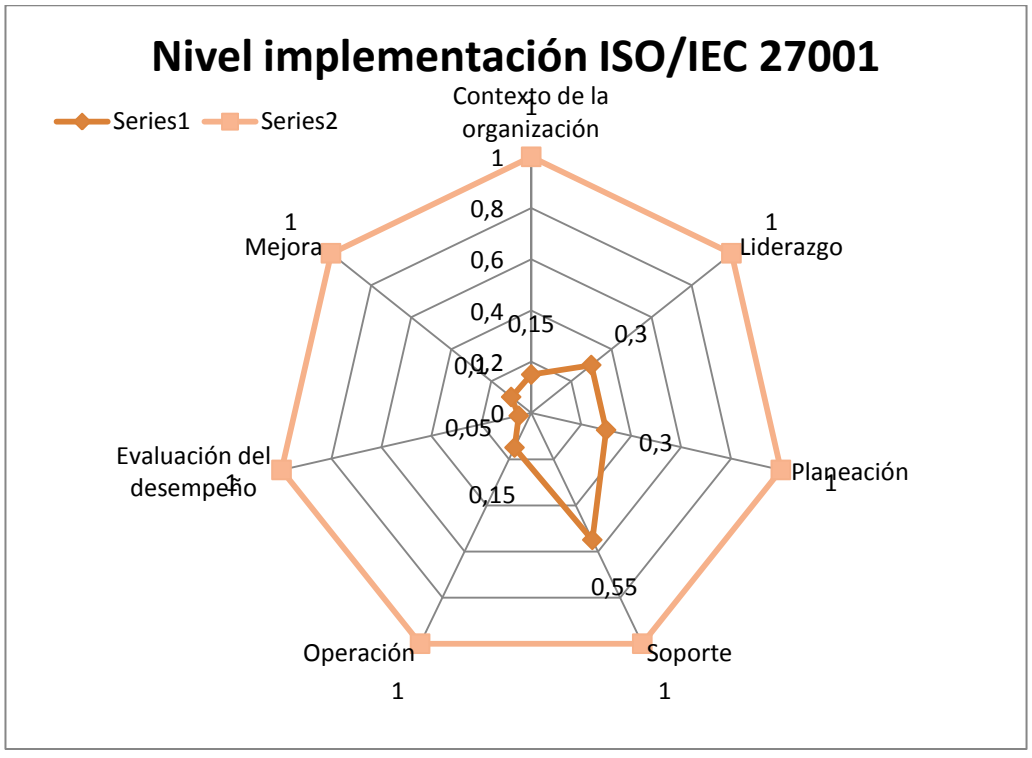

Ilustración 2 Nivel de implementación ISO/IEC 27001:2013

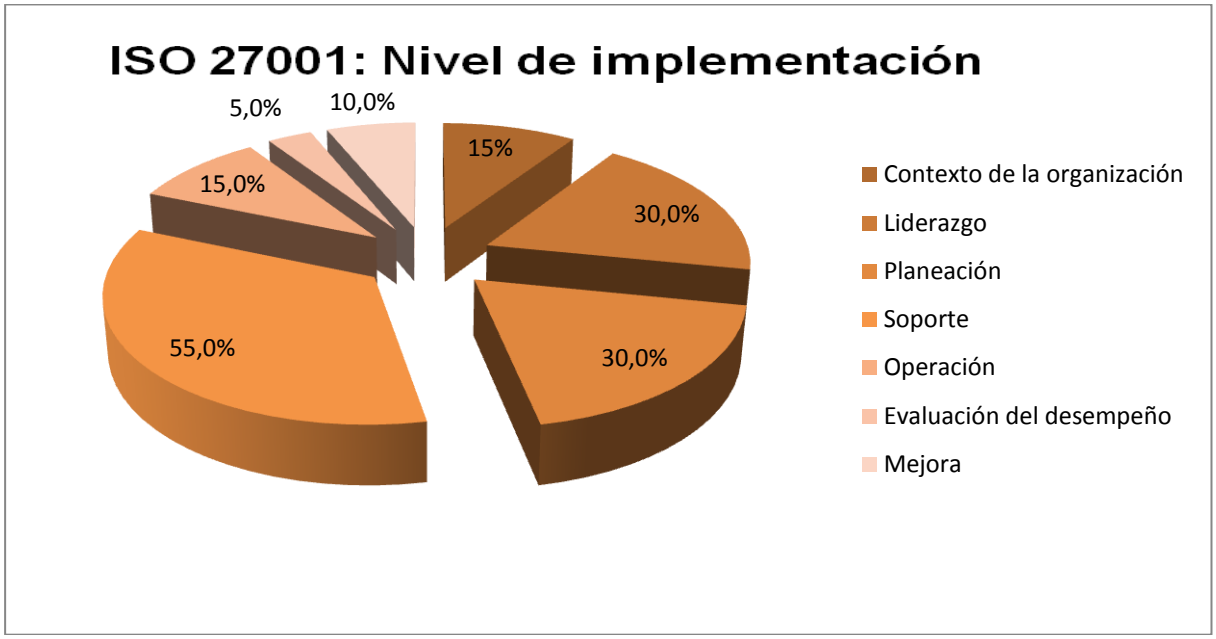

Ilustración 3 Nivel implementación 27001

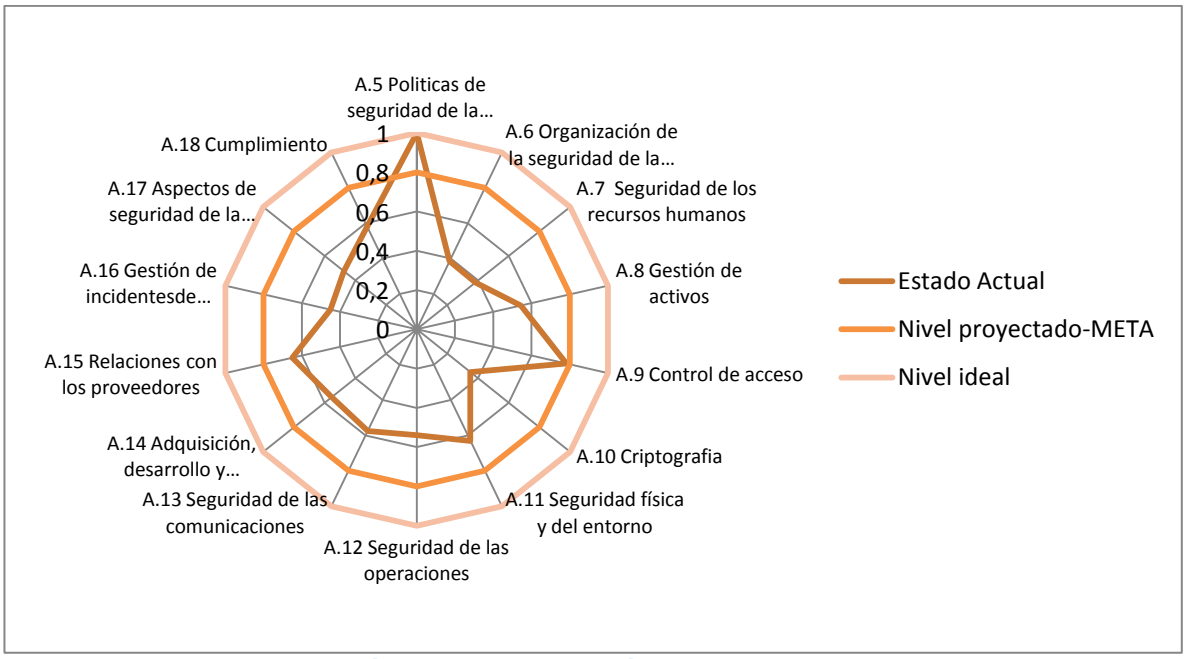

Ilustración 4 Implementación ISO/IEC 27002:2013

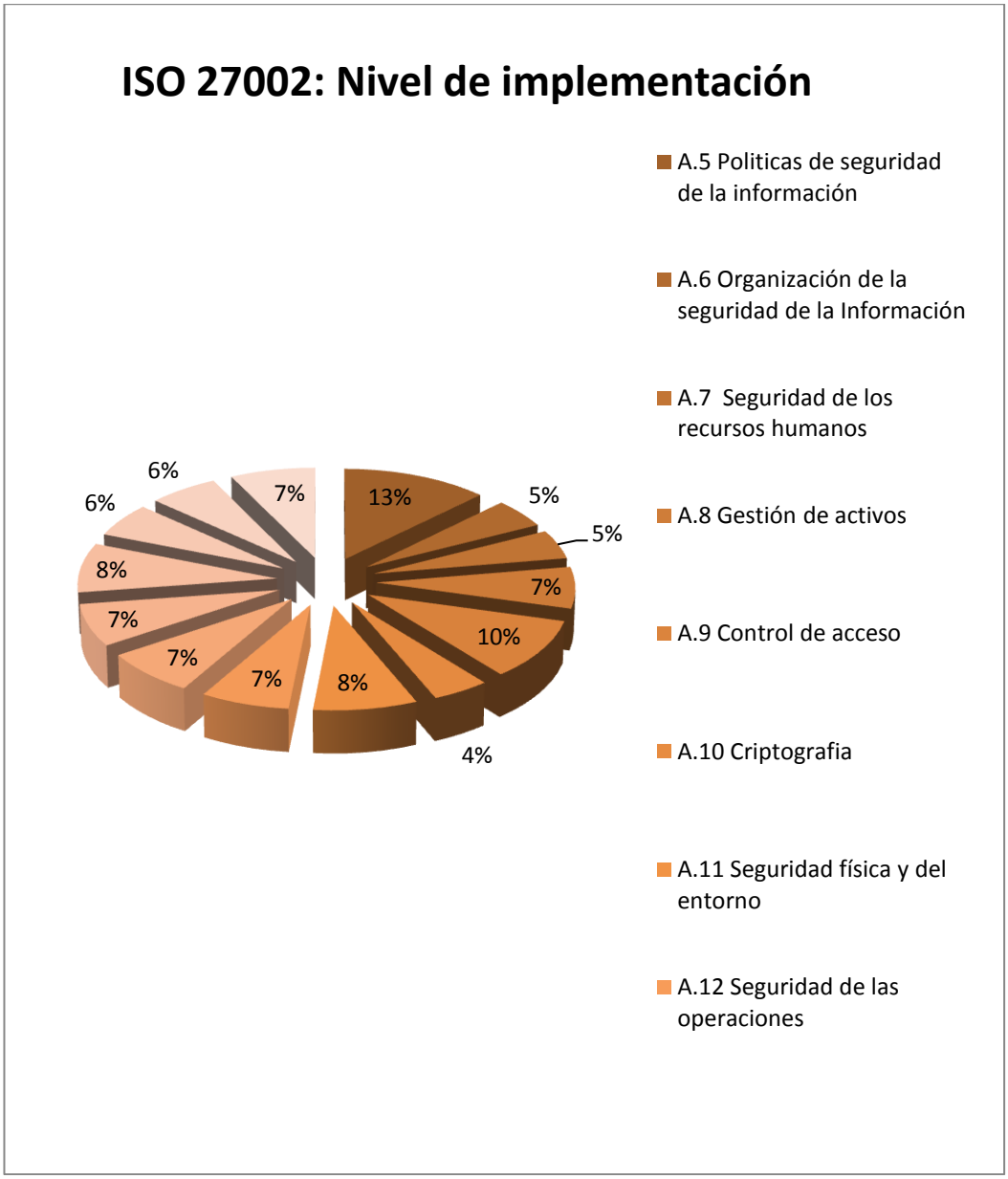

Ilustración 5 Nivel de implementación ISO 27002

Una vez identificados todos los activos de información comprendidos en el alcance, se procede a establecer el SGSI, siguiendo las pautas del estándar ISO 27001:2013 en su sección 4.3. En esencia lo que se exige es efectuar de manera disciplinada y sistemática un análisis y evaluación del riesgo de los activos identificados para determinar cuáles son aquellos que deben ser protegidos para mitigar su riesgo, así como definir también cual es el riesgo residual (el riesgo con el cual la empresa está decidida a convivir)

En la siguiente ilustración se pormenorizan los pasos metodológicos que se siguieron para realizar el análisis y evaluación del riesgo, de los activos de información, del área técnica para cumplir con las exigencias del ISIO 27001:2013. A continuación se hará una descripción de los pasos seguidos para el manejo de la metodología para el análisis y evaluación del riesgo.

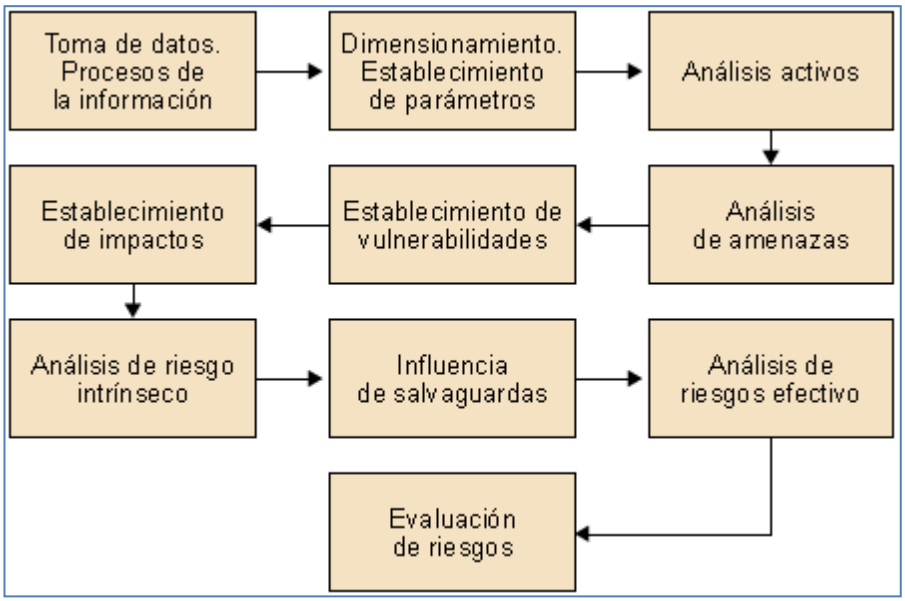

Ilustración 6 Metodología y evaluación de riesgo

1.6 Metodología

La gestión de los riesgos es una piedra angular en las guías de buen gobierno [ISO 38500], público o privado, donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican.

Para realizar el análisis de riesgos nos hemos basado en el modelo **MAGERIT**.

Esta norma establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información. Garantizando que sus organizaciones siguen estos principios ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI

En pocas palabras, la gestión de los riesgos es nuclear al gobierno de las organizaciones.

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo.

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

El análisis de riesgos ejecutado podemos encontrarlo en el documento “Análisis de riesgos”

A continuación se describe las etapas del proceso que sigue MAGERIT y consta de tres etapas.

1. PLANIFICACIÓN: En esta etapa se establecen las consideraciones necesarias para dar inicio al proyecto.

2. ANÁLISIS DE RIESGO: Permite determinar cómo es, cuanto vale y como de protegidos se encuentras los activos. En esta etapa se constituye en el núcleo central de MAGERIT y su correcta aplicación condiciona la validez y utilidad de todo el proyecto.

Los Objetivos del Análisis de Riesgo son:

• Identificar los activos relevantes que poseen la organización.
• Identificar las amenazas a las que están expuestos dichos activos.
• Determinar si existen salvaguardas para los activos.
• Estimar el impacto si una amenaza llegara a materializarse.

Los elementos de Análisis de Riesgos:

1. Caracterización de Activos: Esta actividad es reconocer los activos que componen los procesos necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección. En este grupo encontramos la identificación de los activos y la valoración de los activos
2. Caracterización de las Amenazas: Son los eventos que les pueden pasar a los activos desencadenando un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos, estas pueden ser por accidentes, errores, amenazas intencionales presenciales o remotas. En este grupo encontramos la identificación de las amenazas y la valoración de las amenazas
3. Caracterización de la Salvaguardas son mecanismos de defensa utilizados para que aquellas amenazas no causen tanto daño.
4. Análisis de riesgo residual una vez finalizada la aplicación de salvaguarda se deberá calcular el riesgo incluyendo la reducción resultante después de la aplicación de las salvaguardas.

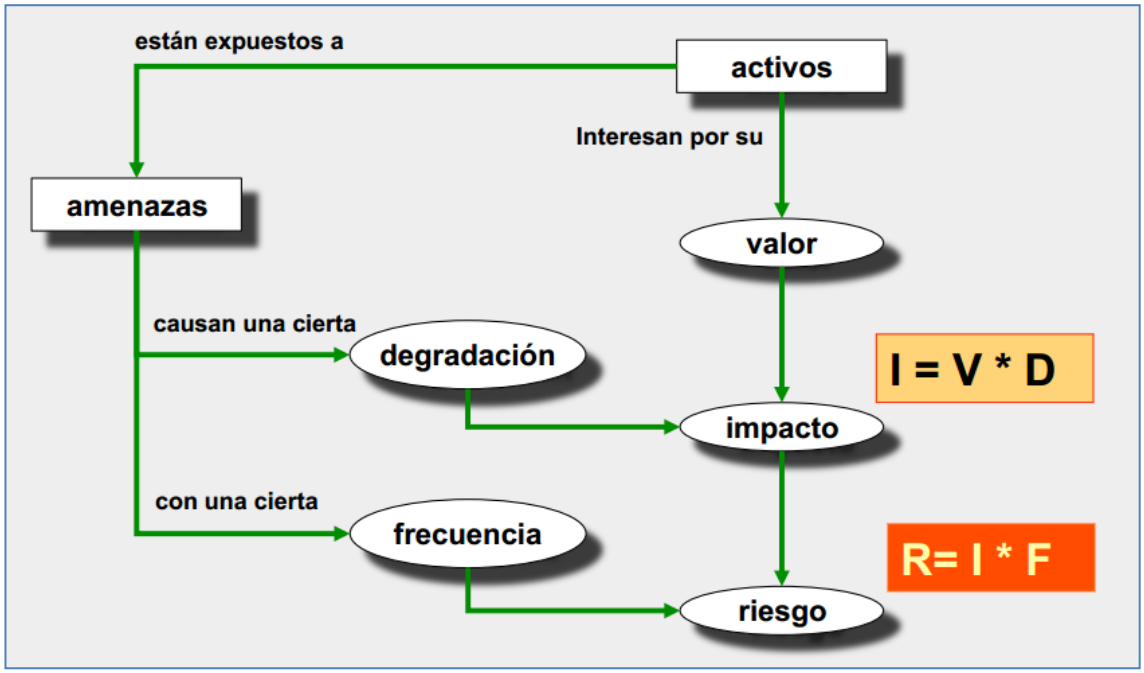

Ilustración 7 Proceso de análisis de riesgos

3. ANÁLISIS DE RIESGO: La gestión de riesgos supone la fase final en la que se deberán presentar los resultados del análisis de riesgos a Dirección y establecer el nivel de riesgos aceptable para la entidad. Una vez esta definido este nivel de riesgo, se debe definir un documento (llámese plan de tratamiento de riesgos, plan de seguridad, etc.) en el que se recojan las salvaguardas y medidas que se van a implantar para minimizar los riesgos que se encuentran por encima del umbral aceptado.

En cualquier caso es aconsejable que este plan recoja como mínimo: una descripción de la medida a implantar, la identificación de la persona responsable de acometerla, una asignación adecuada de recursos y una planificación de la fecha para la implantación efectiva de la medida. Establecido el plan es importante llevar un seguimiento del mismo para comprobar que los hitos marcados se están cumpliendo de acuerdo con la planificación establecida y para la verificación en posteriores iteraciones del análisis de riesgos de que se alcancen los niveles de riesgos adecuados.

2. OBJETIVOS PLAN DIRECTOR

2.1Introducción

El Plan Director tiene como objetivo identificar los proyectos que deben desarrollarse por la organización a corto, medio y largo plazo para reforzar y garantizar la correcta gestión en el marco de la seguridad de la información.

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes. Los objetivos de seguridad de la información deben:

a) ser coherentes con la política de seguridad de la información
b) ser medibles (si aplica)
c) tener en cuenta requisitos de seguridad aplicables y los resultados de valoraciones y de tratamiento de riesgos
d) ser comunicados
e) ser actualizados

Se debe conservar información documentada de los objetivos. En la planificación de los objetivos, se debe determinar:

f) lo que se va a hacer
g) los recursos necesarios
h) responsables
i) cuándo se finalizará
j) cómo se evaluarán los resultados

SpainDeal busca particularmente con ésta actividad, promover la ejecución de prácticas de seguridad adecuadas y la implementación un Sistema de Gestión de Seguridad de la Información (SGSI) con base en la norma ISO/IEC 27001:2013 para cubrir los servicios de Desarrollo, Soporte, Mantenimiento y Sistemas.

Como parte del análisis, se establecerán diferentes frentes de trabajo y etapas de registro de información (contextualización, identificación de activos, análisis de impacto, análisis de riesgo) que posteriormente maduraran y registraran observando los posibles escenarios de riesgo que apareciesen y poder mejorarlos o subsanarlos.

Para la viabilidad del Plan Director se seguirán distintos procesos o mecanismos:

- Buscar el apoyo, dirección y aprobación de manera continua del SGSI en la alta gerencia y hacia las partes interesadas sobre el alcance declarado.

- Identificar, calificar y hacer un tratamiento adecuado de los riesgos que puedan impactar negativamente en la información, en los procesos y en la organización implementando las salvaguardas que permitan reducir el nivel de exposición frente a ataques informáticos o fugas de información.

- Implementar controles que eviten ataques informáticos y sus posteriores modificaciones no autorizadas.

- Dar cumplimiento a la normatividades y legislación en el sector de las comunicaciones acorde a su aplicabilidad

Por otra parte, fomentar el uso de técnicas de recolección de información para consolidación de la información sobre las áreas operacionales de la organización con:

- Cuestionarios: El personal responsable por la valoración de riesgos desarrolla cuestionarios para recoger información sobre los controles administrativos y operacionales planeados o utilizados por las diferentes dependencias de la organización.

- Entrevistas en sitio: Las entrevistas en sitio con personal idóneo (con experiencia y conocimiento de sus funciones y contratiempos manejados) de los procesos con el objeto de obtener información útil para la valoración de riesgos.

- Revisión de documentos: La documentación de ejercicios anteriores, procesos, normas, directrices, formatos, plantillas de control, bitácoras, informes de auditorías previas, proveen excelente información acerca de los controles usados y planeados por la organización.

- Herramientas de escaneo: Mediante el uso de herramientas técnicas, y proactivas se recolecta información complementaria y validan perfiles y configuraciones individuales sobre recursos tecnológicos.

2.2 Objetivos:

SpainDeal desea principalmente mejorar los niveles de seguridad incluidos en sus servicios, con el objeto de optimizar las relaciones de confianza con sus clientes y convertirse en una alternativa más confiable y competitiva frente a otras empresas del mercado.

En segundo lugar SpainDeal, se ha propuesto encauzar sus procesos con practicas adecuadas a nivel de seguridad y solicita del departamento de consultoría: identificar los activos de información relevantes de sus actuales servicios, conocer los riesgos relacionados, los niveles de madurez alcanzados con los controles actualmente implementados y finamente identificar un plan de acción que le permita en un tiempo no mayor a un año acercarse al marco objetivo para la posterior certificación en la norma ISO/IEC 27001:2013 en cuanto sea posible.

Consolidar en el presente documento los resultados, conclusiones, y recomendaciones de la identificación de activos, evaluación y valoración de riesgos, así como determinar las bases para el tratamiento de riesgos y establecer el mapa de ruta o Plan Director de Seguridad de la Información para SpainDeal.

Definir y estructurar procesos y directrices en seguridad de la información para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI).

En general, mitigar riesgos, impacto o consecuencia que podrían materializarse al infringir los niveles de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad además de registrar y documentar:

- La Identificación de recursos críticos en la sección técnica.
- La identificación de las amenazas y vulnerabilidades.
- La estimación de la probabilidad de materialización de cada una de las amenazas identificadas al explotar vulnerabilidades existentes.
- La estimación del impacto de comprometer las operaciones del negocio y amenazar la seguridad de la información con la materialización de amenazas
- La identificación de los controles que actualmente se tienen implementados, y que permiten la mitigación en mayor o menor medida de las fuentes de riesgo.
- Las recomendaciones de mejora.

Facilitar los instrumentos suficientes para refinar compromisos a nivel de seguridad de la información a través de los diferentes roles y perfiles con metas como:

- Empleados y clientes: Garantizar que el uso de los activos de SpainDeal y su información por parte de Empleados y clientes, es congruente con las órdenes administrativas, políticas, guías y reglas de la organización para mitigar los riesgos y proteger adecuadamente los recursos.
- Dueños de la información: En el caso de SpainDeal, y referenciado el alcance, el único dueño de la información existente es el Gerente técnico por lo que él tendrá que definir, aprobar y autorizar la dirección de seguridad y cambios en sus sistemas.
- Administradores y Coordinadores de áreas o dependencias**:** Como responsables de la infraestructura y servicios de SpainDeal (administradores Bases de Datos, Servidores…)
- Analista de monitoreo e incidentes (Sistemas): Contar con un grupo responsable de consolidar log´s y pistas de auditoría y definir los procedimientos para monitorear los comportamientos anormales o posibles incidentes y escalar en tiempos adecuados para tomar las medidas de contención necesarias o realizar investigaciones especiales bajo un procedimiento de recolección de evidencia confiable sin afectar los derechos fundamentales de las personas.
- Responsable de Seguridad de la Información: Ayudara a identificar, evaluar y minimizar los riesgos de los sistemas que soportan la misión de la organización y cumpliendo funciones como:

    - Liderar y coordinar la implementación de políticas de seguridad de la información.
    - Evaluar y coordinar la implementación de controles.
    - Monitorear cambios significativos en los riesgos que afecten los activos de información.
    - Identificar las necesidades y recursos necesarios para el mantenimiento de los niveles de seguridad adecuados.
    - Identificar las necesidades de formación, capacitación o concienciación.
    - Actuar como asesor de la seguridad de la información.
    - Responder al comité de seguridad de la información sobre el estado de la investigación y monitoreo de incidentes de seguridad.
    - Presentar al comité informes periódicos del estado de la seguridad de la información dentro de las áreas y la organización en general.

- Comité de Seguridad de la Información: Para que pueda estar conformado por los líderes o responsables de las diferentes áreas de la organización y determine, apruebe y de seguimiento a políticas, planes y proyectos que requiera la entidad en materia de seguridad de la información y responda por actividades como:

    - Proponer cambios en mejora de los niveles de seguridad de la información.
    - Mantener informada a la alta dirección sobre el estado general de la seguridad de la información.
    - Conocer, vigilar y apoyar las actividades del oficial de seguridad de la información.
    - Proponer iniciativas de inversión a nivel de seguridad de la información.
    - Evaluar y aprobar metodologías y procesos específicos relativos a seguridad de la información.
    - Adoptar indicadores de gestión para seguridad de la información.
    - Promover la difusión y apoyo en campañas de sensibilización o concienciación.

- Alta Dirección: Lograr que la Alta dirección, pueda mantener y apoyar formalmente los proyectos y directrices a nivel de seguridad de la información a fin de garantizar la participación de todas las partes interesadas y sancionar el incumplimiento.

Adicionalmente, ayudar a SpainDeal, a emplazar sus esfuerzos en fines como:

- Disponer de las bases suficientes para establecer y mantener una política y estándares de seguridad de información que cubra toda la organización.
- Tener una metodología estándar de evaluación a procesos y actividades relacionados con la seguridad de Información.
- Establecer un programa de evaluación periódica de vulnerabilidades sobre los activos de la Organización.
- Administrar conscientemente el programa de identificación y clasificación de activos de información.
- Establecer y documentar las responsabilidades de la organización en cuanto a seguridad de información.
- Identificar y Monitorear vulnerabilidades reconocidas sobre funciones de los proveedores.
- Mejorar los procesos de control de incidentes de seguridad o violaciones de seguridad.
- Coordinar todas las funciones relacionadas a seguridad, como seguridad física, seguridad de personal y seguridad de información, etc.
- Desarrollar y administrar con fundamento el presupuesto de seguridad de información.

3. ESTADO DEL RIESGO: IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS Y AMENZAZAS.

Realizaremos un primer levantamiento de situación de activos para obtener una caracterización de los elementos de infraestructura por el tipo de activo, con que otros activos se relacionan y determinar su importancia y su valoración.

¿Qué son los activos?

Son todos aquellos elementos que posee la organización y que serán analizados durante el proceso. Cabe destacar que por activo se entiende todo tipo de elemento que requiere la organización para poder realizar las actividades de negocio que le son propias y que necesita ser protegido o está expuesto.

Esta exposición hace que un activo este afectado a posibles amenazas que les son propias a cada activo, y por lo tanto tendrán controles individualizados pudiendo diferir las salvaguardas entre los distintos activos.

Una clasificación general de estos activos sería:

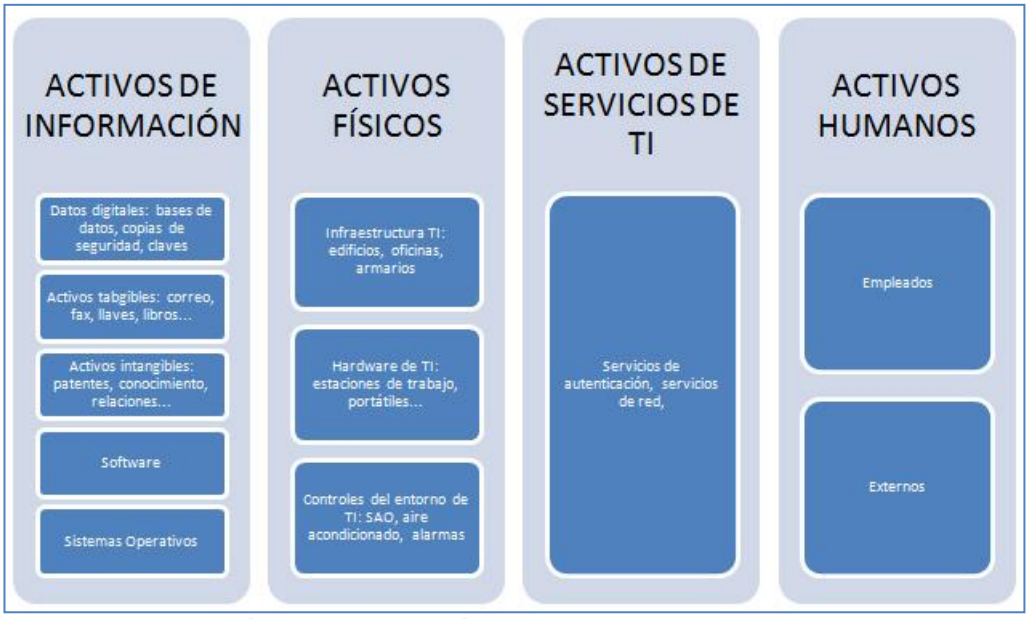

Ilustración 8 Clasificación Activos. Fuente: isotools.org

3.1 Inventario de activos.

El activo esencial es la información y alrededor de esta información encontramos los siguientes activos importantes dentro del alcance a cubrir:

Código	Activo
S1	Servicio de Aplicaciones.
S2	Servicio de BackUp
S3	Servicio WEB - Página
S4	Servicio de BBDD
S5	Servicio Pasarela de Pago
S6	Servicio de cifrado
I1	Información
I2	Pagina Web
I3	Pasarela
I4	Correo electrónico
I5	BBDD
HW1	Servidor de ficheros
HW2	Servidor BackUP
HW3	Servidor WEB
HW4	Servidor Certificados
HW5	Servidor BBDD
HW6	Servidor de Correo
HW7	Servidor Firewall
HW8	Servidor de Desarrollo
HW9	Servidor de Aplicaciones
HW10	PCs empleados
HW11	Impresora
HW12	SAN -Almacenamiento
SF1	Licencias aplicaciones
SF2	Licencias Sistemas Operativos
SF3	Licencias BBDD
SF4	Licencia Antivirus
SF5	Licencias Correo
SW1	Administración y Operación Servidores
SW2	Administración y Gestión aplicaciones
SW3	Administración y Operación BBDD
SW4	Administración WEB
SW5	Administración Servicio DNS
HW13	Switch Central
HW14	Firewall
HW15	Switches
HW16	Router
EQ1	Generadores Eléctricos Principales
EQ2	SAI
P1	Responsable-Administrador
P2	Empleados

3.2 Dimensiones de seguridad y valoración de activos

Los parámetros que utilizaremos durante el análisis de riesgos serán estos:

- Valor de los activos: se asignara un valor al objeto analizado

Niveles de criticidad	Descripción	Valor
Muy alto - MA	Activo cuya afectación genera un daño muy grave a la organización	9-10
Alto - A	Activo cuya afectación genera un daño grave a la organización	6 - 8
Medio - ME	Activo cuya afectación genera un daño importante a la organización	3 - 5
Bajo - B	Activo cuya afectación genera un daño menor a la organización	1- 2
Despreciable - MB	Activo cuya afectación es irrelevante para la organización	0

- Frecuencia de ocurrencia

Nivel	Rangos	Ejemplo detallado de la descripción
5%	Muy bajo	Puede ocurrir solo bajo circunstancias excepcionales
20%	Bajo	Podría ocurrir algunas veces
50%	Medio	Puede ocurrir en algún momento
75%	Alto	Probabilidad de ocurrencia en la mayoría de las circunstancias
100%	Muy alto	La expectativa de ocurrencia se da en la mayoría de circunstancias

- Dimensiones

Dimensiones de seguridad	
A	Autenticidad
C	Confidencialidad
I	Integridad
D	Disponibilidad
T	Trazabilidad

En la siguiente tabla se muestran los activos con las distintas dimensiones de seguridad e identificar el valor y la importancia de cada activo para la empresa en relación a esas dimensiones.

capa	activo	[D]	[I]	[C]	[A]	[T]
[S] Servicios						
	[S1] Servicio de Aplicaciones	**[7]**	**[7]**	**[7]**	**[7]**	**[7]**
	[S2] Servicio de Backup	**[7]**	**[6]**	**[5]**	**[7]**	**[6]**
	[S3] Servicio WEB	**[9]**	**[8]**	**[7]**	**[8]**	**[7]**
	[S4] Servicio Bases de Datos	**[8]**	**[9]**	**[7]**	**[8]**	**[7]**
	[S5] Servicio Pago	**[8]**	**[8]**	**[6]**	**[7]**	**[7]**
	[S6] Servicio criptográfico	**[8]**	**[8]**	**[8]**	**[8]**	**[8]**
	[S7] Comunicaciones	**[6]**	**[6]**	**[7]**	**[6]**	**[6]**
[I] Activos de información						
	[I01] Información	**[7]**	**[7]**	**[7]**	**[7]**	**[7]**
	[I02] Pagina web	**[9]**	**[9]**	**[8]**	**[8]**	**[8]**
	[I03] Pasarela	**[7]**	**[8]**	**[8]**	**[8]**	**[7]**
	[I04] Comunicaciones	**[5]**	**[6]**	**[5]**	**[5]**	**[5]**
	[I05] Bases de datos	**[7]**	**[7]**	**[7]**	**[7]**	**[7]**
[E] Equipamiento						
	[SW] Aplicaciones					
	[SW1] Administración Operación Servidores	**[7]**	**[7]**	**[7]**	**[7]**	**[7]**
	[SW2] Administración y gestión de aplicaciones	**[7]**	**[7]**	**[7]**	**[7]**	**[7]**
	[SW3] Administración y operación BBDD	**[7]**	**[7]**	**[7]**	**[7]**	**[7]**
	[SW4] Administración servicio dns	**[7]**	**[7]**	**[7]**	**[7]**	**[7]**
	[SW5] Administración WEB	**[6]**	**[7]**	**[6]**	**[6]**	**[7]**
	[COM] Comunicaciones					
	[COM1] red telefónica	**[6]**	**[6]**	**[6]**	**[6]**	**[6]**
	[COM2] Firewall	**[8]**	**[8]**	**[7]**	**[7]**	**[7]**
	[COM3] Router	**[8]**	**[7]**	**[8]**	**[8]**	**[8]**
	[COM4] Switch	**[7]**	**[7]**	**[8]**	**[8]**	**[7]**
	[COM5] Red de telecomunicaciones	**[8]**	**[8]**	**[8]**	**[8]**	**[8]**
	[HW] Equipos					
	[HW1] Servidor Ficheros	**[7]**	**[7]**	**[7]**	**[7]**	**[7]**
	[HW2] servidor Backup	**[6]**	**[9]**	**[6]**	**[6]**	**[6]**
	[HW3] Servidor web	**[9]**	**[9]**	**[9]**	**[9]**	**[9]**
	[HW4] Servidor de certificados	**[9]**	**[9]**	**[9]**	**[9]**	**[9]**
	[HW5] Servidor BBDD	**[8]**	**[8]**	**[8]**	**[8]**	**[8]**
	[HW6] Servidor de Correo	**[5]**	**[5]**	**[5]**	**[5]**	**[5]**
	[HW7] Servidor Firewall	**[5]**	**[5]**	**[5]**	**[5]**	**[5]**
	[HW8] Servidor Desarrollo	**[7]**	**[6]**	**[6]**	**[6]**	**[6]**
	[HW9] Servidor de Aplicaciones	**[7]**	**[6]**	**[6]**	**[6]**	**[6]**
	[HW10] Equipos PC empleados	**[4]**	**[4]**	**[4]**	**[3]**	**[3]**
	[HW11] Impresoras	**[0]**	**[0]**	**[0]**	**[0]**	**[0]**
	[HW12] SAN-Almacenamiento	**[8]**	**[8]**	**[7]**	**[7]**	**[8]**

	[HW13] Switch Central	[7]	[7]	[7]	[7]	[7]
	[HW14] Firewall	[7]	[8]	[7]	[8]	[7]
	[HW15] Switch genérico	[5]	[5]	[5]	[5]	[5]
	[HW16] Router	[5]	[5]	[5]	[5]	[5]
	[EQ] Equipamiento					
	[EQ1] SAI	[7]	[7]	[7]	[7]	[7]
	[EQ2] Generadores Principales	[8]	[8]	[8]	[8]	[8]
	[SF] Software					
	[SF1] Licencias Aplicaciones	[5]	[5]	[5]	[5]	[5]
	[SF2] Licencia Sistema Operativo	[5]	[5]	[5]	[5]	[5]
	[SF3] Licencia Bases de Datos	[5]	[5]	[5]	[5]	[5]
	[SF4] Licencia Antivirus	[5]	[5]	[5]	[4]	[5]
	[SF5] Licencia Correo	[5]	[5]	[5]	[5]	[5]
[L] Instalaciones						
	[L1] Centro de Proceso de Datos	[8]	[8]	[7]	[7]	[8]
[P] Personal						
	[P1] Responsable	[7]	[7]	[7]	[7]	[7]
	[P5] Empleados	[5]	[5]	[5]	[5]	[5]

3.3 Dependencia de activos

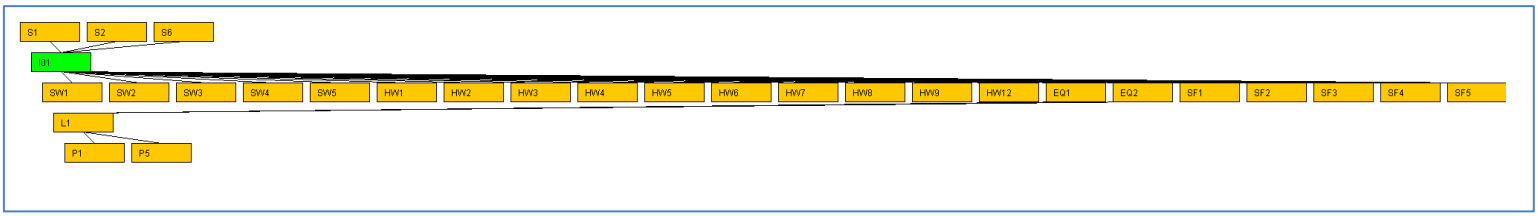

Ilustración 9 Dependecia del activo I01-Información

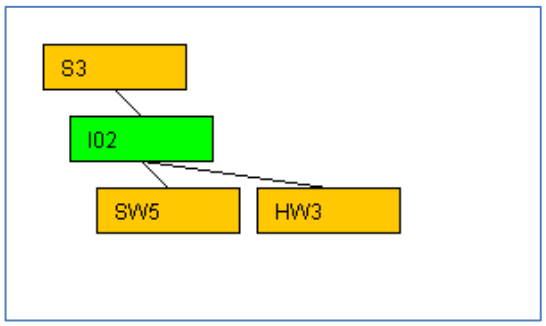

Ilustración 10 Dependecia Activo I02-Página Web

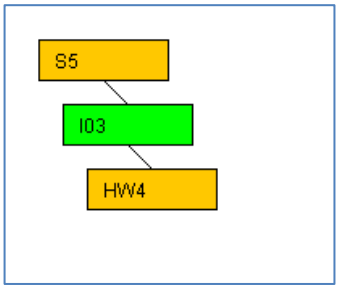

Ilustración 11 Dependencia - I03- Pasarela

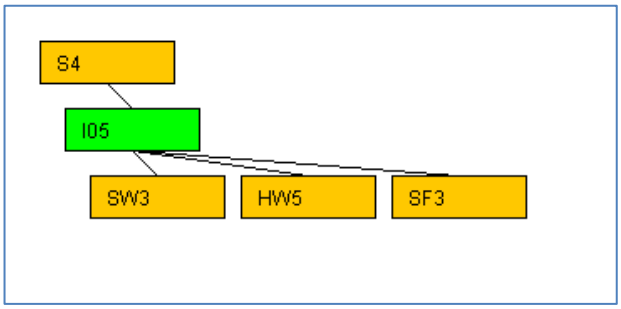

Ilustración 12 Dependencia - I04-Bases de datos

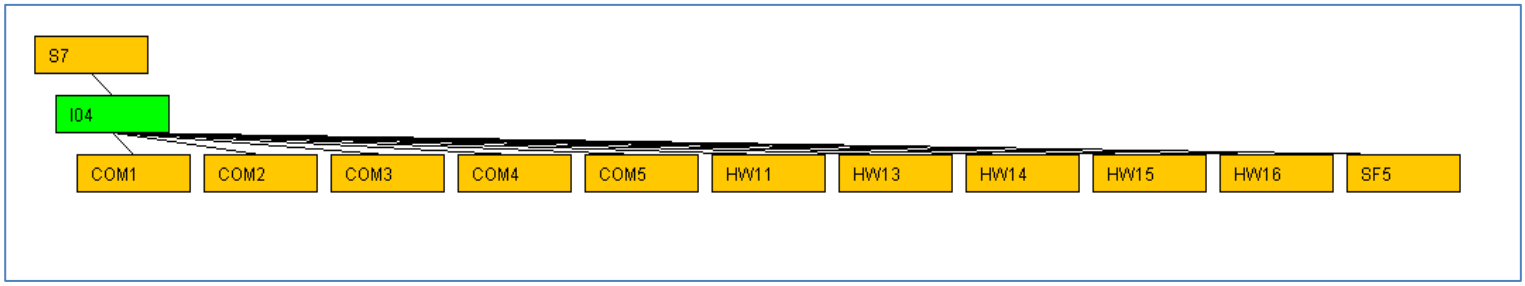

Ilustración 13 Dependencia - I05-Comunicaciones

3.4 Amenazas: Las amenazas a las que creemos que se podrán someter:

Desastres naturales	De origen industrial	Errores y fallos no intencionados	Errores y fallos no intencionados
[N.1] Fuego	[I.1] Fuego	[E.1] Errores de los usuarios	[A.3] Manipulación de los registros de actividad (log)
[N.2] Daños por agua	[I.2] Daños por agua	[E.2] Errores del administrador	[A.4] Manipulación de la configuración
	[I.3] Contaminación mecánica	[E.3] Errores de monitorización (log)	[A.5] Suplantación de la identidad del usuario
	[I.4] Contaminación electroma	[E.4] Errores de configuración	[A.6] Abuso de privilegios de acceso
	[I.5] Avería de origen físico o lo	[E.7] Deficiencias en la organización	[A.7] Uso no previsto
	[I.6] Corte del suministro eléct	[E.8] Difusión de software dañino	[A.8] Difusión de software dañino
	[I.7] Condiciones inadecuadas	[E.9] Errores de [re-]encaminamiento	[A.9] [Re-]encaminamiento de mensajes
	[I.8] Fallo de servicios de comu	[E.10] Errores de secuencia	[A.10] Alteración de secuencia
	[I.9] Interrupción de otros serv	[E.14] Escapes de información	[A.11] Acceso no autorizado
	[I.10] Degradación de los sopo	[E.15] Alteración accidental de la inf	[A.12] Análisis de tráfico
	[I.11] Emanaciones electromag	[E.18] Destrucción de información	[A.13] Repudio
		[E.19] Fugas de información	[A.14] Interceptación de información (escucha)
		[E.20] Vulnerabilidades de los progra	[A.15] Modificación deliberada de la información
		[E.21] Errores de mantenimiento / act	[A.18] Destrucción de información
		[E.23] Errores de mantenimiento / act	[A.19] Divulgación de información
		[E.24] Caída del sistema por agotamie	[A.22] Manipulación de programas
		[E.25] Pérdida de equipos	[A.23] Manipulación de los equipos
		[E.28] Indisponibilidad del personal	[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)

Ilustración 14. La relación completa en Anexo1

3.5. Riesgo

- Riesgo potencial: El riesgo del sistema sin aplicar ninguna salvaguarda
- Riesgo actual: Después del levantamiento de situación, este es el riesgo en el que nos encontramos.
- Riesgo Objetivo: El riesgo al que tenemos que tender.

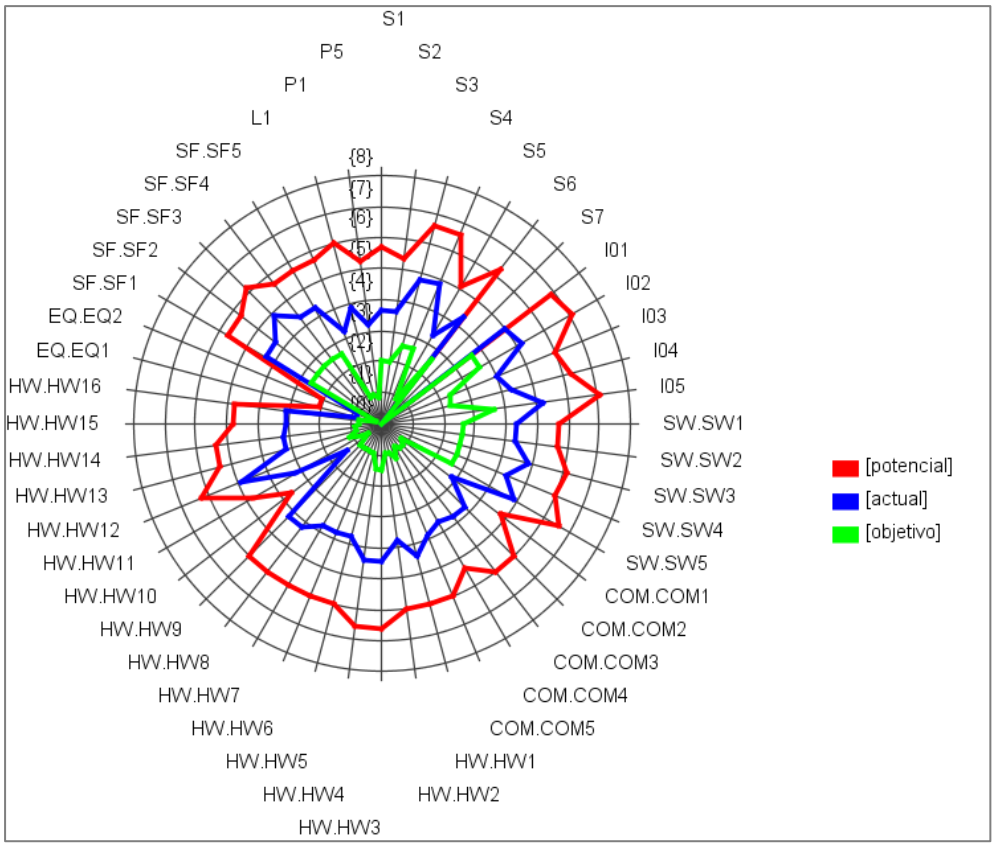

Ilustración 15 Valor-Activo Riesgo Acumulado

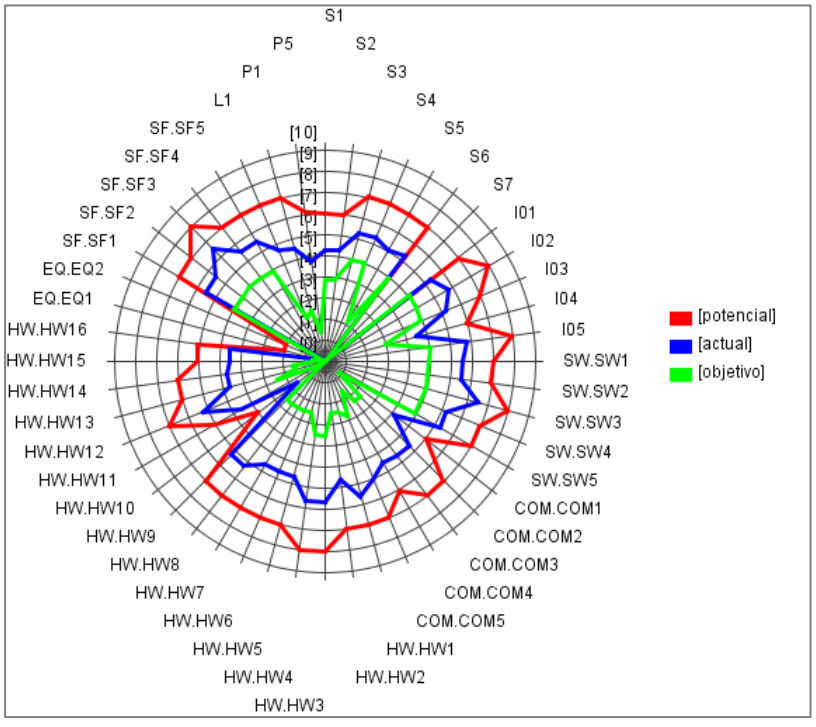

Ilustración 16 Impacto Acumulado por activo

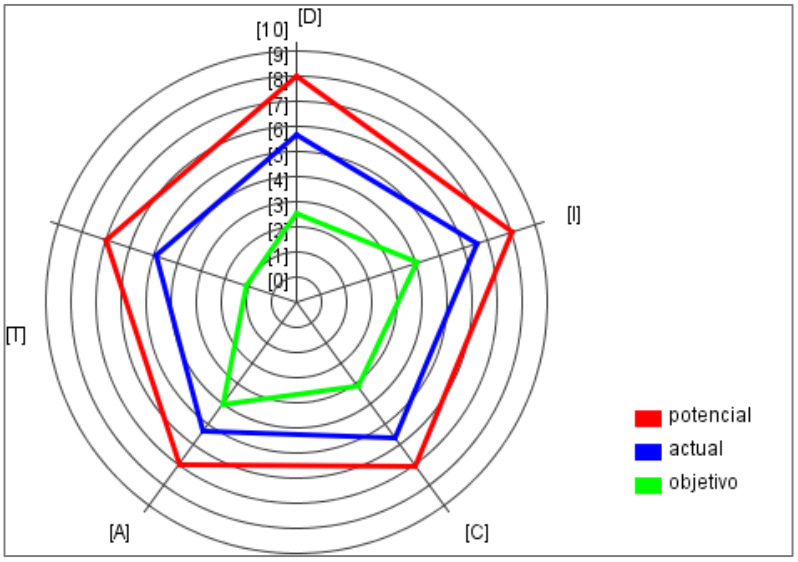

Ilustración 17 Impacto acumulado por dimensión

Así mismo, se adjunta el Riesgo acumulado potencial:

activo	[D]	[I]	[C]	[A]	[T]
[S] Servicios	{6,6}	{6,6}	{5,1}	{5,7}	{6,3}
[S1] Servicio de Aplicaciones	{5,4}	{5,4}	{4,5}	{5,1}	{5,7}
[S2] Servicio de Backup	{5,4}	{4,8}	{3,4}	{5,1}	{5,1}
[S3] Servicio WEB	{6,6}	{6,0}	{4,5}	{5,7}	{5,7}
[S4] Servicio Bases de Datos	{6,0}	{6,6}	{4,5}	{5,7}	{5,7}
[S5] Servicio Pago	{5,1}	{5,1}	{3,9}	{4,5}	{5,1}
[S6] Servicio criptografico	{6,0}	{6,0}	{5,1}	{5,7}	{6,3}
[I] Activos de información	{6,6}	{7,1}	{6,9}	{6,5}	
[I01] Informacion	{6,0}	{6,5}	{6,9}	{6,5}	
[I02] Pagina web	{6,6}	{7,1}	{6,9}	{6,5}	
[I03] Pasarela	{6,0}	{4,8}	{5,1}	{5,7}	
[I04] Comunicaciones	{4,8}	{5,4}	{6,3}	{5,4}	
[I05] Bases de datos	{6,0}	{7,1}	{6,3}	{6,5}	
[E] Equipamiento	{6,6}	{6,6}	{5,7}	{5,7}	{6,3}
[SW] Aplicaciones					
[SW.SW1] Administracion Operacion Servidores	{5,7}	{5,7}	{5,7}	{5,7}	
[SW.SW2] Administracion y gestion de aplicaciones	{5,7}	{5,7}	{5,7}	{5,7}	
[SW.SW3] Administracion y operacion BBDD	{5,7}	{6,2}	{5,7}	{5,7}	
[SW.SW4] Administracion servicio dns	{6,0}	{6,0}	{4,5}	{5,7}	{5,7}
[SW.SW5] Administracion WEB	{6,6}	{6,6}	{5,1}	{5,7}	{6,3}
[COM] Comunicaciones					
[COM.COM1] red telefonica	{4,8}	{3,2}	{4,5}	{4,5}	
[COM.COM2] Firewall	{6,0}	{4,4}	{4,5}		

[COM.COM3] Router	{6,0}	{3,8}	{5,1}		
[COM.COM4] Switch	{5,4}	{3,8}	{5,1}		
[COM.COM5] Red de telecomunicaciones	{6,0}	{4,4}	{5,1}	{5,7}	
[HW] Equipos					
[HW.HW1] Servidor Ficheros	{6,0}	{5,7}	{5,7}		
[HW.HW2] servidor Backup	{6,0}	{5,0}	{5,1}		
[HW.HW3] Servidor web	{6,6}	{5,0}	{5,7}		
[HW.HW4] Servidor de certificados	{6,6}	{5,0}	{5,7}		
[HW.HW5] Servidor BBDD	{6,0}	{5,0}	{5,1}		
[HW.HW6] Servidor de Correo	{6,0}	{4,4}	{5,1}		
[HW.HW7] Servidor Firewall	{6,0}	{4,4}	{5,1}		
[HW.HW8] Servidor Desarrollo	{6,0}	{4,4}	{5,7}		
[HW.HW9] Servidor de Aplicaciones	{6,0}	{4,4}	{5,7}		
[HW.HW10] Equipos PC empleados	{3,7}	{2,1}	{2,8}		
[HW.HW11] Impresoras	{4,8}	{3,2}	{4,5}		
[HW.HW12] SAN-Almacenamiento	{6,0}	{6,3}	{5,7}		
[HW.HW13] Switch Central	{5,4}	{3,8}	{4,5}		
[HW.HW14] Firewall	{5,4}	{4,4}	{4,5}		
[HW.HW15] Switch generico	{4,8}	{3,2}	{4,5}		
[HW.HW16] Router	{4,8}	{3,2}	{4,5}		
[EQ] Equipamiento					
[EQ.EQ1] SAI	{2,1}				
[EQ.EQ2] Generadores Principales	{2,1}				
[SF] Software					
[SF.SF1] Licencias Aplicaciones	{5,7}	{5,7}	{5,7}	{5,7}	
[SF.SF2] Licencia Sistema Operativo	{5,7}	{5,7}	{5,7}	{5,7}	
[SF.SF3] Licencia Bases de Datos	{5,7}	{6,2}	{5,7}	{5,7}	
[SF.SF4] Licencia Antivirus	{5,7}	{5,7}	{5,7}	{5,7}	
[SF.SF5] Licencia Correo	{5,7}	{5,7}	{5,7}	{5,7}	
[L] Instalaciones	{5,7}	{4,5}	{5,7}		
[L1] Centro de Proceso de Datos	{5,7}	{4,5}	{5,7}		
[P] Personal	{5,1}	{5,6}	{6,0}		
[P1] Responsable	{5,1}	{5,6}	{6,0}		
[P5] Empleados	{4,9}	{5,1}	{5,3}		

3.6 Resultados

Mediante el análisis de amenazas observamos que las que genera más impacto en nuestros activos son aquellas que afectan a todos los servidores, lo que implica tomar las medidas pertinentes del caso con el fin de mitigar el riesgo, por lo que los proyectos estarán enfocados en esa dirección.

4. PROPUESTA DE PROYECTOS

4.1 Introducción

Una vez realizado el análisis de riesgos, se han identificado los activos que están afectados por un riesgo mayor del que la organización ha asumido y por otro lado se han identificado las principales amenazas que pueden impactar en cada activo. Asimismo, en la declaración de aplicabilidad se definirán todos los controles que son de aplicación y por tanto es necesario elaborar los procedimientos respecto a cómo se van gestionar e implantar dichos controles.

Por tanto, es necesario por un lado elaborar los procedimientos orientado a implantar y gestionar los controles y por otro lado, realizar una serie de proyectos o planes de tratamiento de riesgos sobre los activos identificados que tienen un riesgo mayor que el aceptable.

4.2 Propuestas

4.2.1 Proyecto1: Puesta en marcha un sistema de defensa

- Objetivo: Mantener a salvo la integridad de la información y del software para evitar inyección de código malicioso o destrucción de la misma. En esta fase del proyecto el responsable del mismo llevara a cabo la adquisición del hardware y software necesario para la implantación de las nuevas mejoras.
- Alcance:
    - Servidores
    - DNS
    - Firewall
    - BBDD
    - Gestor de Correo
    - CPD

- Salvaguardas: Implantación de sistemas de monitorización y de alertas (física y lógica):
    - Adquisición de certificado de empresa de sellado electrónico
    - Aseguramiento de disponibilidad
    - IDS/IPS: Adquisición de hardware especifico
    - Implantación de software para la detección de vulnerabilidades. Al ser software libre no tiene sobre coste. Nessus, Snort y Satan son las elegidas.
    - Adquisición de un Pravail de Arbor Networks para mitigación de DDoS y monitorización de tráfico.

- Detalle: El objetivo de este proyecto no es otro que el crear una serie de controles que disminuyan el ratio de errores para mejorar la respuesta por una denegación de servicio o una mala gestión de la red.
- Impacto: Mejora de la reputación y protección de datos críticos.
- Tiempo estimado: 6 meses
- Costes: El presupuesto general para la puesta en marcha del proyecto será de 20.000€ para pagar los distintos dispositivos a adquirir y el sueldo de los técnicos externos.

4.2.2 Proyecto2: Implantación de salvaguardas imprescindibles

- Objetivo: El análisis de riesgos ha arrojado como resultado que la implantación de una serie de salvaguardas mejoraría sustancialmente los resultados bajando el nivel de riesgo a un nivel medio para la organización. La implantación de estas salvaguardas se considera imprescindible a tenor de los resultados del análisis de riesgos. Estas salvaguardas son las siguientes:

- Alcance:
    - Servidores
    - DNS
    - Firewall
    - BBDD
    - Gestor de Correo
    - CPD

- Salvaguardas: Implantación de sistemas de monitorización y de alertas (física y lógica)
- Detalle: El objetivo de este proyecto no es otro que el crear una serie de controles que disminuyan el ratio de errores para mejorar la respuesta por una denegación de servicio o una mala gestión de la red.
- Impacto: Mejora de la reputación y protección de datos críticos.
- Tiempo estimado: 6 meses
- Costes: El presupuesto para la puesta en marcha del proyecto será de 20.000€.

4.2.3 Proyecto3: Creación del Comité de Seguridad de los Sistemas de Información.

- Objetivo: Se creara el Comité de Seguridad de los Sistemas de Información como órgano adscrito al Comité de Dirección.

- Funciones:

    - Aprobar la Política General de Seguridad de la Información.
    - Revisar el modelo de seguridad de la información por lo menos una (1) vez al año y solicitar los ajustes necesarios.
    - Velar por la divulgación y actualización del modelo de seguridad de la información, incluyendo las Políticas definidas.
    - Proveer de forma razonable los recursos necesarios para implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información.
    - Analizar y establecer acciones frente a incumplimientos de las políticas definidas.

- Composición: El CSISS estará compuesto por los siguientes miembros:

    1. Presidente: El Secretario de Estado de la Seguridad Social o persona que le sustituya.

    2. Vocales: un representante designado por los titulares de cada uno de los siguientes órganos:

        a) Gabinete de la Secretaría.

b) Dirección General.

c) Intervención General.

e) Tesorería General.

g) Servicio Jurídico.

h) Gerencia de Informática.

Estos vocales deberán tener rango de subdirector general o asimilado, entendiéndose también por tales quienes ejerzan competencias en materia de seguridad de los sistemas de información en los órganos anteriores.

3. Secretaría: Con voz y sin voto, será designada por la Gerencia de Informática.

- Funcionamiento:

  - El CSISS se reunirá con carácter ordinario como mínimo tres veces al año o, con carácter extraordinario, cuando el Presidente lo considere necesario.
  - En caso de ser necesario, y por invitación del Presidente del CSISS, podrán asistir en calidad de asesores, con voz pero sin voto, las personas que se estimen convenientes.

5. AUDITORÍA DE CUMPLIMIENTO

5.1 Introducción

Llegados a esta fase, es el momento de evaluar el cumplimiento de la empresa respecto a los controles definidos por la norma ISO/IEC 27001:2013 y determinar cuáles controles serán implementados y cuáles no con el fin de mejorar la seguridad en la Entidad.

5.2 Plan de auditoria

Datos del Servicios Objeto de la Auditoría

RESPONSABLE DE SPAIN DEAL: Jaimito Doroteo Fernandez
DIRECCIÓN DEL CENTRO A AUDITAR: CL Alfonso X el Sabio 55 - 28080 - Madrid

Datos del Equipo Auditor

RESPONSABLE DE SEGURIDAD TIC

Federico Julian - FJ
AUDITOR/ES REVISIÓN TÉCNICA

Francisco Garrido – FG
Sergio Soria – SS
Patricio Tomas – PT
Julian Monago – JM
Javier Lemona – JL
Manuel Cebrian – MC
AUDITORES REVISIÓN NORMATIVA

Eloisa Federico – EF
Enrique Rubio– ER
Celia Baile – CB
Alejandro Rodríguez – AR
Isabel González - IG

PERSONA DE CONTACTO: Roberto.perez.gutierrez@spaindeal.com

DIRECCIÓN DE CONTACTO: Departamento de Informática y Comunicaciones de SpainDeal.

Alcance del Sistema y la Auditoría

El alcance de la auditoría queda acotado al siguiente ámbito:
"Los sistemas y redes que dan soporte la sección técnica"
La reunión inicial y preparación de la auditoría se ha realizado el día 19 de Noviembre de 2014.
El trabajo de campo será realizado tanto en las instalaciones de SpainDeal como en el propio Departamento de Informática y Comunicaciones comenzando el día 2 de Diciembre de 2014. Posteriormente, los informes de auditoría se entregarán en la reunión final, junto con las evidencias que respalden las conclusiones alcanzadas.

Id	Modo de tarea	Nombre de tarea
1		**Auditoria Global Comisarías**
2		Presentación Auditoría Global
3		**Auditoría ISO 27002**
4		Identificación de Responsables
5		Establecer Agenda
6		Realizar Sesiones de Trabajo
7		Análisis y Realización Informe de Resultado
8		Registro y Gestión de las No Conformidades
9		**Análisis de Vulnerabilidades**
10		Identificación Responsable
11		Identificación del Ámbito de Trabajo
12		**Análisis del Ámbito**
13		Servidores
14		Dispositivos de Red
15		Equipos Cliente
16		Realización Informe de Resultados
17		Registro y Gestión de las Vulnerabilidades
18		**Realización Informe Ejecutivo**
19		**Entrega Informe ISO27002 - Análisis de Vulnerabilidades**
20		**Presentación Informe Ejecutivo**

Contenido de la Revisión

Ejecución de la Auditoría

La ejecución de la auditoría es el trabajo in-situ de la auditoría y seguirá los pasos acordados en las reuniones de planificación, atendiendo a unos objetivos básicos. En definitiva, estos objetivos serán:

- Determinar el grado de adecuación a la ISO/IEC 27002:2013.
- Identificar cualquier deficiencia, no conformidad o desviación, comprobando la aplicación de las acciones correctoras y preventivas apropiadas.
- Identificación y explotación de las vulnerabilidades técnicas sobre los sistemas.

Se auditarán con el detalle necesario las partes del sistema que previamente se hayan seleccionado, teniendo en cuenta que la planificación realizada no debe restringir el análisis de aquellos aspectos que durante la ejecución de la auditoría se revelen problemáticos o de esencial importancia. La auditoría se realizará por medio de la supervisión, inspección y revisión de las actuaciones del área auditada correspondiente y de su documentación.

Se deberá facilitar al equipo auditor el acceso a las áreas a auditar, así como a la documentación disponible que precise para el correcto desarrollo de la auditoría y la fundamentación de sus conclusiones. Así mismo para la auditoría técnica se necesitará conocer los rangos de red sobre los cuales se realizará el análisis de vulnerabilidades y la explotación de las mismas, siendo necesario ventanas de tiempo para realizar dicha auditoria. Así mismo se facilitará la dirección o direcciones IP desde se realizarán los test de intrusión.
Se detallan en los dos siguiente apartados los puntos de control que se verificarán referidos a norma UNE-ISO/IEC 27002:2013

Revisión de las Redes y Sistemas

En líneas generales, los sistemas a auditar son los siguientes:

- DESARROLLO
- SOPORTE
- MANTENIMIENTO
- SISTEMAS

Sistema	Procedimiento de verificación	Auditor
MANTENIMIENTO	Seguridad física: Puntos de acceso, personal administrador, registros de entrada, de cambios de puntos de acceso, necesidades de cobertura. Seguridad lógica: Configuración puntos de acceso, revisión logs, arquitectura, dispositivos WIFI no autorizados u ocultos, análisis del tráfico de red, portal cautivo.	FG/SS/PT/JM/JL/MC
DESARROLLO **SOPORTE** **SISTEMAS**	Seguridad física: Servidores, electrónica de red: switches, routers, puntos de acceso, cableado, cuartos técnicos, armarios, etc. Seguridad lógica: Descubrimiento de activos, descubrimiento de elementos de seguridad a nivel de red (firewalls, IDS/IPS, etc.), descubrimiento de servicios/puertos por cada activo, descubrimiento de vulnerabilidades (con posibilidad de explotación), bastionamiento equipos clientes.	FG/SS/PT/JM/JL/MC

SpainDeal debe facilitar:

- Rangos de red utilizados.
- Arquitectura lógica (subredes, vlanes, conexiones).
- Relación de activos (máquinas) y sus funciones.

Revisión de la norma UNE-ISO/IEC 27002:2013

En líneas generales, las verificaciones a realizar y los miembros del equipo auditor participantes son las siguientes:

Capítulo de la norma UNE-ISO/IEC 27002	Procedimiento de verificación	Auditor
5. POLÍTICA DE SEGURIDAD	Comprobar la existencia de una política de seguridad que cumpla con las exigencias definidas en el estándar ISO 27002. Así como que se encuentre aprobada por la dirección y las revisiones correspondientes.	EF/ER/CB/AR/IG
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Comprobar que hay establecida una estructura de gestión para iniciar y controlar la seguridad de la información que cumpla con los puntos de control de este capítulo de la ISO 27002.	EF/ER/CB/AR/IG

Capítulo de la norma UNE-ISO/IEC 27002	Procedimiento de verificación	Auditor
7. SEGURIDAD RELACIONADA CON LOS RECURSOS HUMANOS	Comprobar la seguridad ligada al personal observando la definición del trabajo y los recursos, la formación a los usuarios y la gestión de las incidencias y malos funcionamientos de seguridad.	EF/ER/ CB/AR/I G
8. GESTIÓN DE ACTIVOS	Observar si se mantiene una protección adecuada sobre los activos de la Organización y asegurar un nivel de protección adecuado a los activos de información.	EF/ER/ CB/AR/I G
9. CONTROL DE ACCESO	Comprobar si existen controles de acceso a la información como uso de contraseñas, privilegios, control del acceso remoto,…	EF/ER/ CB/AR/I G
10. SEGURIDAD FISICA Y DEL ENTORNO	Se comprobará la gestión de los recursos de comunicaciones y operaciones.	EF/ER/ CB/AR/I G
11. SEGURIDAD FÍSICA Y DEL ENTORNO	Se deben comprobar el cumplimiento de los puntos de control sobre seguridad física comprobando que existen áreas seguras, seguridad en los equipos y controles generales.	EF/ER/ CB/AR/I G
12. SEGURIDAD DE LAS OPERACIONES	Se comprobara la gestión de las operaciones.	EF/ER/ CB/AR/I G
13. SEGURIDAD DE LAS COMUNICACIONES	Se comprobara la gestión y la seguridad de las comunicaciones.	EF/ER/ CB/AR/I G
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	. Se deben comprobar que se realiza el mantenimiento y el desarrollo de los sistemas según los puntos de control del capítulo	EF/ER/ CB/AR/I G
15. CONFORMIDAD	Se comprobará si se cumplen las leyes civiles o penales, requisitos reglamentarios de seguridad u obligaciones contractuales.	EF/ER/ CB/AR/I G
16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Se comprobará el cumplimiento de los puntos de control descritos para la gestión de incidencias.	EF/ER/ CB/AR/I G
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	Se comprobarán si se cumplen los puntos de control asociados a este capítulo de la ISO 27002 sobre la interrupción de actividades del negocio y la protección de los procesos críticos frente a grandes fallos o desastres	EF/ER/ CB/AR/I G
18. CUMPLIMIENTO	Se comprobará si se cumplen las normativas vigentes.	EF/ER/ CB/AR/I G

Disposiciones sobre la confidencialidad

1) Toda la documentación que se emplee o se genere durante la auditoría, tiene carácter confidencial, no pudiendo transcribirse a terceros o reproducirse sin permiso expreso de SpainDeal.
2) La reunión final tiene por objeto dar lectura al informe de auditoría donde se reflejan los resultados de la auditoría.
3) El equipo auditor debe disponer de una sala o similar donde realizar las reuniones internas.
4) En caso de recusación de auditores rogamos nos lo comuniquen con la mayor brevedad posible.

5.3 Metodología

La metodología utilizada para el análisis del sistema de gestión de seguridad de la información o SGSI corresponde al Modelo de Madurez de la Capacidad CMM en el que se utiliza una escala 0% al 100%, en donde el 100%corresponde a la optimización de los procesos.

EFECTIVIDAD	SIGNIFICADO	CMM	DESCRIPCIÓN
0%	Inexistente	**0**	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	Inicial / Ad-hoc	**L1**	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	Reproducible, pero intuitivo	**L2**	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	Proceso definido	**L3**	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	Gestionado y medible	**L4**	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	Optimizado	**L5**	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

5.4 Evaluación de la madurez

A traves de los analisis realizados y las gráficas obtenidas, vemos como excepto en las politicas de seguridad, el resto falta un empujon para llegar al nivel deseado y habria que seguir trabajando por llegar al nivel aceptable por la organización.

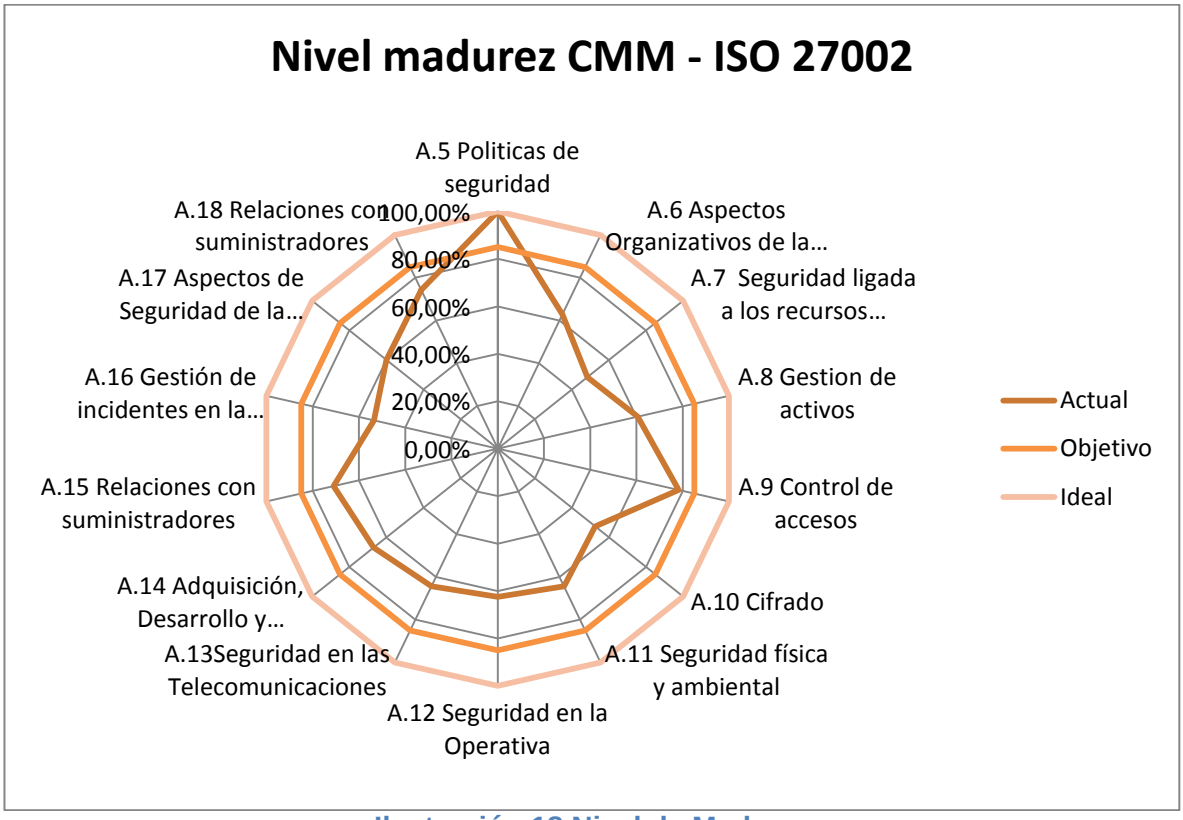

Ilustración 18 Nivel de Madurez

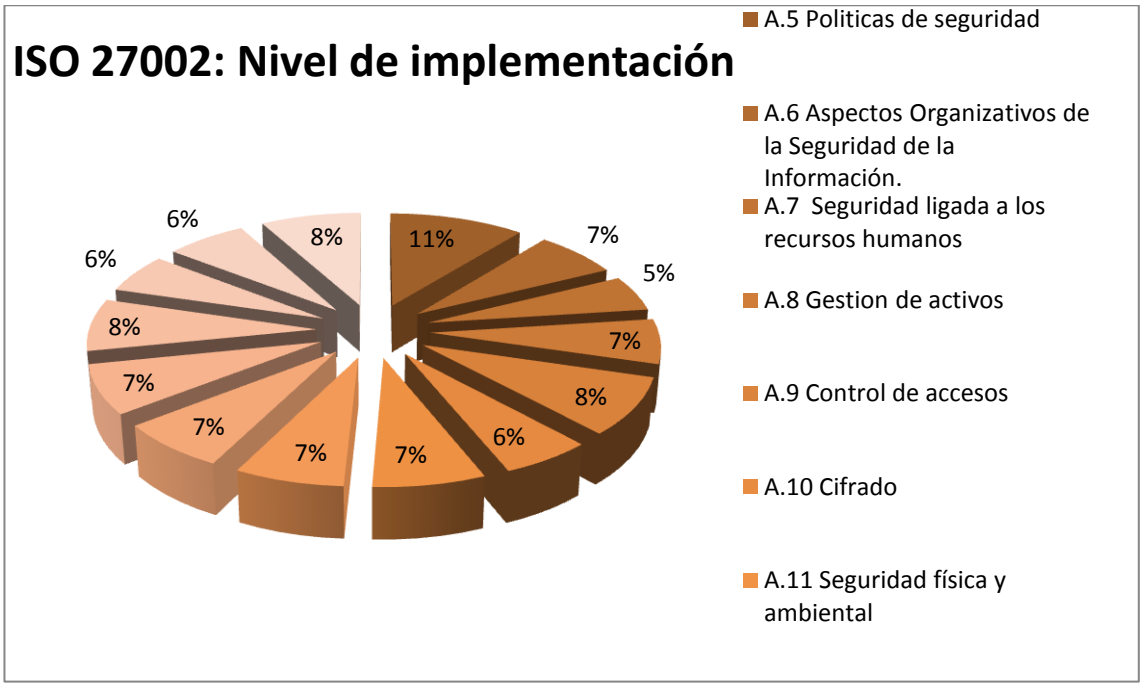

Ilustración 19 Nivel de implementación

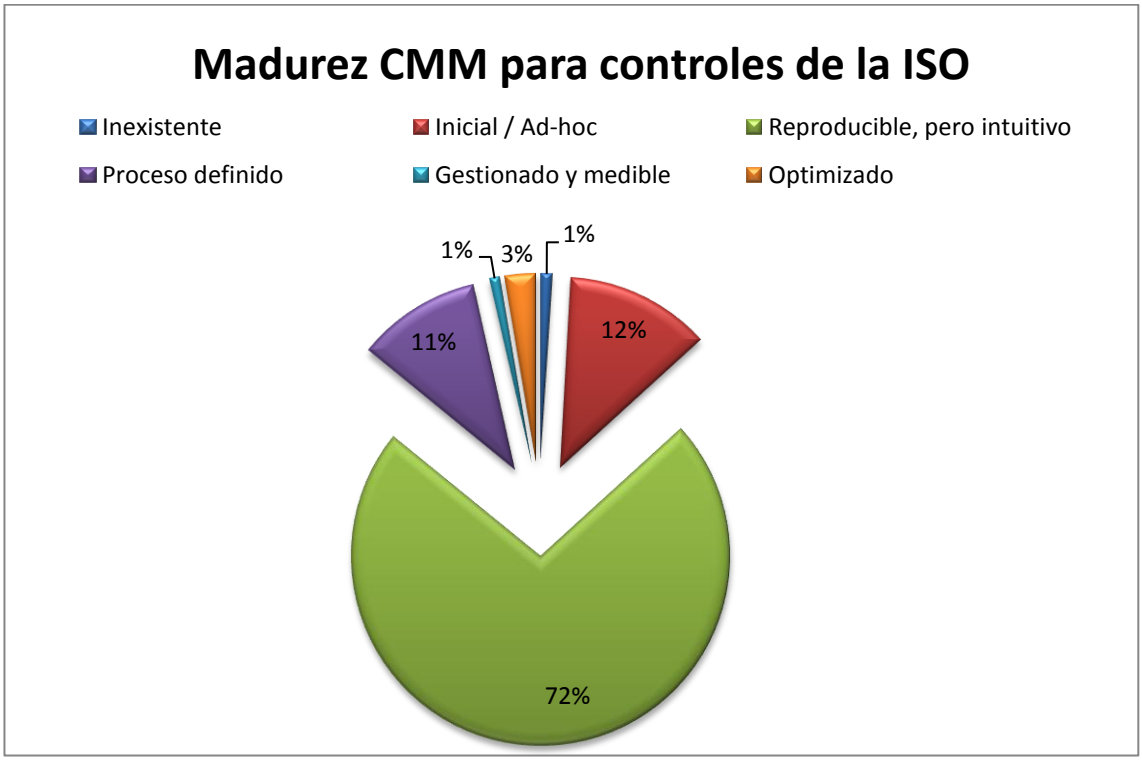

Ilustración 20. Controles

Conclusiones: La organización requiere implementar mayor número de controles y mejorar la eficacia de los existentes con jornadas de sensibilización y divulgación de directrices en seguridad de la información.

Hay que mejorar en en aspecto humano como factor determinante a la hora de securizar la información y mejorar desde la fase de contratación, hasta la formación continuada ya que los controles y procesos manejados por la organización deben ser conocidos por todos los empleados de la organización. Es importante concientizar que la seguridad de la información es responsabilidad de todos.

En lo relativo a la política de seguridad de la información, la empresa dispone de ella y por lo tanto es un factor fundamental para trabajar desde una buena base y con cimientos asentados.

5.5 Informe de auditoria

Nº EXPEDIENTE: 2014/0001/SI/01 NORMA DE APLICACIÓN: ISO/IEC 27001:2013	Nº INFORME: 01 TIPO DE AUDITORÍA: 1ª Seguimiento ISO/IEC 27001:2013

Fecha de realización de la Auditoría: 2014-11-24 y 25

DATOS GENERALES

A. DATOS DE LA ORGANIZACIÓN

Nombre de la Organización	SPAINDEAL
Dirección	CL Alfonso X el Sabio 55 - 28080 - Madrid
Representante de la Organización (nombre y cargo)	D. Eugenio Pérez Gutiérrez (Jefe del Servicio de Seguridad TIC y Gerente Técnico de SpainDeal)

B.EQUIPO AUDITOR

Función	Nombre	Iniciales
AUDITOR JEFE	Alejandro Rodríguez Pubill	ARP

C. MODIFICACIONES SOBRE EL ALCANCE DE LA CERTIFICACIÓN, SI PROCEDE

Se solicita la implantación de la norma de referencia del sistema de gestión de seguridad de la información de la UNE-ISO/IEC 27001:2013.

D. OBJETIVOS DE LA AUDITORÍA

Los objetivos de la auditoría son: determinar la conformidad del sistema de gestión de la organización / empresa auditada con los criterios de auditoría, evaluar su capacidad para

cumplir con los requisitos legales, reglamentarios y contractuales aplicables, así como evaluar su eficacia para cumplir los objetivos especificados y cuando corresponda, identificar posibles áreas de mejora. CUMPLIDOS
Ver apartado de Resumen Ejecutivo de la Auditoría

RESUMEN EJECUTIVO DE AUDITORÍA

Se ha realizado la 1ª auditoría de seguimiento y adaptación Sistema de Gestión de Seguridad de la Información (SGSI), para las actividades reflejadas en la Hoja de Datos y referenciadas en el Plan de Visita y de acuerdo a requisitos de la norma de referencia: ISO/IEC 27001:2013.

De forma general, el Sistema de Gestión de Seguridad de la Información se encuentra correctamente implantado, es coherente con la Política y Objetivos de Seguridad, se adapta a la situación actual de la organización y permite la identificación de oportunidades de mejora, concluyéndose que el Sistema continúa respondiendo de forma satisfactoria a los requisitos de certificación.

Con fecha junio de 2014 se realiza la revisión por la Dirección que contempla todos los elementos de entrada y de salida citados en la norma de referencia, considerándose adecuada, si bien se deberá reforzar el análisis de alguno de los datos de entrada.

Se ha verificado la elaboración de un plan anual de auditorías internas en el que se recogen tanto auditorías a los procesos del sistema como auditorías a los controles. Se revisa el programa y el informe comprobando el tratamiento de las no conformidades y la apertura de las acciones correctivas asociadas.

Para el Análisis de Riesgos se utiliza la metodología MAGERIT y la herramienta EAR. El último análisis de riesgos es de fecha 08-04-2.014 y la selección de controles para las pruebas de cumplimiento se ha realizado tomando como base la declaración de aplicabilidad.

En la revisión han participado las funciones y roles descritos en el ANEXO III de este informe

Cambios significativos del sistema con respecto a la anterior visita:

Además del ya mencionado cambio de norma de referencia a la ISO/IEC 27001:2013, los cambios más significativos del sistema son:

- Se ha procedido al nombramiento de un nuevo Responsable del Sistema de Gestión de Seguridad de la Información
- Utilización de SharePoint para el control de la documentación y para la automatización de procesos
- Ampliación del proyecto Symantec incluyendo VM, LCP y escaneo de dispositivos extraíbles
- Inclusión del CriticalSystemProtection, DLP, etc.

Conclusiones sobre el cumplimiento de los objetivos de la auditoría y la eficacia del sistema de gestión.

Se ha comprobado que el sistema de gestión de seguridad de la información es adecuado a las necesidades de su negocio, cumpliendo las especificaciones de la norma de referencia salvo para lo reflejado en el presente informe como no conformidad y/u observación. Se han detectado 4 no conformidades todas ellas menores para las que la Organización deberá establecer el correspondiente plan de acciones correctivas (PAC).

También se recomienda el tratamiento y gestión de las observaciones reflejadas en el presente informe, con el fin de evitar posibles incumplimientos en el futuro.

Para la adecuación Sistema de Gestión de Seguridad de la Información respecto a los requisitos especificados en la norma de referencia ISO/IEC 27001:2013 será necesario realizar un plan de transición tal y como queda reflejado en la no conformidad identificada al respecto en este informe (NC-01).

Puntos fuertes:

1. Creación del Comité de Seguridad realizando reuniones mensuales en las que está presente la dirección
2. Profesionalidad y esfuerzo del personal con responsabilidades asignadas en el sistema
3. Se tiene perfectamente documentado la Política de Seguridad y el Manual de Seguridad, sin duda, un pilar básico para el buen funcionamiento de un SGSI.

Oportunidades de mejora:

1. Incluir el grado de madurez en la implantación de los controles (SoA).
2. Es necesario mejorar la formación y Concienciación en materia de Seguridad de la Información. A través del conocimiento se puede dar respuesta a las amenazas que afecta a la información que maneja el personal de SpainDeal.
3. Se está realizando teletrabajo, y su política de uso está en proceso de implantación. Debería hacerse en el menor tiempo posible, ya que actualmente se deja a criterio del empleado las medidas de seguridad en lo relativo a este punto.

Observaciones:

1. Puntualmente se detecta algún activo software no incluido en el inventario de activos.
2. Se deberá potenciar el análisis de los costes de los incidentes de seguridad.
3. Se deberá reforzar el análisis de alguno de los datos de entrada al proceso de revisión por la dirección.
4. Se deberá mejorar la trazabilidad entre activo, control y acciones del plan de tratamiento del riesgo.
5. Se detecta un indicador para el que no se cumplen los valores de referencia sin que se pueda verificar el establecimiento formal de acciones correctivas.
6. La Organización se deberá asegurar de que se haya definido, al menos, un indicador por dominio de control del Anexo A de la norma de referencia.
7. Se deberá reforzar la política de copia de seguridad para elementos de configuraciones del networking.
8. Se deberán identificar de forma clara los RTO y RPO de las actividades críticas que luego aplicarán a los procesos de continuidad del negocio.

9. Se deberá revisar la sistemática de recogida de incidentes de seguridad para asegurar que aquellos relativos a informes de seguimiento de servicio por parte de terceros llegan a Seguridad de la Información a efectos de análisis.

Listado de documentos del SGC
Se adjuntan al presente informe los siguientes documentos:

Obligatorios en todos los Sistemas:
☐ Matriz de actividades de auditoría.
☒ Listado de emplazamientos fijos y/o temporales
☒ Listado de participantes
☒ Hoja de Datos (no procede en GFS)
☒ Listado de documentos en vigor

No Obligatorios en todos los Sistemas:
☐ Listado de legislación aplicable
☐ Listado de proyectos (obligatorio en I+D+i)
☐ Listado de proyectos obras y/o servicios (en 9001/14001)
☐ Resumen requisitos verificación medioambiental (EMAS)
☐ Otros:

SGSI:
- No se adjuntan los documentos de Organigrama, diagrama de red y Declaración de Aplicabilidad (SOA), al ser considerado como CONFIDENCIAL por SpainDeal.

CUADRO DE NO CONFORMIDADES Y OBSERVACIONES

Ref. N. C.	DESCRIPCIÓN DE LA NO CONFORMIDAD U OBSERVACIÓN	Apdo. Norma ISO/IEC 27001:2013	Categoría N. C.
NC-01	A fecha de la presente auditoría no se ha completado en su totalidad la adaptación al estándar ISO/IEC 27001:2013	6	menor
NC-02	No se ha podido verificar el cumplimiento de cualificación del auditor interno de la Organización. Así mismo, se deberán concretar los requisitos de cualificación al ser muy generales.	9	menor
NC-03	Respecto a la implementación y operación del SGSI: a) Se detectan elementos aislantes, paneles, etc en la ubicación (planta 0) de los routers de conexión con los operadores. b) Se detecta una actualización legislativa (Ley 9/2.014) que no está recogida en el listado de legislación aplicable al sistema	8	menor
NC-04	El proceso implementado de acciones correctivas no distingue entre tratamiento de la no conformidad y acción correctiva orientada al análisis de las causas de la no conformidad.	10	menor

Ref. N. C.	DESCRIPCIÓN DE LA NO CONFORMIDAD U OBSERVACIÓN	Apdo. Norma ISO/IEC 27001:2013	Categoría N. C.
NC-05	No se dispone de una política de uso de dispositivos para movilidad, habiendo dispositivos usándose actualmente. Pero se está en proceso de su publicación.	6.2.1	Mayor
NC-06	No existe un bastionado de equipos	11	Menor
NC-07	Gestión de Cambios. No existe como tal, los cambios se hacen directamente en producción. En ningún caso se documentan los cambios realizados. No se realiza ningún tipo de evaluación de impacto sobre los cambios realizados en los sistemas de información. Tampoco se hacen pruebas de regresión.	12.1.2	Mayor
NC-08	Respecto a la selección de personal, no siempre se realizan las mismas verificaciones respecto a los antecedentes, experiencia, referencias sobre el personal que presta los servicios a SpainDeal. Tampoco se realizan revisiones más detalladas del personas que va a tener acceso a sistemas de información especialmente sensibles.	7	Observación

Nota 1: Para todas las NC descritas en esta tabla, será necesario que la Organización establezca y documente las acciones correctivas pertinentes.

Nota 2: Aunque puedan existir apartados / subapartados que se auditen conjuntamente (cuando así lo indique la Matriz de Actividades), las NC se asignarán al subapartado específico en el que se detectan.

EL REPRESENTANTE DE LA ORGANIZACIÓN **EL EQUIPO AUDITOR**

DISPOSICIONES FINALES

1. Las observaciones y no conformidades han sido aclaradas y entendidas.

2. Teniendo en cuenta las no conformidades indicadas en este informe, si fuese necesaria la presentación del Plan de Acciones Correctivas, la Organización se compromete a enviarlo al departamento de auditorías en 30 días naturales a partir de la fecha de emisión del informe de auditoría, con la información requerida por la *Guía para la elaboración del plan de acciones correctivas.*

3. Indicar las no conformidades del presente informe a las cuales la organización tiene intención de presentar apelación. En este caso, la organización deberá enviar al departamento de auditorias la justificación y evidencias documentales necesarias para su valoración por los servicios del departamento de auditorias.

4.El equipo auditor informa que esta auditoría se ha realizado a través de un muestreo por lo que pueden existir otras no conformidades no identificadas en este informe.

5.Durante la auditoría se ha comprobado el uso de la marca correspondiente a la/s Norma/s auditada/s, identificándose en el presente informe cualquier desviación que pudiera haberse detectado al respecto.

6. Las no conformidades pueden referirse a incumplimientos de los requisitos de la norma de referencia aplicable, o de cualquier otro requisito establecido en el Sistema de Gestión de la Organización.

7. Se acuerda con la Organización, las siguientes fechas para la realización de la próxima auditoría:

Fecha próxima auditoría: **AS2**	Junio de 2015
Fecha expiración del actual certificado (2014/0001/SI/01):	**2016-07-22**

8. Comentarios si procede, sobre la planificación de la próxima auditoría (a cumplimentar por el Auditor Jefe):N/A

9. Con antelación a la realización de la próxima auditoría, se determinarán en el Plan de Auditoría los centros a visitar y la planificación de actividades prevista.

En Madrid, a 25 de junio de 2.014

El Representante de la Organización **El Equipo Auditor**

ANEXO CENTROS VISITADOS

DIRECCIONES CENTROS AUDITADOS (Detallar la dirección de los centros indicados en la Matriz de Actividades)
CENTRO A: Spain Deal CL Alfonso X el Sabio 55 - 28080 - Madrid

ANEXO RELACIÓN DE PARTICIPANTES (marcar con X el tipo de participación)

Nombre y apellidos	Departamento o cargo	Reunión inicial	Auditoría	Reunión final
	Jefe Área de Telecomunicaciones	x	x	x
	Responsable del Servicio	x	x	X
	Jefe de Servicio de Seguridad TIC			X
	Responsable de Sección y Responsable del SGSI	x	x	X
	Grupo de Seguridad	x	x	X
	Jefe Grupo de Almacenamiento y Seguridad		x	
	Responsable Grupo Técnico		x	
	Jefe de Medios		x	
	Rble de Sistemas		x	
D. Alejandro Rodriguez Pubill	Auditor Jefe	x	x	X

6. POLÍTICA DE SEGURIDAD

El objeto del presente documento es desarrollar la Política de Seguridad de la Información de SpainDeal. Esta Política de Seguridad será de aplicación a los sistemas de información y activos utilizados por SpainDeal, en cualquier tipo de soporte en el que se puedan encontrar.

La Política de Seguridad de la Información será de obligado cumplimiento para todo el personal de SpainDeal así como para terceros que presten servicios para SpainDeal así como colaboradores. Esta Política quedará adherida a la Política de Seguridad de la matriz en Alemania.

6.1 Objetivos de la Política de Seguridad

1. Asegurar que el personal de SpainDeal conoce y comprende los problemas asociados a la seguridad de la información y que asumen y son conscientes de sus responsabilidades en este tema.

2. Proporcionar una guía para establecer los estándares, procedimientos y medidas de seguridad para desarrollar un Sistema de Seguridad de la Información.

3. Asegurar la confidencialidad de la información almacenada en los sistemas de información.

4. Maximizar la disponibilidad e integridad de la información.

5. Reducir o eliminar los peligros y riesgos inherentes a nuestras actividades por medio de la mejora continua del desempeño en seguridad en nuestros procesos y servicios.

6. Garantizar que las operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información.

7. Mantener a disposición de las partes interesadas la Política presente, así como los futuros desarrollos de la misma.

6.2 Marco Legal y Regulatorio

- Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de Diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal.
- UNE - ISO/IEC 27001:2013 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- UNE - ISO/IEC 27002:2013 Código de buenas prácticas para la Gestión de la Seguridad de la información.

6.3 Estructura Organizativa

La estructura organizativa de Seguridad de la Información de SpainDeal, estará compuesta por:

Comité para la Seguridad de la Información:

Es el responsable de velar e impulsar las directrices en materia de Seguridad de la Información de SpainDeal.

Las funciones del Comité de Trabajo para la Seguridad de la Información, en adelante CTSI, serán:

1. Redactar y aprobar las normas de segundo nivel correspondientes al ámbito de influencia de SpainDeal.

2. Velar e impulsar el cumplimiento de las normas de segundo nivel y promover el desarrollo del tercer nivel normativo.

3. Aprobación de documentos de correspondencia de responsables en su ámbito competencial, detallados de acuerdo a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

4. Aprobación de los planes de mejora de la seguridad en su ámbito de competencias, de acuerdo a los presupuestos disponibles.

5. Informar sobre el estado de las principales variables de seguridad de sus sistemas de información, para la elaboración de un perfil general del estado de seguridad.

6. Promover la mejora continua en la gestión de la seguridad de la información en su ámbito de competencias.

7. Impulsar la formación y concienciación en su ámbito.

8. Resolver los conflictos que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Responsable de la Información:

Es la persona o personas que tienen la potestad de establecer los requisitos de la información en materia de seguridad. Serán funciones del Responsable de la Información:

1. Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información.

2. Realización, junto a los Responsables del Servicio y contando con la participación del Responsable de Seguridad, de realizar los análisis de riesgos; seleccionando las salvaguardas a implantar.

3. Aceptación de los riesgos residuales respecto a la información, calculados en el análisis de riesgos.

Para la determinación de los niveles de seguridad de la información, el responsable de la información solicitará informe del Responsable de la Seguridad.

Responsable del Servicio:

Es la persona o personas que tienen la potestad de establecer los requisitos del servicio en materia de seguridad. Esta figura tendrá la responsabilidad de determinar los niveles de seguridad del servicio.

Puede coincidir en la misma persona las responsabilidades de la información y del servicio. La diferenciación tiene sentido cuando el servicio maneja información de diferentes procedencias. Las funciones del Responsable del Servicio serán las siguientes:

4. Determinar los niveles de seguridad del servicio, valorando los impactos de los incidentes que afecten a la seguridad del servicio.

5. Realización, junto a los Responsables del Servicio y contando con la participación del Responsable de Seguridad, de realizar los análisis de riesgos; seleccionando las salvaguardas a implantar.

6. Aceptación de los riesgos residuales respecto a los servicios, calculados en el análisis de riesgos.

7. Para la determinación de los niveles de seguridad del servicio, el responsable del servicio solicitará informe del Responsable de la Seguridad.

Responsable de Seguridad:

Es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Cuando por razones de complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el Director General de SpainDeal podrá designar los Responsables de Seguridad delegados que considere necesarios que tendrán dependencia funcional del Responsable de Seguridad siendo responsables en su ámbito de todas aquellas acciones que les delegue.

Serán funciones del responsable de la Seguridad, dentro de su ámbito de actuación, las siguientes:

1. Desarrollar las directrices, estrategias y objetivos dictados por el CTSI.
2. Proveer de asesoramiento y apoyo al CTSI.
3. Elaborar la normativa de seguridad.
4. Aprobar los procedimientos operativos de seguridad.
5. Mantener la seguridad de la información manejada y los servicios electrónicos prestados por los sistemas.
6. Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

7. Realizar el seguimiento y control del estado de la seguridad de la información dentro de SpainDeal.
8. Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
9. Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
10. Elaborar informes periódicos de seguridad para el CTSI que incluyan los incidentes más relevantes de cada período.
11. Supervisar el registro de activos.
12. Participar en los Grupos de Trabajo de Responsables de Seguridad (GCTRS).

El Responsable del Sistema:

El Responsable del Sistema es la persona o personas que tienen la responsabilidad de desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

Las funciones del Responsable del Sistema serán:

1. Definir la topología del sistema de Información y la gestión del mismo. Estableciendo los criterios de uso y los servicios disponibles.

2. Asegurar que las medidas específicas de seguridad se integran adecuadamente dentro del marco de la seguridad en SpainDeal.

3. Suspensión del manejo de una cierta información o la prestación de un determinado servicio por graves de seguridad. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

6.4 Principios básicos de seguridad en SpainDeal

6.4.1 Gestión de Riesgos

SpainDeal está altamente concienciada en la prevención, detección, corrección y mitigación de los riesgos. Son, los Responsables de la Información y de los Servicios, los encargados de la identificación, tratamiento y control de los riesgos. Las medidas de seguridad a aplicar para el tratamiento de los riesgos serán propuestas por el Responsable de Seguridad, debiendo revisarse al menos una vez al año por dicho responsable.

6.4.2 Desarrollo Normativo

SpainDeal desarrollará su Política de Seguridad de la Información en base a 3 niveles:

1. Nivel Normativo: Política de Seguridad de la Información y Normas Básicas de Seguridad de la Información.

2. Normas Específicas de Seguridad de la Información. Procedimientos, Instrucciones Técnicas, Registros, etc.

El Responsable de Seguridad será el encargado de velar por que la documentación de seguridad se encuentre actualizada y organizada.

6.4.3 Cumplimiento Normativo

SpainDeal cumplirá con la legislación vigente referida a la Protección de Datos de Carácter Personal así como con todas aquellas normativas de obligado cumplimiento en materia de Seguridad de la Información.

6.4.4 Terceras Partes / Colaboradores y Servicios Externos

Cuando por cualquier tipo de relación con SpainDeal un tercero tenga acceso a la información de la misma se asegurará su adhesión a los términos y las condiciones referentes a la Política de Seguridad de la Información.

Cuando algún aspecto de la Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte, se requiera al Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

6.4.5 Concienciación y Formación

SpainDeal velará para que todo el personal relacionado con el tratamiento de la información se encuentre formado e informado de sus deberes y obligaciones en materia de Seguridad de la Información. Para ello SpainDeal dispondrá de una planificación anual donde se detallaran la formación y la concienciación.

6.4.6 Continuidad del Servicio

Es imprescindible para SpainDeal establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de los servicios prestados por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad del servicio en estos casos, SpainDeal establecerá Planes de Contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La Gestión de la continuidad del negocio (Servicio) incluirá, por tanto, diversos controles para la identificación y reducción de riesgos/impactos con el fin de limitar las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

6.5 Revisión de la Política de Seguridad

Se revisará periódicamente y siempre que haya cambios significativos la Política de Seguridad de la Información.

7. MANUAL DE SEGURIDAD

7.1 Control de Documentación

El Marco Normativo de Seguridad de la Información deberá elaborarse teniendo en cuenta los siguientes criterios generales:

1. Se deberán definir las propiedades de la documentación que forma parte del Marco Normativo de Seguridad de información. Dichas propiedades quedarán incluidos en el Procedimiento de Control de Documentación.
2. La nomenclatura se ajustará a los criterios establecidos en el Procedimiento de Control de Documentación.
3. El ciclo de vida de la documentación del Marco Normativo de Seguridad de la Información se realizará con un soporte electrónico único para todo SPAINDEAL, que garantice:
    - La recepción de los borradores de consulta por parte de todos los destinatarios.
    - El registro, acceso y custodia de los comentarios resultado del proceso de consulta.
    - La gestión de cambios y versiones dentro del proceso de consulta.
    - La distribución de los documentos aprobados.
    - La custodia de las versiones electrónicas en un único repositorio.
    - La consulta permanente del sistema normativo actualizado.
4. La documentación debe estar disponible a las personas que deban hacer uso de ella, en los lugares donde sea necesario su uso.
5. Debe ser revisada periódicamente, según sea necesario, con control de versiones.
6. Debe ser retirada inmediatamente cuando quede obsoleta. Cuando sea necesario por motivos legales, o con el fin de preservar el conocimiento, la documentación obsoleta que se conserve se identificará claramente como “Obsoleta” y se referenciará en la portada la nueva versión si estuviera disponible.
7. Cualquier documento deberá tener un responsable de su mantenimiento, que será el encargado de mantenerlo actualizado con los últimos cambios aprobados. Este responsable será igualmente el encargado de establecer las medidas de seguridad necesarias para mantener la seguridad de la información.

7.2 Gestión de Riesgos

7.2.1 Inventario de Activos

SpainDeal dispondrá de un inventario de activos actualizado que será responsabilidad de la Unidad de Informática y Comunicaciones, al efecto en dicho inventario se incluirá la información que se especifica a continuación:

1. Identificador y tipo de activo.
2. Formato.
3. Ubicación física y lógica del activo.
4. Información sobre la licencia si fuera software.
5. Información de copia de respaldo o información necesaria para poder recuperarla en caso de desastre.
6. Persona o cargo encargado de su protección y utilización.
7. Responsable del activo.
8. Clasificación de seguridad.
9. Relación de dependencia con otros activos
10. Métodos de identificación y autenticación de usuarios, detallando cada mecanismo de autenticación.

Deberá existir un procedimiento definido para la realización del inventario de activos, que comprenda la realización del inventariado y clasificación de los mismos.
Asimismo todos los activos, tendrán identificado un propietario, el cual:

1. Asegurará que toda la información, así como los activos asociados con los recursos para el tratamiento de tal información, están adecuadamente clasificados.
2. Definirá y revisará periódicamente las restricciones de acceso y las clasificaciones, teniendo en cuenta las políticas de control de acceso aplicables.

El propietario del activo debe definir, por cada activo:

1. El servicio ofrecido por el activo y su implicación en este.
2. Las actividades en las que está presente.
3. Las aplicaciones que lo utilizan.
4. Los datos que contiene.
5. La valoración del activo por cada dimensión de seguridad (Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad).

La implantación de los controles asociados a las tareas anteriores podrán delegarse, en su caso, pero la responsabilidad de las mismas deberá mantenerse en quien asuma el rol de propietario de cada activo.

Se prevendrá el uso de los activos de SpainDeal para fines no autorizados. Cualquier uso de estos para fines no profesionales que no cuente con la autorización de la Dirección[1] o para cualquier propósito no autorizado será considerado un uso indebido de los recursos de SpainDeal.

[1] Se referirá mediante el término genérico “Dirección”, en el presente documento, a los cargos, órganos y estamentos que ostenten la capacidad de mando de SpainDeal.

Quienes asuman la figura de responsable de los sistemas de información han de aprobar el uso apropiado de los mismos. Se considerará inapropiado el uso de los activos para fines no aprobados y sin autorización de los responsables de dichos sistemas o de la Dirección.
Si se identifica una actividad no autorizada mediante la supervisión o por otros medios, esta actividad deberá ser puesta en conocimiento del encargado de considerar la acción disciplinaria y/o legal más adecuada.

Se informará al personal de los usos permitidos de los recursos, así como de las medidas existentes para detectar el uso inapropiado de los mismos. En este sentido, se obtendrá consejo legal acerca de la posibilidad de utilización de medidas de monitorización del uso de los sistemas, previamente a su implantación.

Al iniciar sesión desde los puestos de trabajo, los sistemas deberán mostrar un mensaje de advertencia informando de la propiedad de SpainDeal del sistema al que se entra y de la prohibición del acceso o realización de actividades no autorizadas. El inicio de sesión sólo continuará cuando el usuario haya aceptado expresamente las condiciones mostradas en el mensaje.

7.2.2 Análisis de Riesgos

El departamento de Informática y Comunicaciones realizará un Análisis de Riesgos sobre todos los activos identificados, teniendo en cuenta para ello las amenazas, riesgos e impactos.
Se define la amenaza como los eventos que pueden desencadenar un incidente en SpainDeal, produciendo daños materiales o pérdidas inmateriales en los activos identificados.
El riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a SpainDeal.

El impacto es la consecuencia que sobre un activo tiene la materialización de una amenaza.
Para la realización del Análisis de Riesgos se seguirá la metodología de MAGERIT, siendo fundamental la recolección de información, por lo que será necesaria la implicación de todo el personal de SpainDeal.

Una vez identificados los activos afectados como se define en el apartado*4.1 Inventario de Activos* del presente documento, se procederá con la **caracterización de las amenazas,** consistente en identificar las amenazas que afectan a los activos y la vulnerabilidad ante esas amenazas en términos de probabilidad y degradación. De este modo, será posible estimar el impacto y riesgo potencial o intrínseco sobre cada uno de los activos.

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es en dos sentidos:

Degradación: cuán perjudicado resultaría el activo

Frecuencia: cada cuánto se materializa la amenaza

La **degradación** mide el daño causado por un incidente en el supuesto de que ocurriera. Se caracterizará como un porcentaje de degradación del valor de los activos sobre su valor en las dimensiones Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad.

La **frecuencia** pone en perspectiva la degradación. Una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; y por el contrario, una amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable. Atendiendo a los distintos grupos de amenazas identificados, se puede decir en líneas generales que:

1. Desastres naturales. Son de muy poca frecuencia, pero causan grandes daños sobre los activos.
2. De origen industrial. Algunas de ellas causan daños muy graves, con una frecuencia algo mayor que los desastres naturales. Algunas pueden llegar a tener una frecuencia anual con impactos importantes, por lo que es vital tratarlas correctamente.
3. Errores y fallos no intencionados. Algunas de ellas pueden ser muy frecuentes, si bien su impacto no suele ser alto, existiendo controles relativamente sencillos para mitigarlas. Por su alta frecuencia, requieren ser tenidas muy en consideración.
4. Ataques intencionados. Son difíciles de predecir y su frecuencia e impacto pueden ser altos, muchas veces en la imagen y confianza de la Organización.

Los valores de degradación y frecuencia se tomarán a partir de la combinación de tres fuentes de conocimiento principales:

1. Los valores de la biblioteca estándar de la herramienta de Análisis de Riesgos.
2. La experiencia previa acumulada en la realización de Análisis de Riesgos.
3. El análisis del entorno de SpainDeal.

El siguiente paso será determinar el nivel actual de gestión de la seguridad en los sistemas a analizar en base a las **salvaguardas** y calificarlo por su eficacia frente a las amenazas que afectan a los activos.

Valoración de las salvaguardas. Las salvaguardas se caracterizarán, además de por su existencia, por su eficacia frente al riesgo que pretenden mitigar.
Los resultados del nivel de cumplimiento se tomarán a partir de la información recabada en las entrevistas con el personal (responsables de los activos, personal técnico de la SpainDeal, etc.).

Combinando los resultados de las actividades anteriores, se deberá dar una respuesta sobre las estimaciones del estado del riesgo. Será fundamental la utilización como soporte de una herramienta automatizada para el Análisis de Riesgos (EAR).

Una vez realizado el Análisis de Riesgos y obtenidas las conclusiones, es preciso seleccionar los objetivos de control y los controles que conformarán el plan de tratamiento de riesgos. Para ello es preciso establecer un nivel de "**Riesgo aceptable**" al que debería llegarse en un plazo dado. El camino que hay que recorrer para ello será lo que conforme el **Plan de tratamiento del riesgo** y la aceptación por parte de la Dirección de un cierto riesgo residual.

La Dirección deberá acordar y aprobar de manera general o para cada riesgo específico, unos **umbrales objetivos** para discernir los riesgos aceptables de los que no lo son.
Para tratarlos riesgos identificados, SpainDeal se encargará de la aplicación de los controles adecuados.

Analizado cada uno de los riesgos presentes, se **identificará aquellos controles** que contribuyen de manera más eficiente a mitigarlos. Se empezará por identificar aquellos que mayor beneficio supondrán para la reducción de cada riesgo, proponiendo la implantación o mejora de estos precisamente.

A la hora de definir un plan para implantar o mejorar controles, habrá que tener en cuenta el nivel de madurez que se pretende alcanzar en cada uno de ellos. En función de cómo de recomendable sea el control, se puede decidir mejorar hasta un cierto nivel de madurez u otro.
Con el resultado de la selección, el Responsable de Seguridad elaborará una declaración de aplicabilidad que proporciona de forma esquemática el plan de tratamiento de riesgos a implementar.

7.2.3 Evaluación de los Riesgos

Los resultandos del Análisis de Riesgos se documentarán, incluyendo los valores obtenidos de la herramienta de Análisis de Riegos, EAR.

Con una **periodicidad anual**, se llevará a cabo el proceso de análisis y gestión de riesgos descritos, detallando los resultados en un informe que abarcará los servicios objeto del alcance indicado en la Política de Seguridad de SpainDeal.

De cada análisis se realizará un informe que deberá ser puesto en conocimiento de SpainDeal. Dichos informes tendrán carácter **DIFUSIÓN LIMITADA**.

7.2.4 Plan de Tratamiento del Riesgo

El Plan de Tratamiento del Riesgo articulará la estrategia a seguir en el plazo indicado. El orden de ejecución de los proyectos se establecerá de acuerdo a los siguientes criterios:

1. La importancia de las situaciones de riesgo a solventar.
2. La dependencia e interrelación con otros proyectos del Plan.
3. Las obligaciones legales.
4. La distribución temporal a lo largo del tiempo, atendiendo a las cargas de trabajo y la disponibilidad de recursos.

El Plan deberá presentar la evolución de la mejora del cumplimiento de los controles aplicables, así como la reducción del riesgo hasta el nivel aceptable.
Todas las acciones correctivas derivadas de los proyectos del Plan de Tratamiento del Riesgo establecido se notificarán a las partes interesadas como medida de refuerzo.

El ciclo de vida de la documentación del Marco Normativo de Seguridad de la Información se articula en torno a:

1. Elaboración
2. Revisión
3. Aprobación
4. Custodia y publicación
5. Derogación

7.2.5 Elaboración

La elaboración del manual, los procedimientos, instrucciones y demás documentos de nivel inferior, recae sobre la unidad organizativa responsable de las actividades documentadas, ya sea el responsable directo o el personal técnico involucrado en las tareas del alcance del documento.

7.2.6 Revisión y Aprobación

Corresponde al GTSI la revisión de la Política de la Información previa a su aprobación por el Órgano correspondiente.

La revisión y aprobación del Manual de Seguridad, los procedimientos, instrucciones técnicas y demás documentos de mayor detalle deberá realizarla el GTSI, de cara a garantizar que cada documento incluye los controles necesarios y está alineado con las directrices de la Política de Seguridad.

Los documentos cuyo alcance u objeto se limiten a actividades específicas de una determinada Unidad Organizativa, serán aprobados por su responsable directo. El responsable del documento deberá informar al Responsable de Seguridad, quien será el encargado de mantener el inventario de documentación actualizado.

Tendrán la consideración de aprobados aquellos documentos presentados y aceptados en el GTSI de SPAINDEAL, para lo que el Secretario del GTSI firmará el acta donde se reflejen el/los documento(s) que ha(n) sido aprobado(s).

7.2.7 Custodia y publicación

Una vez aprobados y publicados los documentos de Política y Manual de Seguridad de la Información, los originales firmados o los ficheros correspondiente validados por firma electrónica, permanecerá bajo la custodia del Responsable de Seguridad de SPAINDEAL.
El Responsable de Seguridad mantiene un repositorio de documentación, que recoge los documentos que conforman el Marco Normativo de Seguridad de la Información Sobre dicho repositorio:

1. Sólo tiene acceso de escritura el Responsable de Seguridad y los miembros del GTSI.
2. El acceso de lectura a los documentos está permitido al personal que preste sus servicios para SPAINDEAL según sea requerido para el desarrollo de sus funciones, pudiendo habilitarse, en caso necesario, acceso a terceras partes.

3. El acceso a documentos cuyo alcance se limite a determinadas Divisiones o Unidades está limitado al personal correspondiente a las mismas, según se especifique en el "Ámbito de aplicación" del documento.

Por el carácter más general los documentos que afecten a usuarios de todo SPAINDEAL, la custodia de estos documentos recae sobre el Responsable de Seguridad.

7.2.8 Derogación

El GTSI someterá a análisis para propuesta de derogación la Política de Seguridad de la Información que, a su criterio, haya dejado de tener vigencia, debiendo ser derogada por el Órgano competente, si lo estima oportuno.
En el caso de los Procedimientos, Instrucciones Técnicas, o documentos de menor nivel, la derogación podrá ser decidida por quien asuma el cargo o la figura con capacidad para aprobar el documento.

7.2.9 Control y Mantenimiento de los Registros

Para mantener el control de los registros relativos a la Seguridad de la Información, el Responsable de Seguridad o la persona en quien delegue mantendrá el fichero para saber en todo momento las revisiones realizadas así como el registro de las evidencias recogidas.

El fichero con el control de registros, es tratado en sí mismo como un registro de la seguridad, siendo almacenado en el repositorio identificado bajo la custodia del Responsable de Seguridad.
La codificación de los nombres de los registros se realizará siguiendo lo indicado en el Procedimiento de Control Documental.

Los registros deberán ser mantenidos durante un periodo de tres años, salvo disposición legal que lo aumente o se indique expresamente otra periodicidad en el documento del que derive.

Los registros electrónicos serán incluidos en los procedimientos de copias de seguridad de SPAINDEAL.

7.3 Revisión por la Dirección

SpainDeal supervisará el documento de revisión que se le presentará una vez al año, sobre la Gestión de la Seguridad de la Información realizada dentro de la organización para asegurar su adecuación, eficacia; siendo posible solicitar revisiones extraordinarias en caso de considerarse necesario.
Las revisiones deben incluir las oportunidades de mejora y la necesidad de cambios en la propia Seguridad de la Información, incluyendo la Política de Seguridad de la Información y los objetivos de seguridad de la información en el caso necesario.
Los resultados de las revisiones deben estar claramente documentados y registrados.

7.3.1 Entradas

Como entrada a la revisión se podrá incluir:

1. Resultados de las auditorias y revisiones de Seguridad de la Información.

2. Comentarios de las partes interesadas.
3. Técnicas, productos o procedimientos, que podrían utilizarse para mejorar el comportamiento en la Gestión de la Seguridad de la Información.
4. Estado de las acciones preventivas o correctivas.
5. Vulnerabilidades o amenazas no abordadas adecuadamente en la evaluación de riesgos previa.
6. Resultados de las mediciones de la eficacia de la Gestión de la Seguridad de la Información.
7. Acciones de seguimiento de las revisiones anteriores.
8. Cualquier cambio pudiera afectar Seguridad de la Información.
9. Recomendaciones de mejora.
10. Análisis de situación
11. Cambios legislativos
12. Revisión, si procede, de la estructura organizativa dedicada a la Seguridad de la Información en la organización
13. Revisión, si procede, de la adecuación de la Política de Seguridad de la Información.
14. Revisión, si procede, de los Análisis de Riesgos y aprobación de los riesgos residuales.
15. Seguimiento del Cumplimiento de Objetivos.

7.3.2 Salidas

Los resultados de la revisión podrán incluir cualquier decisión y acción relativa a lo siguiente:

1. Mejora de la eficacia en lo relativo a la Seguridad de la Información.
2. Modificaciones en la gestión de la seguridad de la información, cuando sea necesario, para responder a los eventos internos o externos que pueden impactar en el mismo.
3. Necesidad de recursos.

7.4 Auditorías

SpainDeal deberá realizar auditorías internas sobre la Seguridad de la Información a intervalos planificados, para determinar si la gestión de la seguridad de la información:

1. Cumple con la legislación y normativa aplicables.
2. Cumple los requisitos de seguridad de la información identificados.
3. Se implantan y se mantienen de forma efectiva dando el resultado esperado.

Anualmente, el Responsable de Seguridad preparará el Programa de Auditorías de manera que asegure que se auditan al menos todos los puntos de la Norma de referencia para la Gestión de la Seguridad de la Información.

El Programa Anual de Auditorías será sometido a la aprobación del GTSI de la Información y deberá contemplar el alcance de las auditorías, las fechas previstas para las inspecciones y las observaciones oportunas si existieran.

En dicho programa anual de auditorías se tendrá en cuenta el estado e importancia de los procesos y las áreas a auditar, así como los resultados de las auditorías previas. Los objetivos básicos de las auditorías son los siguientes:

1. Determinar si el sistema está siendo adecuadamente documentado.
2. Verificar periódicamente si lo establecido en el sistema está siendo correctamente implantado.
3. Evaluar la efectividad alcanzada con la implantación del sistema.
4. Identificar cualquier deficiencia, no conformidad o desviación, comprobando la aplicación de las acciones correctoras y preventivas apropiadas.

Las auditorías programadas pueden ser complementadas con otras no programadas, siempre que se de alguna de las siguientes condiciones:

1. Después de cualquier cambio importante en el sistema para evaluar su impacto (reorganizaciones, revisiones profundas de los documentos del Sistema, etc.).
2. Cuando sea necesario comprobar la ejecución de las acciones correctoras y preventivas establecidas.

En el desarrollo de las auditorías se contemplan una serie de etapas fundamentales que son las que se describen en los siguientes apartados. Estas etapas se deberán respetar siempre que sea posible y sea proporcionado con el alcance de la auditoría.

7.4.1 Preparación

El Responsable de Seguridad preparará la auditoría o formará, en su caso, el equipo auditor. El auditor o equipo auditor, elaborará un plan específico de la auditoría a realizar, que será puesto en conocimiento del Responsable de Seguridad.

7.4.2 Notificación

El Responsable de Seguridad pondrá en conocimiento del personal involucrado en la auditoría el hecho de la misma.

7.4.3 Reunión Previa

Las auditorías comenzarán con una reunión previa, en la cual el auditor o equipo auditor se reunirá con los responsables de las dependencias a auditar y durante la cual se confirmará el alcance de la misma

7.4.4 Ejecución

Se auditarán con el detalle necesario las partes del sistema que previamente se hayan seleccionado, teniendo en cuenta que la planificación realizada no debe restringir el análisis de aquellos aspectos que durante la ejecución de la auditoría se revelen problemáticos o de esencial importancia.
La auditoría se realizará por medio de la supervisión, inspección y revisión de las actuaciones de cada una de las áreas auditadas correspondientes, y de su documentación.

Se deberá facilitar al equipo auditor el acceso a las dependencias a auditar, así como a la documentación disponible que precise para el correcto desarrollo de la auditoría y la fundamentación de sus conclusiones.

7.4.5 Informe y conclusiones

El auditor, o equipo auditor coordinado por el Responsable de Seguridad, preparará un informe de la auditoría donde quedarán incluidas las conclusiones de la auditoría
Con independencia de los criterios de clasificación utilizados por los auditores, los aspectos detectados por ellos deberán incluir una categorización de las debilidades encontradas de la siguiente forma:

- No conformidades *Mayores*: referidas a un punto completo de la Norma de referencia para la Gestión de la Seguridad de la Información, así como incumplimientos legales de considerada importancia.
- No conformidades *Menores*: referidas a un apartado dentro de un punto de la Norma de referencia para la Gestión de la Seguridad de la Información, o de la Norma de referencia utilizada para la selección de controles y objetivos de control aplicables.
- *Observaciones*: necesidades de mejora observadas, referidas a un punto en concreto.

En respuesta al informe de auditoría, la dependencia auditada contestará formalmente con las medidas correctoras y preventivas tomadas o previstas para la corrección de las no conformidades en el plazo acordado.

Cuando la dependencia auditada no considere necesarias acciones correctoras para los aspectos detectados por los auditores, deberá justificarlo y presentar pruebas razonables de este hecho.

7.4.6 Seguimiento y cierre

En caso de haberse detectado deficiencias en el sistema, se abrirá una incidencia de seguridad que será tratada según el procedimiento vigente para la gestión de Incidencias de Seguridad.

Cuando se detecten no conformidades, los responsables o mandos de la dependencia auditada acordarán y programarán las medidas correctoras y preventivas apropiadas y los plazos de aplicación. Terminado el plazo, se podrán realizar auditorías de seguimiento, si la gravedad lo aconseja, o aprovechar las auditorías correspondientes al siguiente ciclo para comprobar el resultado de la implantación de las acciones correctoras y preventivas, así como su eficiencia.

Las acciones de seguimiento tendrán lugar hasta verificar la eliminación completa de las no conformidades, con lo que se darán por cerradas las auditorías en las que fueron identificadas dichas no conformidades.

8. PRESENTACION DE INFORMES

8.1 Introducción

Para la presentación y publicación de resultados del presente ejercicio se entrega una presentación realizada con Prezi.

9. RESUMEN EJECUTIVO

Tras una fuerte demanda en el mercado de la venta online de productos tecnológicos por parte de GermanDeal, se decidió por parte del equipo directivo ampliar el negocio implantando una nueva sede en España, SpainDeal, la cual desempeñara el mismo papel que la matriz. Para ello, SpainDeal, heredara toda la estructura de GermanDeal. Sin embargo, SpainDeal irá un paso más allá, implantando un SGSI en la parte técnica de su negocio.

Las empresas se enfrentan a amenazas y vulnerabilidades de todo tipo, sometiendo a sus activos a un riesgo que debe ser minimizado o incluso mitigado. En caso de ser afectada por este tipo de eventos, podría perder competitividad frente a la competencia, ya que el impacto sobre la organización puede ocasionar un claro impacto sobre la opinión pública y con ellos bajar las ventas de sus productos. Un ejemplo sería un filtrado de la base de datos de clientes que hubieran realizado una compra en SpainDeal y se hicieran públicos esos datos.

Es por esto que SpainDeal basará esta implantación en la norma IEC/ISO 27002:2013 para el establecimiento de una serie de controles que establezcan unos parámetros de seguridad sobre todos los activos de SpainDeal expuestos.

El objetivo principal es realizar un plan de implementación de la ISO 27001:2013 en la sección técnica para su certificación en ISO 27001:2013 durante los 6 meses posteriores a la publicación de la norma, ya que se recomienda usar ese marco de referencia en el caso de que no haber empezado el proceso de implantacion o encontrarse en las fases iniciales del proceso de implantación de un SGSI.

Se empezara el proyecto realizando una auditoria pasando los controles de la ISO/IEC 27002:2013 para ver en que situación partimos para posteriormente realizar el SGSI en base al resultado de la misma.

Esta auditoría nos muestra la situación inicial:

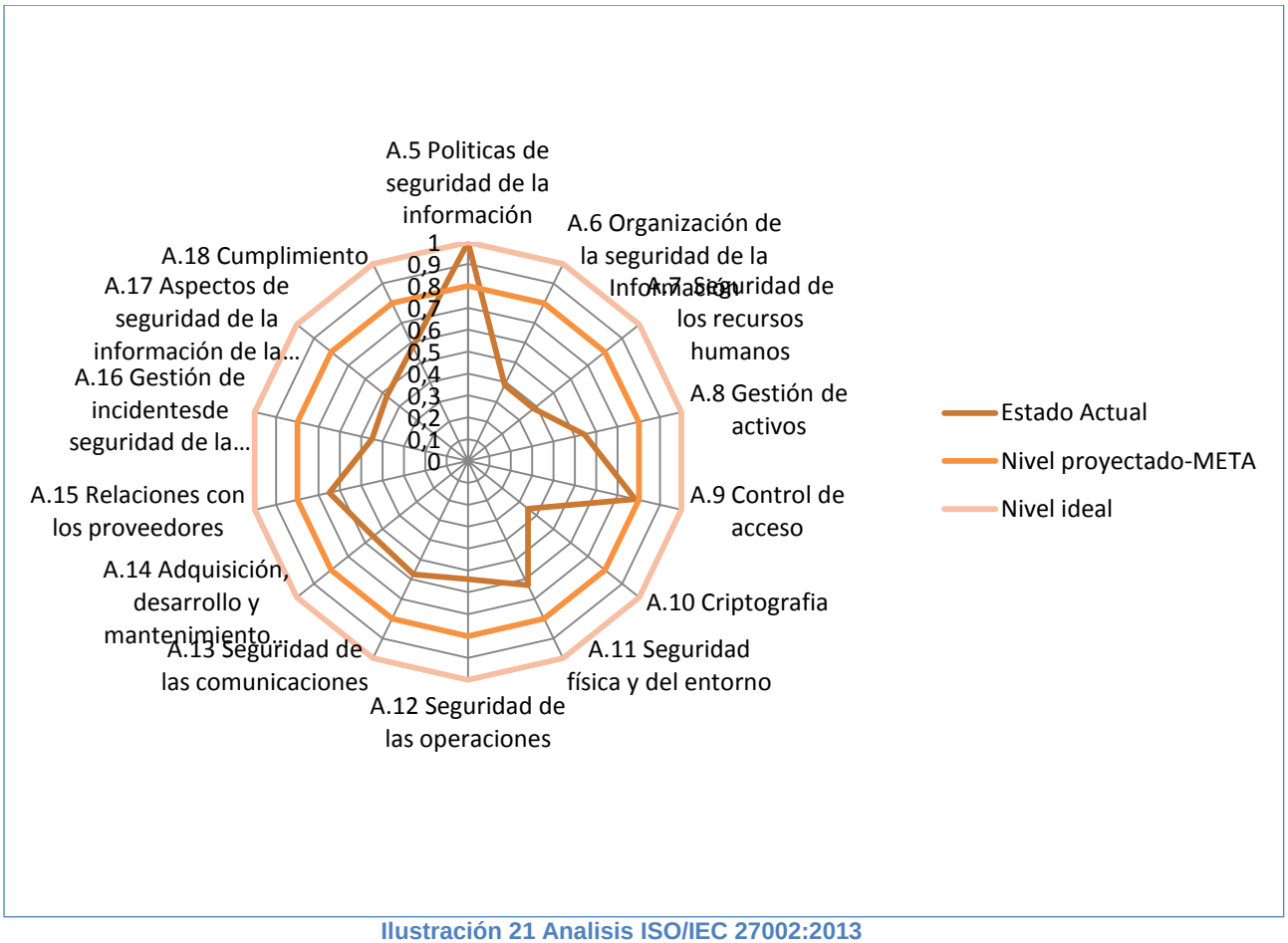

Ilustración 21 Analisis ISO/IEC 27002:2013

Para ello hemos utilizado MAGERIT para realizar el análisis de riesgos. Esta norma establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información. Garantizando que sus organizaciones siguen estos principios ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI.

Una vez identificados todos los activos de información comprendidos en el alcance, se procede a establecer el SGSI, siguiendo las pautas del estándar ISO 27001:2013 en su sección 4.3. En esencia lo que se exige es efectuar de manera disciplinada y sistemática un análisis y evaluación del riesgo de los activos identificados para determinar cuáles son aquellos que deben ser protegidos para mitigar su riesgo, así como definir también cual es el riesgo residual (el riesgo con el cual la empresa está decidida a convivir).

SpainDeal busca particularmente con ésta actividad, promover la ejecución de prácticas de seguridad adecuadas y la implementación un Sistema de Gestión de Seguridad de la Información (SGSI) con base en la norma ISO/IEC 27001:2013 para cubrir los servicios de Desarrollo, Soporte, Mantenimiento y Sistemas.

Como parte del análisis, se establecerán diferentes frentes de trabajo y etapas de registro de información (contextualización, identificación de activos, análisis de impacto, análisis de riesgo) que posteriormente maduraran y registraran observando los posibles escenarios de riesgo que apareciesen y poder mejorarlos o subsanarlos.

Para ello se establece un Plan Director en el que SpainDeal desea principalmente mejorar los niveles de seguridad incluidos en sus servicios, con el objeto de optimizar

las relaciones de confianza con sus clientes y convertirse en una alternativa más confiable y competitiva frente a otras empresas del mercado.

En segundo lugar SpainDeal, se ha propuesto encauzar sus procesos con practicas adecuadas a nivel de seguridad y solicita del departamento de consultoría: identificar los activos de información relevantes de sus actuales servicios, conocer los riesgos relacionados, los niveles de madurez alcanzados con los controles actualmente implementados y finamente identificar un plan de acción que le permita en un tiempo no mayor a un año acercarse al marco objetivo para la posterior certificación en la norma ISO/IEC 27001:2013 en cuanto sea posible.

Consolidar en el presente documento los resultados, conclusiones, y recomendaciones de la identificación de activos, evaluación y valoración de riesgos, así como determinar las bases para el tratamiento de riesgos y establecer el Plan Director de Seguridad de la Información para SpainDeal.

Definir y estructurar procesos y directrices en seguridad de la información para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI), en general, mitigar riesgos, impacto o consecuencia que podrían materializarse al infringir los niveles de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Una vez realizado el análisis de riesgos, se han identificado los activos que están afectados por un riesgo mayor del que la organización ha asumido y por otro lado se han identificado las principales amenazas que pueden impactar en cada activo. Asimismo, en la declaración de aplicabilidad se definirán todos los controles que son de aplicación y por tanto es necesario elaborar los procedimientos respecto a cómo se van gestionar e implantar dichos controles.

Por tanto, es necesario por un lado elaborar los procedimientos orientado a implantar y gestionar los controles y por otro lado, realizar una serie de proyectos o planes de tratamiento de riesgos sobre los activos identificados que tienen un riesgo mayor que el aceptable.

Se establecen 3 proyectos:

- **Proyecto1: Puesta en marcha un sistema de defensa**
- **Proyecto2: Implantación de salvaguardas imprescindibles**
- **Proyecto3: Creación del Comité de Seguridad de los Sistemas de Información**

Llegados a esta fase, es el momento de evaluar el cumplimiento de la empresa respecto a los controles definidos por la norma ISO/IEC 27001:2013 y determinar cuáles controles serán implementados y cuáles no con el fin de mejorar la seguridad en la Entidad. Esto se realizara mediante la auditoria de cumplimiento que nos darán una serie de conclusiones:

- La organización requiere implementar mayor número de controles y mejorar la eficacia de los existentes con jornadas de sensibilización y divulgación de directrices en seguridad de la información.

- Hay que mejorar en en aspecto humano como factor determinante a la hora de securizar la información y mejorar desde la fase de contratación, hasta la formación continuada ya que los controles y procesos manejados por la

organización deben ser conocidos por todos los empleados de la organización. Es importante concientizar que la seguridad de la información es responsabilidad de todos.

- En lo relativo a la política de seguridad de la información, la empresa dispone de ella y por lo tanto es un factor fundamental para trabajar desde una buena base y con cimientos asentados.

Se describen tanto la Política de Seguridad como el Manual de Seguridad.

10. GLOSARIO DE TERMINOS

Términos y definiciones básicas:

- Activo: cualquier cosa que tenga un valor para la empresa
- LOPD: Ley Orgánica de Protección de Datos
- SLA: Nivel de Servicios Acordado
- SGSI: Sistema de Gestión de la Seguridad de la Información
- CPD: Centro de Proceso de Datos
- Magerit: Metodología de análisis y gestión de riesgos
- Salvaguarda: medidas para proteger de las amenazas
- Amenaza: Lo que pone en riesgo a los activos
- EAR: Herramienta utilizada para la realización del análisis de riesgos
- CMM: Capability Maturity Model (Nivel de Madurez)
- CSSI: Comite de Seguridad de los Sistemas de Información

11. BIBLIOGRAFIA

- Guia de aplicacion de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes de AENOR. Autor:Ana Andres y Luis Gómez
- Portal de Soluciones técnicas y organizativas a los controles de la Norma Internacional ISO/IEC 27002. http://www.iso27002.es/
- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Ministerio de Administraciones Públicas, http://administracionelectronica.gob.es
- Norma UNE-ISO/IEC 27001
- Norma UNE-ISO/IEC 27002
- Distintas ilustraciones de http://www.isotools.org
- Metodología Magerit https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf

12. Anexos

- ANEXO 1.Controles-valoracion-amenazas-madurez-resumen
- ANEXO 2.Archivo EAR/Pilar con el que se realizo el análisis de riesgos
- ANEXO 3. Presentacion