TRABAJO FIN DE MÁSTER

Elaboración de un Plan de Implementación y Desarrollo de un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO/IEC 27001:2005

Edición	Fecha	Nota de Cambio	Revisado Por	Preparado Por
01	12/06/2014	Versión final del documento	Antonio José Segovia Henares	Jorge F. Lillo Muñoz

FICHA DEL TRABAJO FINAL DE MÁSTER

Título del trabajo:	Elaboración de un Plan de Implementación y Desarrollo de un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO/IEC 27001:2005
Nombre del autor:	Jorge Francisco Lillo Muñoz
Nombre del consultor:	Antonio José Segovia Henares
Fecha de entrega (mm/aaaa):	06/2014
Área del Trabajo Final:	Sistemas de Gestión de la Seguridad de la Información
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

AGRADECIMIENTOS

En primer lugar, quiero agradecer a mi tutor del TFM y consultor de la asignatura de SGSI, Antonio José Segovia Henares, el apoyo, los consejos, la ilusión que pone en sus enseñanzas y las palabras de ánimo que en todo momento me ha brindado.

Quiero dar las gracias igualmente a los consultores de las asignaturas que he realizado y a los compañeros del Máster por sus consejos y comentarios que siempre han sido positivos.

También quiero agradecer a mis clientes por su compresión y paciencia en este periodo en el que no he podido dedicarles todo el tiempo que hubiera deseado.

Por último, quiero agradece el apoyo prestado por mi familia y amigos y muy especialmente a mi mujer Isa y a mis hijos Jorge y Marta por su paciencia infinita en las horas de estudio interminables.

Gracias a todos vosotros de corazón, sin vuestra ayuda y comprensión esto no hubiera sido posible.

RESUMEN

Las organizaciones deben proteger toda información que consideren que tiene valor y que es importante para el correcto funcionamiento y desempeño de las actividades que desarrollan.

La información deberá protegerse de las posibles amenazas que puedan ocurrir, independientemente del formato en el que esté almacenada. Esta protección debe estar orientada a:

- Minimizar los posibles daños.
- Garantizar la continuidad del negocio.
- Maximizar el retorno de la inversión y las oportunidades de negocio.

Actualmente existen leyes que tienen por objeto la protección de determinada información, como los datos de carácter personal, pero no tienen en cuenta toda la información que puede manejar una empresa u organización.

En este sentido, los Sistemas de Gestión de Seguridad de la Información (SGSI) son normas internacionalmente reconocidas que se establecen para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

Este Trabajo Fin de Máster ha consistido en la implementación y desarrollo de un SGSI, basado en la norma ISO/IEC 27001:2005, en una empresa que desea conocer los riesgos a los que están expuestos sus activos de información y establecer un proceso de mejora continua en la seguridad de la información.

ABSTRACT

Organisations must protect all information they consider valuable and important for the proper operation and performance of their business activities.

Furthermore, this information should be protected against any potential threats, regardless of the format it may be stored. This protection should be directed towards:

- Minimising the damage
- Ensuring business continuity.
- Maximising the return on investment and improving business opportunities.

Nowadays, there are laws aimed to protect certain types of information, such as personal data, but these laws do not take into account all the information a company or organization can manage.

In this sense, Management Security Information Systems (ISMS) are internationally recognized standards used for creating, implementing, operating, monitoring, reviewing, maintaining and improving information security.

This work involves the development and implementation of an ISMS based on ISO/IEC 27001:2005, in a company that wants to know the risks their information assets are exposed to, and establish a process of continuous improvement in information security.

ÍNDICE

1. INTRODUCCIÓN

El Trabajo Fin de Máster (en adelante TFM) se va a centrar en la elaboración de un Plan de Implementación y Desarrollo de un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO/IEC 27001:2005 en una empresa.

Para la elección de la empresa, se ha realizado una simulación de organizaciones y sistemas informáticos existentes en distintos casos reales, de forma que la empresa descrita y elegida para el TFM no permita una identificación real con ninguna empresa concreta, pero al mismo tiempo el proyecto se pueda adaptar a casos concretos realizando los ajustes necesarios.

En el proyecto se van a estudiar aspectos de seguridad en empresas que tienen una amplia trayectoria en la gestión de las tecnologías de la información y que han ido evolucionando pero que actualmente se plantean la disyuntiva entre la computación en sus propios centros de procesos de datos y la computación en la nube o en centros especializados de servicios (ASP e ISP), debiendo analizar las ventajas e inconvenientes y los riesgos a la seguridad inherentes a ambas opciones.

También se va a tener en cuenta aspectos legislativos de aplicación en las empresas que van a condicionar determinados aspectos en cuanto a la seguridad.

2. ENFOQUE Y SELECCIÓN DE LA EMPRESA

Para realizar el TFM hemos seleccionado a una empresa del sector del transporte de viajeros por carretera que tiene como razón social EMPTRAVEL S.A. y domicilio social en Málaga.

2.1. DESCRIPCIÓN DE LA EMPRESA

La empresa se dedica al transporte de viajeros por carretera tanto en el ámbito del transporte regular como del transporte discrecional.

La empresa se constituyó en 1970 como empresa de transporte regular de viajeros entre distintas localidades de Málaga y posteriormente comenzó a realizar transporte regular entre distintas provincias de Andalucía.

Recientemente, a raíz del establecimiento del puerto de Málaga como punto de atraque de cruceros, ha creado una división de transporte discrecional de viajeros orientado tanto a las compañías de cruceros como a los propios cruceristas que pueden contratan estos servicios para realizar viajes turísticos.

La empresa cuenta actualmente con una flota de unos 70 autobuses y tiene una sede en Málaga y otra en Sevilla para cubrir Andalucía Oriental y Occidental respectivamente. Asimismo, tiene oficinas propias de venta y atención al cliente en las estaciones de autobuses de las principales ciudades andaluzas y opera mediante servicios auxiliares de agentes no exclusivos en las estaciones de autobuses de las localidades de menor población.

La plantilla de la empresa es de 300 personas, de las cuales 75 corresponden a personal de oficinas y 225 a personal de producción (conductores, mecánicos, mantenimiento, etc…)

2.2. EVOLUCIÓN DE LOS SISTEMAS DE INFORMACIÓN

La empresa comenzó su informatización en los años 80 utilizando aplicaciones a medida que fueron desarrolladas por una empresa local. Posteriormente se creó el departamento de informática en la empresa tanto para controlar el desarrollo externalizado como para al mismo tiempo desarrollar y ampliar la aplicación de gestión adaptándola a las nuevas necesidades del negocio.

La primera decisión importante se tuvo que tomar a finales de los años 90 ya que la aplicación a medida que se utilizaba no estaba preparada para el año 2000. Además, también era necesario tener en cuenta la entrada del EURO.

- Las opciones eran si se procedía a modificar y adaptar la aplicación que se utilizaba o por otro lado se optaba a implantar un paquete. Una vez analizados ventajas e inconvenientes de ambas soluciones, así como los costes de modificación por un lado y los costes de implantación por otro, la empresa decide migrar todas sus aplicaciones a medidas a un paquete informático. Entre los paquetes existentes en el mercado se tomó la decisión de implantar SAP/R3 como sistema de gestión empresarial ya que permitía futuras evoluciones, además de ser un sistema parametrizable y adaptable a cualquier empresa y por otro lado, también permitía mediante el lenguaje de programación propio, Abap/IV, desarrollar de forma integrada las partes que fueran necesarias para completar las necesidades del negocio.

La segunda decisión importante que se tuvo que tomar una vez pasado los periodos de adaptación al nuevo ERP y la posterior entrada del Euro y una vez recuperados de la inversión realizada, fue la presencia en Internet, tanto orientada a la venta de

billetes para el transporte regular como a la contratación de paquetes de viajes turísticos de transporte discrecional.

- Las opciones eran igualmente si se utilizaban las extensiones de SAP para el comercio electrónico (paquetes estándares) o por el contrario se decidía desarrollar un portal propio. Además, se tenía que tener en cuenta que había incentivos y subvenciones para el desarrollo de Software Libre. En este caso, se optó por contratar el desarrollo de un portal a una empresa con la condición que tenía que estar conectado al sistema SAP de la empresa utilizando las API.

Por último, en el año 2012 han modernizado el sistema de control de billetes de los autobuses y han incorporado un sistema de gestión de flotas por GPS. El sistema, denominado ÚltimaGPS, ha sido comprado a una empresa local y está basado en dispositivos móviles que utilizan HTML5 y un servicio web para el envío de datos y comprobación de los billetes expedidos. El sistema permite que en caso de que no haya conexión entre el dispositivo móvil y el servicio web, la información se almacene en el dispositivo hasta que se reestablezca la conexión y pueda enviar y comprobar los datos. Las funciones de la aplicación ÚltimaGPS son las siguientes:

- El conductor tiene que autenticarse e incluir el número de autobús en el dispositivo móvil.
- Envío al servicio web asociado de la ruta que realiza el autobús (envío de parámetros GPS).
- Envío de los billetes expedidos en el propio autobús.
- Envío de las lecturas de los billetes de los pasajeros que han realizado la compra por Internet o en las taquillas de las estaciones de autobuses.

2.2.1. INFRAESTRUCTURA INFORMÁTICA

En cuanto a la infraestructura informática, la gerencia de la empresa estableció en su momento la estrategia de tener todos los sistemas y servidores en sus propias instalaciones, por lo que la empresa tiene un Centro de Proceso de Datos propio donde alberga a sus servidores.

2.2.2. ESTRUCTURA DE PERSONAL DE INFORMÁTICA

Para dar soporte informático, la empresa cuenta con 5 personas en plantilla más servicios subcontratados.

El personal de plantilla está compuesto por:

- Responsable del Departamento de Informática. Es el responsable de seguridad de protección de datos de la empresa y además posee conocimientos técnicos por lo que da soporte tanto a tareas de desarrollo como de administración de sistemas. Además, gestiona los contratos de prestación de servicios con los proveedores.
- Mantenimiento y desarrollo. Realiza el mantenimiento y algunas modificaciones al sistema SAP. Coordina las relaciones con los proveedores de las aplicaciones a nivel técnico (aplicación de comercio electrónico y ÚltimaGPS).
- Administración de sistemas. Realiza administración de los servidores y de la red y gestiona las relaciones con los proveedores de comunicaciones a nivel técnico.
- Soporte. Dos personas para realizar las tareas de soporte y administración a nivel básico. Asimismo, también realizan las tareas de revisión y control.

2.3. SITUACIÓN ACTUAL DE LOS SISTEMAS DE INFORMACIÓN

A continuación se identifican los sistemas de información utilizados en la empresa, diferenciados en:

- Aplicaciones utilizadas.
- Infraestructura informática.
- Infraestructura de comunicaciones.
- Infraestructura de seguridad.

2.3.1. APLICACIONES

Se utilizan las siguientes aplicaciones:

- SAP/R3 para la gestión empresarial. Tienen implantados los siguientes módulos: Finanzas, Gestión de Costes, Manejo de Materiales, Gestión de Clientes, Gestión de Servicios y Gestión de Mantenimiento.
- Portal de Internet. Para la gestión de las ventas de billetes y paquetes turísticos.
- Aplicación ÚltimaGPS para el control de flotas y el control de los billetes y pasajeros que utilizan el autobús.
- Aplicación para control de presencia y control de los turnos de los trabajadores.
- Aplicaciones ofimáticas.
- Correo electrónico basado en protocolo POP-3 y SMTP.
- La empresa actualmente envía las comunicaciones comerciales utilizando una cuenta de correo electrónico del departamento comercial pero no tiene una aplicación para gestionar los envíos comerciales.

2.3.2. INFRAESTRUCTURA INFORMÁTICA

La infraestructura informática se compone de los siguientes elementos:

- La empresa tiene implantado el Directorio Activo de Windows para gestionar de forma centralizada a los usuarios. Para ello dispone de un servidor con Windows 2008 en la sede de Málaga y un servidor con Windows 2008 en la sede de Sevilla.
    - Los Servidores hacen la función de servidor de ficheros y aplicaciones de usuarios.
    - Todos los PC están incorporados al directorio activo y los usuarios se tienen que autenticar en el directorio activo para poder acceder a los recursos compartidos de los servidores. Los usuarios guardan toda la información en los servidores de ficheros, pudiendo guardar información temporal en los PC de usuarios.
- PC de usuarios con Windows XP y Windows 7. Los equipos de atención al público están dotados de SAI individuales.
- PC Portátiles.
- Dispositivos móviles ubicados en los autobuses para el control de la ruta GPS y expedición y control de billetes y pasajeros.

- 1 Servidor con Linux CentOS, servicio web y base de datos MySQL para la recolección de los datos de GPS y los datos para la expedición de tickets y control de pasajeros.
- 3 servidores con Windows 2008 para el sistema SAP/R3: uno para el entorno de producción, otro para el entorno de pruebas y otro para el entorno de desarrollo y parametrización.
- 1 Servidor con Linux CentOS para el servidor de correo electrónico de la empresa con sistema antivirus y antispam.
- 1 Servidor con Linux CentOS para el servidor de DNS y MX Relay.
- 2 Servidores con la distribución de Linux CentOS donde está la aplicación portal. Están configurados para funcionar de forma balanceada.

2.3.3. INFRAESTRUCTURA DE COMUNICACIONES

La infraestructura de comunicaciones se compone de los siguientes elementos:

- Sistema de comunicaciones con centralita de VozIP.
- Acceso a Internet contratado con una empresa comunicaciones de 10 Mb simétricos.
- Acceso mediante VPN desde los distintos puntos de acceso.
- Armario rack de comunicaciones con switches gestionables.

2.3.4. INFRAESTRUCTURA DE SEGURIDAD LÓGICA

La infraestructura de seguridad de la empresa se compone de los siguientes elementos:

- 1 cortafuegos Checkpoint en la sede de Málaga.
- 1 cortafuegos Linksys en la sede de Sevilla para realizar la conexión VPN con la sede principal.
- Antivirus en todos los puestos de trabajo.
- 1 servidor con Linux CentOS que funciona como servidor Proxy para el acceso a Internet y que tiene control de páginas prohibidas.

2.3.5. INFRAESTRUCTURA DE SEGURIDAD FÍSICA

La infraestructura de seguridad física de la empresa se compone de lo siguiente:

- Control de acceso a las instalaciones con guardia de seguridad y que cuenta con las cámaras de videovigilancia del edificio.
- Zona de archivo dotada de puerta de acceso con cerradura.
- Centro de Proceso de Datos con suelo técnico, sistema de climatización y de control de humedad y sistema automático de detección y extinción de incendios por CO2 y sistema de alimentación ininterrumpida (SAI). El acceso se realiza mediante puerta cerrada con llave. La sala tiene instalada una cámara de videovigilancia que está monitorizada en la sala de control de videovigilancia.
- Rack con cerradura con llave para el servidor y las comunicaciones de la sede de Sevilla.

- 1 servidor con Linux CentOS que funciona como servidor Proxy para el acceso a Internet y que tiene habilitado lista de páginas restringidas.
- Sistema de videovigilancia.

2.3.6. ESQUEMA DE LA RED Y DE LA INFRAESTRUCTURA INFORMÁTICA

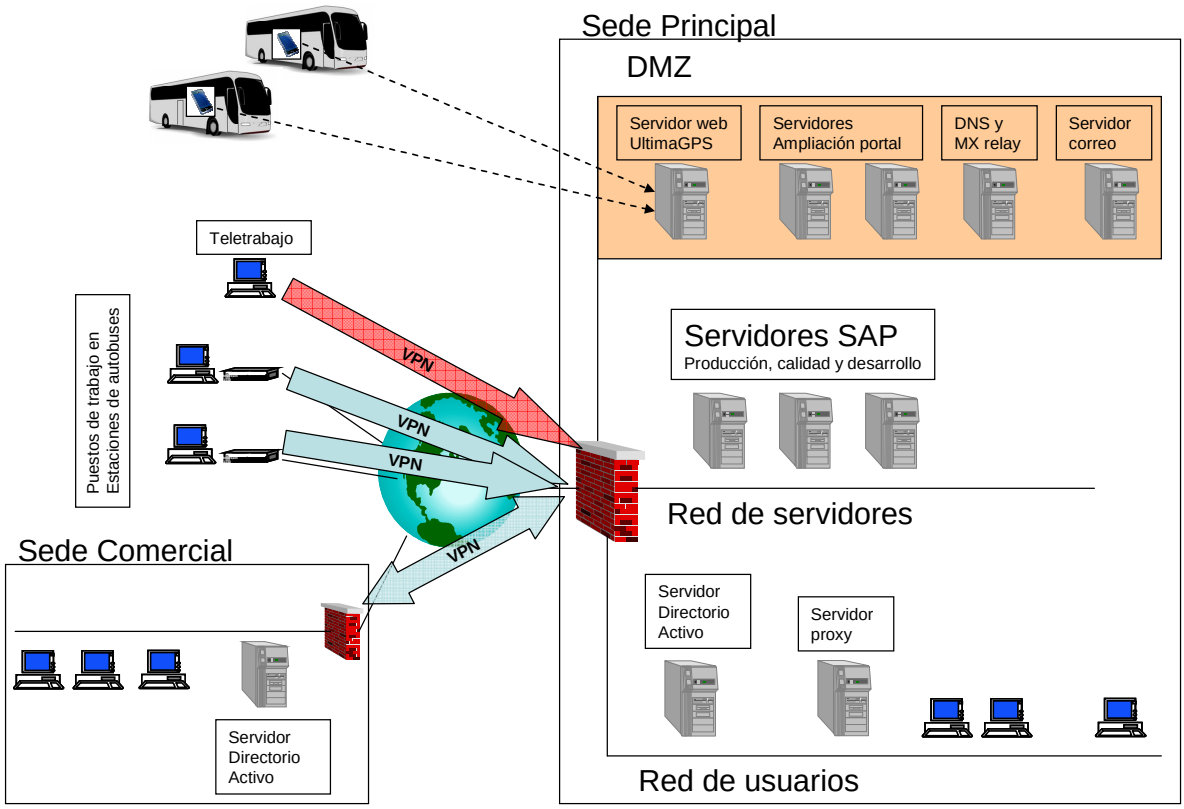

Figura 1: Esquema de la infraestructura informática y de comunicaciones de la empresa

2.4. ORGANIZACIÓN DE LA EMPRESA

La empresa tiene la siguiente organización interna:

- Dirección General
  - Dirección Financiera
    - Departamento de Contabilidad y Finanzas.
    - Departamento de Recursos Humanos.
    - Departamento de Sistemas de Información.
      - Mantenimiento y desarrollo.
      - Administración de Sistemas.
      - Soporte.
  - Dirección Comercial
    - Departamento Comercial.
      - Sede en Málaga.
      - Sede en Sevilla.
    - Departamento de Ventas.

- Departamento de Atención a Clientes.
  - Call Center.
- Gestión de la Calidad.

o Dirección de la Producción

- Gestión Logística.
- Gestión de Almacenes.
- Gestión de Talleres.

2.4.1 ORGANIGRAMA

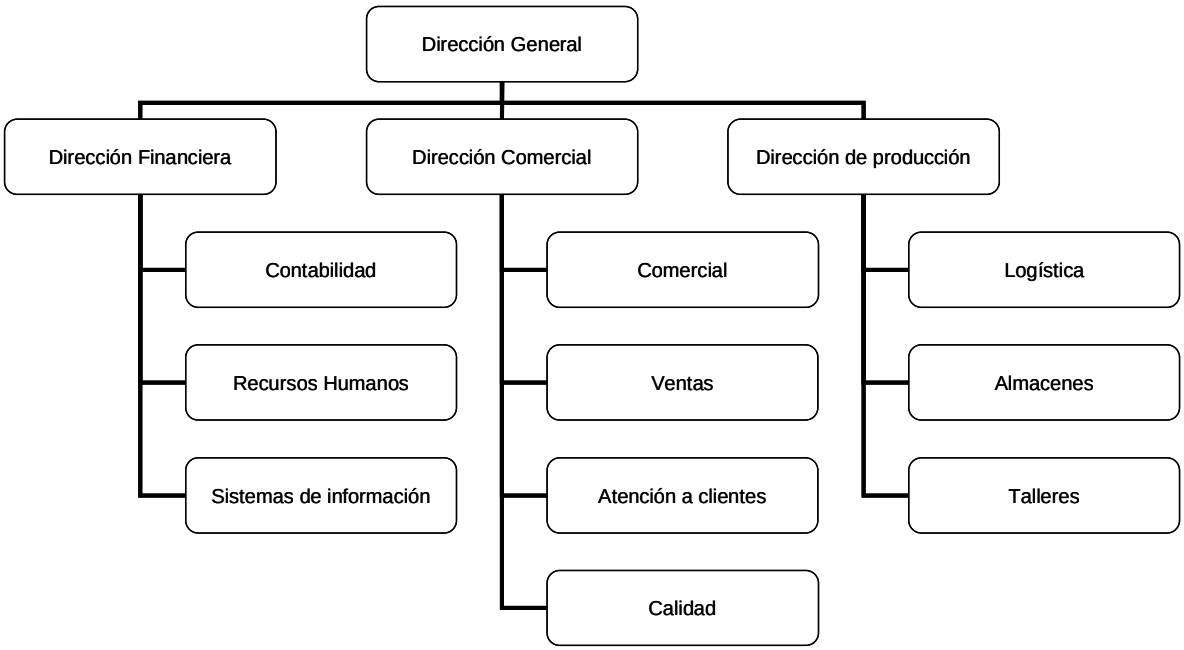

Figura 2: Estructura organizativa de la empresa

2.4.2 SERVICIOS SUBCONTRATADOS

Por otro lado, la empresa tiene subcontratados los siguientes servicios:

- Servicios de asesoría jurídica ante reclamaciones de clientes.
- Asesoría laboral para la gestión de la nómina.
- Servicio de prevención de riesgos laborales y vigilancia de la salud.
- Servicios de administración de los servidores y de la seguridad informática de la empresa.

2.5. SISTEMAS DE GESTIÓN Y CONTROL DE LA EMPRESA

La empresa tiene implantados los sistemas de gestión de la calidad ISO 9001 y los sistemas de gestión medioambiental ISO 14001.

Por otro lado está sometida a las auditorías de cuentas anuales.

Respecto a la LOPD, la empresa tiene inscritos sus ficheros, cuenta con un documento de seguridad, está nombrado el responsable de seguridad y realiza las

auditorías cada dos años. Para mejorar la gestión de la protección de datos, se ha integrado con el sistema de gestión de la calidad, de esta forma las incidencias de seguridad y las acciones de mejora y las no conformidades detectadas en las auditorías de protección de datos se gestionan dentro del sistema de gestión de la calidad garantizándose el seguimiento de las mismas de forma integrada.

3. DEFINICIÓN DE LOS OBJETIVOS

Actualmente la empresa se encuentra en un momento en que ha dejado de ser pequeña y por tanto ha pasado a ser atractiva a posibles ataques y denuncias, por lo que se ha comenzado a exponer a riesgos que antes eran insignificantes.

Por un lado, ha comenzado a sufrir si bien no de forma continuada, sí con más frecuencia de la que sería deseable, una serie de ataques en su servicio web que en algunos casos llegaron a producir la denegación del servicio. La empresa que tiene subcontratado los servicios de seguridad ha informado que habría que mejorar las medidas de seguridad como podrían ser incluir sistemas de detección y de prevención de intrusos, aumentar el ancho de banda y el número de servidores, etc… lo que supondría realizar inversión en infraestructura de seguridad.

Por otro lado, se ha producido últimamente una serie de quejas de clientes que han recibido de forma errónea las comunicaciones comerciales de la empresa, ya que según se hacía constar en las quejas realizadas por los mismos, en algunos casos los clientes no habían autorizado a la empresa a que se le enviara información comercial y en otros casos se habían dado de baja de las comunicaciones comerciales y sin bien durante un tiempo no las recibieron, ahora han vuelto a recibirlas. Analizado el caso, se ha observado que ha sido debido a cambios de personal del Departamento Comercial con insuficiente formación y también debido a que existe una deficiente gestión de la seguridad en las comunicaciones comerciales.

La empresa ha decidido que de forma previa a realizar inversiones, quiere conocer y cuantificar todos los riesgos de seguridad a los que está expuesto de forma que pueda tomar decisiones basándose en dichos datos y analizar distintas alternativas que se puedan llevar a cabo. Para ello ha decidido implantar un SGSI basado en la norma ISO 27001:2005.

Aunque la empresa que presta los servicios de administración y mantenimiento de los servidores y de la seguridad les ha ofrecido los servicios de consultoría, formación e implantación del SGSI, la empresa ha decidido utilizar los servicios de una consultora independiente.

Los principales objetivos que actualmente preocupan a la empresa y que se deben tener en cuenta el Plan Director de Seguridad son los siguientes:

1. Ofrecer un servicio web a los clientes de forma segura y fiable y con un nivel de servicio mayor del 99,99%.
2. Garantizar el cumplimiento de la legislación vigente que se le aplique a la empresa en materia de protección de datos y de comercio electrónico.
3. Analizar los costes de seguridad de forma que se puedan asumir por la organización teniendo en cuenta los riesgos de seguridad a los que está expuesta.
4. Garantizar la continuidad del negocio y de sus sistemas de información. Asimismo, minimizar los impactos ante incidentes de seguridad y garantizar la correcta reacción y resolución de problemas en tiempos aceptables.
5. Mejorar la imagen de la organización hacia sus clientes garantizando la seguridad de la información a través de un Sistema de Gestión.

4. ANÁLISIS DIFERENCIAL

A continuación se va a proceder a realizar un análisis diferencial (GAP analysis) respecto a cómo la empresa se encuentra en relación a las normas de referencia que pretende implantar. Por tanto, se va a analizar el nivel de cumplimiento de la empresa respecto a la ISO 27001 y a la ISO 27002.

Para determinar el nivel de cumplimiento respecto a cada requisito de la norma ISO 27001 o respecto a cada control de la norma ISO 27002 se va a utilizar la siguiente nomenclatura:

- SI: cumple totalmente con el requisito.
- NO: incumple totalmente con el requisito.
- PARCIAL: cumple parcialmente con el requisito.
- N/A: No es de aplicación el control o no está aplicado en el momento del análisis diferencial.

4.1. ANÁLISIS DIFERENCIAL RESPECTO A LA ISO 27001

A continuación se detalla, de acuerdo con la nomenclatura anteriormente citada, el nivel de cumplimiento de la organización respecto a la norma ISO 27001.

Observaciones: La empresa va a comenzar a implantar un SGSI, por lo que actualmente solamente tiene el compromiso de la Dirección para la implantación del sistema.

REQUISITO	NIVEL CUMPL.	OBSERVACIONES
4.1 Requisitos generales	**NO**	
4.2 CREACIÓN Y GESTIÓN DEL SGSI		
4.2.1 Creación del SGSI	**NO**	
4.2.2 Implantar y operar el SGSI	**NO**	
4.2.3 Supervisión y revisión del SGSI	**NO**	
4.2.4 Mantener y mejorar el SGSI	**NO**	
4.3 REQUISITOS DE LA DOCUMENTACIÓN		
4.3.1 Generalidades	**NO**	
4.3.2 Control de documentos	**NO**	
4.3.3 Control de registros	**NO**	
5 RESPONSABILIDAD DE LA DIRECCIÓN		
5.1 Compromiso de la Dirección	**PARCIAL**	La Dirección ha impulsado y aprobado el proyecto para la implantación de un SGSI basado en la norma ISO 27001
5.2 GESTIÓN DE LOS RECURSOS		

5.2.1 Provisión de los recursos	**PARCIAL**	La Dirección ha aprobado el presupuesto para la implantación del SGSI.
5.2.2 Concienciación, formación y capacitación	**PARCIAL**	La Dirección ha establecido con el departamento de RR.HH. el plan de formación de las personas involucradas dentro de la organización en la gestión del SGSI.
6 AUDITORÍAS INTERNAS DEL SGSI		
6 Auditorias internas	**PARCIAL**	Se está realizando la primera auditoría del SGSI. Sin embargo, tiene un carácter de análisis de situación respecto a la norma ya que no existe documentación de la misma.
7 REVISIÓN DEL SGSI POR LA DIRECCIÓN		
7.1 Generalidades	**NO**	
7.2 Datos iniciales de la revisión	**NO**	
7.3 Resultados de la revisión	**NO**	
8 MEJORA DEL SGSI		
8.1 Mejora continua	**NO**	
8.2 Acción correctiva	**PARCIAL**	Existen acciones correctivas respecto a incidencias y no conformidades detectadas en las auditorías de protección de datos y que se gestionan mediante el procedimiento de revisión establecido.
8.3 Acción preventiva	**NO**	

4.2. ANÁLISIS DIFERENCIAL RESPECTO A LA ISO 27002

A continuación se detalla, de acuerdo con la nomenclatura anteriormente citada, el nivel de cumplimiento de la organización respecto a la norma ISO 27002.

REQUISITO	NIVEL CUMPL.	OBSERVACIONES
A.5 POLÍTICA DE SEGURIDAD **A.5.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**		
5.1.1 Doc. de política de S. I.	**NO**	No está definida la política de S.I.
5.1.2 Revisión de la política de S.I.	**NO**	No está definida la política de S.I.
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN **A.6.1 ORGANIZACIÓN INTERNA**		
6.1.1. Compromiso de la Dirección con la S.I.	**SI**	Existe un compromiso de la Dirección en la implantación de un SGSI.
6.1.2 Coordinación de la S. I.	**PARCIAL**	Existen funciones definidas de seguridad pero se deben redefinir de cara a la implantación del SGSI.
6.1.3 Asignación de responsabilidades relativas a la S.I.	**NO**	No están definidas las responsabilidades de acuerdo a la política de S.I. ya que la misma no está definida ni aprobada

6.1.4 Proceso de autorización de recursos para el tratamiento de la información.	**PARCIAL**	No está definido según la norma SGSI pero existe un procedimiento en la empresa para la aprobación de cualquier tipo de recurso incluidos los de tratamiento de la información
6.1.5 Acuerdos de confidencialidad	**SI**	Todos los trabajadores y personal externo tienen firmado un acuerdo de confidencialidad para proteger información de la empresa y los datos de carácter personal.
6.1.6 Contacto con las autoridades	**SI**	Existe una circular de la empresa donde se informa a los trabajadores de los números de emergencia y los números de teléfono de contacto que deben ser conocidos por todos los trabajadores.
6.1.7 Contacto con grupos de especial interés	**SI**	El responsable de seguridad está suscrito a las listas de distribución que envía INTECO.
6.1.8 Revisión independiente de la S.I.	**PARCIAL**	Se realizan auditorías de protección de datos cada dos años y se está realizando la primera auditoría de la Seguridad conforme a la norma ISO 27002.
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN **A.6.2. TERCEROS**		
6.2.1 Identificación de los riesgos derivados del acceso de terceros	**PARCIAL**	Se han analizado de forma general los riesgos derivados de los prestadores de servicios que tratan información, datos y la seguridad de la organización.
6.2.2 Tratamiento de la seguridad en la relación con clientes	**PARCIAL**	Está definido de forma general en el Documento de Seguridad de la Organización.
6.2.3 Tratamiento de la seguridad en contratos con terceros	**SI**	Existen contratos de confidencialidad con todos los proveedores.
A.7 GESTIÓN DE ACTIVOS **A.7.1 RESPONSABILIDAD SOBRE LOS ACTIVOS**		
7.1.1 Inventario de activos	**PARCIAL**	Existe el inventario de servidores pero no está incluido el inventario completo de todos los activos de la organización.
7.1.2 Propiedad de los activos	**NO**	No están asignados los propietarios de los activos.
7.1.3 Uso aceptable de los activos	**SI**	Existe un documento de funciones y obligaciones del personal en el que se establece la normativa para el uso de los recursos de la organización.
A.7 GESTIÓN DE ACTIVOS **A.7.2 CLASIFICACIÓN DE LA INFORMACIÓN**		
7.2.1 Directrices de clasificación	**NO**	No está clasificada la información que existe en la empresa.
7.2.2 Etiquetado y manipulado de la Inf.	**NO**	No está clasificada la información que existe en la empresa.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS **A.8.1 ANTES DEL EMPLEO**		
8.1.1 Funciones y responsabilidades	**SI**	Todo el personal tiene conocimiento de sus funciones u obligaciones en el tratamiento de la información y los datos personales. Existe un documento que está en la intranet y es accesible y se ha distribuido entre todos los trabajadores.

8.1.2 Investigación de antecedentes	**SI**	Existe un procedimiento para identificar que los candidatos cumplen los requisitos del puesto y tienen las titulaciones establecidas. Por otro lado, el proceso de selección de personal se basa siempre en la contratación de personal en prácticas de forma previa a su contratación definitiva, por lo que todo el personal de la empresa ha pasado por un proceso de prácticas previo a su contratación.
8.1.3 Términos y condiciones de contratación	**SI**	Todos los trabajadores deben firmar un acuerdo de confidencialidad y se le entrega el documento de funciones y obligaciones del personal en el momento de la firma del contrato.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS **A.8.2 DURANTE EL EMPLEO**		
8.2.1 Responsabilidades de la Dirección	**PARCIAL**	En el documento de seguridad está establecido que todos los proveedores y el personal deben comprometerse con la seguridad de la información y la protección de los datos de carácter personal
8.2.2 Concienciación, formación y capacitación en S. I.	**PARCIAL**	Los trabajadores están informados de sus funciones y obligaciones y se realizan planes de formación orientados actualmente a la protección de datos. Se ha establecido un plan de formación para los trabajadores en seguridad de la información pero todavía no se ha llevado a cabo.
8.2.3 Proceso disciplinario	**SI**	Está definido en el documento de seguridad y en el documento de funciones y obligaciones del personal que es conocido por los trabajadores
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS **A.8.3 CESE DEL EMPLEO O CAMBIO DE PUESTO DE TRABAJO**		
8.3.1 Responsabilidad del cese o cambio	**SI**	Están establecidos los procedimientos en el documento de seguridad de la organización.
8.3.2 Devolución de activos	**SI**	Están establecidos los procedimientos en el documento de seguridad de la organización.
8.3.3 Retirada de los derechos de acceso	**SI**	Están establecidos los procedimientos en el documento de seguridad de la organización.
A.9 SEGURIDAD FÍSICA Y AMBIENTAL **A.9.1 ÁREAS SEGURAS**		
9.1.1 Perímetro de seguridad física	**SI**	Existen controles de accesos tanto a las instalaciones como a las zonas de acceso restringido (CPD, archivo, etc…).
9.1.2 Controles físicos de entrada	**SI**	Existe un control a la entrada del edificio y todas las personas que van a acceder se deben identificar.
9.1.3 Seguridad de oficinas, despachos e instalaciones	**SI**	Existe control de acceso a las oficinas.
9.1.4 Protección de amenazas externas y de origen ambiental	**SI**	El CPD está dotado de sistemas de prevención y extinción de incendios. No está en zona de aguas.
9.1.5 Trabajo en áreas seguras	**SI**	En las oficinas el acceso está controlado.
9.1.6 Áreas de acceso público, y de carga y descarga	**SI**	Están establecidas las zonas de carga y descarga de proveedores y de material logístico y de reparaciones en zonas donde no existe información
A.9 SEGURIDAD FÍSICA Y AMBIENTAL **A.9.2 SEGURIDAD DE LOS EQUIPOS**		

9.2.1 Emplazamiento y protección de equipos	**SI**	Los servidores están instalados en zona de acceso restringido. Los equipos del personal que atiende al público están dotados de pantalla con filtros de privacidad.
9.2.2 Instalaciones de Suministro	**SI**	El CPD está dotado de SAI. Los equipos en los periféricos tienen un pequeño SAI.
9.2.3 Seguridad del cableado	**SI**	El sistema de cableado de las oficinas no está en zonas públicas ni accesibles por personal no autorizado
9.2.4 Mantenimiento de los equipos	**SI**	Los servidores (equipos críticos) tienen contrato de mantenimiento con los fabricantes.
9.2.5 Seguridad de los equipos fuera de las instalaciones	**PARCIAL**	Existen normas pero no siempre se llevan a la práctica.
9.2.6 Reutilización o retirada segura de equipos	**SI**	Está establecido el procedimiento tanto en el documento de seguridad como en los manuales de operación del departamento de sistemas de información.
9.2.7 Retirada de materiales propiedad de la empresa	**SI**	Está establecido el procedimiento tanto en el documento de seguridad como en los manuales de operación del departamento de sistemas de información.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN		
10.1.1 Documentación de los procedimientos de operación	**SI**	Existen procedimientos de explotación y operación de los sistemas en el departamento de sistemas de información.
10.1.2 Gestión de cambios	**SI**	El propio sistema SAP/R3 lleva un control de los cambios mediante el sistema de gestión propio de SAP.
10.1.3 Segregación de tareas	**PARCIAL**	Aunque existe el procedimiento de entrada en producción, existen ocasiones en los que por urgencia no se cumplen dichos procedimientos. De hecho esta circunstancia ha provocado en determinados casos un incidente de seguridad que ha hecho necesario restaurar el sistema.
10.1.4 Separación de los recursos de desarrollo, prueba y operación	**SI**	El sistema SAP está dotado de 3 servidores completamente separados para desarrollo, pruebas y producción. En el caso del servicio web, las modificaciones se prueban en un entorno virtual de pruebas dentro del Departamento de Informática.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS		
10.2.1 Provisión de servicios	**NO**	Existen contratos de prestación de servicios y se incluyen en los mismos las obligaciones de seguridad, pero no se están comprobando.
10.2.2 Supervisión y revisión de los servicios prestados por terceros	**NO**	No se están auditando los servicios que son prestados por terceros.
10.2.3 Gestión del cambios en los servicios prestados por terceros	**NO**	No se está llevando un control de los cambios en los servicios prestados por terceros.

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.3 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA		
10.3.1 Gestión de capacidades	**NO**	No existen controles de detección de posibles problemas de capacidades.
10.3.2 Aceptación del sistema	**PARCIAL**	En determinados sistemas se prueban previamente las nuevas versiones, pero en determinados casos, se instalan nuevas versiones sin probarlas previamente.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.4 PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y DESCARGABLE		
10.4.1 Controles contra el código malicioso	**SI**	Existen antivirus instalados en todos los ordenadores y están actualizados.
10.4.2 Controles contra el código descargado en el cliente	**SI**	Los usuarios no pueden instalar aplicaciones en sus ordenadores ya que no tienen privilegios de administración en sus equipos. Cualquier instalación debe ser realizada por el Departamento de Informática.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.5 COPIAS DE SEGURIDAD		
10.5.1 Copias de Seguridad de la Información.	**PARCIAL**	Se realizan copias de seguridad de las aplicaciones y bases de datos instaladas en los servidores. Asimismo, se realizan restauraciones (copias homogéneas) del sistema SAP en el entorno de calidad cada 3 meses. No se están realizando copias de seguridad de los buzones de correo de los usuarios. Depende de los usuarios que copien sus buzones en el servidor de ficheros que sí está sujeto a copias de seguridad. Esto ha provocado que determinados usuarios hayan perdido todos sus correos electrónicos.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.6 GESTIÓN DE LA SEGURIDAD DE LAS REDES		
10.6.1 Controles de red	**PARCIAL**	Los sistemas permiten gestión pero no se están monitorizando las actividades de la red.
10.6.2 Seguridad de los servicios de red	**PARCIAL**	No se están monitorizando los servicios de red.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.7 MANIPULACIÓN DE LOS SOPORTES		
10.7.1 Gestión de soportes extraíbles	**NO**	Solamente existen procedimientos organizativos pero no se impide físicamente que el personal pueda instalar soportes extraíbles.
10.7.2 Retirada de soportes	**NO**	Cualquiera puede utilizar un pendrive.
10.7.3 Procedimientos de manipulación de la Información.	**NO**	Cualquiera puede utilizar un pendrive.
10.7.4 Seguridad de la documentación del sistema	**SI**	Toda la documentación de los sistemas de información está custodiada en armarios dotados de cerradura en el Departamento de Sistemas de Información.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.8 INTERCAMBIO DE INFORMACIÓN		

10.8.1 Políticas y procedimientos de intercambios de información	**SI**	Está establecido el procedimiento para el envío de la información a las empresas que prestan servicios. Existen procedimientos de intercambios con los bancos para el pago del comercio electrónico.
10.8.2 Acuerdos de intercambio	**SI**	Existe un contrato con el banco para los medios de pago en el sistema de comercio electrónico.
10.8.3 Soportes físicos en transito	**N/A**	
10.8.4 Mensajería electrónica	**PARCIAL**	No toda la información que se envía por correo electrónico mantiene unos correctos niveles de seguridad. Está establecido el procedimiento en el documento de seguridad pero no se cumple por todos los usuarios.
10.8.5 Sistemas de información empresariales	**SI**	Toda la información empresarial se encuentra en SAP que está dotado de los controles de acceso por niveles de privilegios de usuarios.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.9 SERVICIOS DE COMERCIO ELECTRÓNICO**		
10.9.1 Comercio electrónico	**SI**	Existe una aplicación para la gestión de la venta de billetes y compra de paquetes. El acceso se realiza mediante protocolo seguro https, los usuarios deben autenticarse para poder realizar las compras y existe una pasarela de pago con el banco.
10.9.2 Transacciones en línea	**SI**	Está establecido un protocolo con el banco que realiza la pasarela de pago y a la aplicación solamente se le informa que el pago es correcto o incorrecto.
10.9.3 Información públicamente disponible	**SI**	La información que se expone públicamente debe estar previamente aprobada por el responsable.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.10 SUPERVISIÓN**		
10.10.1 Registro de auditorias	**PARCIAL**	Existen registros de auditorías en los distintos sistemas pero algunos no están configurados correctamente y no recogen la información necesaria.
10.10.2 Supervisión del uso del sistema	**NO**	No se están revisando los registros de los sistemas ni comprobando los accesos realizados.
10.10.3 Protección de la información de los registros	**SI**	A los registros del sistema solamente accede el personal autorizado.
10.10.4 Registros de administración y operación	**NO**	No están activadas las auditorías de registro de acceso en todos los sistemas.
10.10.5 Registro de fallos	**NO**	No se está analizando el visor de sucesos.
10.10.6 Sincronización del reloj	**NO**	No está establecida la sincronización del reloj por directivas de seguridad. Depende de cada PC de usuario.
A.11 CONTROL DE ACCESO **A.11.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO**		
11.1.1 Política de control de acceso	**SI**	Está establecida en el documento de seguridad.
A.11 CONTROL DE ACCESO **A.11.2 GESTIÓN DE ACCESO DE USUARIO**		

11.2.1 Registro de usuario	**SI**	El procedimiento está establecido en el documento de seguridad. En el Departamento de Informática se lleva un registro de todas las peticiones y autorizaciones.
11.2.2 Gestión de privilegios	**SI**	El procedimiento está establecido en el documento de seguridad. En el Departamento de Informática se lleva un registro de todas las peticiones y autorizaciones.
11.2.3 Gestión de contraseñas de usuario	**SI**	Los usuarios conocen sus obligaciones respecto a la contraseña ya que están descritas en el documento de funciones y obligaciones del personal. Además, la contraseña que se asigna debe ser cambiada por el usuario la primera vez que entra al sistema.
11.2.4 Revisión de los derechos de acceso a usuario	**NO**	Aunque el documento de seguridad establece la obligación, no se están realizando las revisiones de los derechos de acceso ya que si bien técnicamente es posible, requiere la colaboración del responsable de activo/fichero que no siempre se lleva a cabo.
A.11 CONTROL DE ACCESO **A.11.3 RESPONSABILIDADES DE USUARIO**		
11.3.1 Uso de contraseña	**NO**	Aunque el sistema obliga a contraseñas que estén compuestas por números y letras y que tengan más de 7 caracteres, se ha comprobado que los usuarios tienen contraseñas fácilmente descifrables.
11.3.2 Equipo de usuarios desatendido	**SI**	Los equipos tienen activadas por directivas de seguridad el bloqueo de la pantalla a los 20 minutos de inactividad. Igualmente las aplicaciones tienen activada el bloqueo del usuario por inactividad.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia	**NO**	Aunque la organización está haciendo un esfuerzo, aun no se ha conseguido implantar la política de puesto de despejado.
A.11 CONTROL DE ACCESO **A.11.4 CONTROL DE ACCESO A LA RED**		
11.4.1 Política de uso de los servicios en red	**SI**	Los usuarios tienen acceso solamente a los recursos que les son necesarios. Existe un Proxy que impide el acceso a páginas y servicios no deseados.
11.4.2 Autenticación de usuario para conexiones externas	**SI**	Las conexiones remotas se tienen que realizar mediante VPN y los usuarios se deben autenticar previamente a poder realizar la conexión.
11.4.3 Identificación de los equipos en las redes	**N/A**	
11.4.4 Diagnóstico remoto y protección de los puertos de configuración	**SI**	Los puertos de diagnostico remoto solamente están habilitados de forma interna.
11.4.5 Segregación de las redes	**SI**	Existe un cortafuego con distintas DMZ que permite la segregación de las distintas redes.
11.4.6 Control de la conexión a la red	**SI**	El acceso de los usuarios mediante VPN se realiza de acuerdo con los niveles de aprobación que han sido otorgados a cada usuario.
11.4.7 Control de encaminamiento (routing) de red	**SI**	El servicio está externalizado con el proveedor de servicios de Internet.

A.11 CONTROL DE ACCESO **A.11.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO**		
11.5.1 Procedimientos seguros de inicio de sesión	**SI**	Está restringido sólo a los administradores de sistema. Los usuarios no tienen privilegios de administración en sus equipos.
11.5.2 Identificación y autenticación de usuario	**NO**	Se utiliza normalmente la cuenta administrador y no se tienen creados usuarios administradores personalizados.
11.5.3 Sistema de gestión de contraseñas	**SI**	Las contraseñas de administración son complejas y se cambian cada 30 días.
11.5.4 Uso de los recursos del sistema	**SI**	Está restringido solo a los administradores de sistema
11.5.5 Desconexión automática de sesión	**SI**	Los sistemas cierran la sesión a los 20 minutos de inactividad.
11.5.6 Limitación del tiempo de conexión	**NO**	No está habilitado un tiempo de conexión.
A.11 CONTROL DE ACCESO **A.11.6 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN**		
11.6.1 Restricción del acceso a la información	**SI**	Cada usuario tiene un perfil de acceso específico según su nivel de autorización.
11.6.2 Aislamiento de sistemas sensibles	**N/A**	
A.11 CONTROL DE ACCESO **A.11.7 ORDENADORES PORTÁTILES Y TELETRABAJO**		
11.7.1 Ordenadores portátiles y comunicaciones móviles	**NO**	Existe una política general en el documento de seguridad pero en la práctica no se está llevando a cabo ya que depende del personal.
11.7.2 Teletrabajo	**SI**	En el documento de seguridad están definidas las personas autorizadas a realizar teletrabajo.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.1 REQUISITOS DE SEGURIDAD DE LOS S. I.**		
12.1.1 Análisis y especificación de los requerimientos de seguridad	**SI**	Se exige a los proveedores que las aplicaciones cumplan con lo establecido en la disposición adicional única respecto a productos de software establecida en el Real Decreto 1720/2007 por el que se desarrolla la LOPD.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.2 TRATAMIENTO CORRECTO DE LAS APLICACIONES**		
12.2.1 Validación de los datos de entrada	**SI**	Tanto la aplicación de gestión empresarial como la aplicación de comercio electrónico tienen controles de validación de los datos de entrada.
12.2.2 Control del procesamiento interno	**SI**	Las aplicaciones para la interconexión de los sistemas están programadas para comprobar y generar errores.
12.2.3 Integridad de los mensajes	**SI**	Las aplicaciones utilizadas para carga de datos en SAP desde fuentes externas tienen programadas un control de la integridad de la información
12.2.4 Validación de los datos de salida	**SI**	Previo a la entrada en producción de una nueva aplicación que genera información de salida, dicha información es comprobada por el responsable. Asimismo, cualquier información que se vaya a enviar fuera se comprueba que sea correcta.

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. A.12.3 CONTROLES CRIPTOGRÁFICOS		
12.3.1 Política de uso de los controles criptográficos	**NO**	Actualmente no está establecida una política de uso de la firma digital en la empresa. Se utiliza la firma electrónica de persona jurídica en el Departamento de Contabilidad y en el Departamento de Personal.
12.3.2 Gestión de claves	**SI**	La claves para el uso de la firma electrónica de la empresa está restringida sólo al personal autorizado y el certificado es custodiado y renovado por el Departamento de Informática. Asimismo, las claves tanto para la web de comercio electrónico como las utilizadas para montar la VPN entre las dos sedes están custodiadas por el Departamento de Informática.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. A.12.4 SEGURIDAD DE LOS ARCHIVOS DE SISTEMA		
12.4.1 Control del software de explotación	**SI**	Solamente los administradores del Departamento de Informática realizan las instalaciones.
12.4.2 Protección de los datos de prueba del sistema	**SI**	Se utiliza una copia completa de la aplicación SAP en el sistema de calidad para realizar las pruebas. Dichas pruebas están restringidas sólo al personal autorizado de la empresa.
12.4.3 Control de acceso al código fuente de los programas	**SI**	Solamente los programadores de SAP tienen acceso a los códigos fuentes de la aplicación. Asimismo, el código fuente de la aplicación de comercio electrónico es propiedad intelectual de la empresa y está custodiado y controlado por el Departamento de Informática.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. A.12.5 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE		
12.5.1 Procedimientos de control de cambios	**SI**	Está establecido el procedimiento de entrada en producción dentro del entorno SAP. Además, la entrada en producción de cualquier otro entorno (portal de Internet para venta de billetes) debe ser previamente probada y validada por el Departamento de Informática.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	**SI**	Previo a la entrada en producción de cualquier cambio, se procede a probar en el entorno de pruebas o calidad.
12.5.3 Restricciones a los cambios en los paquetes de software	**SI**	Se han mantenido los paquetes estándares. De hecho en SAP se ha mantenido el estándar si bien se han realizado desarrollos adicionales que no influyen en el correcto despliegue de futuras versiones.
12.5.4 Fugas de información	**SI**	Solamente se utiliza software licenciado o que están debidamente probados.
12.5.5 Externalización del desarrollo de software	**SI**	Cualquier desarrollo externo está sujeto a un contrato de prestación de servicios y a un cumplimiento y control del desarrollo por parte del Departamento de Informática y el departamento peticionario.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. A.12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA		

12.6.1 Control de las vulnerabilidades técnicas	**NO**	No se han analizados las vulnerabilidades.
A.13 GESTIÓN DE INCIDENTES DE S. I. **A.13.1 NOTIFICACIÓN DE EVENTOS Y PUNTOS DÉBILES DE S. I.**		
13.1.1 Notificación de los eventos de S. I.	**PARCIAL**	Está definida en el documento de seguridad la gestión de incidentes de seguridad.
13.1.2 Notificación de los puntos debilidades de Seguridad	**PARCIAL**	Está descrito en el documento de funciones y obligaciones del personal que cualquier incidencia de seguridad que se observe se notifique al responsable de seguridad.
A.13 GESTIÓN DE INCIDENTES DE S. I. **A.13.2 GESTIÓN DE INCIDENTES DE S. I. Y MEJORAS**		
13.2.1 Responsabilidades y procedimientos	**PARCIAL**	Está definida en el documento de seguridad la gestión de incidentes de seguridad.
13.2.2 Aprendizaje de los incidentes de S. I.	**PARCIAL**	Los incidentes de seguridad se gestionan dentro del sistema de calidad y quedan registrados por lo que existe un registro de los mismos.
13.2.3 Recopilación de evidencias	**NO**	No existe el procedimiento en el documento de seguridad.
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO **A.14.1 ASPECTOS DE S. I. EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
14.1.1 Inclusión de la S. I. en el proceso de gestión de la continuidad del negocio	**NO**	No existe actualmente un plan de continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos	**NO**	No existe actualmente un plan de continuidad del negocio.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la S. I.	**PARCIAL**	Existen algunos procedimientos aislados para el plan de continuidad de las aplicaciones de gestión empresarial SAP.
14.1.4 Marco de referencia para la planificación de la continuidad del negocio	**NO**	No existe actualmente un plan de continuidad del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	**NO**	No existe actualmente un plan de continuidad del negocio.
A.15 CUMPLIMIENTO **A.15.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES**		
15.1.1 Identificación de la legislación aplicable	**NO**	No se tiene identificada toda la legislación que es de aplicación. De hecho, la empresa no se ha adaptado todavía a la última modificación de la LSSI respecto al uso de las cookies ya que no conocía la citada modificación.
15.1.2 Derechos de propiedad intelectual	**NO**	Se ha observado que existen algunas aplicaciones que no están correctamente licenciadas.

15.1.3 Protección de los documentos de la organización	**SI**	Todos los documentos importantes de la organización están correctamente archivados.
15.1.4 Protección de datos y privacidad de la Inf. de carácter personal	**SI**	La empresa cumple con lo establecido con la legislación vigente en materia de protección de datos.
15.1.5 Prevención del uso indebido de los recursos de tratamiento de la Inf.	**SI**	Existe un documento que informa a los usuarios de la obligación de usar correctamente los recursos de la organización. Asimismo, los usuarios al no tener privilegios de administración no pueden instalar ni modificar ningún programa del ordenador.
15.1.6 Regulación de los controles criptográficos	**SI**	Se utilizan las firmas digitales de personas jurídicas y de personas físicas para los distintos trámites con las administraciones públicas. Asimismo, se utilizan para los envíos de correos electrónicos firmados y cifrados. También se utilizan para el certificado de la página web que se usa para el comercio electrónico y para la VPN que está montada para la conexión de las dos sedes.
A.15 CUMPLIMIENTO **A.15.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO**		
15.2.1 Cumplimiento de las políticas y normas de Seguridad	**NO**	Los directores no realizan comprobaciones periódicas.
15.2.2 Comprobación del cumplimiento técnico	**PARCIAL**	El sistema SAP incluye en la descripción técnica las medidas de seguridad que cumple. Las aplicaciones utilizadas para el comercio electrónico no han sido comprobadas ni se le han realizado test de penetración.
A.15 CUMPLIMIENTO **A.15.3 CONSIDERACIONES SOBRE LA AUDITORIA DE LOS S. I.**		
15.3.1 Controles de auditoría de los S. I.	**SI**	Hasta la fecha las auditorías de protección de datos se han planificado de forma que no han provocado interrupciones en el servicio.
15.3.2 Protección de las herramientas de auditoría de los S. I.	**SI**	Todas las auditorías se han realizado por personal externo y han utilizado sus propias herramientas para las pruebas. Los accesos a los sistemas se han realizado mediante usuarios controlados y creados sólo y exclusivamente para los auditores con acceso de sólo lectura a los sistemas auditados y se han bloqueado una vez finalizado su uso.

4.3. RESULTADOS DEL ANÁLISIS Y CONCLUSIONES

A continuación se muestran los resultados en modo gráfico para analizar el nivel de cumplimiento. Se puede observar que se cumple con el 56% de los controles, que no se cumple o no se aplican el 27% y existe un cumplimiento parcial del 17%.

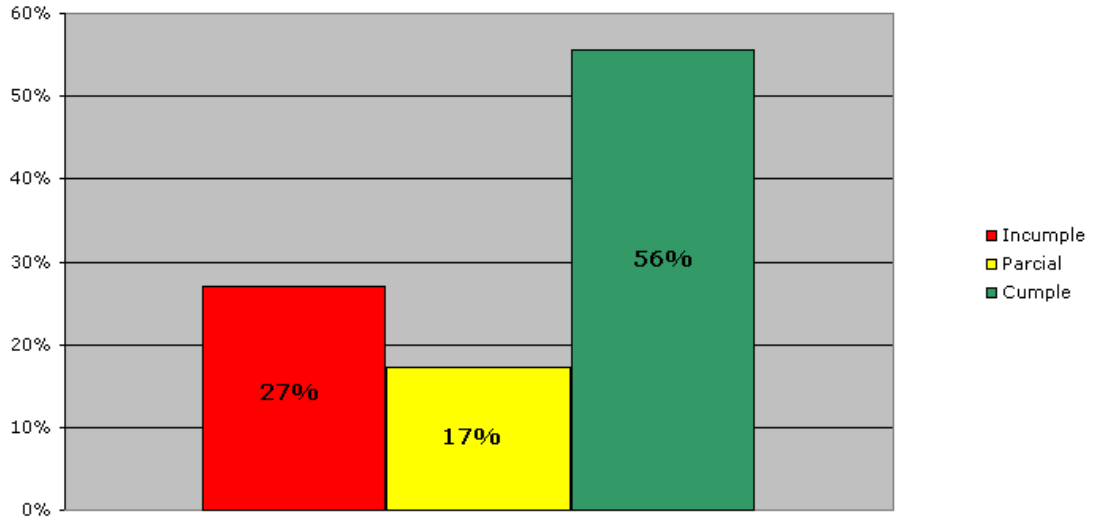

Figura 3: Gráfico con el porcentaje de controles que se cumplen, incumplen o cumplen parcialmente

Si se analiza el nivel de cumplimiento respecto a los dominios de los controles, se puede observar que donde menos se cumple es en el análisis de riesgos, las políticas de seguridad, la gestión de los activos, la continuidad del negocio y la gestión de incidentes de seguridad.

Observaciones: Para la realización del gráfico, se le ha asignado el valor 1 a los controles que no cumplen o no se aplican, el valor 2 a los controles que se cumplen parcialmente y el valor 3 a los controles que se cumplen.

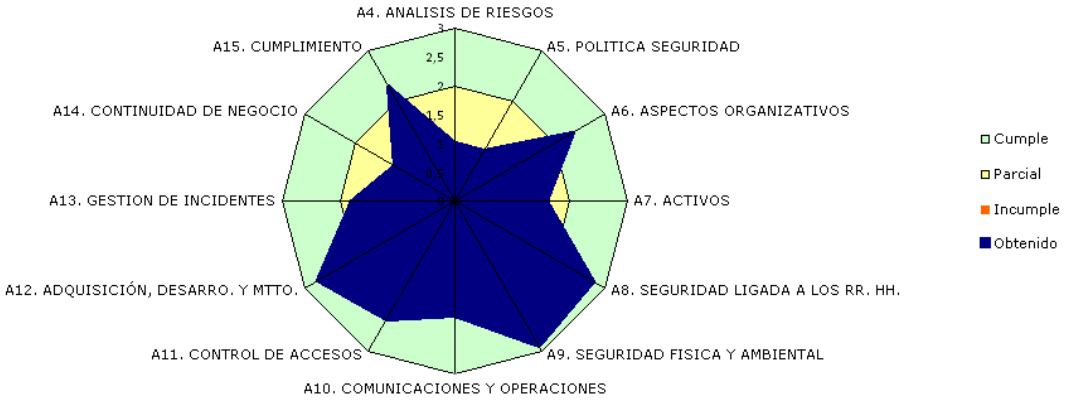

Figura 4: Diagrama de radar del Análisis GAP.

5. ALCANCE DEL SGSI

La Dirección de la empresa ha decidido implantar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 que tiene el siguiente alcance.

- La gestión de la seguridad de la información de las actividades relacionadas con el tratamiento de la información que dan soporte a los servicios de transporte regular y discrecional de viajeros por carretera de acuerdo con la Declaración de Aplicabilidad versión 1 de fecha 27/03/2014.

5.1. DESCRIPCIÓN DEL ALCANCE

El alcance del SGSI va a cubrir los servidores, aplicaciones informáticas y la información tanto en soporte automatizado como en soporte papel que son necesarias para que se pueda realizar de forma correcta y eficaz los servicios de transporte que presta la empresa a sus clientes.

Las localizaciones y sistemas involucrados en el alcance son:

- La sede principal de la empresa en Málaga con todos sus sistemas informáticos y archivo.
- La sede comercial en Sevilla con sus sistemas informáticos y gestión documental tratada en dicha sede.
- Los puestos de acceso ubicados en las distintas estaciones de autobuses.
- Los sistemas de control y localizaciones ubicados en los autobuses.

6. SISTEMA DE GESTIÓN DOCUMENTAL DEL SGSI

El sistema de gestión documental del SGSI se va a basar en la siguiente estructura documental:

- Políticas de Seguridad.
- Manuales. En el caso que se agrupen varios procedimientos.
- Procedimientos Generales.
- Instrucciones Técnicas.
- Registros.

6.1. GESTIÓN DE DOCUMENTOS Y REGISTROS

La empresa, como se ha comentado anteriormente en el apartado "2.5. Sistemas de gestión y control de la empresa", tiene implantado y funcionando dos sistemas de gestión, uno de Calidad (SGCA) y otro Ambiental (SGA).

Por tanto, la documentación del SGSI va a seguir el mismo modelo documental y formatos que ya están establecidos en los Sistemas de Gestión actualmente implantados en la empresa.

Asimismo, la documentación del Sistema se va a integrar dentro del sistema documental definido en la empresa para la gestión de todos los sistemas. Para lo cual se abrirá una carpeta dentro del sistema de gestión de calidad para la incorporación de los documentos del SGSI.

Por tanto, el procedimiento de gestión de documentos y registros del SGCA se va a ampliar y va a ser único para todos los sistemas de gestión y deberá incluir las codificaciones y responsabilidades específicas del SGSI que se incluyen a continuación.

6.1.1. CODIFICACIÓN DE LA DOCUMENTACIÓN

Todos los documentos del SGSI comenzarán con las letras SI y seguirán la misma codificación documental que para el resto de documentación de los sistemas de gestión que es la siguiente SI-XX-AAA-NN, siendo:

- XX: indicará el tipo de documento, PO (Política), PG (Procedimiento General), IT (Instrucción Técnica), MN (Manual), NO (Norma), RG (Registro), etc….
- AAA: hará una referencia al tipo de documentación que se trata, bien indicando el apartado de la norma al que hace referencia o con 3 letras que lo identifiquen.
- NN: Indicará el número de versión del documento de forma que observando el nombre del documento se pueda ver la versión del mismo.

A título de ejemplo, el documento que va a contener la Política de Seguridad de la Información que va a ser el primer documento que se definirá tendrá la siguiente codificación: SI-PO-GEN-01

6.1.2. RESPONSABILIDADES

Las responsabilidades en cuanto a la gestión documental son las siguientes:

La Dirección será la responsable de:

- Elaborar y aprobar la Política de Seguridad.
- Aprobar los procedimientos generales y manuales.

El Comité de Seguridad es el encargado de:

- Revisar los procedimientos generales y los manuales.
- Aprobación de las instrucciones técnicas.

El Responsable del SGSI es el encargado de:

- Dar soporte y asesoramiento a la Dirección para la elaboración de la Política de Seguridad.
- Elaboración de los manuales y procedimientos, así como la revisión de las instrucciones técnicas.
- Custodia de la documentación de SGSI respecto a las versiones que están en vigor y el archivado de las versiones obsoletas.
- Asegurarse que los registros se custodien y estén disponibles durante el periodo de vigencia de los mismos.
- Asegurarse que las políticas de seguridad y documentos sean conocidas por el personal y las partes implicadas.

El Responsable de Seguridad es el encargado de:

- Trabajar conjuntamente con el responsable del SGSI para dar soporte y asesoramiento a la Dirección para la elaboración de la Política de Seguridad.
- Elaboración de las instrucciones técnicas.

7. POLÍTICA DE SEGURIDAD

La empresa ha definido una política de seguridad donde se establece la estrategia de la empresa y el compromiso de la Dirección respecto a la implantación, mantenimiento y desarrollo de un SGSI, así como el desarrollo de políticas específicas que la Dirección de la empresa considera deben ser de obligado cumplimiento por todos los trabajadores y personal externo que trata con información de la empresa.

OBJETIVO

La Política de Seguridad de la empresa tiene los siguientes objetivos:

- La seguridad de la información es un aspecto esencial para el desarrollo de la actividad de la empresa. Por lo que la empresa proveerá de las medidas técnicas y organizativas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información orientadas a detectar y corregir las vulnerabilidades de seguridad que se detecten e intentar garantizar un entorno seguro en el tratamiento de la información.
- Los trabajadores deberán incluir la cultura de seguridad de la información como parte de su trabajo, ya que sin la colaboración, implicación y cumplimiento de las normas de seguridad por parte de los trabajadores y prestadores de servicio es imposible proteger adecuadamente la información de la empresa.
- Los trabajadores deberán ser proactivos en el mantenimiento y mejora del SGSI, de tal que forma que propongan las mejoras que estimen oportunas y pongan en conocimiento del responsable de seguridad o del SGSI cualquier incidente de seguridad que observen.
- Los trabajadores y cualquier persona que trate con información de la empresa estarán obligados a guardar el deber de secreto respecto a la información a la que hayan accedido no debiendo revelarla ni facilitarla a ningún tercero sin la debida autorización.
- Todos los trabajadores y personal que trate con la información deberá conocer y aceptar la política de seguridad de la empresa.
- La empresa tomará las medidas y acciones que considere oportunas para hacer cumplir con la política de seguridad.

ALCANCE

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

POLÍTICAS DE SEGURIDAD

Para dar soporte a las líneas generales antes descritas, la empresa ha definido las siguientes políticas:

- Política de Seguridad de alto nivel. Este documento formará parte del documento de políticas de seguridad de la organización y además tendrá un código de documento independiente denominado SI-PO-PAN-01 con sus distintas versiones que estará firmado por la Dirección y públicamente disponible tanto en las instalaciones como en la página web.

- El resto de documentos que se describen a continuación, formarán parte del documento de Política de Seguridad.
    - Política de clasificación de la información.
    - Política de control de acceso y protección ambiental.
    - Política de uso adecuado de los recursos de la empresa.
    - Política de acceso remoto o teletrabajo.
    - Política de comunicación de información.
    - Política de uso de firma electrónica.
    - Política de gestión de incidentes y mejora del sistema.
    - Política de privacidad y conformidad legal.

Se incluyen en documentos anexos la política de alto nivel y las políticas de seguridad de la información.

Observaciones

La Dirección, una vez realizado el análisis de riesgos, la declaración de aplicabilidad y los planes de tratamiento específicos, podrá crear nuevas políticas o aprobar procedimientos que desarrollen las políticas establecidas.

Poniendo un ejemplo para una mejor compresión, no será lo mismo realizar un procedimiento de copia de seguridad o un plan de contingencia si en el plan de tratamiento del riesgo la Dirección ha decidido externalizar determinados servicios o bien si ha decidido mantener los servidores en las instalaciones.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Dirección ha desarrollado la Política de Seguridad de la Organización y ha establecido la estructura organizativa de seguridad para implantar, desarrollar, mantener y mejorar el SGSI.

8.1. COMPROMISO DE LA DIRECCIÓN

La Dirección a través de la Política ha establecido directrices claras y ha demostrado su compromiso respecto a la seguridad de la información:

1. Firmando las Políticas de Seguridad de la Información.
2. Haciendo que se divulguen las políticas entre todo el personal.
3. Dotado de los recursos necesarios para la implantación, desarrollo y mejora continua del SGSI.
4. Identificando los Objetivos de Seguridad.
5. Aprobando los criterios de aceptación del riesgo y el riesgo residual.
6. Participando en el Comité de Seguridad.
7. Velando porque se realicen las auditorías internas.
8. Realizando la revisión del Sistema.
9. Estableciendo los roles y responsabilidades en materia de seguridad de la información.

8.2. ESTRUCTURA ORGANIZATIVA DE SEGURIDAD

La estructura organizativa de seguridad dentro de la empresa es la siguiente:

- Responsable del SGSI.
- Responsable de Seguridad.
- Comité de Seguridad.

Nombramientos

El Responsable del SGSI es la persona que actualmente ocupa el puesto de Gestión de Calidad.

El Responsable de Seguridad es la persona responsable del Departamento de Sistemas de Información y al mismo tiempo es también el responsable de seguridad de Protección de Datos.

El Comité de Seguridad está compuesto por:

- El responsable del SGSI.
- El responsable de Seguridad.
- El Director Financiero.
- El Director Comercial.
- El Director de Producción.

8.2.3. RESPONSABILIDADES DEL COMITÉ DE SEGURIDAD

El Comité de Seguridad se reunirá con periodicidad semestral, asimismo se podrá convocar de forma extraordinaria.

Respecto a la composición del Comité de Seguridad es necesario tener en cuenta lo siguiente: De los tres directores que están en el Comité de Dirección, es imprescindible la participación de al menos dos de ellos para que se pueda celebrar el comité. En determinadas reuniones y dependiendo de los aspectos a tratar y a decidir, especialmente si es necesario la dotación de recursos, se invitará al Director General.

Las responsabilidades del Comité de Seguridad son las siguientes:

1. Revisar y presentar para su aprobación los manuales y procedimientos.
2. Revisar y aprobar las instrucciones técnicas.
3. Promover la concienciación del personal en materia de seguridad.
4. Analizar el estado y evolución de las incidencias de seguridad ocurridas durante el período.
5. Seguimiento de las medidas correctoras y acciones de mejora del sistema.
6. Estudio y análisis de las medidas de seguridad a implantar, así como el análisis de posibles cambios en los riesgos y amenazas.
7. Estudio y análisis de planes de tratamiento y planes de mejora en la seguridad.
8. Revisión de las inspecciones y auditorías internas de verificación de la política de seguridad y del SGSI.

8.2.4. RESPONSABILIDADES DEL RESPONSABLE DEL SGSI

El Responsable del SGSI tiene las siguientes funciones:

1. Dar soporte y asesoramiento a la Dirección para la elaboración de la Política de Seguridad.
2. Elaboración de los manuales y procedimientos.
3. Llevar a cabo los procedimientos de seguridad una vez estén aprobados por la Dirección.
4. Revisión de las instrucciones técnicas.
5. Custodia de la documentación del SGSI tanto de la versión en vigor como el archivado de las versiones obsoletas.
6. Asegurarse que los registros se custodien y estén disponibles durante el período de vigencia de los mismos.
7. Asegurar que las políticas de seguridad y documentos sean conocidos por el personal y las partes implicadas.
8. Realizar, revisar y mantener el sistema de análisis de riesgo y aplicar el plan de tratamiento de riesgos.

8.2.5. RESPONSABILIDADES DEL RESPONSABLE DE SEGURIDAD

El Responsable de Seguridad tiene las siguientes funciones:

1. Trabajar conjuntamente con el responsable del SGSI para dar soporte y asesoramiento a la Dirección para la elaboración de la Política de Seguridad.
2. Elaboración de las instrucciones técnicas.
3. Mantener y revisar el Documento de Seguridad y velar por que se realicen las auditorías de protección de datos.

4. Gestionar las incidencias de seguridad.
5. Aplicar los planes de tratamientos que son de aplicación al Departamento de Sistemas de Información.
6. Controlar los indicadores.
7. Asegurar conjuntamente con el responsable del SGSI que las políticas de seguridad y documentos sean conocidas por el personal y las partes implicadas.

8.2.6. RESPONSABILIDADES DE LAS JEFATURAS

Las Jefaturas, como responsables de sus activos, tienen las siguientes responsabilidades:

1. Velar por que se cumplan las políticas de seguridad en los activos sobre los que son propietarios.
2. Autorizar formalmente el acceso a los usuarios a los activos de información de los que son responsables.
3. Clasificar la información que generan según los criterios de clasificación establecidos por la empresa.

8.2.7. RESPONSABILIDADES DEL PERSONAL

Los usuarios y cualquier personal que trate con información, tendrán las siguientes responsabilidades:

1. Cumplir con las medidas de seguridad establecidas por la empresa.
2. Ser proactivos referente a proponer mejoras en la seguridad de la empresa.
3. Comunicar cualquier incidente de seguridad que observen.

9. PROCEDIMIENTOS

Dentro de este apartado se describen los procedimientos generales necesarios para garantizar el correcto funcionamiento del Sistema de Gestión.

Los procedimientos incluidos son los siguientes:

- Organización de la Seguridad de la Información.
- Revisión del Sistema por la Dirección.
- Auditorías Internas.
- Gestión de Indicadores.
- Gestión de las No conformidades.
- Metodología de Análisis de Riesgos.

Una vez realizado el análisis de riesgos y la selección de controles, se definirán procedimientos específicos para cada grupo de controles que sean de aplicación en la empresa.

10. DECLARACIÓN DE APLICABILIDAD

Este documento tiene por objeto establecer la declaración de aplicabilidad establecida en el punto 4.1.2.j de la norma, de forma que se describan los controles que son relevantes para el SGSI de la empresa en base al análisis de riesgos.

10.1. APROBACIÓN POR LA DIRECCIÓN

La Dirección aprueba la presente declaración de aplicabilidad en versión 1.0 en fecha 27 de marzo de 2014.

Fdo: la Dirección.

10.2. DECLARACIÓN DE APLICABILIDAD

A continuación se identifican los controles de la norma ISO/IEC 27002:2005 que son de aplicación en la empresa. Se incluirá un breve explicación si el control es aplicable y una justificación si la organización ha decidido no aplicar un control.

Asimismo, los controles que no son de aplicación se marcarán en color para que se puedan apreciar de forma clara.

CONTROL	APLICA	JUSTIFICACIÓN
A.5 POLÍTICA DE SEGURIDAD **A.5.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**		
5.1.1 Doc. de política de S. I.	**SI**	La Dirección tiene que aprobar el documento de política de seguridad.
5.1.2 Revisión de la política de S.I.	**SI**	La Dirección tiene que revisar y mantener actualizada la política.
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN **A.6.1 ORGANIZACIÓN INTERNA**		
6.1.1. Compromiso de la Dirección con la S.I.	**SI**	Tiene que existir un compromiso de la Dirección en la implantación de un SGSI.
6.1.2 Coordinación de la S. I.	**SI**	Al existir distintas funciones y roles en la organización debe existir la coordinación.
6.1.3 Asignación de responsabilidades relativas a la S.I.	**SI**	Las responsabilidades deben estar claramente definidas
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.	**SI**	La Dirección es quien tiene que aprobar cualquier gasto o recurso que se necesite.
6.1.5 Acuerdos de confidencialidad	**SI**	La organización tiene que establecer medidas organizativas para proteger su información.
6.1.6 Contacto con las autoridades	**SI**	La organización debe mantener contacto con las autoridades.
6.1.7 Contacto con grupos de especial interés	**SI**	Se deben mantener contactos para mantenerse actualizado.

6.1.8 Revisión independiente de la S.I.	**SI**	La revisión debe realizarse por personal independiente de forma que no esté condicionado.
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN A.6.2. TERCEROS		
6.2.1 Identificación de los riesgos derivados del acceso de terceros	**SI**	Existen agentes (acuerdos y contratos) que tienen que acceder a los sistemas de información de la organización. Y clientes que pueden acceder a las instalaciones.
6.2.2 Tratamiento de la seguridad en la relación con clientes	**SI**	Los clientes acceden al servicio de comercio electrónico para realizar las compras.
6.2.3 Tratamiento de la seguridad en contratos con terceros	**SI**	Existen proveedores que tratan información.
A.7 GESTIÓN DE ACTIVOS A.7.1 RESPONSABILIDAD SOBRE LOS ACTIVOS		
7.1.1 Inventario de activos	**SI**	Existe un inventario de activos sobre los que se aplica el SGSI.
7.1.2 Propiedad de los activos	**SI**	Cada activo tiene asignado un propietario.
7.1.3 Uso aceptable de los activos	**SI**	La organización ha definido las políticas de uso de sus activos.
A.7 GESTIÓN DE ACTIVOS A.7.2 CLASIFICACIÓN DE LA INFORMACIÓN		
7.2.1 Directrices de clasificación	**SI**	La empresa ha definido una clasificación de la información.
7.2.2 Etiquetado y manipulado de la Inf.	**SI**	La documentación tiene que estar etiquetada con su clasificación.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS A.8.1 ANTES DEL EMPLEO		
8.1.1 Funciones y responsabilidades	**SI**	El personal tiene que conocer sus funciones y obligaciones.
8.1.2 Investigación de antecedentes	**SI**	Se realiza con las restricciones legales existentes.
8.1.3 Términos y condiciones de contratación	**SI**	Todo el personal y contratistas que tratan con información deben conocer las políticas de seguridad de la empresa que les son de aplicación.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS A.8.2 DURANTE EL EMPLEO		
8.2.1 Responsabilidades de la Dirección	**SI**	La Dirección ha elaborado las políticas de obligado cumplimiento.
8.2.2 Concienciación, formación y capacitación en S. I.	**SI**	El personal debe estar formado y los responsables del SGSI deben recibir formación específica.
8.2.3 Proceso disciplinario	**SI**	Está descrito en las políticas.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS A.8.3 CESE DEL EMPLEO O CAMBIO DE PUESTO DE TRABAJO		
8.3.1 Responsabilidad del cese o cambio	**SI**	Existe información dentro del alcance que es tratada por personal que puede ser cesado.
8.3.2 Devolución de activos	**SI**	Existe información dentro del alcance que es tratada por personal que puede ser cesado.
8.3.3 Retirada de los derechos de acceso	**SI**	Existe información dentro del alcance que es tratada por personal que puede ser cesado.

A.9 SEGURIDAD FÍSICA Y AMBIENTAL **A.9.1 ÁREAS SEGURAS**		
9.1.1 Perímetro de seguridad física	**SI**	Existen zonas de acceso restringido en el alcance del SGSI (instalaciones, oficinas, CPD, archivo, etc…)
9.1.2 Controles físicos de entrada	**SI**	Se debe controlar el personal que accede a las instalaciones.
9.1.3 Seguridad de oficinas, despachos e instalaciones	**SI**	Se debe controlar el personal que accede a las oficinas.
9.1.4 Protección de amenazas externas y de origen ambiental	**SI**	Los activos de información pueden estar expuestos a amenazas externas.
9.1.5 Trabajo en áreas seguras	**SI**	En determinados momentos personal externo tiene que trabajar en las zonas de acceso restringido (CPD, archivo, etc…)
9.1.6 Áreas de acceso público, y de carga y descarga	**SI**	Existen zonas donde los clientes y proveedores pueden acceder y deben estar controladas.
A.9 SEGURIDAD FÍSICA Y AMBIENTAL **A.9.2 SEGURIDAD DE LOS EQUIPOS**		
9.2.1 Emplazamiento y protección de equipos	**SI**	Existen equipos que deben estar protegidos frente a posibles riesgos externos.
9.2.2 Instalaciones de Suministro	**SI**	Existen equipos que deben mantener su funcionamiento aunque existan cortes eléctricos.
9.2.3 Seguridad del cableado	**SI**	El cableado y los rack de comunicaciones deben estar protegidos.
9.2.4 Mantenimiento de los equipos	**SI**	Los equipos que dan soporte a las aplicaciones deben estar en correcto mantenimiento.
9.2.5 Seguridad de los equipos fuera de las instalaciones	**SI**	Existen dispositivos como los equipos portátiles, móviles y los terminales móviles de los autobuses que deben ser protegidos.
9.2.6 Reutilización o retirada segura de equipos	**SI**	Existen activos que se quedan obsoletos y por tanto se deben retirar de forma segura.
9.2.7 Retirada de materiales propiedad de la empresa	**SI**	Cualquier salida de equipos de la empresa (portátiles) debe ser autorizada.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN**		
10.1.1 Documentación de los procedimientos de operación	**SI**	Los servidores de aplicaciones, los equipos informáticos, terminales y el CPD entran dentro del ámbito de aplicación.
10.1.2 Gestión de cambios	**SI**	Las aplicaciones pueden sufrir actualizaciones que es necesario controlar.
10.1.3 Segregación de tareas	**SI**	Deben estar delimitadas y segregar las tareas en el entorno de producción.
10.1.4 Separación de los recursos de desarrollo, prueba y operación	**SI**	Existe mantenimiento del sistema de gestión (SAP) por lo que se tiene que tener diferenciados los entornos para evitar problemas.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS**		
10.2.1 Provisión de servicios	**SI**	Existen subcontratistas que prestan servicios en los activos de información, tanto en seguridad como en las aplicaciones de gestión.

10.2.2 Supervisión y revisión de los servicios prestados por terceros	**SI**	Existen subcontratistas que prestan servicios en los activos de información, tanto en seguridad como en las aplicaciones de gestión.
10.2.3 Gestión del cambios en los servicios prestados por terceros	**SI**	Existen subcontratistas que prestan servicios en los activos de información, tanto en seguridad como en las aplicaciones de gestión.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.3 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA		
10.3.1 Gestión de capacidades	**SI**	Se debe controlar el nivel de uso de los activos para prevenir una problema de no disponibilidad.
10.3.2 Aceptación del sistema	**SI**	Las actualizaciones y nuevos sistemas deben estar previamente probados y validados.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.4 PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y DESCARGABLE		
10.4.1 Controles contra el código malicioso	**SI**	Los ordenadores de usuarios deben estar protegidos.
10.4.2 Controles contra el código descargado en el cliente	**SI**	Los ordenadores de los usuarios deben estar controlados para que no se puedan realizar descargas.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.5 COPIAS DE SEGURIDAD		
10.5.1 Copias de Seguridad de la Información.	**SI**	Existe información que es necesario salvaguardar.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.6 GESTIÓN DE LA SEGURIDAD DE LAS REDES		
10.6.1 Controles de red	**SI**	La red y las conexiones entran dentro del ámbito de aplicación del SGSI.
10.6.2 Seguridad de los servicios de red	**SI**	La red y las conexiones entran dentro del ámbito de aplicación del SGSI.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.7 MANIPULACIÓN DE LOS SOPORTES		
10.7.1 Gestión de soportes extraíbles	**SI**	Está definido en la política que sólo puede realizarse por el Departamento de Informática.
10.7.2 Retirada de soportes	**SI**	Los soportes que no vayan a ser utilizados deben ser devueltos o destruidos.
10.7.3 Procedimientos de manipulación de la Información.	**SI**	Está definido en la política que sólo puede realizarse por el Departamento de Informática.
10.7.4 Seguridad de la documentación del sistema	**SI**	Existen sistemas que tienen documentación que entran dentro del ámbito.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.8 INTERCAMBIO DE INFORMACIÓN		
10.8.1 Políticas y procedimientos de intercambios de información	**SI**	Existe información que debe comunicarse a terceros. Por ejemplo con los bancos para los pagos del sistema de comercio electrónico.
10.8.2 Acuerdos de intercambio	**SI**	Existe información que debe comunicarse a terceros. Por ejemplo con los bancos para los pagos del sistema de comercio electrónico.

10.8.3 Soportes físicos en transito	**NO**	No se realiza la comunicación mediante soportes físicos.
10.8.4 Mensajería electrónica	**SI**	Se utiliza la mensajería electrónica para las comunicaciones con clientes, con el banco, etc…
10.8.5 Sistemas de información empresariales	**SI**	Existen sistemas de información que entran dentro del ámbito de aplicación.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.9 SERVICIOS DE COMERCIO ELECTRÓNICO**		
10.9.1 Comercio electrónico	**SI**	El sistema de venta de billetes por Internet entra dentro del ámbito de aplicación del SGSI.
10.9.2 Transacciones en línea	**SI**	Existen transacciones tanto con los clientes como con el banco.
10.9.3 Información públicamente disponible	**SI**	Existe una web corporativa donde se publica la información de la empresa.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.10 SUPERVISIÓN**		
10.10.1 Registro de auditorias	**SI**	Existen sistemas dentro de ámbito de aplicación del SGSI que deben ser supervisados.
10.10.2 Supervisión del uso del sistema	**SI**	Existen sistemas dentro de ámbito de aplicación del SGSI que deben ser supervisados.
10.10.3 Protección de la información de los registros	**SI**	Existen sistemas dentro de ámbito de aplicación del SGSI que deben ser supervisados.
10.10.4 Registros de administración y operación	**SI**	Existen sistemas dentro de ámbito de aplicación del SGSI que deben ser supervisados.
10.10.5 Registro de fallos	**SI**	Existen sistemas dentro de ámbito de aplicación del SGSI que deben ser supervisados.
10.10.6 Sincronización del reloj	**SI**	Se debe mantener un único sistema de sincronización del reloj especialmente en los sistemas en producción.
A.11 CONTROL DE ACCESO **A.11.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO**		
11.1.1 Política de control de acceso	**SI**	El acceso a la información tiene que estar controlada y se ha establecido una política al respecto.
A.11 CONTROL DE ACCESO **A.11.2 GESTIÓN DE ACCESO DE USUARIO**		
11.2.1 Registro de usuario	**SI**	Se tiene que controlar a los usuarios que acceden a los sistemas de información.
11.2.2 Gestión de privilegios	**SI**	Se tiene que controlar el nivel de privilegios de los usuarios a la información.
11.2.3 Gestión de contraseñas de usuario	**SI**	Se utilizan contraseñas para el acceso a al información.
11.2.4 Revisión de los derechos de acceso a usuario	**SI**	Se tienen que revisar los accesos de forma periódica de forma que se eviten derechos de acceso no controlados y desactualizados.
A.11 CONTROL DE ACCESO **A.11.3 RESPONSABILIDADES DE USUARIO**		
11.3.1 Uso de contraseña	**SI**	Se utilizan contraseñas para el acceso a la información.
11.3.2 Equipo de usuarios desatendido	**SI**	Las aplicaciones y los equipos se deben bloquear cuando no se están utilizando.

11.3.3 Política de puesto de trabajo despejado y pantalla limpia	**SI**	Se debe mantener el puesto de trabajo sin información accesible.
A.11 CONTROL DE ACCESO A.11.4 CONTROL DE ACCESO A LA RED		
11.4.1 Política de uso de los servicios en red	**SI**	Se ha definido una política en la que los usuarios deben acceder solamente a lo que están autorizados.
11.4.2 Autenticación de usuario para conexiones externas	**SI**	Existen conexiones remotas mediante VPN por lo que es de aplicación.
11.4.3 Identificación de los equipos en las redes	**NO**	La autenticación se realiza a nivel alto (usuario y contraseña del usuario). Además, los equipos son intercambiables potenciando la movilidad, por lo que no se aplica.
11.4.4 Diagnóstico remoto y protección de los puertos de configuración	**SI**	Se deben controlar los accesos a los puertos de diagnóstico y configuración de los equipos para evitar mal uso.
11.4.5 Segregación de las redes	**SI**	Existen una DMZ y zonas de servidores y de usuarios, por lo que es de aplicación.
11.4.6 Control de la conexión a la red	**SI**	Se debe controlar el acceso remoto.
11.4.7 Control de encaminamiento (routing) de red	**SI**	Servicio externalizado pero es importante para la organización.
A.11 CONTROL DE ACCESO A.11.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO		
11.5.1 Procedimientos seguros de inicio de sesión	**SI**	Se administran equipos en la organización por lo que es necesario el control.
11.5.2 Identificación y autenticación de usuario	**SI**	Se administran equipos en la organización por lo que es necesario el control.
11.5.3 Sistema de gestión de contraseñas	**SI**	Se administran equipos en la organización por lo que es necesario el control.
11.5.4 Uso de los recursos del sistema	**SI**	Se administran equipos en la organización por lo que es necesario el control.
11.5.5 Desconexión automática de sesión	**SI**	Se administran equipos en la organización por lo que es necesario el control.
11.5.6 Limitación del tiempo de conexión	**SI**	Se administran equipos en la organización por lo que es necesario el control.
A.11 CONTROL DE ACCESO A.11.6 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN		
11.6.1 Restricción del acceso a la información	**SI**	Cada usuario tiene acceso solamente a la información a la que está autorizado.
11.6.2 Aislamiento de sistemas sensibles	**NO**	No se han establecido por los propietarios sistemas especialmente sensibles que necesiten una protección especial.
A.11 CONTROL DE ACCESO A.11.7 ORDENADORES PORTÁTILES Y TELETRABAJO		

11.7.1 Ordenadores portátiles y comunicaciones móviles	**SI**	Está definido el teletrabajo dentro de la política por lo que es de aplicación.
11.7.2 Teletrabajo	**SI**	Está definido el teletrabajo dentro de la política por lo que es de aplicación.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.1 REQUISITOS DE SEGURIDAD DE LOS S. I.**		
12.1.1 Análisis y especificación de los requerimientos de seguridad	**SI**	Se tienen contratados desarrollos de aplicaciones con proveedores.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.2 TRATAMIENTO CORRECTO DE LAS APLICACIONES**		
12.2.1 Validación de los datos de entrada	**SI**	Se tienen que validar los datos de entrada en las aplicaciones.
12.2.2 Control del procesamiento interno	**SI**	Existe interconexión entre las aplicaciones de comercio electrónico y control de billetes de los autobuses con el ERP por lo que es necesario controlar las aplicaciones.
12.2.3 Integridad de los mensajes	**SI**	Existe interconexión entre las aplicaciones de comercio electrónico y control de billetes de los autobuses con el ERP por lo que es necesario controlar las aplicaciones.
12.2.4 Validación de los datos de salida	**SI**	Existen salidas desde el ERP y el sistema de comercio electrónico que se deben verificar.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.3 CONTROLES CRIPTOGRÁFICOS**		
12.3.1 Política de uso de los controles criptográficos	**SI**	Se utilizan controles criptográficos en la firma electrónica, en las conexiones VPN y la comunicación segura del servicio de comercio electrónico.
12.3.2 Gestión de claves	**SI**	Existen claves para los controles criptográficos que es necesario proteger.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.4 SEGURIDAD DE LOS ARCHIVOS DE SISTEMA**		
12.4.1 Control del software de explotación	**SI**	Se debe controlar el aplicativo que está en producción.
12.4.2 Protección de los datos de prueba del sistema	**SI**	Se realizan pruebas en el entrono de calidad con datos reales, por lo que es necesario controlar el mismo.
12.4.3 Control de acceso al código fuente de los programas	**SI**	Existen códigos fuentes de las aplicaciones que es necesario controlar.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.5 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**		
12.5.1 Procedimientos de control de cambios	**SI**	Se deben controlar los cambios en los procesos de desarrollo.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	**SI**	Se deben probar y revisar los sistemas respecto a cualquier cambio producido.

12.5.3 Restricciones a los cambios en los paquetes de software	**SI**	Se tiene que controlar cualquier cambio en los paquetes instalados.
12.5.4 Fugas de información	**SI**	Se tiene que evitar usar aplicaciones que no estén probadas y correctamente licenciadas.
12.5.5 Externalización del desarrollo de software	**SI**	Se utiliza desarrollo externo.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA**		
12.6.1 Control de las vulnerabilidades técnicas	**SI**	Se deberían realizar pruebas de vulnerabilidades en las aplicaciones desarrolladas y en los paquetes comprados.
A.13 GESTIÓN DE INCIDENTES DE S. I. **A.13.1 NOTIFICACIÓN DE EVENTOS Y PUNTOS DÉBILES DE S. I.**		
13.1.1 Notificación de los eventos de S. I.	**SI**	Se tienen que gestionar los incidentes de seguridad.
13.1.2 Notificación de los puntos debilidades de Seguridad	**SI**	Se tienen que gestionar los incidentes de seguridad.
A.13 GESTIÓN DE INCIDENTES DE S. I. **A.13.2 GESTIÓN DE INCIDENTES DE S. I. Y MEJORAS**		
13.2.1 Responsabilidades y procedimientos	**SI**	Se tienen que gestionar los incidentes de seguridad.
13.2.2 Aprendizaje de los incidentes de S. I.	**SI**	Se tienen que gestionar los incidentes de seguridad y aprender de los mismos.
13.2.3 Recopilación de evidencias	**SI**	Se tienen que analizar la causa del problema por si hubiera que iniciar acciones legales o disciplinarias.
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO **A.14.1 ASPECTOS DE S. I. EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
14.1.1 Inclusión de la S. I. en el proceso de gestión de la continuidad del negocio	**SI**	Se tiene que gestionar la continuidad del negocio en los sistemas de información que son de aplicación.
14.1.2 Continuidad del negocio y evaluación de riesgos	**SI**	Se tiene que gestionar la continuidad del negocio en los sistemas de información que son de aplicación.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la S. I.	**SI**	Se tiene que gestionar la continuidad del negocio en los sistemas de información que son de aplicación.
14.1.4 Marco de referencia para la planificación de la continuidad del negocio	**SI**	Se tiene que gestionar la continuidad del negocio en los sistemas de información que son de aplicación.
14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	**SI**	Se tiene que gestionar la continuidad del negocio en los sistemas de información que son de aplicación.
A.15 CUMPLIMIENTO **A.15.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES**		

15.1.1 Identificación de la legislación aplicable	**SI**	Se tienen que identificar la legislación que es de aplicación.
15.1.2 Derechos de propiedad intelectual	**SI**	Se tiene que cumplir con los derechos de propiedad intelectual.
15.1.3 Protección de los documentos de la organización	**SI**	Se tienen que proteger los documentos de la organización.
15.1.4 Protección de datos y privacidad de la Inf. de carácter personal	**SI**	Se tratan datos de carácter personal por lo que es obligatorio su cumplimiento.
15.1.5 Prevención del uso indebido de los recursos de tratamiento de la Inf.	**SI**	Se debe tratar la información de forma correcta.
15.1.6 Regulación de los controles criptográficos	**SI**	Se utilizan controles criptográficos por lo que es necesario cumplir con la legislación aplicable.
A.15 CUMPLIMIENTO **A.15.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO**		
15.2.1 Cumplimiento de las políticas y normas de Seguridad	**SI**	Se debe comprobar el cumplimiento de las políticas.
15.2.2 Comprobación del cumplimiento técnico	**SI**	Se debe comprobar que las aplicaciones cumplen las normas legales.
A.15 CUMPLIMIENTO **A.15.3 CONSIDERACIONES SOBRE LA AUDITORIA DE LOS S. I.**		
15.3.1 Controles de auditoría de los S. I.	**SI**	Se debe controlar que las auditorías se realicen sin interrumpir el servicio.
15.3.2 Protección de las herramientas de auditoría de los S. I.	**SI**	Se debe controlar que las auditorías se realicen sin interrumpir el servicio.

11. ANÁLISIS DE RIESGOS

De acuerdo con el procedimiento establecido denominado "SI-PG-MAR-01: Metodología de Análisis de Riesgos", se procede a realizar el análisis de riesgos de los activos que están dentro del ámbito de aplicación del SGSI.

En este sentido, es muy importante tener en cuenta que la Dirección quiere conocer el nivel de riesgo que tiene con las salvaguardas que están implantadas, por lo que se van a tener en cuenta las mismas en las frecuencias de los impactos.

11.1. INVENTARIO DE ACTIVOS

La empresa ha inventariado sus activos, asignándoles el propietario de los mismos para que de forma pueda decidir la valoración de los mismos de acuerdo con la importancia que tengan para la organización.

Es importante tener en cuenta que los activos que afectan a más de una persona (por ejemplo el ERP en el que se trata información de todo el negocio) se han asignado directamente al director general, que delegará en los directores comercial, financiero y de producción respectivamente en sus ámbitos de competencia.

Por otro lado, se ha procedido a agrupar activos teniendo en cuenta la valoración de los mismos y un mismo nivel de riesgo para todos los elementos del grupo.

Código activo	Nombre del Activo	Descripción del Activo	Tipo de Activo	Responsable del activo
S-01	Venta y gestión	Servicios para la venta de los billetes de pasajeros y el control de los mismos.	[S] Servicios	Director general
S-02	Comercio electrónico	Servicio de comercio electrónico prestado a los usuarios.	[S] Servicios	Director comercial
S-03	Comunicaciones comerciales	Servicios de comunicaciones comerciales y electrónicas que deben estar de acuerdo con la legislación vigente.	[S] Servicios	Director comercial
D-01	Datos ERP	Base de Datos SAP/R3 para la gestión empresarial y comercial.	[D] Datos/ información	Director general
D-02	Datos Servidor ficheros	Ficheros e información almacenada en el servidor de ficheros. Incluyendo la Base de Datos de Personal que está en el mismo servidor.	[D] Datos/ información	Director general
D-03	Datos Producción	Base de Datos MySQL para el control de rutas y almacenamiento temporal de control de pasajeros y de expedición de billetes.	[D] Datos/ información	Director de producción
D-04	Correo electrónico	Ficheros de almacenamiento de correo electrónico en los PC de usuarios.	[D] Datos/ información	Director general
D-05	Portal de Internet	Información del portal de Internet	[D] Datos/ información	Director general

Código activo	Nombre del Activo	Descripción del Activo	Tipo de Activo	Responsable del activo
D-06	Datos Centralita	Grabaciones de voz de la centralita de VozIP para el control de la calidad de la atención telefónica del Call Center.	[D] Datos/ información	Director financiero
K-01	Claves VPN	Claves de cifrado para las VPN entre sedes y para el acceso remoto.	[K] Claves Cript.	Jefe de informática
K-02	Firma electrónica	Certificados digitales para firmas electrónicas.	[K] Claves Cript.	Director general
SW-01	Aplicación SAP/R3	Aplicación ERP SAP/R3.	[SW] Aplicación	Director general
SW-02	Aplicación ÚltimaGPS	Aplicación ÚltimaGPS para el control de rutas, así como la expedición y control de billetes y de pasajeros. Los datos se almacenan temporalmente y se vuelcan al ERP de la empresa.	[SW] Aplicación	Director de producción
SW-03	Control de presencia	Aplicación de control de presencia.	[SW] Aplicación	Director financiero
SW-04	Aplicación portal	• Aplicación para el portal de Internet y comercio electrónico. Está conectado con el ERP de la empresa. • Código fuente de la aplicación para el portal de Internet y para la aplicación de gestión del comercio electrónico.	[SW] Aplicación	Director general
SW-05	S.O. Servidores	• Windows 2008 Server (D.A., ficheros) • Linux CentOS con aplicación Proxy • Linux CentOS con SMTP y DNS	[SW] Aplicación	Jefe de informática
SW-06	Antivirus	Sistema antivirus instalado en todos los PC.	[SW] Aplicación	Jefe de informática

Código activo	Nombre del Activo	Descripción del Activo	Tipo de Activo	Responsable del activo
HW-01	Grupo servidores CPD	• Servidor de SAP/R3 producción con discos duros en Raid 1 S.O. y Raid 5 Datos (1 para producción, 1 desarrollo y 1 calidad) • 2 Servidores linux de SMTP, MX relay y DNS con discos duros en Raid 1 • 2 Servidores linux del portal de Internet con discos duros en Raid 1 • Servidor linux para aplicación UltimaGPS con discos duros en Raid 1 • Servidor linux con discos duros en Raid 1 para el acceso proxy a Intenet con listas negras de restricción. • Servidores con Windows 2008 Server para la gestión del Directorio Activo (principal) y almacenamiento de ficheros. Sistemas de discos montados en Raid 5.	[HW] Hardware	Jefe de informática
HW-02	Servidor fichero 2	Servidor con Windows 2008 Server en oficina comercial para la gestión del Directorio Activo (secundario) y almacenamiento de ficheros. Sistemas de discos montados en Raid 5.	[HW] Hardware	Jefe de informática
HW-03	Centralita VozIP	Centralita VozIP que permite la gestión y grabación de las llamadas para el control del Call Center.	[HW] Hardware	Jefe de informática
HW-04	Dispositivos autobuses	80 Dispositivos móviles (70 instalados y 10 en el almacén) ubicados en los autobuses para control de la ruta GPS y expedición y control de billetes y pasajeros.	[HW] Hardware	Director de producción
HW-05	PC usuarios con UPS	10 PC usuarios con Windows 7 con UPS (Estaciones de autobuses).	[HW] Hardware	Jefe de informática
HW-06	PC usuarios	75 PC usuarios con Windows 7 y XP (75 instalados y 5 en el Departamento de S.I. para pruebas y posibles sustituciones urgentes).	[HW] Hardware	Jefe de informática
HW-07	Portátiles	10 PC portátiles con Windows 7.	[HW] Hardware	Jefe de informática

Código activo	Nombre del Activo	Descripción del Activo	Tipo de Activo	Responsable del activo
HW-08	Impresoras	10 impresoras multifunción.	[HW] Hardware	Jefe de informática
HW-09	FW checkpoint	Cortafuego checkpoint CPD principal.	[HW] Hardware	Jefe de informática
HW-10	FW linksys	Cortafuego linksys sede comercial.	[HW] Hardware	Jefe de informática
HW-11	switch	4 switch gestionables de 20 y 40 puertos 100/1000.	[HW] Hardware	Jefe de informática
AUX-01	Adap PC-VozIP	10 adaptadores PC - VozIP para servicio de atención telefónica.	[AUX] Auxiliar	Jefe de informática
AUX-02	Destructoras	10 destructoras de documentos.	[AUX] Auxiliar	Jefe de informática
M-01	Backup	Copias de seguridad de los datos de los servidores.	[Media] Soporte	Jefe de informática
M-02	Documentación Negocio	Documentación en papel referente a contratos, facturas, albaranes, tiques de ventas, escrituras, etc….	[Media] Soporte	Director general
M-03	Documentación técnica	Manuales y documentación de los sistemas, aplicaciones, operación y mantenimiento.	[Media] Soporte	Jefe de informática
M-04	Doc. SG y Seg.	Documentación de los Sistemas de Gestión (CA y MA), de Protección de Datos, así como guías y procedimientos de seguridad establecidos.	[Media] Soporte	Director general
COM-01	Internet principal	Línea de comunicación Internet 10 Mb.	[COM] Redes	Jefe de informática
COM-02	Internet satélites	10 Líneas de comunicaciones Internet ADSL.	[COM] Redes	Jefe de informática
COM-03	Telefonía	40 teléfonos VozIP.	[COM] Redes	Jefe de informática
L-01	CPD principal	CPD Sede principal con climatización, SAI, sistema antiincendios.	[L] Instalaciones	Jefe de informática
L-02	Archivo principal	Archivo en sede principal.	[L] Instalaciones	Director general
L-03	Edificio Oficinas Principal	Edificio Oficinas Sede Principal con sistema de vigilancia y control de acceso.	[L] Instalaciones	Director general
L-04	Oficinas comercial	Oficinas sede comercial.	[L] Instalaciones	Director comercial
L-05	Oficinas remotas	Oficinas en Estaciones de autobuses.	[L] Instalaciones	Director comercial
L-06	Autobuses	70 Autobuses.	[L] Instalaciones	Director de producción

Código activo	Nombre del Activo	Descripción del Activo	Tipo de Activo	Responsable del activo
P-01	Personal estratégico	Personal directivo y con responsabilidad, así como el personal altamente especializado y estratégico.	[P] Personal	Director general
P-02	Personal técnico	• Personal técnico cualificado. • Servicios externos de administración de servidores y de seguridad informática.	[P] Personal	Director general
P-03	Personal	Personal de administración y conductores.	[P] Personal	Director general
P-04	Personal Call Center	Personal de atención al cliente.	[P] Personal	Director comercial
P-05	Asesoría jurídica y laboral	Asesoría jurídica para reclamaciones de clientes y asesoría laboral y servicio de prevención de riesgos laborales y vigilancia de la salud.	[P] Personal	Director general
P-06	Seguridad privada	Servicio de seguridad privada, control de acceso y videovigilancia.	[P] Personal	Director general
P-07	Agentes comerciales	Agentes comerciales en Estaciones de Autobuses.	[P] Personal	Director comercial

11.2. VALORACIÓN DE LOS ACTIVOS

A los activos se le ha asignado una valoración económica basada principalmente en el coste que tiene dicho activo en la organización o su coste de reposición. También se ha tenido en cuenta para la valoración de los activos las relaciones y dependencias de los activos esenciales (datos, información y servicios) que no tienen una valoración económica fácilmente cuantitativa ya que dependen de aspectos intangibles.

11.2.1 ANÁLISIS DE DEPENDENCIAS DE ACTIVOS

Se ha procedido a realizar un análisis de dependencias de los activos esenciales.

- [D] Datos/información
- [S] Servicios

Es importante tener en cuenta que se han tenido en cuenta las dependencias que de alguna forma afectan directamente al activo, y solamente en los casos en los que el tratamiento se realiza de forma manual (correo electrónico que está almacenado en los PC de los usuarios o comunicaciones comerciales que se realizan de forma manual) se ha tenido en cuenta el activo tipo personal [P].

Por otro lado, solamente en las relaciones entre los activos de servicio y activos de datos se ha indicado el porcentaje de la relación de forma que se puede comprender claramente la valoración del activo superior, ya que en algunos casos (Comercio Electrónico o Comunicaciones Comerciales) su valoración es inferior al activo del cual depende.

Dependencias del activo [S-01] Venta y Gestión

Está incluidas en este análisis las relaciones de los activos [D-01] Datos ERP y [D-03] Datos Producción.

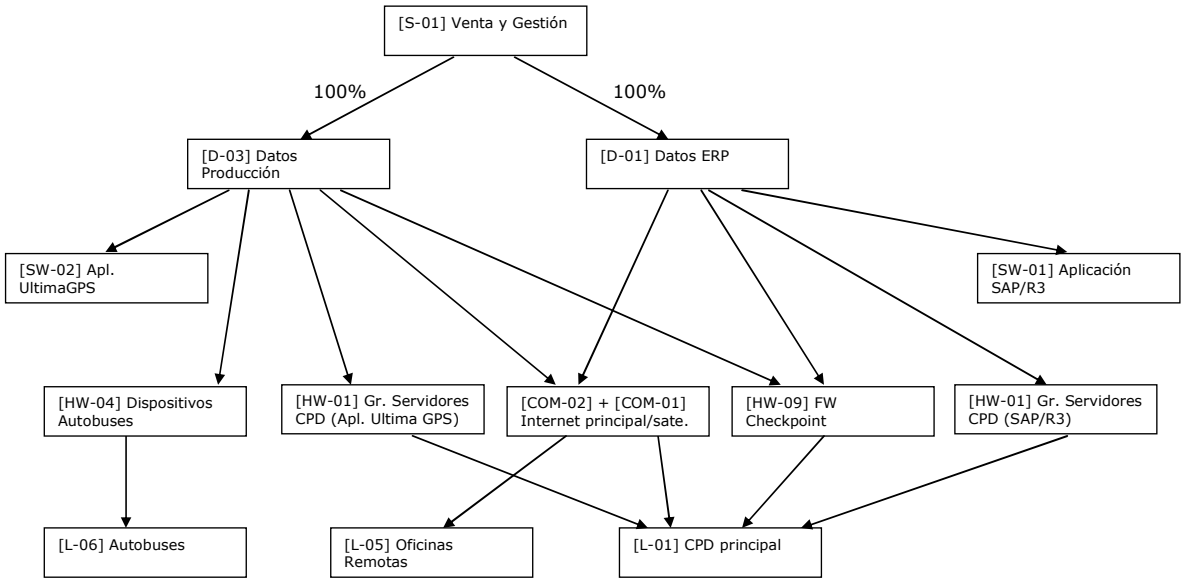

Figura 5: Diagrama de dependencias del activo [S-01] Venta y Gestión.

Dependencias del activo [S-02] Comercio Electrónico

En este diagrama se incluye la relación del activo [D-01] Datos ERP con el sistema de comercio electrónico que es otro canal más de venta dentro del módulo de ventas del ERP.

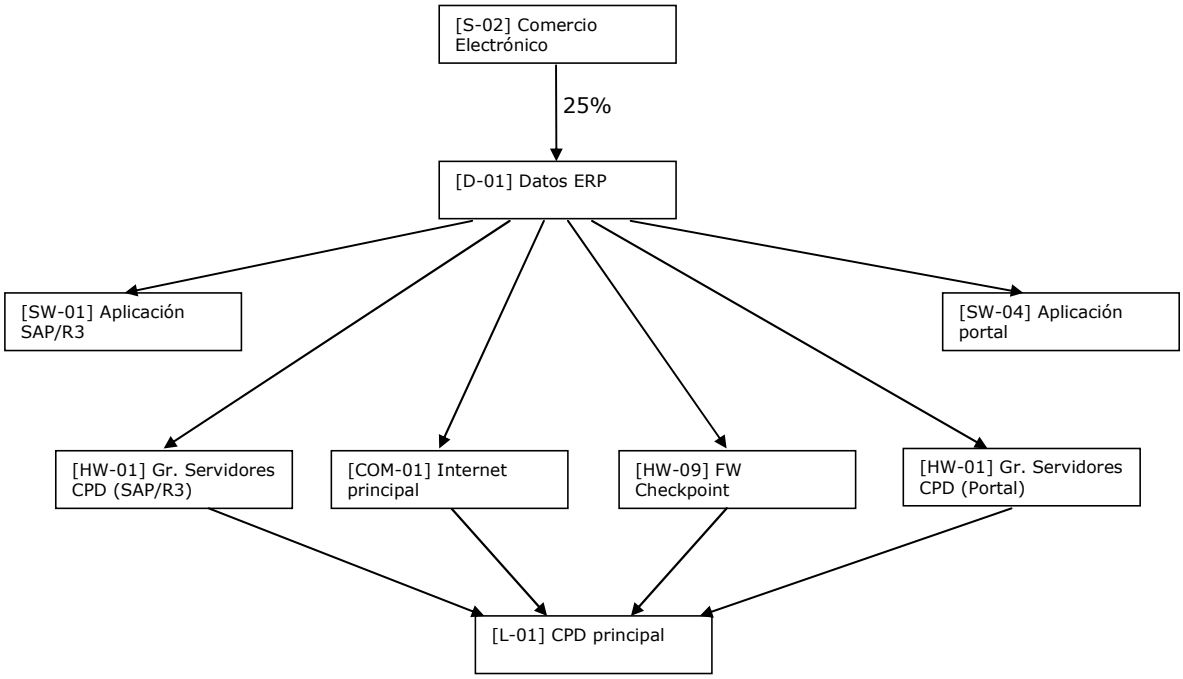

Figura 6: Diagrama de dependencias del activo [S-02] Comercio Electrónico.

Dependencias del activo [S-03] Comunicaciones Comerciales

Están incluidas en este análisis las relaciones del activo [D-04] Datos Correo Electrónico.

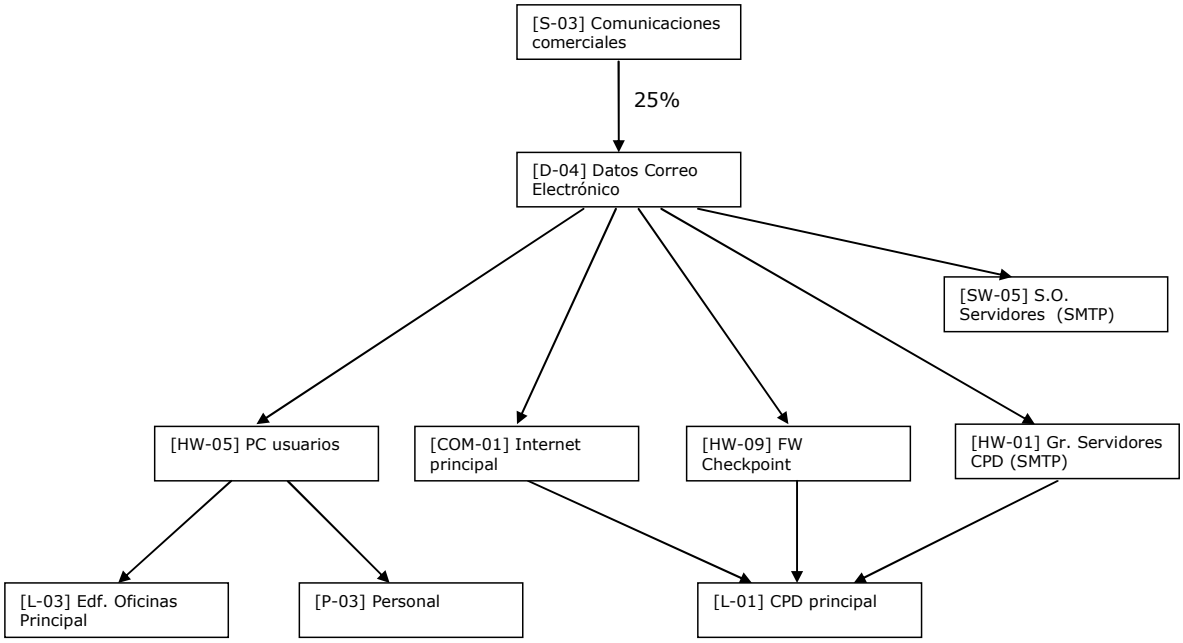

Figura 6: Diagrama de dependencias del activo [S-03] Comunicaciones comerciales.

Dependencias del activo [D-02] Datos Servidor de Ficheros

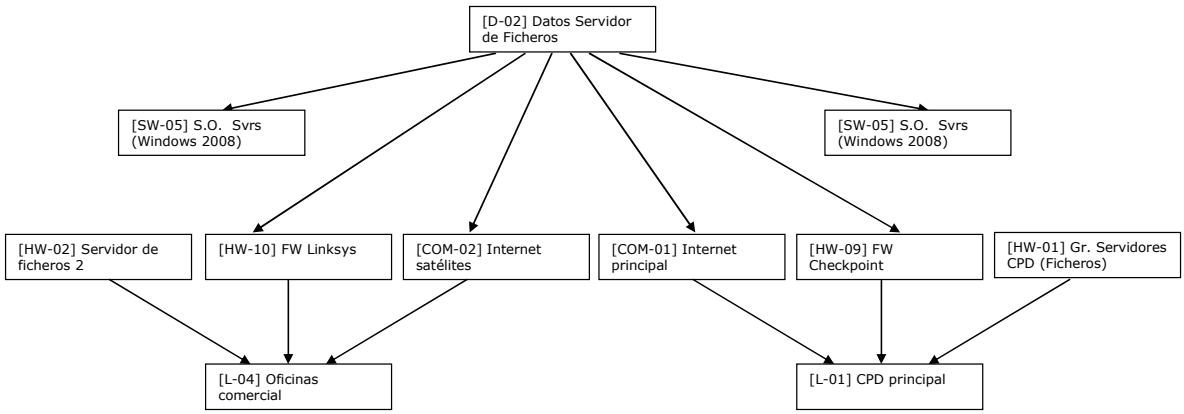

Figura 7: Diagrama de dependencias del activo [D-02] Datos Servidor de Ficheros.

Dependencias del activo [D-04] Datos Servidor de Ficheros

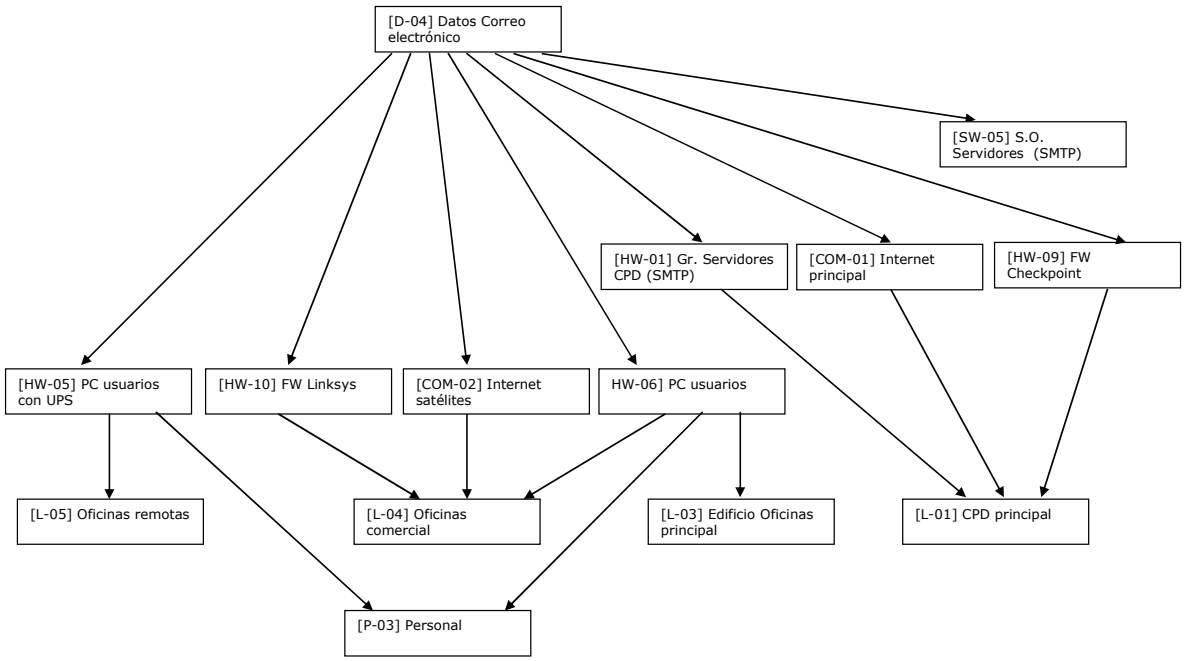

Figura 8: Diagrama de dependencias del activo [D-04] Datos Correo electrónico.

Dependencias del activo [D-05] Datos portal de Internet

Este activo solamente tiene en cuenta la información que públicamente dispone la empresa en Internet.

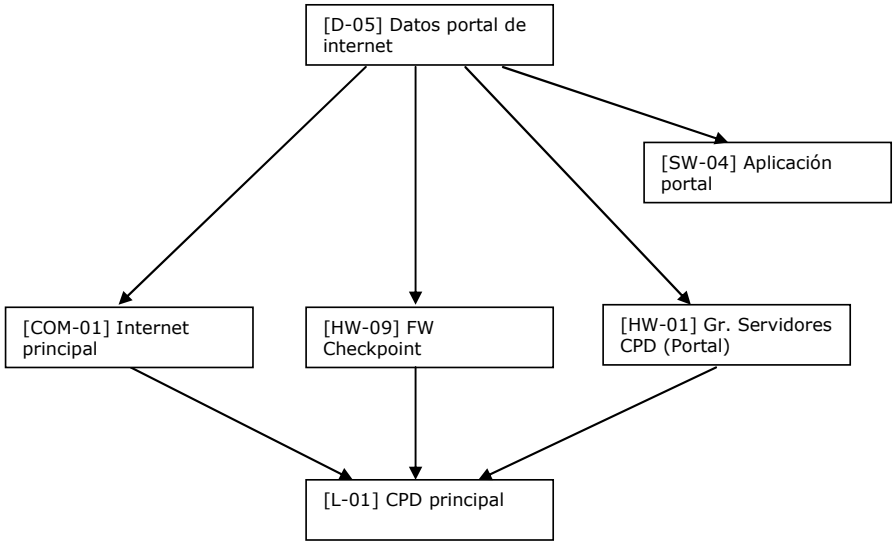

Figura 9: Diagrama de dependencias del activo [D-05] Datos portal de Internet.

Dependencias del activo [D-06] Datos Centralita

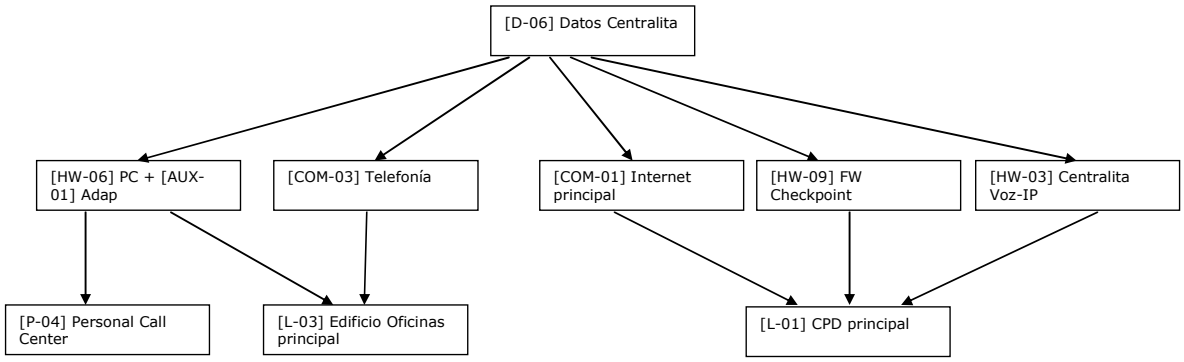

Figura 10: Diagrama de dependencias del activo [D-05] Datos Centralita.

11.2.2 VALORACIÓN DE LOS ACTIVOS

Tipo de Activo	Código activo	Nombre del Activo	Valoración del activo	Valoración cuantitativa
[S]	S-01	Venta y gestión	MA	500.000,00 €
[S]	S-02	Comercio electrónico	M	150.000,00 €
[S]	S-03	Comunicaciones comerciales	B	50.000,00 €
[D]	D-01	Datos ERP	MA	500.000,00 €
[D]	D-02	Datos Servidor ficheros	M	150.000,00 €
[D]	D-03	Datos Producción	A	300.000,00 €
[D]	D-04	Correo electrónico	M	150.000,00 €
[D]	D-05	Portal de Internet	B	50.000,00 €
[D]	D-06	Datos Centralita	B	50.000,00 €
[K]	K-01	Claves VPN	B	50.000,00 €
[K]	K-02	Firma electrónica	B	50.000,00 €
[SW]	SW-01	Aplicación SAP/R3	M	150.000,00 €
[SW]	SW-02	Aplicación ÚltimaGPS	M	150.000,00 €
[SW]	SW-03	Control de presencia	B	50.000,00 €
[SW]	SW-04	Aplicación portal	M	150.000,00 €
[SW]	SW-05	S.O. Servidores	MB	1.000,00 €
[SW]	SW-06	Antivirus	MB	1.000,00 €
[HW]	HW-01	Grupo servidores CPD	M	150.000,00 €
[HW]	HW-02	Servidor fichero 2	B	50.000,00 €
[HW]	HW-03	Centralita VozIP	B	50.000,00 €
[HW]	HW-04	Dispositivos autobuses	B	50.000,00 €
[HW]	HW-05	PC usuarios con UPS	B	50.000,00 €
[HW]	HW-06	PC usuarios	B	50.000,00 €
[HW]	HW-07	Portátiles	B	50.000,00 €
[HW]	HW-08	Impresoras	MB	1.000,00 €
[HW]	HW-09	FW checkpoint	M	150.000,00 €
[HW]	HW-10	FW linksys	B	50.000,00 €
[HW]	HW-11	switch	MB	1.000,00 €
[AUX]	AUX-01	Adap PC-VozIP	MB	1.000,00 €
[AUX]	AUX-02	Destructoras	MB	1.000,00 €
[Media]	M-01	Backup	B	50.000,00 €
[Media]	M-02	Documentación Negocio	M	150.000,00 €
[Media]	M-03	Documentación Técnica	B	50.000,00 €
[Media]	M-04	Doc. SG y Seg.	B	50.000,00 €
[COM]	COM-01	Internet principal	M	150.000,00 €
[COM]	COM-02	Internet satélites	B	50.000,00 €
[COM]	COM-03	Telefonía	B	50.000,00 €
[L]	L-01	CPD principal	M	150.000,00 €
[L]	L-02	Archivo principal	M	150.000,00 €
[L]	L-03	Edificio Oficinas Principal	MA	500.000,00 €
[L]	L-04	Oficinas comercial	M	150.000,00 €
[L]	L-05	Oficinas remotas	B	50.000,00 €
[L]	L-06	Autobuses	A	300.000,00 €
[P]	P-01	Personal estratégico	A	300.000,00 €
[P]	P-02	Personal técnico	M	150.000,00 €
[P]	P-03	Personal	B	50.000,00 €
[P]	P-04	Personal Call Center	B	50.000,00 €

Tipo de Activo	Código activo	Nombre del Activo	Valoración del activo	Valoración cuantitativa
[P]	P-05	Asesoría jurídica y laboral	B	50.000,00 €
[P]	P-06	Seguridad privada	B	50.000,00 €
[P]	P-07	Agentes comerciales	B	50.000,00 €

11.3. VALORACIÓN DE LOS IMPACTOS

Se ha procedido a dar un valor al impacto que tendría que se materializase una amenaza en un activo en cada una de las dimensiones de seguridad que se han tenido en cuenta para el desarrollo del SGSI ([C] Confidencialidad, [I] Integridad, [D] Disponibilidad).

Los valores utilizados son los siguientes:

valoración	Criterio de valoración del impacto
10	Daño extremadamente grave para la organización
9	Daño muy grave para la organización
6-8	Daño grave para la organización
3-5	Daño importante para la organización
1-2	Daño menor para la organización
0	Irrelevante para la organización.

11.3.1 VALORACIÓN POR ACTIVOS

Tipo de Activo	Código activo	Nombre del Activo	[C]	[I]	[D]
[S]	S-01	Venta y gestión	8	8	9
[S]	S-02	Comercio electrónico	6	7	7
[S]	S-03	Comunicaciones comerciales	6	6	6
[D]	D-01	Datos ERP	8	8	9
[D]	D-02	Datos Servidor ficheros	6	6	6
[D]	D-03	Datos Producción	6	7	8
[D]	D-04	Correo electrónico	6	6	6
[D]	D-05	Portal de Internet	2	7	7
[D]	D-06	Datos Centralita	6	6	6
[K]	K-01	Claves VPN	8	8	8
[K]	K-02	Firma electrónica	8	7	6
[SW]	SW-01	Aplicación SAP/R3	8	8	9
[SW]	SW-02	Aplicación ÚltimaGPS	6	7	8
[SW]	SW-03	Control de presencia	6	6	6
[SW]	SW-04	Aplicación portal	4	7	7
[SW]	SW-05	S.O. Servidores	5	5	5
[SW]	SW-06	Antivirus	5	5	7
[HW]	HW-01	Grupo servidores CPD	8	8	9
[HW]	HW-02	Servidor fichero 2	5	5	5
[HW]	HW-03	Centralita VozIP	6	6	6

Tipo de Activo	Código activo	Nombre del Activo	[C]	[I]	[D]
[HW]	HW-04	Dispositivos autobuses	6	7	8
[HW]	HW-05	PC usuarios con UPS	5	5	5
[HW]	HW-06	PC usuarios	4	4	3
[HW]	HW-07	Portátiles	8	4	3
[HW]	HW-08	Impresoras	0	0	2
[HW]	HW-09	FW checkpoint	8	8	9
[HW]	HW-10	FW linksys	5	5	6
[HW]	HW-11	switch	5	5	6
[AUX]	AUX-01	Adap PC-VozIP	0	0	4
[AUX]	AUX-02	Destructoras	0	0	3
[Media]	M-01	Backup	8	8	9
[Media]	M-02	Documentación Negocio	7	5	5
[Media]	M-03	Documentación Técnica	7	6	4
[Media]	M-04	Doc. SG y Seg.	5	7	7
[COM]	COM-01	Internet principal	8	8	9
[COM]	COM-02	Internet satélites	6	6	6
[COM]	COM-03	Telefonía	0	0	6
[L]	L-01	CPD principal	5	5	9
[L]	L-02	Archivo principal	7	5	5
[L]	L-03	Edificio Oficinas Principal	7	5	9
[L]	L-04	Oficinas comercial	6	5	5
[L]	L-05	Oficinas remotas	6	5	4
[L]	L-06	Autobuses	7	5	7
[P]	P-01	Personal estratégico	8	8	8
[P]	P-02	Personal técnico	7	7	7
[P]	P-03	Personal	4	4	4
[P]	P-04	Personal Call Center	3	3	3
[P]	P-05	Asesoría jurídica y laboral	6	6	5
[P]	P-06	Seguridad privada	3	3	6
[P]	P-07	Agentes comerciales	4	4	5

11.4. ANÁLISIS DE LAS AMENAZAS

Para realizar el análisis de riesgos se han tenido en cuenta las siguientes amenazas, las dimensiones de seguridad en las que se pueden materializar y el tipo de activo al cual pueden afectar.

código	Amenaza	Tipos de activos afectados
[N.1]	Fuego	[HW],[Media],[AUX],[L]
[N.2]	Daño por agua de origen natural	[HW],[Media],[AUX],[L]
[N.3]	Desastres naturales	[HW],[Media],[AUX],[L]
[I.1]	Fuego (Incendio) de origen industrial	[HW],[Media],[AUX],[L]
[I.2]	Daño por agua de origen industrial	[HW],[Media],[AUX],[L]
[I.3]	Contaminación mecánica (polvo, suciedad)	[HW],[Media],[AUX]
[I.4]	Contaminación electromagnética	[HW],[Media],[AUX]
[I.5]	Avería de origen físico o lógico	[HW],[Media],[AUX],[L]
[I.6]	Corte del suministro eléctrico	[HW],[Media],[AUX]
[I.7]	Condiciones inadecuadas de temperatura o humedad	[HW],[Media],[AUX]

código	Amenaza	Tipos de activos afectados
[I.8]	Fallo de servicios de comunicaciones	[COM]
[I.9]	Interrupción de otros servicios y suministros esenciales	[AUX]
[I.10]	Degradación de los soportes de almacenamiento de la información	[Media]
[I.11]	Emanaciones electromagnéticas	[HW],[Media],[AUX],[L]
[I.12]	Otros desastres industriales (explosión, derrumbes, etc…)	[HW],[Media],[AUX],[L]
[E.1]	Errores de los usuarios	[D],[K],[S],[SW],[Media]
[E.2]	Errores del administrador	[D],[K],[S],[SW],[HW], [COM],[Media]
[E.3]	Errores de monitorización (log)	[D]
[E.4]	Errores de configuración	[D]
[E.7]	Deficiencias en la organización	[P]
[E.8]	Difusión de software dañino	[SW]
[E.9]	Errores de [re-]encaminamiento	[S],[SW],[COM]
[E.10]	Errores de secuencia	[S],[SW],[COM]
[E.15]	Alteración accidental de la información	[D],[K],[S],[SW],[COM], [Media],[L]
[E.18]	Destrucción de información	[D],[K],[S],[SW],[COM], [Media],[L]
[E.19]	Fugas de información	[D],[K],[S],[SW],[COM], [Media],[L],[P]
[E.20]	Vulnerabilidades de los programas (software)	[SW]
[E.21]	Errores de mantenimiento/actualización de programas (SW)	[SW]
[E.23]	Errores de mantenimiento/actualización de equipos (HW)	[HW],[Media],[AUX]
[E.24]	Caída del sistema por agotamiento de recursos	[S],[HW],[COM]
[E.25]	Pérdida de equipos	[HW],[Media],[AUX]
[E.28]	Indisponibilidad del personal	[P]
[A.3]	Manipulación de los registros de actividad (log)	[D]
[A.4]	Manipulación de la configuración	[D]
[A.5]	Suplantación de la identidad del usuario	[D],[K],[S],[SW],[COM]
[A.6]	Abuso de privilegios de acceso	[D],[K],[S],[SW],[HW], [COM]
[A.7]	Uso no previsto	[S],[SW],[HW],[COM], [Media],[AUX],[L]
[A.8]	Difusión de software dañino	[SW]
[A.9]	[Re-]encaminamiento	[S],[SW],[COM]
[A.10]	Alteración de secuencia	[S],[SW],[COM]
[A.11]	Acceso no autorizado	[D],[K],[S],[SW],[HW], [COM],[Media],[AUX],[L]
[A.12]	Análisis de tráfico	[COM]
[A.13]	Repudio	[D],[S]
[A.14]	Interceptación de información (escucha)	[COM]
[A.15]	Modificación deliberada de la información	[D],[K],[S],[SW],[COM], [Media],[L]
[A.18]	Destrucción de información	[D],[K],[S],[SW],[Media] ,[L]

código	Amenaza	Tipos de activos afectados
[A.19]	Divulgación de información	[D],[K],[S],[SW],[COM], [Media],[L]
[A.22]	Manipulación de programas	[SW]
[A.23]	Manipulación de los equipos	[HW],[Media],[AUX]
[A.24]	Denegación de servicio	[S],[HW],[COM]
[A.25]	Robo	[HW],[Media],[AUX]
[A.26]	Ataque destructivo	[HW],[Media],[AUX],[L]
[A.27]	Ocupación enemiga (huelguistas o manifestantes)	[L]
[A.28]	Indisponibilidad del personal	[P]
[A.29]	Extorsión	[P]
[A.30]	Ingeniería social (picaresca)	[P]

11.4.1 DETERMINACIÓN DEL IMPACTO DE LAS AMENAZAS EN LOS ACTIVOS

Para determinar el impacto de las amenazas en los activos, se ha realizado el siguiente análisis:

1. Cada activo tiene valorado el nivel de criticidad que tendría que una amenaza se materializara en cada dimensión de seguridad (valorado del 0 al 10).
2. Cada amenaza puede tener una frecuencia de materialización en un activo dependiendo de las salvaguardias que la empresa tiene implantadas, valoradas entre muy frecuente (diaria) a despreciable (más de 10 años).
3. Para calcular el valor que tendrá que una amenaza se materialice, se tendrá en cuenta la perdida que dicho activo tendría en la organización, pudiendo ir entre el 0% (despreciable) al 100% (daño irreparable para la organización).
    a. Para calcular este porcentaje de pérdida del valor, se ha realizado una traslación directa entre los valores de los posibles impactos en las dimensiones de seguridad. De esta forma, el valor 0 (despreciable) se corresponderá con el 0% de pérdida del valor del activo y el valor 10 (daño extremadamente grave) se corresponderá con el valor 100% ya que producirá un daño irreparable para la organización.
    b. En los casos que un activo tenga distintos valores por cada dimensión de seguridad, se elige el valor mayor. Por ejemplo: [C]=8, [I]=7, [D]=9, el valor del impacto será 90%.

El cálculo de los impactos de las amenazas en cada activo se ha realizado en un documento anexo.

11.5. CALCULO DEL RIESGO

Una vez realizado el cálculo del riesgo, se han determinado los siguientes niveles de riesgo en base al cálculo del riesgo diario por activo.

valoración	Rango
Alto	Mas de 5000 €
Medio	Entre 2000 € y 5000 €
Bajo	Entre 1000 € y 2000 €
mínimo	Entre 150 € y 1000 €
Despreciable	Menos de 150 €

Por tanto, todo el riesgo que sea mayor de 5.000€ deberá ser tratado con un nivel de prioridad alto.

El riesgo que supere los 2000 € deberá se tratado con un nivel de prioridad medio.

El riesgo que sea inferior a 2000 € no será tratado y por tanto será aceptado por la Dirección de la empresa.

De acuerdo con lo anteriormente expuesto, la empresa ha determinado como un nivel de riesgo aceptable, todos los riesgos que tengan un valor menor que el nivel medio.

11.5.1 CALCULO DEL RIESGO POR ACTIVOS

Una vez calculado el riesgo por activo, los resultados son los siguientes:

Código Activo	Nombre del Activo	Riesgo del Activo
S-01	Venta y gestión	14.027,40 €
D-01	Datos ERP	12.054,79 €
L-03	Edificio Oficinas Principal	11.150,68 €
HW-09	FW checkpoint	9.887,67 €
L-06	Autobuses	7.923,29 €
S-02	Comercio electrónico	7.508,22 €
COM-01	Internet principal	6.554,79 €
HW-01	Grupo servidores CPD	6.189,04 €
D-03	Datos Producción	5.523,29 €
SW-02	Aplicación ÚltimaGPS	4.495,89 €
S-03	Comunicaciones comerciales	4.315,07 €
D-04	Correo electrónico	3.945,21 €
SW-04	Aplicación portal	3.789,04 €
SW-01	Aplicación SAP/R3	3.501,37 €
L-01	CPD principal	2.995,89 €
M-02	Documentación Negocio	2.815,07 €
D-02	Datos Servidor ficheros	2.712,33 €
L-04	Oficinas comercial	2.634,25 €
P-01	Personal estratégico	2.630,14 €
HW-04	Dispositivos autobuses	2.260,27 €
L-02	Archivo principal	1.980,82 €
P-02	Personal técnico	1.726,03 €
HW-10	FW linksys	1.475,34 €
K-02	Firma electrónica	1.397,26 €
HW-07	Portátiles	1.282,19 €
HW-05	PC usuarios con UPS	1.246,58 €
HW-02	Servidor fichero 2	1.178,08 €
M-01	Backup	1.161,64 €
HW-03	Centralita VozIP	1.142,47 €
M-04	Doc. SG y Seg.	1.138,36 €
D-05	Portal de Internet	1.119,18 €
COM-02	Internet satélites	1.027,40 €
HW-06	PC usuarios	946,58 €
M-03	Documentación Técnica	941,10 €
SW-03	Control de presencia	813,70 €
D-06	Datos Centralita	780,82 €
K-01	Claves VPN	767,12 €

Código Activo	Nombre del Activo	Riesgo del Activo
L-05	Oficinas remotas	694,52 €
COM-03	Telefonía	657,53 €
P-03	Personal	438,36 €
P-07	Agentes comerciales	397,26 €
P-06	Seguridad privada	369,86 €
P-05	Asesoría jurídica y laboral	335,62 €
P-04	Personal Call Center	328,77 €
SW-05	S.O. Servidores	23,15 €
HW-11	switch	20,11 €
SW-06	Antivirus	17,73 €
AUX-01	Adap PC-VozIP	11,73 €
AUX-02	Destructoras	8,38 €
HW-08	Impresoras	8,05 €

Gráfica de riesgos por activo

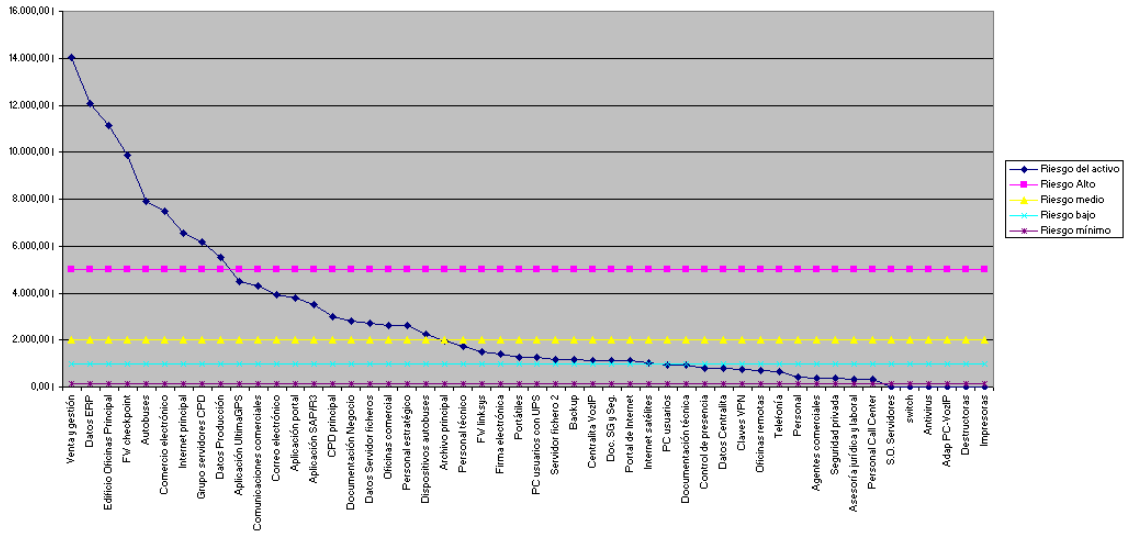

Figura 11: Grafica de los valores del riesgo por cada activo.

Gráfica de los activos con nivel de riesgo mayor que el riesgo aceptable

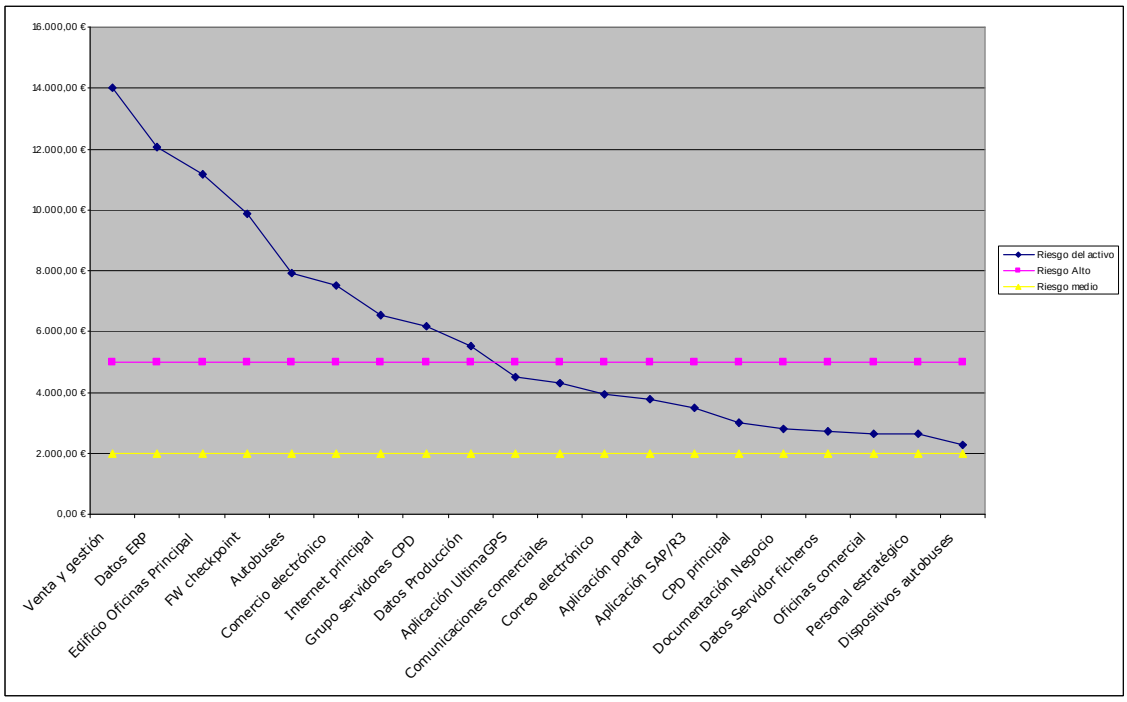

Figura 12: Activos que tiene un valor de riesgo superior al medio y que serán tratados.

Gráfica de los activos con nivel de riesgo menor que el riesgo aceptable

Los riesgos asociados a estos activos no serán tratados

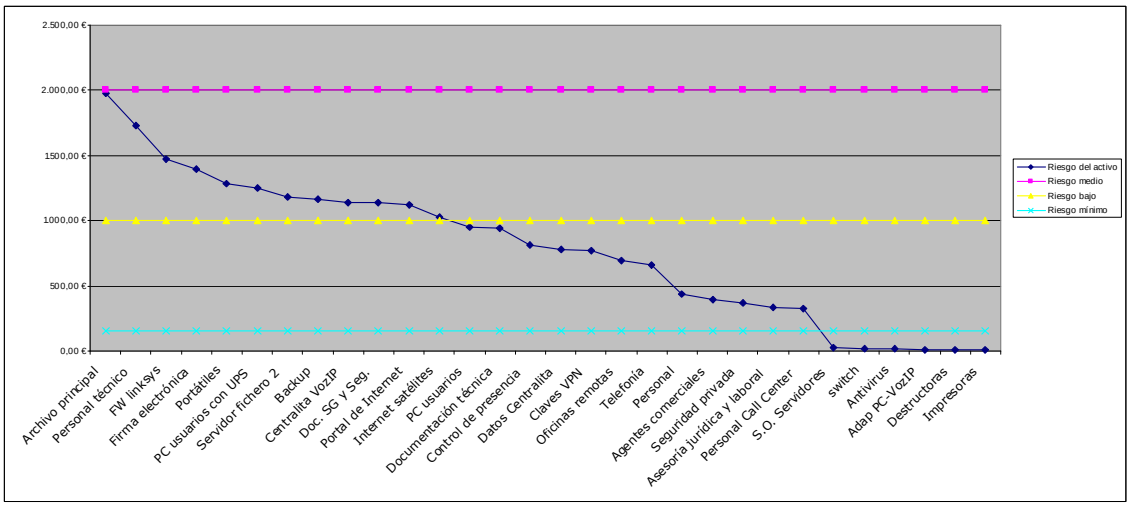

Figura 13: Activos que tiene un valor de riesgo inferior al medio y que no serán tratados.

11.6. APROBACIÓN DEL RIESGO RESIDUAL

Una vez realizado el análisis de riesgos se ha decidido establecer un umbral de riesgo asumible teniendo en cuenta el coste de implantación de las salvaguardias frente al coste de asumir el riesgo.

El nivel de riesgo asumible se fija en el nivel medio (más de 2.000€ de riesgo diario). Por encima del nivel medio están 20 activos de 50 lo que supone un 40% del total de los activos incluidos en el SGSI.

Por tanto, los activos que tienen un nivel de riesgo por encima del nivel alto (9 activos) y los que están por encima del nivel medio (11 activos) se incluirán dentro de un plan de tratamiento de riesgos donde se especificarán las acciones encaminadas a disminuir el riesgo soportado.

El riesgo de los activos que tienen un nivel de riesgo inferior el medio (30 activos) que suponen el 60% del total de activos, son asumidos por la Dirección de la empresa.

La Dirección aprueba la presente aprobación del riesgo residual en fecha 22 de abril de 2014.

Fdo: la Dirección.

12. ELABORACIÓN DE PROYECTOS

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 han definido 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.

12.1. PROCEDIMIENTOS PARA LA GESTIÓN DE LOS CONTROLES

Una vez aprobados y definidos los controles que son de aplicación en la declaración de aplicabilidad, es necesario proceder a desarrollar los procedimientos respecto a cómo se van a implantar dichos controles, así como los procedimientos de medición de la eficacia del control implantado.

12.1.1. SITUACIÓN INICIAL

La empresa dispone de una serie de procedimientos que están descritos tanto en el Documento de Seguridad de Datos de Carácter Personal como en distintos manuales y procedimientos aislados que fueron elaborados por el Departamento de Informática.

Por tanto, el proceso va a ir encaminado a unificar y racionalizar los procedimientos ya existentes y completarlos con los nuevos procedimientos que son necesarios desarrollar por implantarse controles que no estaban siendo tratados anteriormente.

12.1.2. RECURSOS NECESARIOS

Uno de los aspectos que se ha analizado a raíz de la implantación del SGSI, es que va a ser necesario disponer de recursos que estén dedicados a la realización de auditorías y verificación del nivel de cumplimiento de los controles. Por lo que inicialmente se había pensado en ampliar la plantilla o subcontratar este servicio.

Sin embargo, determinados proyectos que se van a ejecutar para el tratamiento del riesgo van a llevar aparejada la externalización de servicios de comunicaciones y de infraestructuras, con la consecuente descarga de trabajo del Departamento de Sistemas de Información de la empresa.

Debido a ello se ha propuesto a la Dirección un cambio en la estructura del Departamento de Informática y la creación de un nuevo Servicio de Control y Auditoría del Sistema de Gestión. Por lo que la nueva estructura del Departamento de Sistemas de Información pasa a ser de la siguiente forma:

- Mantenimiento y desarrollo.
- Administración de Sistemas.
- Control y auditoría.
- Soporte.

12.1.3. DESARROLLO DE LOS PROCEDIMIENTOS

Una vez aprobados los recursos necesarios, se va a proceder a normalizar, unificar y desarrollar los procedimientos de gestión y medición de los controles que están incluidos en la declaración de aplicabilidad.

Para el desarrollo de los procedimientos de seguridad, debido a que el personal interno debe ir adquiriendo la formación necesaria, se cuenta con los consultores externos que está realizando la implantación del SGSI de forma que puedan dar soporte y asesoramiento en la correcta elaboración de los procedimientos al personal interno de la empresa asignado a estas tareas.

Debido a que el personal tiene que ir adquiriendo formación y no se puede dedicar inicialmente a tiempo completo, se ha planificado un mes para la elaboración de todos los procedimientos.

Código	Titulo	Breve descripción
PT-00	Elaboración de los procedimientos de gestión de los controles	Analizar y normalizar los procedimientos existentes así como la creación de nuevos procedimientos orientados a establecer cómo se van a gestionar los controles que son de aplicación y cómo se van a proceder a realizar las mediciones de cumplimiento.

12.2. IDENTIFICACIÓN DE LAS MEJORAS NECESARIAS

Es importante tener en cuenta que por la metodología de análisis de riesgos que se ha empleado, en la que se ha realizado el análisis de riesgos sobre todos los activos (esenciales y dependientes), es necesario realizar una labor de análisis y de síntesis de forma que el plan de tratamiento se aplique sobre el activo que requiere dicho plan y que puede afectar a toda la jerarquía de los activos. Por esta causa, es necesario que los proyectos se expliquen de forma clara y concisa de forma que puedan ser fácilmente expuestos a la Dirección de la empresa que debe comprender su importancia y aprobarlos.

Por tanto, lo primero que se va a realizar es identificar en un lenguaje comprensible las mejoras que se deben realizar, indicando cuales son las principales amenazas que pueden afectar a los activos y motivando las causa de las mejoras necesarias.

El objetivo de este primer análisis es poder agrupar y realizar de forma conjunta proyectos que traten de resolver los mismos problemas, así como describirlos de una forma que pueda ser fácilmente comprensible por la Dirección de la empresa, que es quien debe tomar las decisiones al respecto y aprobar los proyectos.

Identificación de mejoras necesarias	Amenazas detectadas que motivan las mejoras necesarias	Motivación de las mejoras
Elaboración de un plan de formación en el uso de las herramientas y en la concienciación del personal en materia de seguridad, así como la divulgación de las políticas establecidas por la empresa.	Errores en el uso de las distintas aplicaciones. Divulgación de la información (confidencialidad). Incumplimiento de políticas de seguridad por uso no individualizado de usuarios y contraseñas inadecuadas.	Concienciar al personal de la empresa en la seguridad. Capacitación en el correcto uso de las aplicaciones para evitar errores de uso.
Disponer de una red de comunicaciones y seguridad en los servicios de Internet que permita prestar los servicios de forma correcta.	Existe un riesgo alto al existir un único elemento como es el Cortafuegos principal y la red de Internet de la sede principal que hace de "cuello de botella" en el acceso a todos los datos de la empresa. Además estos elementos están expuestos a ataques.	Evitar que un único elemento sea la causa de la no disponibilidad de todos los recursos de la empresa. Mejorar en las medidas de seguridad.
Mejorar los servicios de Venta y Gestión y la disponibilidad del ERP garantizando que se puedan utilizar en caso de caída del servidor principal.	Actualmente la información reside en un único servidor que está ubicado en el CPD del edificio principal que en caso de indisponibilidad del mismo implicará que no se pueda prestar servicios de venta y de gestión.	Evitar que por problemas en el único punto de servicio la empresa no pueda prestar sus servicios en los tiempos de respuesta establecidos.
Mejorar la disponibilidad de los ficheros y documentación de la empresa almacenada en el servidor de ficheros.	Actualmente la información reside en un único servidor que está ubicado en el CPD del edificio principal que en caso de indisponibilidad del servidor implicará que no se pueda prestar servicios de venta y de gestión.	Evitar que la empresa no pueda acceder a la documentación en los tiempos establecidos y requeridos por el negocio.

Identificación de mejoras necesarias	Amenazas detectadas que motivan las mejoras necesarias	Motivación de las mejoras
Mejorar la disponibilidad y confidencialidad de la documentación de la empresa.	Actualmente la información reside en el archivo o en las zonas de oficinas. Además, no se está aplicando política de puesto despejado por lo que existe documentación que es accesible.	Evitar posibles pérdidas de información y acceso no autorizado a la misma.
Mejorar la disponibilidad en los servicios de comercio electrónico e información del portal de Internet así como prevenir y minimizar los ataques que se están produciendo.	El servicio de comercio electrónico y la información de la empresa (portal) se presta desde servidores que están ubicados en una DMZ que está gestionado por la propia empresa. Este servicio depende de las comunicaciones y el cortafuegos de la empresa. Actualmente se han producido ataques que han provocado la interrupción del servicio.	Garantizar que el servicio se pueda seguir prestando independientemente del cortafuegos que existe actualmente y se puedan detectar y controlar los ataquen existentes actualmente.
Mejorar la disponibilidad de los datos de gestión de rutas y producción	Los datos de producción están almacenados en un único servidor que está en la DMZ (expuesto a ataques desde Internet) además depende de las comunicaciones de la empresa.	Garantizar que el servicio se pueda seguir prestando independientemente del cortafuegos que existe actualmente y se puedan detectar y controlas los ataquen existentes actualmente.
Mejorar la seguridad de los dispositivos instalados en los autobuses.	Al ser dispositivos tipo tabletas, y estar ubicados de forma visible, se han producido robos de dichos dispositivos ya que pueden ser utilizados para otros fines.	Establecer un sistema tipo "caja negra" de forma que el acceso a las tabletas no sea fácil y por tanto evitar el robo de las mismas.
Cumplir con la legislación en las comunicaciones comerciales	Actualmente las comunicaciones comerciales se realizan de forma manual, por lo que se producen errores que pueden dar lugar a infracciones y sanciones de acuerdo con la legislación vigente.	Automatizar las comunicaciones comerciales de forma que se minimice el impacto de errores humanos.
Mejorar el sistema de correo electrónico de la empresa.	El sistema de correo electrónico de la empresa está basado en que los buzones se almacenan en los PC de los propios usuarios, por lo que los usuarios no pueden acceder de forma remota a los buzones y existe el riesgo de perdida de la información.	Evitar perdidas de información y al mismo tiempo mejorar la disponibilidad del sistema.
Minimizar el riesgo de la existencia de personal estratégico	Actualmente existe personal que es en teoría "imprescindible" por sus conocimientos y la labor que realiza, por lo que la "fuga" de este personal puede suponer un grave problema para la empresa.	Evitar que la perdida de personal estratégico implique pérdida de conocimiento y la capacidad de gestión de la empresa.

12.3. IDENTIFICACIÓN Y ESTRATEGIA PARA LA ELABORACIÓN DE LOS PROYECTOS

Una vez identificadas todas las mejoras que son necesarias, es necesario evaluar las mismas y clasificarlas, así como identificar las distintas alternativas que existen para llevar a cabo el desarrollo de los proyectos.

Los distintos proyectos que se han identificados se pueden clasificar en:

- Proyectos de carácter organizativo y de formación y capacitación del personal.
- Proyectos tecnológicos de infraestructura y de comunicaciones.

Respecto a los proyectos organizativos, podemos agruparlos en los siguientes:

- Formación y capacitación del personal en el uso de las herramientas y en las medidas y políticas de seguridad establecidas en la empresa.
- Organización y digitalización del archivo y del acceso a la documentación.
- Plan de gestión del personal. Orientado a minimizar los riesgos del personal estratégico y mantener el conocimiento de la empresa.

Respecto a los proyectos tecnológicos, podemos agruparlos en los siguientes:

- Proyecto de racionalización de las comunicaciones y de Internet.
- Proyecto para la seguridad y continuidad de los servicios ofrecidos por Internet (actual DMZ).
- Proyecto para mejorar las comunicaciones comerciales.
- Proyecto para garantizar la continuidad de las operación internas.

Respecto a los proyectos de infraestructuras, podemos agruparlos en los siguientes:

- Proyecto para mejorar la seguridad en los dispositivos móviles ubicados en los autobuses.
- Proyecto para garantizar la continuidad de los servicios ofrecidos por la empresa.

Para el desarrollo de los proyectos, se han analizado distintas alternativas y se ha tenido en cuenta si el proyecto se puede desarrollar y mantener de forma interna o si por el contrario una externalización de servicios ofrecería una mejor calidad en los servicios prestados a un coste razonable y ofreciendo al mismo tiempo una mejora sustancial en la seguridad de los servicios prestados.

Por tanto, se ha tenido en cuenta no solamente el coste sino también la calidad de los servicios que pueden ser prestados internamente o por empresas especializadas. Además, en determinados casos se ha tenido que analizar la posible resistencia de la Dirección de la empresa a externalizar servicios e información, ya que lo ven como una perdida de la información y/o un riesgo a la confidencialidad de la información ya que va a estar albergada en Datacenter de proveedores.

Asimismo, es muy importante observar que existen proyectos que están interrelacionados y de la consecución de uno depende el éxito de los otros.

12.4. DESARROLLO DE LOS PROYECTOS

A continuación se enumeran los principales proyectos que se van a acometer para realizar una correcta gestión del riesgo de los activos que la empresa ha decidido que sean tratados.

Para que se pueda relacionar cada activo con los proyectos que le son de aplicación se han realizado la siguiente codificación de proyectos:

Código	Titulo	Breve descripción
PT-01	Comunicaciones y servicios de Internet	Racionalizar y mejorar las comunicaciones evitando el riesgo de elementos no redundantes y al mismo tiempo mejorando los servicios que se ofrecen en Internet.
PT-02	Plan de contingencia y de racionalización de servidores	Establecer un plan de continuidad en los servicios prestados por el ERP de la empresa y los prestados por los servidores de ficheros. Así como la racionalización de los servidores que no se externalizan.
PT-03	Comunicaciones comerciales	Automatizar los envíos de comunicaciones comerciales evitando que se puedan producir errores y conocimiento de la legislación aplicable.
PT-04	Seguridad en los dispositivos de los autobuses	Mejorar la seguridad de las tabletas utilizadas de forma que se evite la pérdida o robo de las mismas.
PT-05	Plan de capacitación y formación del personal	Establecer un plan de formación orientado a formar en el uso de las herramientas y en las medidas y políticas de seguridad establecidas en la empresa así como de actualización permanente en la legislación vigente.
PT-06	Organización de la documentación y digitalización del archivo	Establecer las medidas orientadas al cumplimiento de la política de puesto despejado y establecer un plan para digitalizar el archivo y minimizar la dependencia del documento en papel.
PT-07	Plan de gestión de personal	Establecer un plan de gestión del personal estratégico de la empresa.
PT-08	Plan de continuidad del negocio	Establecer un plan de continuidad del negocio.

A continuación se va a proceder a describir cada proyecto, indicando la estrategia que se va a seguir, el coste y la planificación del mismo. No es objeto de este documento establecer y desarrollar completamente cada uno de los proyectos.

12.4.1. COMUNICACIONES Y SERVICIOS DE INTERNET

Tal y como se ha analizado anteriormente, existe un riesgo alto en las comunicaciones de la empresa debido a la actual topología que hace que todos los servicios que se prestan en la empresa dependan de dos activos (cortafuegos principal y la red de Internet de la sede principal). Por tanto, una caída o un ataque a estos activos significaría que no se podría acceder al resto de servicios ni activos esenciales que dependan de ellos, tales como los servicios de comercio electrónico, accesos externos por usuarios y/o aplicaciones al ERP, etc….

Por otro lado, de una red de comunicaciones correctamente dimensionada y que permita tolerancia a fallos va a depender que otros servicios y proyectos se puedan ejecutar correctamente y de esta forma mejorar la seguridad de la información de la empresa.

Para poder mejorar los servicios de comunicaciones se han analizado distintas alternativas tanto internas (dotar de redundancia las comunicaciones y el cortafuegos) como el estudio de la externalización de los servicios en empresas especializadas.

12.4.1.1. EXTERNALIZACIÓN DE LOS SERVICIOS DE COMUNICACIONES

La opción que se ha elegido es eliminar el riesgo asociado al cortafuego y a las comunicaciones de Internet externalizando los servicios. Para ello, se han pedido ofertas a los principales operadores de telecomunicaciones.

Los objetivos a cumplir con los siguientes:

- Gestión de las comunicaciones globales de la empresa, incluyendo los accesos remotos o de teletrabajo.
- Gestión de la salida a Internet de la empresa.
- Gestión de los servicios de Internet de la Empresa (DMZ).
- Gestión de las comunicaciones de las tabletas de los autobuses de forma que estén restringidas solamente para el acceso al servidor.

Se ha procedido a pedir distintas ofertas para analizar el coste y los servicios ofertados. El coste anual de los servicios de comunicaciones externalizados depende de las distintas ofertas y ronda entre 25.000€ a 40.000€ dependiendo del operador y de los servicios prestados y si incluyes accesos de backup o no.

Plazo estimado para la ejecución del proyecto

Los plazos para la ejecución del proyecto una vez que está aprobado por la Dirección es de unos 3 meses.

12.4.1.2. EXTERNALIZACIÓN DE LOS SERVIDORES UBICADOS EN DMZ

Por otro lado, los servicios que se están ofreciendo actualmente en Internet por la empresa no se encuentran correctamente protegidos y tal y como se ha observado en el análisis de riesgos sus principales amenazas vienen por ataques externos que pueden provocar la denegación del Servicio (DoS)

La opción que se ha elegido es la de externalizar estos servicios. Esto va a permitir que la Dirección pueda apreciar las ventajas asociadas a la externalización de servicios en proveedores expertos en la prestación de los mismos, encaminadas a evitar por un lado los gastos de mantenimiento interno asociado y por otro la mejora de los servicios ofrecidos por la empresa.

Los servicios que se van a externalizar son los siguientes:

- Aplicación ÚltimaGPS.
- Aplicación Portal y comercio electrónico.
- Servicios de DNS y de correo electrónico.

Para la externalización de los servicios se ha optado por servidores virtuales dedicados ubicados en un Datacenter del tipo Tier 3 (99,982% de disponibilidad) y las alternativas para las copias de seguridad que se están analizando serían Warn-site que sería la adecuada para el servicio ÚltimaGPS que por la arquitectura de dicho servicio puede permitir no estar disponible durante un máximo de 4 horas, y sistema de copia tipo Hot-site que sería la adecuada para los servicios de comercio electrónico.

Por otro lado, para los servicios de correo electrónico se ha optado por contratar el servicio y no contratar el servidor. De esta forma se pagaría por uso y sería el prestador de servicios el encargado de prestar el servicio con las condiciones acordadas.

En todos los casos se firmaría un contrato de prestación de servicios con el operador que incluyera las condiciones del servicio y el SLA acordado tanto en tiempos de respuestas como de recuperación de datos.

Los costes aproximados, que dependen del servicio finalmente contratado y de los precios ofertados por distintos proveedores y las características de los servicios, serían los siguientes:

- Aplicación ÚltimaGPS externalizada en un servidor Linux virtualizado dedicado. Sistema de copia de seguridad tipo Warn-site en otro Datacenter. Coste aproximado entre 5.000€ a 7.000€ anuales.
- Aplicación Portal y Comercio Electrónico externalizada en un servidor Linux virtualizado dedicado. Sistema de copia de seguridad tipo Hot-site en otro Datacenter. Coste 10.000€ a 15.000€ anuales.
- Servicios de DNS y de correo electrónico. En este caso se ha optado por contratar un servicio de correo Exchange con una capacidad de almacenamiento por buzón de usuario de 1GB. El coste anual rondaría entre los 3.000 € y los 6.000€ dependiendo del número de usuarios y del tamaño del buzón de correo por usuario que finalmente se contrate, así como el tipo de copia de seguridad contratado.

Plazo estimado para la ejecución del proyecto

Una vez aprobado el proyecto por la Dirección, los plazos de ejecución dependen del servicio a externalizar.

- El servicio de correo electrónico no depende de otros proyectos y puede estar operativo en 1 mes (requiere configuración e instalación de cada puesto de trabajo)
- Los servicios de Aplicación Portal y Comercio Electrónico así como los de Aplicación ÚltimaGPS dependen del proyecto de externalización de las comunicaciones. Por lo el plazo de ejecución específico de estos proyectos se ha estimado entre 1 mes y mes y medio para las tareas de instalación, pruebas piloto y puesta en producción definitiva.

12.4.2. PLAN DE CONTINGENCIA Y DE RACIONALIZACIÓN DE SERVIDORES

Si bien inicialmente se había planteado el proyecto de externalización de todos los servicios de sistemas de información, finalmente se ha optado por comenzar a externalizar los servicios satélites y de Internet (descritos en el apartado anterior) de forma que la Dirección de la empresa pueda comprobar que la externalización de servicios en proveedores solventes y de confianza va a ayudar a la organización a prestar sus servicios de forma adecuada evitando riesgos.

Por lo que se ha optado por no externalizar los servicios del ERP de la empresa ni del servicio de ficheros y de Directorio Activo. En ambos casos, los servidores que prestan estos servicios no están amortizados y además el coste de la externalización de los servicios del ERP de SAP ronda entre los 80.000€ a 120.000€ anuales y además esto no incluiría los servicios de parametrización y mantenimiento del sistema, que tendría que seguir siendo prestado por personal interno. Por otro lado, la externalización de los servidores de ficheros llevaría

aparejada una necesidad de incrementar el ancho de banda en la red de comunicaciones.

Para solventar las amenazas que pueden provocar una parada en los servicios del ERP de la empresa y del servidor de ficheros que se prestan desde el CPD principal con un único servidor se ha optado por un plan de contingencia. Debido a que la única salvaguardia de los datos que se realiza es mediante copia de seguridad que permite recuperación de datos en los propios servidores en tiempos aceptables pero no permiten la recuperación en caso de desastre en los tiempos que el negocio necesita, que están establecidos en 4 horas para el servicio de ERP y en un máximo de 2 días para los servicios de ficheros.

El proyecto de plan de continencia se ha dividido en dos partes:

- Utilizar la sede comercial como centro de respaldo y disponer en esta localización de los servidores necesarios para garantizar la continuidad de los servicios en los tiempos acordados por la empresa.
    - ERP. Se establece que tiene que recuperar en un máximo de 4 horas, por lo que se establece un sistema de copia tipo Warn-site.
    - El servicio de ficheros tiene que quedar reestablecido en un máximo de 2 días. No obstante se ha establecido un procedimiento de replica de la información entre ambos servidores de forma diaria. Por lo que el sistema se utiliza un sistema de replicación asíncrona.
- Realizar un proyecto de racionalización y de virtualización de los servidores existentes de forma que permita una mayor facilidad en los procedimientos de replicación y de copia, permitiendo al mismo tiempo una mayor versatilidad y agilidad en la prestación de servicios sin tener una dependencia física de las máquinas.

Descripción del proceso del proyecto y costes asociados

El proyecto se va a acometer en varias fases. Por un lado, se va a proceder a reutilizar los servidores que se han dejado de utilizar al producirse la externalización de los servicios de Internet. Por tanto, se va a aprovechas el armario de servidores que se ha quedado sin uso en el CPD principal para enviarlo a la sede comercial de forma que los servidores que se van a disponer en dicha ubicación estén dotados de un sistema de control de acceso físico (armario de servidores con cerradura). Por otro lado, se ha inicializado un proyecto de virtualización de servidores orientado a mejorar la disponibilidad de los mismos y a la realización de replicas tipo snapshot.

Los costes asociados van a ser costes internos tanto del personal del Departamento de Sistemas de Información como de la empresa que presta los servicios de administración y seguridad.

Respecto a posibles ampliaciones de memoria, licencias y soporte en el aplicativo de virtualización y de discos necesarios se ha presupuestado unos 6.000€

Plazo estimado para la ejecución del proyecto

Este proyecto va a estar condicionado al proyecto de comunicaciones y a la externalización de los servicios ubicados en los servidores actuales de Internet, primero por la disponibilidad de los servidores y por otro lado por el ancho de banda actual ya que los tiempos necesarios de sincronización no serían los adecuados y podrían saturar el ancho de banda actual con las réplicas.

La planificación de la fase 1 sería de 1 mes para la preparación de servidores, pruebas y planificación y afinamiento de los procesos de replicación.

La planificación de la segunda fase (virtualización) es más delicada y técnica y debe ser llevada a cabo evitando riesgos innecesarios de configuración, por lo que la planificación sería de 2 meses.

12.4.3. COMUNICACIONES COMERCIALES

Este proyecto se inicia para eliminar el riesgo de posibles infracciones y sanciones tanto por el incumplimiento de la LOPD como de la LSSI en los envíos comerciales debido a la no automatización del proceso de envío.

Por otro lado, se analiza y se tiene en cuenta el uso que se va a hacer en la empresa que no es un uso intensivo sino que una vez al mes se envían las noticias a los clientes y cuando existen promociones y ofertas se realizan envíos masivos.

Por tanto, se analizan distintas alternativas tanto de servicios externalizados como de aplicaciones que permiten la automatización de los envíos y la posibilidad de mantener y gestionar listas de exclusión.

Una vez analizado el uso y los costes asociados, se opta por comprar una aplicación que permite gestionar los envíos comerciales de forma fácil y con un coste asequible (entre 500€ y 1000€ el coste de la aplicación).

Una vez que se haya elegido la aplicación se procederá a escribir y a divulgar entre los usuarios afectados por el uso el procedimiento de uso de la aplicación y los requisitos legales necesarios para poder enviar comunicaciones comerciales que si bien están descritos en las políticas de la empresa, se ve conveniente que quede reflejado en un procedimiento específico.

Plazo estimado para la ejecución del proyecto

El plazo para la ejecución del proyecto una vez aprobado por la Dirección es de 2 meses que incluyen la elección de la aplicación, la instalación, formación del personal, así como la elaboración del procedimiento de comunicaciones comerciales.

12.4.4. SEGURIDAD EN LOS DISPOSITIVOS DE LOS AUTOBUSES

Uno de los riesgos que se habían detectado es el de los robos y pérdidas de los dispositivos móviles que se utilizan en los autobuses para la gestión de las rutas (control de producción) y para la gestión de las ventas directas y control de lo billetes de los pasajeros.

El principal problema radica en que los dispositivos utilizados son tipo tablet y al ser visibles pueden ser sustraídos cuando el conductor se encuentra ausente. Asimismo, pueden ser manipulables y por tanto susceptibles de que se puedan desconectar de los dispositivos auxiliares (lector, impresora, etc…).

El proyecto consiste en diseñar una caja que se pueda cerrar y ubicar de forma anclada en el autobús y que permita albergar los dispositivos móviles de forma que garantice la seguridad de los mismos en cuanto a los posibles robos y que no permita el manipulado de los dispositivos.

Para el desarrollo del proyecto se ha contratado con una empresa el diseño de la caja y al mismo tiempo se ha llegado a un acuerdo con la Universidad para que participe en el diseño y la seguridad de dichos dispositivos.

El coste total del proyecto se ha presupuestado en un máximo de 10.000€ que debe incluir la fase de diseño y las 70 cajas que se deben colocar en los autobuses.

Plazo estimado para la ejecución del proyecto

El plazo para la ejecución del proyecto es de 2 meses para el diseño y homologación del prototipo y de 6 meses para la producción y colocación en todos los autobuses de la flota. El plazo total de proyecto es de 8 meses.

12.4.5. PLAN DE CAPACITACIÓN Y FORMACIÓN DEL PERSONAL

Una de las amenazas detectadas en el análisis de riesgos se debe fundamentalmente a los errores cometidos por el personal y que son producto del desconocimiento del uso de las aplicaciones y de las políticas de seguridad de la información establecidas por la empresa.

Si bien las políticas de seguridad de la información de la empresa se han distribuido y existen manuales para el uso de las aplicaciones, se ha comprobado que es mucho más efectivo establecer un programa de formación y concienciación del personal.

Para ello, se ha establecido de forma conjunta con el Departamento de Recuross Humanos un plan de formación que cubra los siguientes aspectos:

- Formación básica en los fundamentos y políticas de seguridad de la información establecida por la empresa y la legislación que se aplica.
- Formación en los módulos de ventas y de gestión de la aplicación SAP/R3 utiliza en la empresa.
- Formación a los responsables el SGSI.

La formación se ha programado para que sea recibida por el personal de la empresa en horario laboral ya que es de obligada asistencia. Las sesiones formativas son de un máximo de 2 horas al día y se han programado para que no se impartan más de una o dos sesiones semanales a la misma persona. Se han programado sesiones formativas regladas (de un mínimo de 8 horas) y sesiones divulgativas en las políticas de la empresa con una duración de un máximo de 2 horas. Estas últimas serán impartidas por el Responsable de Seguridad y el Responsable del SGSI de la empresa.

El coste de las acciones formativas se ha presupuestado en 10.000€ para el año y en los casos en los que se cumplan los requisitos legales, la formación se bonificará de los créditos de formación que se pueden deducir de los seguros sociales, por lo que el coste real para la empresa será como mucho de 1.000€.

Plazo estimado para la ejecución del proyecto

El plazo que se ha establecido para la formación es de 6 meses para que todo el personal de la empresa haya recibido o bien formación reglada (bonificable) o bien sesiones formativas divulgativas.

12.4.6. ORGANIZACIÓN DE LA DOCUMENTACIÓN Y DIGITALIZACIÓN DEL ARCHIVO

Este proyecto tiene parte organizativa y parte técnica. La parte organizativa está orientada al cumplimiento de la política de puesto despejado y por tanto está ligada al plan de formación establecido en el proyecto (PT-05) en el que se ha informado de las políticas de seguridad establecidas en la empresa.

Por otro lado, tiene una parte técnica que es la digitalización del Archivo de forma que la empresa no sea dependiente de una posible pérdida de información del

archivo en papel. Este proyecto está ligado también con la política de la empresa de convertirse en una "paper-less company" o empresa sin papeles.

Uno de los problemas que se ha detectado es la existencia de documentación antigua pero que está vigente por lo que es necesario proceder a su digitalización.

Para proceder a la digitalización del Archivo se ha firmado un convenio con la Universidad de forma que se contrate personal becado o en prácticas de archivística para realizar dicha digitalización y catalogación. Al mismo tiempo se han comprado dos impresoras multifunción de alta capacidad de escaneado de forma que no solamente sirvan para la digitalización, sino que puedan ser utilizadas para otros propósitos.

Por ultimo, para comprobar la evolución de la política de puesto despejado, se han planificado auditorías del cumplimiento en horario no laboral cada 3 meses y se han establecido indicadores sobre la evolución del cumplimiento de la política hasta alcanzar el objetivo del 99%.

El coste del proyecto es el siguiente:

- Coste de las auditorías de cumplimiento realizadas por personal externo: 1.000€ anuales.
- Coste de impresoras multifunción de alto volumen: 1.000€
- Coste del personal becado o en prácticas durante 6 meses: 4.800€

Plazo estimado para la ejecución del proyecto

El plazo para la ejecución del proyecto de digitalización del archivo se ha estimado en un año. Asimismo y debido a la necesidad de concienciación del personal se ha establecido un plazo de un año para alcanzar el 100% del cumplimiento en la política de puesto despejado.

12.4.7. PLAN DE GESTIÓN DE PERSONAL

Uno de los riesgos detectados en la empresa es el personal estratégico ya que no hay establecido en la empresa un plan de carrera del personal orientado a la renovación y la continuidad del personal directivo y estratégico existente, permitiendo la renovación con personal interno, teniendo como única alternativa actual el recurrir a personal externo que no conoce la empresa.

Por otro lado, tampoco se ha establecido en la empresa un plan de motivación del personal que tenga en cuenta las iniciativas y las expectativas que tiene el mismo y cual sería el posible desarrollo profesional del personal.

Para ello, el Departamento de Personal ha elaborado un proyecto conjuntamente con una empresa consultora externa especializada en recursos humanos orientado a lo siguiente:

- Conocer las expectativas y la motivación del personal.
- Establecer un plan de motivación del personal.
- Seleccionar a posibles candidatos en la empresa que puedan ser futuros directivos.
- Establecer un plan de carrera del personal adecuado a cada perfil.

Presupuesto y plazo estimado para la ejecución del proyecto.

El presupuesto que se ha reservado para este proyecto es de 12.000€ para ser ejecutado durante un plazo de 6 meses.

12.4.8. PLAN DE CONTINUIDAD DEL NEGOCIO

Uno de los proyectos fundamentales es la elaboración del plan orientado a garantizar la continuidad del negocio.

A este respecto, el objetivo de este proyecto es garantizar que la empresa pueda seguir prestando sus servicios y tener la información básica necesaria para el correcto funcionamiento de las actividades que desarrolla.

El plan de continuidad del negocio tendrá que abordar los siguientes aspectos:

- Las situaciones que pueden provocar la discontinuidad del negocio, indicando cuales son los activos afectados y las causas que podrían provocar esta discontinuidad.
- Elaboración de los planes de contingencias concretos, estableciendo responsabilidades y el punto de disparo de cada plan.
- Elaboración de los procedimientos de pruebas del plan de continuidad.
- Elaboración de los procedimientos de mejoras del plan de continuidad basados en las pruebas.

Las situaciones que tiene que controlar el plan de continuidad son las siguientes:

- Indisponibilidad de las instalaciones.
- Indisponibilidad de los servidores y las comunicaciones.
- Indisponibilidad de las aplicaciones y los datos.
- Indisponibilidad del personal.

En los proyectos citados anteriormente (proyectos PT-01 y PT-02) se han elaborado planes de contingencia parciales orientados a garantizar la continuidad de los servicios de sistemas de información básicos que son necesarios para que el negocio pueda seguir prestado sus servicios. Además, se ha establecido el tiempo en el que la información deberá está disponible en caso de que se tenga que activar el plan de continuidad, por lo que teniendo en cuenta el tiempo de restauración o de disponibilidad de la información en la otra localización, se establece el punto de disparo del plan. El responsable de iniciar estos planes parciales será el responsable del SGSI y en su defecto el responsable del Departamento de Sistemas de Información.

Por tanto, este proyecto tendrá que completar los planes parciales y establecer procedimientos encaminados a solventar las contingencias en las instalaciones y el personal.

12.4.8.1. SUBPROYECTO DE CONTINGENCIA DE INSTALACIONES.

Las instalaciones que pueden estar involucradas son las siguientes:

- Sede principal.
- Sede comercial.
- Autobuses.
- Oficinas en las estaciones de autobuses.

Por lo que este subproyecto tendrá que buscar alternativas a que se produzca una indisponibilidad temporal o permanente de las instalaciones.

Instalaciones de la sede principal

En este sentido se establece un plan con la sede comercial que actuará como sede principal en caso de contingencia de la sede principal. Además, tiene la característica que está lo suficientemente alejadas la una de la otra (más de 200 Km) por lo que una posible catástrofe que afecte a una, difícilmente afectará a la otra.

Para este proyecto es necesario adecuar y dotar de unas mínimas medidas de seguridad la sede comercial, que además va a albergar el CPD secundario. Por ello, hay que realizar una serie de modificaciones y adaptaciones. También es necesario dotarla de un servicio de comunicaciones de voz (Centralita VozIP) de contingencia que esté preparado para entrar en funcionamiento en caso que la sede principal no esté operativa.

El plan sería el siguiente:

- Habilitar las comunicaciones VozIP en la sede comercial.
- Habilitar el servicio call-center mínimo (1 operadora) en la sede comercial.
- Establecer los servicios mínimos de atención a la gestión para que trabajen de forma remota (teletrabajo) desde sus domicilios.
- Activar los planes de contingencia de servidores PT-02.

Instalaciones de la sede comercial

En el caso de producirse una contingencia en la sede comercial, será la propia sede principal la que actúe para absorber los servicios, encaminado los números de atención telefónica utilizados en la sede comercial al Departamento Comercial de la sede principal.

Por otro lado, el personal afectado trabajará de forma remota mediante teletrabajo.

Instalaciones en estaciones de autobuses

Respecto a las oficinas de estaciones de autobuses, se iniciarán conversaciones orientadas a la firma de acuerdos con oficinas de servicios multiempresas de las estaciones de autobuses para que presten los servicios de venta en caso de indisponibilidad de la oficina o incluso del personal.

Autobuses

Se debe establecer una estrategia orientada a que no estén todos los autobuses ubicados en un mismo lugar y en un mismo tiempo, especialmente en las horas nocturnas y de descanso.

Por otro lado, es necesario realizar un acuerdo con empresas del sector de autobuses que se dediquen al transporte discrecional, y por tanto no sean competencia directa, para que en caso de necesidad puedan alquilar autobuses de forma que con este acuerdo se vean beneficiadas ambas partes al ser recíproco.

Asimismo, será necesario revisar el contrato con la aseguradora para mejorar las prestaciones y ampliar la cobertura del seguro.

12.4.8.2. SUBPROYECTO DE CONTINGENCIA DE PERSONAL

El personal que puede verse afectado por este plan es el que directamente está relacionado con los servicios que presta la empresa:

- Conductores.
- Agentes comerciales y personal de las Estaciones de Autobuses.
- Personal de atención a clientes.
- Personal técnico.
- Resto del personal.

Parte de este proyecto se contempla en el proyecto de Gestión de Personal (PT-07) pero dicho proyecto está orientado a la mejora y dotación de posibles alternativas al personal estratégico y no contempla de forma plena al personal directo (conductores, administrativos, agentes comerciales, personal de atención a clientes) que al mismo tiempo es el personal menos cualificado de la empresa y por tanto, más sujeto a rotación.

Personal administrativo

Para el personal administrativo, la empresa va a proceder a firmar un acuerdo con centros de formación profesional para ofrecer prácticas a estudiantes y de esta forma, tener personal preparado que haya trabajado en la empresa que en caso necesario se pueda contratar y no haya que perder tiempo en formación.

Conductores

En el caso de conductores es un tema más complicado ya que los conductores necesitan haber pasado el CAP y además necesitan tener el carnet de conducir adecuado para el transporte de viajeros. Además, los conductores deben cumplir con una serie de horas de trabajo y horas de descanso por lo que no se puede ampliar el horario de los conductores que continúe en la empresa.

En este caso la alternativa que se ve viable es firmar un contrato con una empresa de colocación y de gestión de personal para que tenga disponibles conductores en caso de necesidad y al mismo tiempo se utilice dicha empresa para la sustitución de los conductores que están de baja o de vacaciones, de forma que exista una contrapartida para ambas partes.

Por otro lado, se crea una bolsa de trabajo de posibles conductores que quieran formar parte de la plantilla para que en caso de necesidad puedan ser contratados directamente por la empresa.

Presupuesto y plazo estimado para la ejecución del proyecto.

En proyecto debe quedar redactado y completado en un plazo no superior a los 2 meses. Es necesario tener en cuenta que este proyecto depende de otros que tienen un plazo superior en su ejecución, pero una vez estén aprobados dichos proyectos se irán incorporando a este plan general. El presupuesto que se ha dotado para este proyecto se ha estimado en 60.000€.

Existen proyectos que son cuantificables económicamente como son la dotación y mejoras de la sede comercial, la ampliación en las coberturas de los seguros, los gastos de personal en prácticas, los acuerdos con las empresas multiservicios de las estaciones de autobuses y los acuerdos con la empresa de colocación y de gestión de personal. Sin embargo, otros acuerdos no tienen una cuantificación económica

ya que están basados en la prestación de servicios de forma recíproca entre empresas para garantizar la continuidad.

12.4.9. ESQUEMA DE LA RED Y DE LA INFRAESTRUCTURA INFORMÁTICA

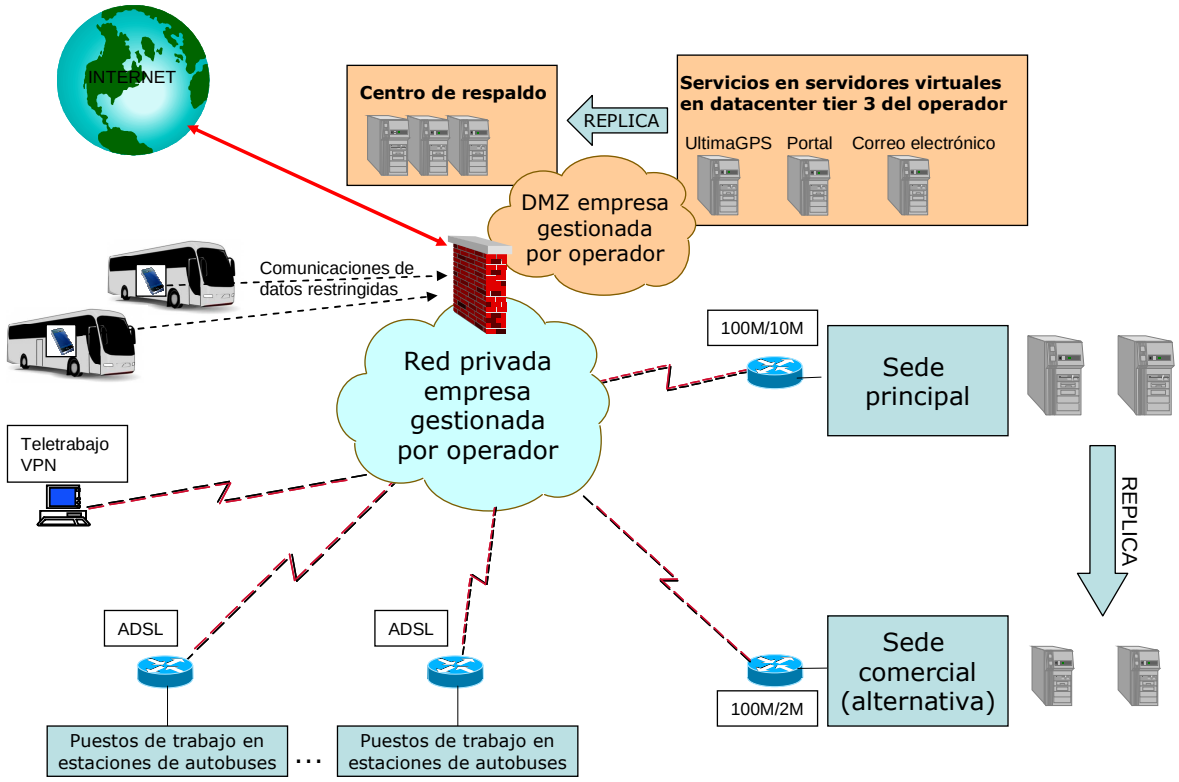

Figura 14: Infraestructura informática y de comunicaciones una vez realizado los proyectos de externalización incluidos en el plan de tratamiento.

12.5. ASIGNACIÓN DE PROYECTOS A ACTIVOS

A continuación se relaciona cada activo que es necesario que sea tratado para minimizar el riesgo con los proyectos que le afectan:

Código activo	Nombre del Activo	Planes de tratamiento del riesgo (Proyectos)
S-01	Venta y gestión	PT-01, PT-02, PT-05, PT-08
D-01	Datos ERP	PT-01, PT-02, PT-05
L-03	Edificio Oficinas Principal	PT-08
HW-09	FW checkpoint	PT-01
L-06	Autobuses	PT-08
S-02	Comercio electrónico	PT-01
COM-01	Internet principal	PT-01
HW-01	Grupo servidores CPD	PT-01, PT-02
D-03	Datos Producción	PT-01, PT-02, PT-04, PT-05
SW-02	Aplicación ÚltimaGPS	PT-01, PT-05
S-03	Comunicaciones comerciales	PT-03
D-04	Correo electrónico	PT-01
SW-04	Aplicación portal	PT-01
SW-01	Aplicación SAP/R3	PT-05, PT-02
L-01	CPD principal	PT-08
M-02	Documentación Negocio	PT-06
D-02	Datos Servidor ficheros	PT-01, PT-02, PT-05
L-04	Oficinas comercial	PT-08
P-01	Personal estratégico	PT-07
HW-04	Dispositivos autobuses	PT-04

12.6. RESUMEN Y PLANIFICACIÓN DE PROYECTOS

Una vez que se ha descrito en detalle todos los proyectos, incluido el necesario para la elaboración de los procedimientos de gestión de los controles, se incluye una planificación detallada que incluye recursos y plazos asignados a cada proyecto.

Códigos de recursos

Para una mejor compresión, especialmente en el diagrama de Gantt, se han realizado las siguientes codificaciones respecto a los recursos asignados a cada proyecto:

- RSGSI: Responsable del SGSI.
- RSEG: Responsables de Seguridad.
- DSI: Departamento de Sistemas de Información.
- CSI: Comité de Seguridad de la Información.
- DIR: Dirección.
- DAC: Persona del departamento de Auditoría y Control.
- RHR: Responsable departamento de Recursos Humanos.
- DFI: Director Financiero.
- DCOM: Director Comercial.

- DPRO: Director de Producción.
- PPRAC: Personal en prácticas.
- CRH: Empresa consultora y formadora externa para la gestión de RR.HH.
- SESI: Consultora externa para la implantación y formación en el SGSI.
- SEXT: Empresa de servicios externos de informática y seguridad.
- COM: Operador de Comunicaciones para la externalización de servicios.

Diagrama de Gantt de los proyectos y recursos

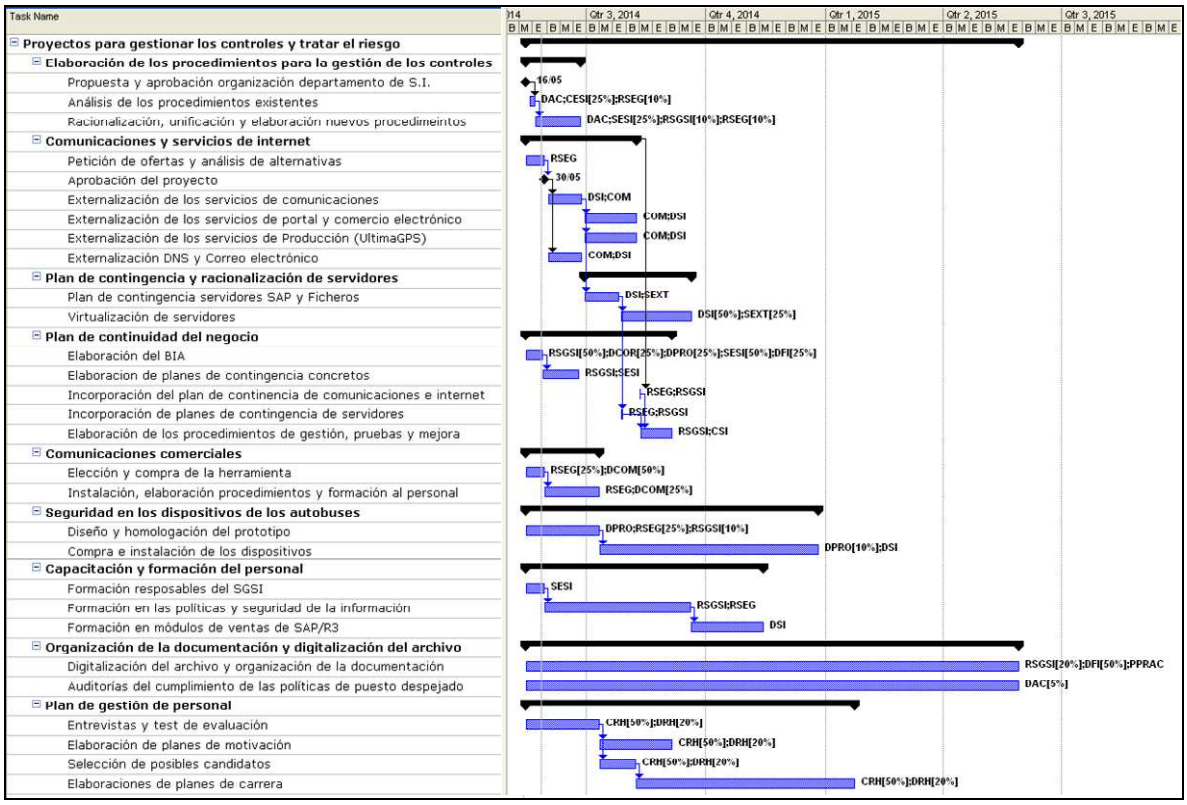

Figura 15: Diagrama de Gantt con la planificación de los proyectos y los recursos asignados.

12.7. EVOLUCIÓN DE LOS RESULTADOS

Los proyectos van a tener una implicación en la reducción del riesgo de los activos y en el cumplimiento de los dominios de control.

Para poder comprobar la evolución, se indica el estado del nivel de cumplimiento de los dominios de control previo a la implantación de los proyectos, de forma que se puedan comparar los resultados con los obtenidos en la auditoría que se realice con posterioridad a la implantación y desarrollo de los proyectos.

12.7.1. ESTADO DEL CUMPLIMIENTO DE LOS DOMINIOS DE FORMA PREVIA

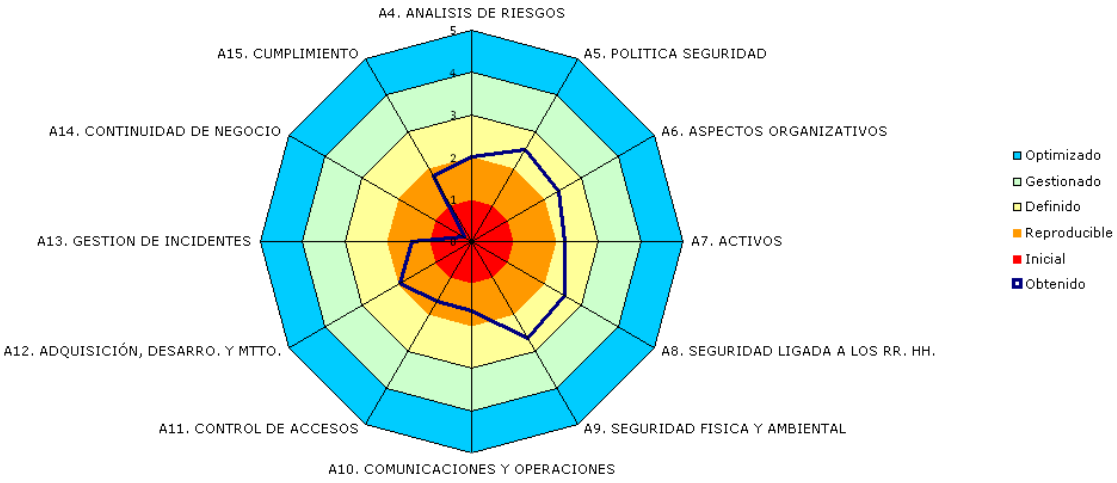

Figura 16: Grafico tipo radar del nivel de cumplimiento de los dominios de control de forma previa al desarrollo de los proyectos y elaboración de los procedimientos de gestión de los controles.

12.7.2. ESTADO DEL CUMPLIMIENTO DE LOS DOMINIOS POSTERIOR A LA IMPLANTACIÓN DE LOS PROYECTOS

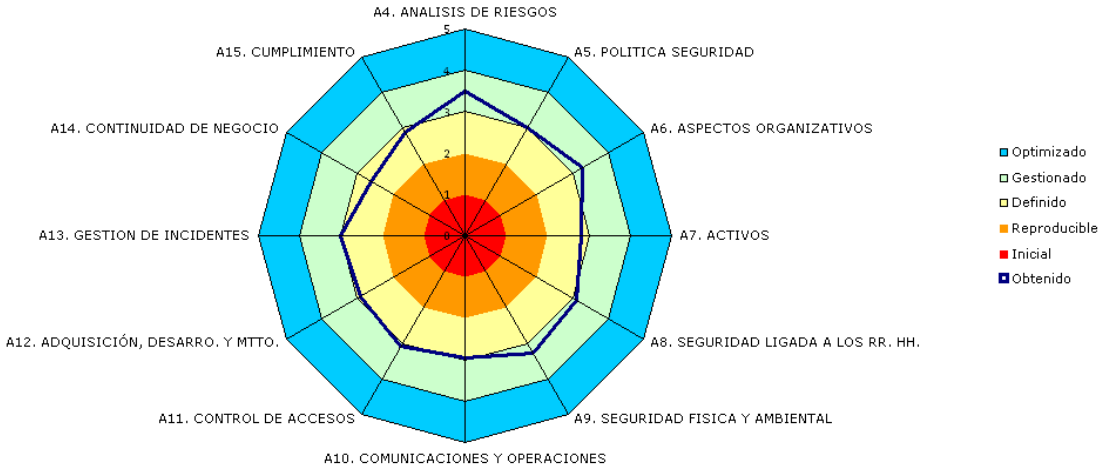

Figura 17: Grafico tipo radar del nivel de cumplimiento de los dominios de control de forma posterior a la aprobación y desarrollo de los proyectos y elaboración y aprobación de los procedimientos de gestión de los controles.

13. AUDITORÍA DEL CUMPLIMIENTO

Una vez aprobados los planes de tratamiento y desarrollados y aprobados los procedimientos para la implantación de los controles que están incluidos en la declaración de aplicabilidad, y una vez pasado un plazo prudencial, que se puede estimar entre 4 y 6 meses, se procede a realizar una auditoría de la implantación del SGSI y de los controles, así como un análisis de la madurez que tienen los controles implantados.

13.1. AUDITORÍA DEL CUMPLIMIENTO DEL SGSI

Se ha procedido a realizar la primera auditoría interna de acuerdo con el Plan de Auditoría establecido en el procedimiento "SI-PG-AUD-01: Auditorías Internas".

El informe de auditoría está en el documento SI-IA-001-01.pdf.

Las no conformidades detectadas en la auditoría interna serán tratadas conforme al procedimiento "SI-PG-GNC-01: Gestión de las No Conformidades"

13.2. EVALUACIÓN DE LA MADUREZ DE LOS CONTROLES

A continuación se incluye el nivel de madurez de cada control de acuerdo con la tabla de madurez definida en el procedimiento "SI-PG-MAR-01: Metodología de Análisis de Riesgos".

REQUISITO	CMM	OBSERVACIONES
A.5 POLÍTICA DE SEGURIDAD **A.5.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**		
5.1.1 Doc. de política de S. I.	**L3**	La política está definida por la Dirección, se ha divulgado entre todo el personal y se ha impartido formación.
5.1.2 Revisión de la política de S.I.	**L3**	Se han definido los procedimientos de revisión y están asignadas las responsabilidades.
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN **A.6.1 ORGANIZACIÓN INTERNA**		
6.1.1. Compromiso de la Dirección con la S.I.	**L4**	La Dirección ha establecido la política y las directrices y presta todo el apoyo necesario. Se puede comprobar y medir dicha implicación mediante la existencia de actas y correos.
6.1.2 Coordinación de la S. I.	**L2**	Se han definido las responsabilidades dentro de la organización pero todavía existen departamentos que es necesario se involucren más activamente en el sistema.
6.1.3 Asignación de responsabilidades relativas a la S.I.	**L4**	Están definidos los responsables y los miembros del Comité de Seguridad y existen actas de reuniones que se pueden evidenciar.
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.	**L3**	Se ha definido el procedimiento de autorización y aprobación de recursos. Actualmente solamente se puede evidenciar que se han aprobado los proyectos dentro del plan de tratamiento.
6.1.5 Acuerdos de confidencialidad	**L4**	Está definido el procedimiento y se puede evidenciar que todos los trabajadores y personal externo tienen firmado un acuerdo de confidencialidad para proteger información confidencial de la empresa y los datos de carácter personal.

6.1.6 Contacto con las autoridades	**L3**	Está establecido el procedimiento y existe una circular de la empresa donde se informa a los trabajadores de los números de emergencia y de los números de teléfono de contacto que deben ser conocidos por todos los trabajadores.
6.1.7 Contacto con grupos de especial interés	**L3**	Se ha establecido el procedimiento por el cual el Responsable de Seguridad, además de recibir las noticias y boletines de Inteco, se ha suscrito a las noticias de la AEPD y boletines de noticias de seguridad. Asimismo, se ha aprobado la asistencia del responsable a un congreso anual en seguridad.
6.1.8 Revisión independiente de la S.I.	**L3**	Se ha establecido el procedimiento y ésta es la primera auditoría que se realiza.
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN **A.6.2. TERCEROS**		
6.2.1 Identificación de los riesgos derivados del acceso de terceros	**L3**	Se han definido los procedimientos y es necesario analizar la evolución y medición de los mismos.
6.2.2 Tratamiento de la seguridad en la relación con clientes	**L3**	Se han definido los procedimientos y es necesario analizar la evolución y medición de los mismos.
6.2.3 Tratamiento de la seguridad en contratos con terceros	**L4**	Se han definido los procedimientos y existen contratos de confidencialidad con todos los proveedores de servicios. Se pueden comprobar en los contratos firmados.
A.7 GESTIÓN DE ACTIVOS **A.7.1 RESPONSABILIDAD SOBRE LOS ACTIVOS**		
7.1.1 Inventario de activos	**L2**	Se ha realizado un inventario de activos para realizar el análisis de riesgos. No está catalogado todo el inventario completo de activos de la organización de forma coordinada, está en proceso.
7.1.2 Propiedad de los activos	**L3**	Están definidos los propietarios de los activos y han participado en las sesiones de formación específica para responsables.
7.1.3 Uso aceptable de los activos	**L3**	Todo el personal conoce las políticas de seguridad que ha establecido la organización y han recibido formación específica al respecto.
A.7 GESTIÓN DE ACTIVOS **A.7.2 CLASIFICACIÓN DE LA INFORMACIÓN**		
7.2.1 Directrices de clasificación	**L3**	Se han establecido las políticas y se han divulgado las directrices.
7.2.2 Etiquetado y manipulado de la Inf.	**L3**	La política y los procedimientos están establecidos. Es necesario analizar el nivel de evolución.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS **A.8.1 ANTES DEL EMPLEO**		
8.1.1 Funciones y responsabilidades	**L3**	Todo el personal ha sido formado en las políticas de seguridad y tiene conocimiento de sus funciones y obligaciones en el tratamiento de la información y los datos personales.
8.1.2 Investigación de antecedentes	**L3**	Está establecido el procedimiento por el Departamento de RR.HH.

8.1.3 Términos y condiciones de contratación	**L4**	Está establecido el procedimiento y se sigue desde hace años. Todos los trabajadores tienen firmado un acuerdo de confidencialidad y ahora se le entrega la política de seguridad de la empresa en el momento de la contratación.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS A.8.2 DURANTE EL EMPLEO		
8.2.1 Responsabilidades de la Dirección	**L3**	La Dirección ha establecido y se ha encargado de que se divulguen las políticas de obligado cumplimiento
8.2.2 Concienciación, formación y capacitación en S. I.	**L3**	Todos los trabajadores han recibido formación en las políticas de seguridad y en procedimientos de seguridad.
8.2.3 Proceso disciplinario	**L3**	Está definido en los procedimientos y en las políticas de la empresa.
A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS A.8.3 CESE DEL EMPLEO O CAMBIO DE PUESTO DE TRABAJO		
8.3.1 Responsabilidad del cese o cambio	**L3**	Los procedimientos se han actualizado y distribuido.
8.3.2 Devolución de activos	**L3**	Los procedimientos se han actualizado y distribuido.
8.3.3 Retirada de los derechos de acceso	**L3**	Los procedimientos se han actualizado y distribuido.
A.9 SEGURIDAD FÍSICA Y AMBIENTAL A.9.1 ÁREAS SEGURAS		
9.1.1 Perímetro de seguridad física	**L4**	Se han normalizado y actualizado los procedimientos. Asimismo, existen controles de acceso tanto a las instalaciones como a las zonas de acceso restringido (CPD, archivo, etc…) y se pueden medir el cumplimiento del control.
9.1.2 Controles físicos de entrada	**L4**	Se han normalizado y actualizado los procedimientos. Existe un control a la entrada del edificio y todas las personas que van a acceder se deben identificar. Asimismo, se controlan y se registran los accesos durante el tiempo legalmente establecido
9.1.3 Seguridad de oficinas, despachos e instalaciones	**L3**	Se han normalizado y actualizado los procedimientos. Existe control de acceso a las oficinas y se controla que el personal que accede a las mismas esté autorizado.
9.1.4 Protección de amenazas externas y de origen ambiental	**L4**	Se ha establecido el procedimiento para controlar el cumplimiento y el mantenimiento de los sistemas de control.
9.1.5 Trabajo en áreas seguras	**L3**	Se han definido y distribuido los procedimientos entre el personal afectado.
9.1.6 Áreas de acceso público, y de carga y descarga	**L4**	Se han normalizado los procedimientos y están definidas las zonas de carga y descarga. Además se controla que no exista información en las zonas donde pueden acceder los proveedores.
A.9 SEGURIDAD FÍSICA Y AMBIENTAL A.9.2 SEGURIDAD DE LOS EQUIPOS		
9.2.1 Emplazamiento y protección de equipos	**L4**	Se han normalizado los procedimientos y se han distribuido entre el personal afectado. Los servidores están instalados en zona de acceso restringido. Los equipos del personal que atiende al público están dotados de pantalla con filtros de privacidad.

9.2.2 Instalaciones de Suministro	**L3**	El CPD está dotado de SAI. Los equipos en los periféricos tienen un pequeño SAI. Se ha dotado de SAI igualmente el centro de respaldo de la oficina comercial.
9.2.3 Seguridad del cableado	**L4**	El sistema de cableado de las oficinas no está en zonas públicas ni accesibles por personal no autorizado.
9.2.4 Mantenimiento de los equipos	**L3**	Los servidores (equipos críticos) tienen contrato de mantenimiento con los fabricantes. Además, se ha procedido a externalizar servicios por lo que existen equipos libres que pueden ser utilizados de respaldo.
9.2.5 Seguridad de los equipos fuera de las instalaciones	**L2**	Se han establecido las políticas y se han divulgado. Se ha formado al personal. Asimismo, se han escrito y divulgado los procedimientos de obligado cumplimiento, pero no todo el personal ha sido formado.
9.2.6 Reutilización o retirada segura de equipos	**L2**	Se ha normalizado el procedimiento existente y se ha divulgado entre el personal afectado. Existen algunos registros que evidencian que se está llevando a cabo el procedimiento parcialmente.
9.2.7 Retirada de materiales propiedad de la empresa	**L3**	Se ha normalizado el procedimiento existente y se ha divulgado entre el personal afectado. Existen algunos registros que evidencian que se está llevando a cabo el procedimiento.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN**		
10.1.1 Documentación de los procedimientos de operación	**L4**	Están establecidos y normalizados todos los procedimientos de operación de los sistemas.
10.1.2 Gestión de cambios	**L3**	Se ha establecido el procedimiento para la gestión de los cambios tanto en los sistemas mantenidos localmente como los externalizados.
10.1.3 Segregación de tareas	**L3**	Se ha establecido un procedimiento y se ha prohibido a los desarrolladores el acceso al entorno de producción de forma que se eviten errores y que por urgencias puedan desarrollar en producción.
10.1.4 Separación de los recursos de desarrollo, prueba y operación	**L4**	Están separados los entornos de desarrollo, prueba y producción. Además, se ha establecido el procedimiento que se debe seguir y el personal de desarrollo conoce la forma de trabajar.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS**		
10.2.1 Provisión de servicios	**L3**	Se han incluido todos los requisitos de seguridad en los contratos de servicios que se han firmado para la externalización de las comunicaciones y los servidores.
10.2.2 Supervisión y revisión de los servicios prestados por terceros	**L1**	Se ha incluido en algunos contratos de servicios la posibilidad de realizar auditorías periódicas. No se ha planificado ninguna auditoría en proveedores.
10.2.3 Gestión del cambios en los servicios prestados por terceros	**L2**	Se ha previsto en los contratos de externalización la posibilidad de realizar cambios y mejoras. Pero no se ha incluido en todos los contratos.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.3 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA**		

10.3.1 Gestión de capacidades	**L3**	Se han establecido los procedimientos orientados a controlar la capacidad del sistema y preveer futuros requisitos. En el SLA firmado con el prestador de servicios se ha incluido la opción de poder incrementar los recursos.
10.3.2 Aceptación del sistema	**L3**	Se ha establecido un procedimiento en el que las nuevas versiones deben ser probadas antes de su entrada en producción.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.4 PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y DESCARGABLE		
10.4.1 Controles contra el código malicioso	**L4**	Se han establecido los procedimientos de control y de medición.
10.4.2 Controles contra el código descargado en el cliente	**L3**	Se ha desarrollado y unificado el procedimiento y se ha difundido entre el personal.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.5 COPIAS DE SEGURIDAD		
10.5.1 Copias de Seguridad de la Información.	**L4**	Se ha establecido el procedimiento tanto para las aplicaciones que se gestionan internamente como las que se han externalizado.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.6 GESTIÓN DE LA SEGURIDAD DE LAS REDES		
10.6.1 Controles de red	**L4**	Se han externalizado los servicios y se realizan mediciones por el proveedor de servicios que son analizadas por el personal del Departamento de Informática.
10.6.2 Seguridad de los servicios de red	**L4**	Se han externalizado los servicios y se realizan mediciones por el proveedor de servicios que son analizadas por el personal del Departamento de Informática.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.7 MANIPULACIÓN DE LOS SOPORTES		
10.7.1 Gestión de soportes extraíbles	**L2**	Se ha establecido la política y se ha dado a conocer a todo el personal. Asimismo, se han establecido los procedimientos y controles técnicos. Pero aún no se está llevando a cabo al 100%.
10.7.2 Retirada de soportes	**L3**	Se ha establecido la política y se ha dado a conocer a todo el personal. Asimismo, se han establecido los procedimientos y controles técnicos.
10.7.3 Procedimientos de manipulación de la Información.	**L3**	Se ha establecido la política y se ha dado a conocer a todo el personal. Asimismo, se han establecido los procedimientos y controles técnicos.
10.7.4 Seguridad de la documentación del sistema	**L3**	Se ha establecido el procedimiento respecto a cómo se debe custodiar la documentación del sistema.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES A.10.8 INTERCAMBIO DE INFORMACIÓN		
10.8.1 Políticas y procedimientos de intercambios de información	**L3**	Se han establecido los procedimientos y se han divulgado entre el personal.
10.8.2 Acuerdos de intercambio	**L3**	Se han establecido los procedimientos y se han divulgado entre el personal.

10.8.3 Soportes físicos en transito	**N/A**	No es de aplicación de acuerdo con la Declaración de Aplicabilidad.
10.8.4 Mensajería electrónica	**L3**	Se ha establecido la política y se ha dado a conocer entre el personal. Asimismo, se han desarrollado los procedimientos específicos respecto a como el personal autorizado debe realizar las comunicaciones comerciales.
10.8.5 Sistemas de información empresariales	**L3**	Toda la información empresarial se encuentra en SAP que está dotado de los controles de acceso por niveles de privilegios de usuarios.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.9 SERVICIOS DE COMERCIO ELECTRÓNICO**		
10.9.1 Comercio electrónico	**L3**	Se ha establecido y normalizado el procedimiento. Asimismo, se ha externalizado el servidor que presta el servicio de forma que se eviten ataques al mismo.
10.9.2 Transacciones en línea	**L3**	Se ha establecido y normalizado el procedimiento. Asimismo, se ha incrementado la seguridad con la externalización de los servicios.
10.9.3 Información públicamente disponible	**L3**	Se ha establecido la política y se ha divulgado. Asimismo, se ha establecido el procedimiento que se ha divulgado entre las personas afectadas.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES **A.10.10 SUPERVISIÓN**		
10.10.1 Registro de auditorias	**L3**	Se ha establecido el procedimiento y se han activados las auditorías en los sistemas.
10.10.2 Supervisión del uso del sistema	**L1**	Se ha establecido el procedimiento pero no se están realizando las revisiones en todos los sistemas.
10.10.3 Protección de la información de los registros	**L3**	Está establecido el procedimiento y además los registros solamente son accedidos por personal autorizado.
10.10.4 Registros de administración y operación	**L3**	Se ha establecido el procedimiento y se han activados las auditorías en los sistemas.
10.10.5 Registro de fallos	**L1**	Se ha establecido el procedimiento pero actualmente no se están analizando los registros.
10.10.6 Sincronización del reloj	**L3**	Se ha establecido el procedimiento y se han incluido en las directivas del sistema de forma que la sincronización es automática sin la intervención del usuario.
A.11 CONTROL DE ACCESO **A.11.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO**		
11.1.1 Política de control de acceso	**L3**	Se ha establecido la política y se ha divulgado entre todo el personal.
A.11 CONTROL DE ACCESO **A.11.2 GESTIÓN DE ACCESO DE USUARIO**		
11.2.1 Registro de usuario	**L4**	El procedimiento está establecido y normalizado. Existen registros que permiten conocer el estado de cumplimiento y medirlo.
11.2.2 Gestión de privilegios	**L4**	El procedimiento está establecido y normalizado y es conocido por los responsables de autorizar los privilegios de acceso así como por el personal de Informática. Se registran todas las peticiones por lo que se puede conocer el estado de cumplimiento y medirlo.

11.2.3 Gestión de contraseñas de usuario	**L3**	El procedimiento de gestión y asignación de contraseñas está establecido y normalizado. Se ha divulgado entre todo el personal. Asimismo, el procedimiento de asignación de contraseña inicial se ha mejorado.
11.2.4 Revisión de los derechos de acceso a usuario	**L3**	Se ha establecido el procedimiento de revisión y es conocido por las responsables de realizar la revisión y comprobación.
A.11 CONTROL DE ACCESO **A.11.3 RESPONSABILIDADES DE USUARIO**		
11.3.1 Uso de contraseña	**L3**	Se han divulgado las políticas y se han establecido procedimiento de uso de contraseña compleja por los usuarios.
11.3.2 Equipo de usuarios desatendido	**L3**	Se ha establecido los procedimientos y son conocidos por el personal que debe llevarlo a cabo. Además, el personal ha sido formado en la política de bloqueo de terminal sin tener que esperar al bloqueo automático.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia	**L2**	Se ha establecido la política y se ha divulgado entre todo el personal. Aún no se está cumpliendo al 100% ya que no todo el personal está convencido por lo que será necesario reforzar la formación en este aspecto.
A.11 CONTROL DE ACCESO **A.11.4 CONTROL DE ACCESO A LA RED**		
11.4.1 Política de uso de los servicios en red	**L4**	Se han divulgado las políticas, se han establecido los procedimientos y se controlan que los accesos y el uso de la red sean correctos.
11.4.2 Autenticación de usuario para conexiones externas	**L4**	Se ha externalizado el servicio en un operador de comunicaciones externo de forma que existen indicadores que pueden ser controlados y analizados por el personal de la empresa. Además, cualquier mal uso o incidente es notificado al Responsable de Seguridad.
11.4.3 Identificación de los equipos en las redes	**N/A**	No es de aplicación de acuerdo con la Declaración de Aplicabilidad.
11.4.4 Diagnóstico remoto y protección de los puertos de configuración	**L3**	Se ha desarrollado el procedimiento y es conocido por el personal que debe realizar esta labor ya que ha participado en la redacción del mismo.
11.4.5 Segregación de las redes	**L3**	Los servicios de red están externalizados, el procedimiento de gestión del cortafuego externalizado está establecido y es conocido por el personal encargado.
11.4.6 Control de la conexión a la red	**L4**	Se ha externalizado el servicio en un operador de comunicaciones externo de forma que existen indicadores que pueden ser controlados y analizados por el personal de la empresa. Además, cualquier mal uso o incidente es notificado al Responsable de Seguridad.
11.4.7 Control de encaminamiento (routing) de red	**L4**	Las comunicaciones se han externalizado completamente en un proveedor externo que envía datos de tráfico y de uso.
A.11 CONTROL DE ACCESO **A.11.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO**		

11.5.1 Procedimientos seguros de inicio de sesión	**L3**	Se han unificado y normalizado los procedimientos existentes y se ha formado al personal del Departamento de Informática.
11.5.2 Identificación y autenticación de usuario	**L1**	Se han unificado y normalizado los procedimientos existentes y se ha formado al personal del Departamento de Informática. Pero el procedimiento no está implantado ya que se siguen utilizando usuarios administradores genéricos.
11.5.3 Sistema de gestión de contraseñas	**L3**	Se han unificado y normalizado los procedimientos existentes y se ha formado al personal del Departamento de Informática.
11.5.4 Uso de los recursos del sistema	**L3**	Se han unificado y normalizado los procedimientos existentes y se ha formado al personal del Departamento de Informática.
11.5.5 Desconexión automática de sesión	**L3**	Se han unificado y normalizado los procedimientos existentes y se ha formado al personal del Departamento de Informática.
11.5.6 Limitación del tiempo de conexión	**L1**	No se han implantado el procedimiento.
A.11 CONTROL DE ACCESO **A.11.6 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN**		
11.6.1 Restricción del acceso a la información	**L4**	Se han establecido los procedimientos de control de acceso y se han establecido indicadores para comprobar que el control está implantado.
11.6.2 Aislamiento de sistemas sensibles	**N/A**	No es de aplicación de acuerdo con la Declaración de Aplicabilidad.
A.11 CONTROL DE ACCESO **A.11.7 ORDENADORES PORTÁTILES Y TELETRABAJO**		
11.7.1 Ordenadores portátiles y comunicaciones móviles	**L3**	Se ha definido la política y se ha formado al personal. Asimismo, se han establecido procedimientos de obligado cumplimiento que se han entregado al personal que realiza teletrabajo y al personal de Informática que debe realizar las comprobaciones e instalaciones pertinentes.
11.7.2 Teletrabajo	**L3**	Se ha definido la política y se ha formado al personal. Asimismo, se han establecido procedimientos de obligado cumplimiento que se han entregado al personal que realiza teletrabajo.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.1 REQUISITOS DE SEGURIDAD DE LOS S. I.**		
12.1.1 Análisis y especificación de los requerimientos de seguridad	**L3**	Se ha establecido las normas y requisitos que deben cumplir los proveedores tanto para el desarrollo de sistemas como para la prestación de servicios.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. **A.12.2 TRATAMIENTO CORRECTO DE LAS APLICACIONES**		
12.2.1 Validación de los datos de entrada	**L3**	Se ha establecido el procedimiento ya que de forma previa existían manuales aislados. Se ha divulgado entre el personal que debe realizar los controles.
12.2.2 Control del procesamiento interno	**L3**	Se ha establecido el procedimiento ya que de forma previa existían manuales aislados. Se ha divulgado entre el personal que debe realizar los controles.
12.2.3 Integridad de los mensajes	**L3**	Se ha establecido el procedimiento ya que de forma previa existían manuales aislados. Se ha divulgado entre el personal que debe realizar los controles.

12.2.4 Validación de los datos de salida	**L3**	Se ha establecido el procedimiento ya que de forma previa existían manuales aislados. Se ha divulgado entre el personal que debe realizar los controles.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. A.12.3 CONTROLES CRIPTOGRÁFICOS		
12.3.1 Política de uso de los controles criptográficos	**L3**	Se ha establecido la política y se ha divulgado entre todo el personal.
12.3.2 Gestión de claves	**L3**	Se ha establecido la política y se ha divulgado entre todo el personal. Asimismo, se ha establecido el procedimiento y se ha formado al personal involucrado.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. A.12.4 SEGURIDAD DE LOS ARCHIVOS DE SISTEMA		
12.4.1 Control del software de explotación	**L3**	Se han completado y unificado los procedimientos existentes y el personal del Departamento de Informática conoce dicho procedimiento y está formado.
12.4.2 Protección de los datos de prueba del sistema	**L3**	Se han completado y unificado los procedimientos existentes y el personal del Departamento de Informática conoce dicho procedimiento y está formado.
12.4.3 Control de acceso al código fuente de los programas	**L3**	Se han completado y unificado los procedimientos existentes y el personal del Departamento de Informática conoce dicho procedimiento y está formado.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. A.12.5 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE		
12.5.1 Procedimientos de control de cambios	**L3**	Se han completado y unificado los procedimientos existentes y el personal del Departamento de Informática conoce dicho procedimiento y está formado.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	**L3**	Se han completado y unificado los procedimientos existentes y el personal del Departamento de Informática conoce dicho procedimiento y está formado.
12.5.3 Restricciones a los cambios en los paquetes de software	**L3**	Se han completado y unificado los procedimientos existentes y el personal del Departamento de Informática conoce dicho procedimiento y está formado.
12.5.4 Fugas de información	**L3**	Se han completado y unificado los procedimientos existentes y el personal del Departamento de Informática conoce dicho procedimiento y está formado.
12.5.5 Externalización del desarrollo de software	**L3**	Se han completado y unificado los procedimientos existentes y el personal del Departamento de Informática conoce dicho procedimiento y está formado.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S. I. A.12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA		
12.6.1 Control de las vulnerabilidades técnicas	**L2**	Se ha establecido dentro del plan de auditoría, la realización de pruebas de control de vulnerabilidades pero el personal de Informática no se ha formado todavía en el uso de las herramientas.

A.13 GESTIÓN DE INCIDENTES DE S. I. **A.13.1 NOTIFICACIÓN DE EVENTOS Y PUNTOS DÉBILES DE S. I.**		
13.1.1 Notificación de los eventos de S. I.	**L3**	Se han definido los procedimientos y se ha informado a todo el personal de cómo se deben realizas las notificaciones.
13.1.2 Notificación de los puntos debilidades de Seguridad	**L3**	Se han definido los procedimientos y se ha informado a todo el personal de cómo se deben realizas las notificaciones.
A.13 GESTIÓN DE INCIDENTES DE S. I. **A.13.2 GESTIÓN DE INCIDENTES DE S. I. Y MEJORAS**		
13.2.1 Responsabilidades y procedimientos	**L3**	Se han definido los procedimientos y se ha formado al personal involucrado.
13.2.2 Aprendizaje de los incidentes de S. I.	**L3**	Se han definido los procedimientos y se ha formado al personal involucrado.
13.2.3 Recopilación de evidencias	**L3**	Se han definido los procedimientos y se ha formado al personal involucrado.
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO **A.14.1 ASPECTOS DE S. I. EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
14.1.1 Inclusión de la S. I. en el proceso de gestión de la continuidad del negocio	**L2**	Se ha realizado un proyecto para la redacción de un plan de continuidad del negocio. Pero todavía no está entrenado ni formado todo el personal involucrado.
14.1.2 Continuidad del negocio y evaluación de riesgos	**L3**	Se ha realizado el plan teniendo en cuenta los activos afectados y los riesgos a los que están expuestos. El personal que debe mantener el plan está formado. Además, ha participado en la redacción del mismo.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la S. I.	**L3**	Se han realizado los planes de continuidad del negocio.
14.1.4 Marco de referencia para la planificación de la continuidad del negocio	**L3**	Se ha tenido en cuenta el negocio para la realización del plan de continuidad del negocio y no solamente los sistemas de información.
14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	**L2**	Se ha establecido el plan de pruebas pero todavía no se ha realizado ninguna de forma coordinada. Se han realizado pruebas aisladas.
A.15 CUMPLIMIENTO **A.15.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES**		
15.1.1 Identificación de la legislación aplicable	**L3**	Se ha establecido el procedimiento para identificar la legislación aplicable y las actualizaciones de la misma. Se ha formado al personal encargado de llevar a cabo el procedimiento.
15.1.2 Derechos de propiedad intelectual	**L3**	Se ha aprobado un plan de licenciamiento correcto de todo el aplicativo utilizado en la organización.
15.1.3 Protección de los documentos de la organización	**L3**	Se ha establecido la política y se han desarrollado los procedimientos.

15.1.4 Protección de datos y privacidad de la Inf. de carácter personal	**L4**	Todos los procedimientos de protección de datos están implantados y se realizan las auditorías de cumplimiento. Además, las acciones de mejora y correctivas se han integrado con el SGSI.
15.1.5 Prevención del uso indebido de los recursos de tratamiento de la Inf.	**L3**	Se ha definido la política y se ha divulgado entre todo el personal. Asimismo, los usuarios, al no tener privilegios de administración, no pueden instalar ni modificar ningún programa del ordenador.
15.1.6 Regulación de los controles criptográficos	**L3**	Se han establecido las políticas y desarrollado los procedimientos de uso de firma digital.
A.15 CUMPLIMIENTO **A.15.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO**		
15.2.1 Cumplimiento de las políticas y normas de Seguridad	**L3**	Se ha establecido un plan de revisión del cumplimiento de normas y políticas. Se ha formado a los responsables de llevar a cabo dichas revisiones y se ha informado al personal que se van a realizar las revisiones.
15.2.2 Comprobación del cumplimiento técnico	**L1**	Se ha establecido el procedimiento de comprobación del cumplimiento técnico pero el personal no está entrenado ni se ha realizado ninguna prueba.
A.15 CUMPLIMIENTO **A.15.3 CONSIDERACIONES SOBRE LA AUDITORIA DE LOS S. I.**		
15.3.1 Controles de auditoría de los S. I.	**L3**	Se ha establecido el procedimiento de realización de auditorías en el que se ha tenido en cuenta los casos en los que las pruebas de auditoría puedan poner en peligro la continuidad del sistema.
15.3.2 Protección de las herramientas de auditoría de los S. I.	**L3**	Dentro del Departamento de Sistemas de Información se han adquirido herramientas para auditar y monitorizar los sistemas. Se ha establecido el procedimiento de uso y de salvaguardia de los registros de auditoría y se ha formado al personal.

13.2.1 RESULTADOS OBTENIDOS

A continuación se representa de forma gráfica los resultados obtenidos de forma porcentual por cada nivel de madurez.

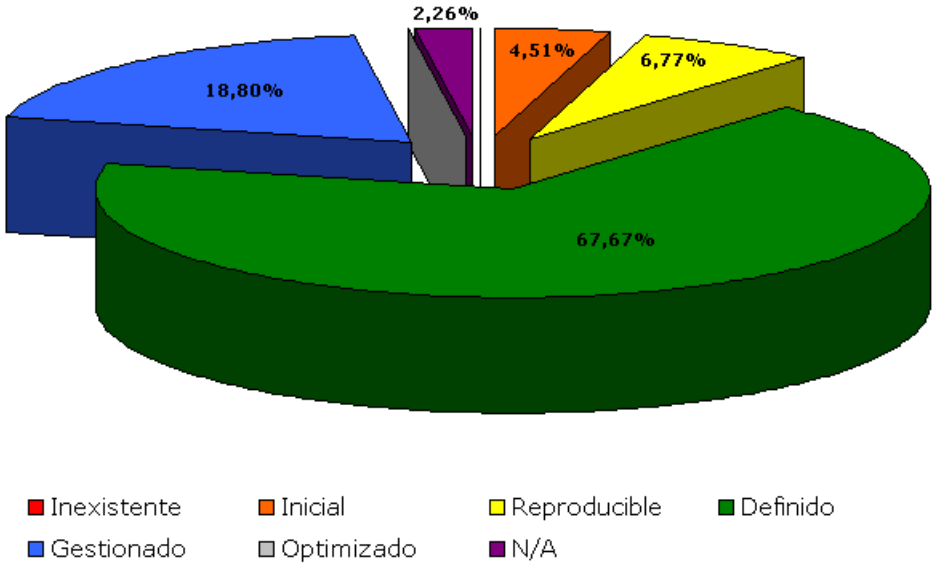

Figura 18: Grafico con el porcentaje de controles por nivel de madurez.

14. RESUMEN EJECUTIVO

El TFM ha consistido en el desarrollo de un sistema de seguridad de la información basado en la norma ISO 27001:2005 en una empresa privada del sector transporte.

El modelo de empresa elegido podría perfectamente adaptarse a numerosas pequeñas y medianas empresas que comienzan a exponerse a riesgos al aumentar su tamaño y al mismo tiempo utilizar servicios de Internet como comercio electrónico, comunicaciones comerciales, etc... Asimismo, estas empresas se encuentran en la disyuntiva entre intentar minimizar los riesgos de forma interna o por el contrario externalizar sus servicios de sistemas de información.

Se ha elegido una empresa que ya tiene implantado sistemas de gestión (SGC y SGA) por lo que conoce el modelo de mejora continua y solamente tiene que conocer e implantar las partes específicas de un SGSI. En este aspecto, se ha hecho especial hincapié en que la empresa cumple con lo establecido en la LOPD, no de forma testimonial como la mayoría de las empresas, sino llevando a cabo los procedimientos establecidos en el Documento de Seguridad y realizando las auditorías bienales, hecho que se ha evidenciado en el Análisis GAP del inicio del proyecto.

Por tanto, la empresa se encuentra en un momento que sabe que tiene que realizar acciones encaminadas a reforzar la seguridad, conocer los riesgos a los que está expuesta y tratarlos adecuadamente. Todo sin olvidar la necesidad de un cumplimiento legislativo cada vez más complejo y cambiante con la transposición de directivas comunitarias y el desarrollo de Internet.

En este sentido, lo primero que ha tenido que hacer la empresa es tomar la decisión de implantar un SGSI. A este respecto, la propia experiencia de la empresa, conocedora de cómo un sistema de gestión ayuda a la mejora continua si realmente se cree en el mismo, y el apoyo de la Dirección han ayudado a tomar esta decisión de forma que la empresa conozca dónde están los riesgos y amenazas y tratarlos adecuadamente.

La segunda decisión es cómo implantar el SGSI: con personal interno, utilizando la empresa de seguridad que le presta servicios o utilizando servicios de asesoramiento externo independiente. En este sentido, la decisión de contar con una consultoría independiente ha facilitado la labor de análisis desde un punto de vista imparcial e independiente.

Por lo que la decisión es: Implantar un SGSI basado en la norma ISO 27001:2005 con la ayuda de asesores externos independientes.

El primer paso que se ha dado es involucrar y concienciar al personal que va a estar afectado por el SGSI. Para ello, se han realizado las reuniones de inicio de proyecto y formación específica al personal que va a intervenir activamente en la realización del proyecto durante la primera fase del proyecto.

A continuación, se han realizado todas las fases para la implantación de un SGSI en la empresa seleccionada:

- Comenzando por un análisis diferencial que ha ayudado a conocer cómo de lejos o cerca está la empresa respecto a los requisitos de la norma (análisis GAP).
- A continuación se ha definido el alcance del SGSI de forma que cubra las partes que la empresa considera deben ser tratadas de forma prioritaria y que están expuestas a un mayor riesgo, tales como los servicios de Internet, cumplimiento legislativo y los servicios de sistemas de información de la empresa.

- Se ha procedido a definir la política de seguridad de la información de la empresa orientada a establecer unas directrices claras de obligado cumplimiento por todo el personal que trate información de la empresa independientemente que sea interno o externo.
- Definir la organización de seguridad de la empresa. En este sentido, la experiencia de la empresa en sistemas de gestión ha ayudado ya que el personal designado conoce procedimientos de gestión.
- Elaboración de los procedimientos de gestión y metodología de análisis de riesgos que se va a aplicar en la empresa.
- Realización del inventario de activos, valoración y análisis de riesgos, así como el procedimiento de gestión del riesgo con la aprobación del riesgo residual.
- Seleccionar los controles que se van a implantar de la norma ISO 27002:2005 y aprobar la Declaración de Aplicabilidad (SOA).
- Implantación de los controles y elaboración de los planes de tratamientos de riesgos.

Una vez que se han elaborado todas las fases para planificar y operar el SGSI, se ha procedido a realizar una auditoría interna para verificar el cumplimiento de los requisitos de la norma y el nivel de cumplimiento de los controles. Por otro lado, se ha evaluado el nivel de madurez que tendrían los controles una vez implantados los planes de tratamiento.

Finalmente, se ha realizado una presentación a la Dirección de la empresa con los principales hitos, el resultado obtenido y las siguientes acciones.

Unos de los aspectos que se han analizado en los planes de tratamiento es la posibilidad de externalización de los servicios de sistemas de información a un coste razonable en empresas especializadas, de forma que se puedan minimizar riesgos y establecer planes de contingencias de una forma transparente a la empresa sin tener la necesidad de realizar esfuerzos tecnológicos que no tienen ningún valor añadido, especialmente en empresas "no tecnológicas". En este sentido, es necesario analizar y tener en cuenta en qué empresa se externaliza, qué servicios y garantías ofrece y la legislación que se le aplica. Por lo que una de las condiciones establecidas por la empresa en el proceso de contratación es que el Datacenter principal y el Centro de Respaldo del prestador de servicios elegido tienen que estar ubicados en un país miembro de la Unión Europea.

No me gustaría finalizar sin comentar que uno de los aspectos que he visto más crítico es la elección de la metodología de análisis de riesgos, ya que es una elección que condicionará a la empresa y una mala elección puede hacer que en el futuro la propia empresa no sea capaz de gestionar su propio sistema de gestión de riesgos. Aquí debo ser crítico con la metodología de análisis de riesgos elegida (basada en Magerit) ya que posiblemente no sea la más adecuada para este tipo de empresas que precisan de una metodología más orientada a la gestión y visión del negocio sin entrar en el detalle.

Por último, y aunque el desarrollo se ha basado en la norma ISO 27001:2005, muchos de los procedimientos y documentos podrán ser utilizados por la empresa para su adaptación a la norma ISO 27001:2013, con la única salvedad de cambiar los controles y las referencias a los apartados específicos de la norma. Otros, sin embargo, deberán ser revisados en mayor profundidad.

15. DEFINICIONES BÁSICAS

A los efectos de este documento, se entenderá por:

- Usuario: sujeto o proceso autorizado para acceder a datos o recursos de los sistemas de información.
- Identificación: procedimiento de reconocimiento de la identidad de un usuario.
- Autenticación: procedimiento de comprobación de la identidad de un usuario.
- Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
- Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.
- Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.
- Activo de información: cualquier información que tiene un valor para la organización.
- LOPD: Ley Orgánica 15/1.999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.
- RDLOPD: Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- ASP: Proveedor de Servicios de Aplicaciones (del inglés Application Service Provider).
- ISP: Proveedor de Servicios de Internet (del inglés Internet Service Provider).
- SLA: Nivel de Servicios Acordado (del inglés Services Level Agreement).
- SOA: Declaración de Aplicabilidad (del inglés Statement of Applicability).
- ISO: International Organization for Standardization.
- COBIT: Control Objectives for Information and related Technology.
- LSSI: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- SGCA: Sistema de Gestión de la Calidad.
- SGSI: Sistema de Gestión de Seguridad de la Información.
- GPS: Sistema de Posicionamiento Global (Global Positioning System).
- HTML5: versión 5 del lenguaje HyperText Markup Language.
- ERP: Sistema de gestión para planificar y gestionar los recursos de la empresa (del inglés Enterprise Resource Planning).
- SAP: Aplicación empresarial desarrollada por SAP AG que se utiliza para la gestión integral de la empresa (ERP). El nombre SAP® está registrado por SAP AG.
- ABAP: Lenguaje de programación utilizado para el desarrollo de aplicaciones en SAP. El nombre ABAP™ está registrado por SAP AG.

- CPD: Centro de Proceso (o de Procesamiento) de Datos.
- Datacenter: (o también denominado CPD) Ubicación acondicionada para albergar el equipamiento informático (normalmente servidores) que realiza el procesamiento de la información de la organización.
- Tier 1: Datacenter básico. Tiene una disponibilidad de los servicios de 99,671% lo que se traduce a 22,8 horas/año de indisponibilidad de servicios.
- Tier 2: Datacenter con componentes redundantes. Tiene una disponibilidad de los servicios de 99,741% lo que se traduce a 22 horas/año de indisponibilidad de servicios.
- Tier 3: Datacenter con sistema de mantenimiento concurrente. Tiene una disponibilidad de los servicios de 99,982% lo que se traduce a 1,6 horas/año de indisponibilidad de servicios.
- Tier 4: Datacenter con tolerancia a fallos. Tiene una disponibilidad de los servicios de 99,995% lo que se traduce a 0,4 horas/año de indisponibilidad de servicios.
- Virtualización: Es la creación a través de herramientas software (aplicaciones de virtualización) de la versión virtual de una máquina física o un entorno.
- Warn-site: Estrategia de un plan de contingencia que consiste en disponer de equipos parcialmente preparados y configurados para poder ser arrancados en un breve periodo de tiempo.
- Hot-site: Estrategia de un plan de contingencia que consiste en disponer de equipos preparados y configurados para poder ser arrancados de forma inmediata en caso necesario.
- Directorio Activo: Servicio de Directorio utilizado en redes de Microsoft que permite una administración y gestión de los nodos y usuarios de la red.

16. DOCUMENTOS E INFORMACIÓN RELACIONADA

Bibliografía, documentación e información consultada:

- Norma UNE-ISO/IEC 27001.
- Norma UNE-ISO/IEC 27002.
- Magerit versión 3.
- COBIT versión 4.1 y 5.
- Políticas de Seguridad Informática - Mejores Prácticas Internacionales. Charles Cresson Wood.
- Material docente de la UOC de la asignatura "Sistema de gestión de la seguridad de la información".
- Material docente de la UOC de la asignatura "Auditoría técnica y de certificación".
- Material docente de la UOC de la asignatura "Aspectos legales de la seguridad informática".
- Material docente de la UOC de la asignatura "Comercio Electrónico".
- Ley Orgánica 15/1.999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Información disponible desde la página web de Inteco en www.inteco.es.
- El portal de la ISO en español en www.iso27000.es.

17. ANEXOS

Adjunto a esta memoria, se incluyen los siguientes documentos:

Documento	Descripción
SI-PO-PAN-01.pdf	Política de seguridad de alto nivel.
SI-PO-GEN-01.pdf	Políticas de seguridad de la información.
SI-PG-DOC-01.pdf	Gestión de la documentación del SGSI.
SI-MN-001-01.pdf	Manual de Procedimientos.
SI-PG-RSD-01.pdf	Revisión del Sistema por la Dirección.
SI-PG-AUD-01.pdf	Auditorías Internas.
SI-PG-IND-01.pdf	Gestión de Indicadores.
SI-PG-GNC-01.pdf	Gestión de las No Conformidades.
SI-PG-MAR-01.pdf	Metodología de Análisis de Riesgos.
AR-TFM-JorgeFranciscoLilloMuñoz.xls	Análisis de riesgos.
SI-AI-001-01.pdf	Informe de auditoría interna.
Presentación de inicio-TFM-JorgeFranciscoLilloMuñoz.pps	Presentación de inicio del proyecto.
Presentación a la Dirección-TFM-JorgeFranciscoLilloMuñoz.pps	Presentación a la Dirección al final del proyecto.