Màster Interuniversitari en la Seguretat de les TIC (MISTIC)

Proyecto Final de Master

Elaboración de un Plan de Implementación de la ISO/IEC 27001:2005

Memoria descriptiva

Director: Arsenio Tortajada Gallego

Fecha de realización: Primavera 2013

Juan Berlanga Fuentes

Resumen del Proyecto de Final de Master

Castellano:

El siguiente proyecto tiene como objetivo el estudio del estado actual de la compañía ConTec S.L en términos de la seguridad de la información, con tal de establecer las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información).

English:

This Project aims to study the current state of ConTec S.L in terms of information security in order to cover the description of the tasks that enable the creation of the ISMS (Information security management system) bases.

ÍNDICE

1. INTRODUCCIÓN

El presente documento refleja la elaboración del Proyecto de Final de Master "Elaboración de un Plan de Implementación de la ISO/IEC 27001:2005" a la compañía ConTec S.L. Se ha planteado la realización de un plan director de seguridad, siendo éste la hoja de ruta que debe seguir la organización con tal de gestionar de forma adecuada la seguridad, permitiendo no solo conocer el estado de la misma, sino también las líneas de actuación para su mejora.

ConTec S.L. es una consultora tecnológica catalana de capital privado con más de 10 años de experiencia dando servicio a más de 150 empresas en su estrategia TIC.

Actualmente, ConTec S.L. se encuentra en fase de crecimiento con la intención de expandir su área de negocio a Madrid, manteniendo y aumentando el número de clientes en Barcelona. Esta fase de crecimiento hace necesaria la revisión de la operativa de ConTec S.L..

La información y los sistemas informáticos son valores de vital importancia para ConTec S.L, y la reputación de la compañía está estrechamente ligada a la gestión de ambos. Por ello, la dirección de la compañía es consciente de la importancia que tiene para la compañía la seguridad de la información de cara a conseguir un mayor grado de competitividad en el mercado actual de las TIC fortaleciendo la relación de confianza entre el cliente y la organización.

El objetivo de este proyecto consiste en la elaboración de un plan Director de Seguridad de la Información que defina las bases para la consolidación de la compañía ejecutando las prácticas de seguridad necesarias para conocer su estado actual en términos de seguridad para posteriormente poder definir las acciones necesarias con tal de minimizar los riesgos a los que puede estar expuesta. En definitiva, su alcance consistiría en reforzar la seguridad en los servicios y procesos internos en las tecnologías de la información de la compañía al ser uno de los principales responsables del tratamiento y conservación de la información.

Con esto se conseguiría una compañía más robusta y de mayor confianza, con el objetivo de intentar ser referente en el mundo de las TIC a nivel español en los próximos años.

A nivel metodológico, se ha realizado una aproximación del proyecto en fases:

- En primer lugar, se ha realizado un estudio de la compañía para conocer más en profundidad su funcionamiento, concretar el alcance del proyecto, definir las bases del plan de seguridad de la información y finalmente realizar un análisis diferencial para conocer de manera global el estado actual de la compañía en relación a la seguridad de la información. Este estudio se realiza en el apartado 2, 3 y 4 de este mismo documento.
- En segundo lugar, se ha desarrollado un esquema documental con los documentos necesarios que define la ISO/IEC 27001. Estos documentos se pueden encontrar en los Anexos II a VII.
- En tercer lugar, se realizó un análisis de riesgos mediante la metodología MAGERIT, esta es la herramienta que permite identificar las amenazas a las que se encuentran expuestos los activos, para luego evaluar la frecuencia de

que pudieran suceder y finalmente valorar el impacto que supondría su materialización. Este estudio se puede encontrar en el apartado 5 de este mismo documento.

- En cuarto lugar y conociendo el estado actual de la compañía se idearon un conjunto de proyectos con tal de mejorar la seguridad de la información utilizando como base el análisis de riesgos y el análisis diferencial. Este estudio se puede encontrar en el apartado 6 de este mismo documento.
- Por último se realizó una auditoría de cumplimiento para evaluar la madurez de la seguridad según los diferentes dominios de control y los 133 controles planteados por la ISO/IEC 27002:2005. Este estudio se puede encontrar en el apartado 7 de este mismo documento.

Como se puede ver la memoria está organizada en el orden según se han desarrollado las diferentes fases. Asimismo, se han adjuntado diversos anexos con información adicional que añade contenido a estas fases.

2. CONTEXTUALIZACIÓN

ConTec S.L. es una consultora tecnológica catalana de capital privado con más de 10 años de experiencia dando servicio a más de 150 empresas en su estrategia TIC. Con base central en Barcelona, actualmente está en proceso de expansión y hace 2 años abrió una nueva oficina en Madrid.

2.1. Áreas de negocio

ConTec S.L. centra sus servicios bajo las siguientes áreas de negocio:

- **Área de desarrollo**
  - Desarrollo de soluciones web
    - Área especializada en el ámbito de soluciones web.
  - Desarrollo de aplicaciones personalizadas
    - Área especializada en desarrollos personalizados de aplicaciones y en su mantenimiento adoptando la solución que mejor se adapte a sus clientes.

- **Área de sistemas e infraestructuras**
  - En el área de Sistemas se ofrecen soluciones para dar soporte a las infraestructuras que requiere cualquier proyecto en Internet. Para ello mantiene un contrato con un conocido proveedor de servicios de comunicaciones y Data Center en Barcelona donde implantar la infraestructura necesaria para cubrir los servicios necesarios por el cliente, garantizando la continuidad de la plataforma.

- **Área de outsourcing**
  - ConTec S.L. dispone de una sección con personal especializado para proporcionar soporte a sus clientes cubriendo las necesidades del cliente en cuanto a la infraestructura de sus sistemas, ofreciendo servicios de monitorización, resolución de incidencias, gestión de almacenamiento, administración y gestión remota.

2.2. Infraestructura de la compañía

La compañía dispone de 2 oficinas en Barcelona y en Madrid. A continuación se expone una breve explicación de ambas oficinas.

Barcelona

La sede central se sitúa en Barcelona con 50 empleados. La mayor parte de las actividades llevadas a cabo por la compañía se realizan en esta oficina.

La dirección y los departamentos de administración, finanzas, contabilidad, marketing y recursos humanos también se ubican en la oficina de Barcelona. Por tanto, además de las tareas de gestión, la mayor parte de las decisiones estratégicas se deciden desde Barcelona.

En cuanto a las áreas de negocio, engloba las áreas de desarrollo, sistemas e infraestructuras y la de outsourcing.

Madrid

La oficina de Madrid con 15 empleados, dispone de menos recursos y es fruto de la expansión de la compañía.

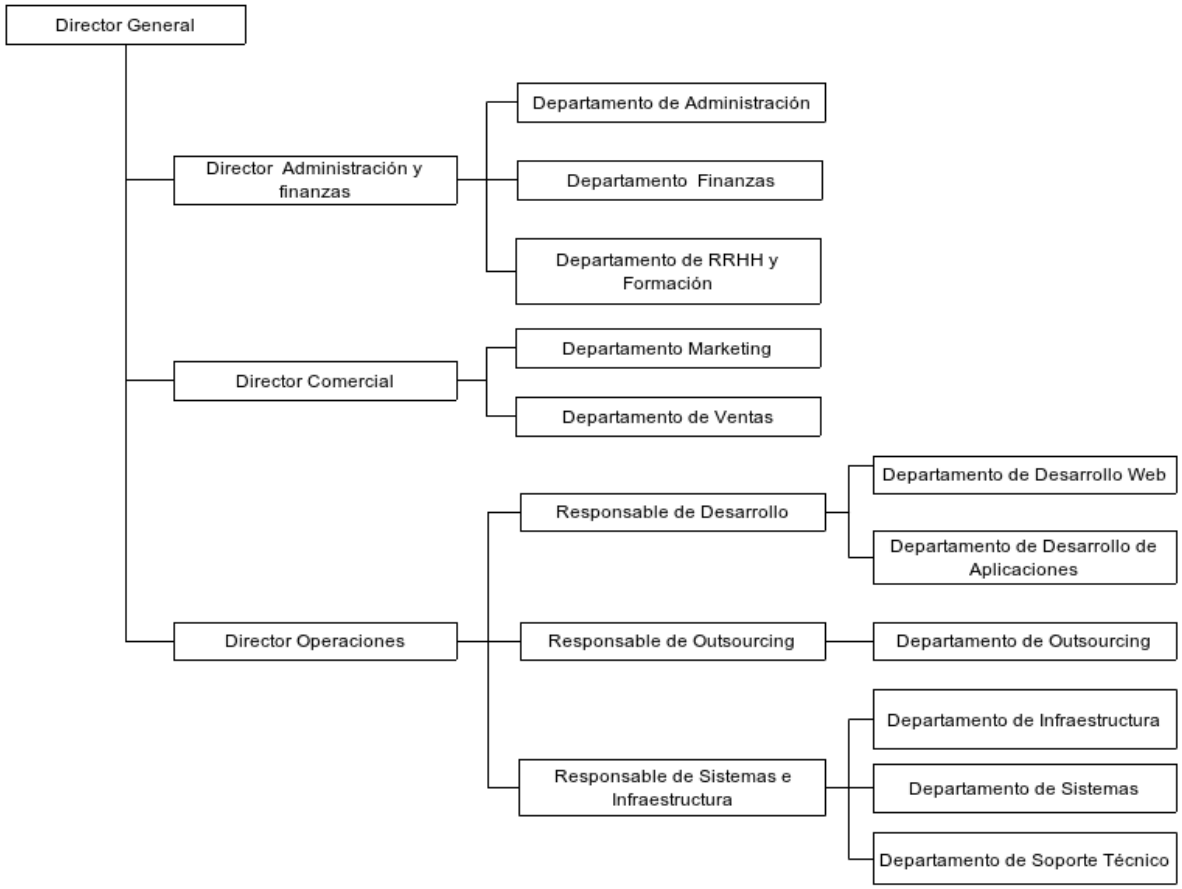
Principalmente lleva a cabo actividades del área de desarrollo, tanto de aplicaciones web como personalizadas, pudiéndose también hacerse cargo del mantenimiento.

A pesar de esto, está previsto que en un futuro abra su mercado y se implante un departamento de sistemas y de outsourcing con las mismas funciones que el de la sede de Barcelona.

2.3. Organigrama

La siguiente estructura organizativa se refiere a la oficina de Barcelona al ser la sede central y el objeto de estudio.

La estructura organizativa se puede observar en la siguiente figura:



Destacar el área de operaciones con las distintas áreas de negocio y sus responsables asociados.

El departamento de desarrollo se divide en 15 trabajadores, 10 de ellos especializados en las distintas tecnologías web, y por otro lado un pequeño departamento de 5 trabajadores para el desarrollo de aplicaciones específicas cubriendo también ámbitos como BMP (Business Process Management), BI (Business Intelligence), CRM (Customer Relationship Management) o soluciones Cloud.

El departamento de outsourcing con 5 trabajadores ofrece soporte puntual o a largo plazo a los clientes. Estos trabajadores turnan guardias para dar soporte 24x7 todos los días del año.

Habitualmente los departamentos de sistemas e infraestructura y el de outsourcing trabajan juntos. En ciertos proyectos, el departamento de outsourcing dará soporte 24x7 a la infraestructura creada por el departamento de sistemas y el de infraestructura. Este último departamento le facilita toda la información necesaria para gestionar la infraestructura.

El departamento de soporte técnico compuesto por 2 trabajadores da soporte interno, especialmente como helpdesk a la dirección, y a los departamentos de Sistemas e Infraestructura, outsourcing, administración, finanzas, contabilidad, marketing, ventas y recursos humanos.

2.4. Métodos de trabajo

La mayor parte del trabajo realizado por los empleados se realiza desde las oficinas. Los trabajadores hacen uso de ordenadores de sobremesa para llevar a cabo sus funciones conectándose a la red local de la compañía.

Los ordenadores que son administrados por el soporte técnico son los correspondientes a la dirección, y los trabajadores de los departamentos de sistemas e infraestructura, outsourcing, administración, finanzas, contabilidad, marketing y recursos humanos.

El área de sistemas e infraestructura dispone además de varios ordenadores portátiles por si deben desplazarse al CPD para alguna labor de implantación o revisión de los sistemas.

Por otro lado, además del trabajo de oficina, es necesario mantener el servicio de outsourcing activo 24 horas al día, por lo que los empleados del departamento de outsourcing se turnan las guardias para abordar cualquier incidencia que pudiera ocurrir en horario no laboral. Para ello, el técnico de guardia dispone de un ordenador portátil y un móvil, al cual recibirá las llamadas ante cualquier incidencia desde el data center del proveedor donde tienen implantadas las infraestructuras de sus clientes. El proveedor es el responsable de monitorización si deja de funcionar cualquier servicio monitorizado que está contratado en las infraestructuras que tiene implantadas. Dependiendo del alcance de la incidencia, el técnico de guardia deberá resolver la incidencia presencialmente en el CPD o por el contrario solucionarlo remotamente, conectándose por VPN a la red de la oficina y una vez conectado a la red de la oficina, solucionar la incidencia.

Los trabajadores tienen acceso libre a internet, sin ningún tipo de proxy que filtre contenido.

2.5. Estado de la seguridad de las oficinas

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

La conexión entre las dos oficinas se realiza mediante conexión VPN por hardware. La sede de Barcelona tiene contratadas dos líneas ADSL de diferentes compañías de telefonía, la oficina de Madrid tiene una única línea ADSL.

La red está segmentada, los empleados de las distintas áreas trabajan de forma aislada de las demás áreas de negocio y sólo tienen acceso a los sistemas necesarios para poder llevar a cabo sus funciones.

Respecto al acceso físico a las oficinas, ambas disponen de una recepción en horario de oficina. Para el acceso al interior de la oficina, es necesario que cada empleado lleve consigo una tarjeta de identificación necesaria para abrir el torno que da acceso al interior. Al firmar el contrato de trabajo, por motivos de seguridad, en la recepción de las oficinas está implantado un sistema de grabación de imagen y cada empleado da su visto bueno a que pueda ser grabado en el momento de entrada/salida a la oficina.

3. OBJETIVOS DEL PLAN DIRECTOR

3.1. Motivación del Plan Director de Seguridad

ConTec S.L. se encuentra actualmente en una fase de crecimiento. La compañía tiene la intención de expandir su área de negocio a Madrid, manteniendo y aumentando el número de clientes en Barcelona. Esta fase de crecimiento hace necesaria la revisión de la operativa de ConTec S.L..

La información y los sistemas informáticos son valores de vital importancia para ConTec S.L, y la reputación de la compañía está estrechamente ligada a la gestión de ambos. Por ello, la dirección de la compañía es consciente de la importancia que tiene para la compañía la seguridad de la información de cara a conseguir un mayor grado de competitividad en el mercado actual de las TIC fortaleciendo la relación de confianza entre el cliente y la organización.

Para conseguir este hito, la dirección pretende definir y establecer las directrices de seguridad de la información que debe adoptar ConTec S.L. en consonancia con los objetivos de negocio, fundamentándose en la norma ISO 27001 en lo referente a planes estratégicos y políticas. Se necesitará llevar a cabo ciertas técnicas para recopilar la mayor información de la compañía posible mediante:

- **Plan de reuniones con personal de la empresa**: se intentará obtener información para la valoración de riesgos de cada uno de los departamentos de la compañía mediante entrevistas personales a personal con experiencia en los temas de gestión de la seguridad de la información, sistemas de información, administración de activos de información, infraestructura tecnológica, gestión de proveedores, seguridad física, recursos humanos, continuidad de negocio, auditoría y operación.
- **Cuestionarios:** Al igual que con las entrevistas al personal, también se recogerá información de interés para estudiar los riesgos mediante cuestionarios repartidos a los empleados.
- **Revisión de documentos**: La revisión de todos los documentos que pueda aportar la compañía facilitará el estudio.

Gracias a esto, la compañía podrá conocer el estado actual de la misma y plantear los riesgos potenciales los cuales debe afrontar.

Una vez llevado a cabo todo el proceso, la dirección se planteará crear un departamento de seguridad dentro del área de sistemas e infraestructuras.

3.2. Alcance del Plan Director de Seguridad

Este Plan Director de Seguridad estará enfocado a la sede principal de la compañía en Barcelona, puesto que la mayor parte de las actividades, departamentos y áreas de negocio se llevan a cabo en Barcelona. Actualmente la oficina de Madrid representa una pequeña parte de la compañía centrada en el desarrollo de aplicaciones y que se estudiaría en un siguiente proceso. Aún así se deberá tener en cuenta en el presente plan, la seguridad en las comunicaciones entre ambas oficinas.

Una vez aclarado que el Plan Director de Seguridad se centrará en la oficina de Barcelona, podemos analizar con mayor detalle el objetivo de este plan:

- El principal objetivo para ConTec S.L es el de mejorar los niveles de seguridad de la información de la compañía conociendo el actual nivel de madurez alcanzado con los controles actualmente implementados, para finalmente desarrollar un plan de acción que facilite un marco de referencia certificable en temas de seguridad de la información. Por tanto, el alcance consistiría en reforzar la seguridad en los servicios y procesos internos en las tecnologías de la información de la compañía al ser uno de los principales responsables del tratamiento y conservación de la información.

Fruto de este objetivo, se desea ofrecer servicios tecnológicos de mayor confianza a sus clientes garantizando la continuidad de sus plataformas de forma segura. Teniendo en cuenta los riesgos de seguridad informática, vulnerabilidades y problemas de seguridad existentes y reportados a la organización, es objetivo principal, obtener medidas para mitigar, transferir o aceptar estos riesgos. estudiando cual es la mejor opción para cada uno de los casos. Finalmente, se estudiaría crear un departamento de seguridad informática.

La realización de un correcto plan permitirá a ConTec S.L. obtener importantes beneficios, entre ellos podemos comentar:

- Definición clara de la situación actual de la compañía
- Definir los requisitos y objetivos de seguridad
- Definir el grado de cumplimiento de políticas, directivas, estándares y procedimientos de seguridad actuales
- Asegurar el cumplimiento de leyes y regulación vigente.
- Análisis de las amenazas y riesgos asociados a la situación actual de la compañía para así poder gestionarlos de forma más efectiva

3.3. Soporte por parte de la organización y empleados

Para poder realizar este proyecto será necesaria una restructuración de la organización para poder dar un correcto soporte a éste.

La compañía debería crear su propio esquema organizativo interno, asegurando que todas las responsabilidades y funciones en materia de seguridad de la información

se han pactado correctamente y garantizan, siempre y cuando sea posible, la segregación de funciones.

Además, todo trabajador independientemente de su rol dentro de la compañía deberá cumplir con la normativa de seguridad que se pacte. Los empleados que no cumplan esta normativa estarán sujetos a acciones disciplinarias.

En el *Anexo VI – Gestión de Roles y Responsabilidades* se detalla la estructura organizativa pero deberán aparecer los siguientes niveles:

- **Comité de Dirección**
  - En primer lugar se deberá crear un Comité de Dirección con los altos cargos de la compañía. Estará constituido por el director de la compañía, el director de administración y finanzas, el director comercial y el director de operaciones.

- **Comité de seguridad de la información**
  - Las decisiones en materia de seguridad de la información son tomadas de forma consensuada por un grupo formado por diferentes responsables dentro de la compañía, en este caso será formado por los mismos integrantes que el Comité de Dirección al ser una compañía pequeña, junto con el responsable de Sistemas e Infraestructura como Responsable de seguridad de la información.

- **Responsable de seguridad de la información**
  - El responsable de Sistemas e Infraestructura tomaría el puesto de Responsable de seguridad de la información (RSI), y formaría parte del Comité de Seguridad de la información.

4. ANÁLISIS DIFERENCIAL

Una vez que conocemos los objetivos del Plan Director, antes de iniciar la siguiente fase, se recomienda realizar un análisis diferencial de las medidas de seguridad y la normativa que tiene la compañía respecto a la ISO/IEC 27001 e ISO/IEC 27002. Este análisis consiste en la revisión del estado inicial de la entidad. Con este análisis se fija el punto de partida y de referencia para medir el progreso que se va a lograr con la implantación del SGSI.

Se ha realizado un estudio sobre las deficiencias en cuanto a los controles según los dominios definidos en la ISO/IEC 27002. Para cada dominio se revisa si los controles aplican a la organización o por el contrario no deben ser tratados.

En el Anexo I – Análisis diferencial se incluye una tabla con el estudio de la aplicación de cada uno de los controles. A continuación se detalla la explicación de los controles que no aplican a la organización:

9. SEGURIDAD FÍSICA Y DEL ENTORNO	
9.1 Áreas seguras	
9.1.5 Trabajo en áreas seguras	**N.A. - No aplica**
9.1.6 Áreas de acceso público y de carga y descarga	**N.A. - No aplica**

No existen áreas seguras donde trabajan los empleados, ni existen áreas de acceso público o de carga y descarga. Todo el trabajo es de índole informática o de gestión y se realiza en las mismas oficinas.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	
10.9 Servicios de comercio electrónico	
10.9.1 Comercio electrónico	**N.A. - No aplica**
10.9.2 Transacciones en línea	**N.A. - No aplica**
10.9.3 Información públicamente disponible	**N.A. - No aplica**

No se desarrollan actividades relacionados con el comercio electrónico por lo que estos 3 controles relacionados con este sector no aplican a la organización.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	
12.5.5 Externalización del desarrollo de software	**N.A. - No aplica**

No se subcontrata esta tarea, todo el desarrollo del software se realiza por personal propia de la compañía

5. Análisis de riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo al que está expuesto una organización. En el *Anexo VII - Metodología de análisis* de riesgos se incluye la metodología seguida en este proyecto.

Existen diferentes maneras de tratar el riesgo, por un lado limitando las consecuencias que conlleva, evitando que ocurra o reduciendo sus posibilidades o por otro lado si interesa, aceptarlo y mantener recursos para actuar cuando sea necesario.

En esta fase del documento, el objetivo consiste en la evaluación de los activos relacionados con la actividad de negocio de ConTec S.L. Una vez realizadas todas las tareas, se obtiene:

- Un análisis detallado de los activos relevantes a nivel de seguridad de la empresa
- Un estudio de las posibles amenazas del sistema de información, así como su impacto.
- Evaluación del impacto potencial que implicaría la materialización de las diferentes amenazas con las que están expuestos los activos.

En primer lugar se identificarán los activos, considerando las dependencias existentes entre ellos y haciendo la valoración de estos.

5.1. Inventario y valoración de activos

Inventario de activos

Un activo es un recurso del sistema de información o relacionado con éste, necesario para que la compañía pueda desempeñar correctamente sus tareas.

El siguiente estudio se lleva a cabo según la metodología MAGERIT. Según está metodología agruparemos los activos en los siguientes grupos:

- Instalaciones: Donde se acogen equipos informáticos y de comunicaciones
- Hardware: Equipos informáticos que permiten hospedar datos, aplicaciones y servicios
- Aplicaciones: que permiten manejar datos
- Datos: que materializan la información
- Redes de comunicaciones: que permiten intercambiar datos
- Servicios auxiliares: que se necesitan para poder organizar el sistema
- Equipamiento auxiliar: complementa el material informático
- Personal: que explotan u operan todos los elementos anteriores

Dimensión de seguridad

Una vez valorados los activos, se debe valorar la importancia de cada uno de ellos en función de la valoración ACIDT. Este análisis permitirá en fases posteriores, poder escoger salvaguardas teniendo en cuenta y dando prioridad a los aspectos de seguridad que más críticos sean para la compañía.

Las cinco dimensiones de seguridad según la valoración ACIDT, se utilizan para valorar las consecuencias de la materialización de una amenaza. Estas dimensiones son las siguientes:

- **Autenticidad [A]**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos
- **Confidencialidad de la información [C]:** Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad de los datos [I]:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Disponibilidad [D]:** Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieran
- **Trazabilidad [T]:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Para cada dimensión en un activo se le asociará una valoración según los siguientes criterios definidos en la versión 3 de Magerit:

Valoración	Criterio
10	Daño extremo para la compañía
9	Daño muy grave para la compañía
6-8	Daño grave para la compañía
4-6	Daño importante para la compañía
1-3	Daño menor para la compañía
0	Daño irrelevante para la compañía

Para poder discernir entre los distintos valores, existen criterios definidos por Magerit con tal de guiar con más detalle y valorar de forma homogénea los activos. Estas valoraciones se basan en las siguiente escalas:

- Información de carácter personal [pi]
- Obligaciones legales [lpo]
- Seguridad [si]
- Intereses comerciales o económicos [cei]
- Interrupción del servicio [da]
- Orden público [po]
- Operaciones [olm]
- Administración y gestión [adm]

- Pérdida de confianza [lg]
- Persecución de delitos [crm]
- Tiempo de recuperación del servicio [rto]
- Información clasificada (nacional) [lbl.nat]
- Información clasificada (Unión Europea) [lbl.ue]

Tabla resumen de valoración

ÁMBITO	ACTIVO		DEPENDENCIA	VALOR	ASPECTOS CRÍTICOS				
	ID	NOMBRE			A	C	I	D	T
INSTALACIONES [L]	[L.1]	Sala CPD	-	Alto	5	9	9	7	7
	[L.2]	Oficinas	-	Alto	5	6	5	7	7
	[L.3]	Recepción	-	Medio	5	6	5	7	7
HARDWARE [HW]	[HW.1]	Firewall externo	[L.1], [COM.2], [AUX.5]	Bajo	5	7	5	7	7
	[HW.2]	Servidores de datos	[L.1], [HW.12], [COM.2], [AUX.5]	Medio	5	9	9	7	7
	[HW.3]	Servidor de nóminas/finanzas/administración	[L.1], [HW.12], [HW.4], [SW.4], [COM.2], [AUX.5]	Bajo	5	7	9	5	7
	[HW.4]	Servidores de BBDD	[L.1], [HW.12], [COM.2], [AUX.5]	Bajo	5	7	9	7	7
	[HW.5]	Servidor web	[L.1], [HW.1], [COM.2], [AUX.5]	Bajo	5	7	5	5	7
	[HW.6]	Servidor de correo	[L.1], [HW.1], [COM.2], [AUX.5]	Bajo	5	7	7	5	7
	[HW.7]	Servidor DNS	[L.1], [HW.1], [COM.2], [AUX.5]	Bajo	5	7	5	5	7
	[HW.8]	Servidores de desarrollo	[L.1], [HW.12], [COM.2], [AUX.5]	Medio	3	3	3	3	3
	[HW.9]	Estaciones de trabajo	[L.2], [HW.12], [HW.15], [COM.2], [AUX.5]	Medio	3	3	1	1	3
	[HW.10]	Portátiles de guardias	[L.2], [HW.12], [COM.2], [AUX.5], [S.1]	Medio	5	5	5	3	3
	[HW.11]	Cámara de vigilancia	[L.3], [HW.12], [COM.2], [AUX.5]	Muy bajo	5	6	5	7	7
	[HW.12]	Firewal interno	[L.1], [HW.1], [COM.2], [AUX.5]	Bajo	5	7	5	7	7
	[HW.13]	Servidor NIDS	[L.1], [HW.1], [COM.2], [AUX.5]	Bajo	5	3	9	3	7
	[HW.14]	Impresoras	[L.2], [HW.12], [COM.2], [AUX.5]	Muy bajo	1	1	1	1	1
	[HW.15]	Switches	[L.2], [AUX.5]	Muy bajo	1	1	1	1	1
	[HW.16]	Torno de acceso a oficina	[L.3], [AUX.5]	Bajo	5	6	5	7	7
	[HW.17]	Routers wifi	[L.2], [HW.12], [COM.2], [AUX.5]	Muy bajo	5	6	5	1	7
	[HW.18]	VPN CISCO	[L.1], [COM.2], [AUX.5]	Bajo	5	9	9	5	7
APLICACIONES [SW]	[SW.1]	Aplicación web	[HW.5]	Medio	5	7	5	5	7
	[SW.2]	Aplicaciones de gestión	[HW.3]	Medio	5	7	9	5	7
	[SW.3]	Servidor de correo	[HW.6]	Bajo	5	7	7	5	7
	[SW.4]	Antivirus	[SW.8],[SW.9]	Bajo	5	3	3	5	3
	[SW.5]	Servidor de ficheros	[HW.2]	Bajo	5	9	9	7	7
	[SW.6]	Microsoft SQL Server 2000	[HW.4]	Bajo	5	7	9	7	7
	[SW.7]	Servidor de DNS	[HW.7]	Bajo	5	7	5	5	7

	[SW.8]	**Microsoft Windows Server 2000**	[HW.3], [HW.4], [HW6]	Bajo	5	7	9	7	7
	[SW.9]	**Microsoft Windows XP Professional**	[HW.9]	Medio	3	3	1	1	3
	[SW.10]	**Microsoft Office Professional**	[HW.9]	Medio	3	3	1	1	1
DATOS [D]	**[D.1]**	**Bases de datos**	[SW.6], [SW.8]	Alto	5	7	9	7	7
	[D.2]	**Datos en servidor de datos**	[HW.2]	Muy alto	5	9	9	5	7
	[D.3]	**Backups**	[HW.2]	Muy alto	5	9	9	5	7
	[D.4]	**Datos administrativos y gestión**	[SW.2]	Alto	5	8	9	5	7
	[D.5]	**Logs**	[HW.2]	Medio	5	7	9	5	7
RED [COM]	**[COM.1]**	**Red telefónica**	[AUX.5]	Bajo	5	3	1	7	3
	[COM.2]	**Líneas ADSL**	[AUX.5], [L.1]	Bajo	5	7	9	5	7
	[COM.3]	**VPN Madrid**	[HW.18]	Bajo	5	7	9	5	7
	[COM.4]	**Red Inalámbrica**	[HW.17]	Muy bajo	5	7	9	1	7
SERVICIOS [S]	**[S.1]**	**Acceso remoto**	-	Bajo	5	7	7	5	7
	[S.2]	**Monitorización**	[HW.1], [HW.2], [HW.3], [HW.4], [HW.5], [HW.6], [HW.7], [HW.8], [HW.9], [HW.10], [HW.11], [HW.12], [HW.13], [SW.1], [SW.2], [SW.3], [SW.5], [SW.6], [SW.7], [SW.8], [SW.9]	Bajo	5	5	7	5	7
	[S.3]	**Correo electrónico**	[SW.3]	Bajo	5	7	7	5	7
	[S.4]	**Transferencia de ficheros**	[SW.5]	Bajo	5	9	9	5	7
	[S.5]	**Gestión de acceso físico a oficinas**	[HW.11], [HW.16]	Bajo	5	6	5	7	7
	[S.6]	**Web**	[SW.1]	Medio	5	7	5	5	7
EQUIPAMIENTO AUXILIAR [AUX]	**[AUX.1]**	**Armario con llave de entrada a sala CPD**	[L.2]	Muy bajo	-	6	-	7	-
	[AUX.2]	**Armario con llave con documentos en papel**	[L.2]	Muy bajo	-	6	5	5	-
	[AUX.3]	**Aire acondicionado**	[L.1], [AUX.5]	Bajo	-	-	-	5	-
	[AUX.4]	**SAI para el CPD**	[L.1], [AUX.5]	Medio	-	-	-	5	-
	[AUX.5]	**Corriente eléctrica**	-	Bajo	-	-	-	5	-
PERSONAL [P]	**[P.1]**	**Responsable de operaciones**	-	Alto	-	-	-	3	-
	[P.2]	**Responsable de Sistemas e infraestructura**	-	Medio	-	-	-	3	-
	[P.3]	**Resto personal TIC**	-	Muy alto	-	-	-	1	-
	[P.4]	**Personal de administración/finanzas**	-	Muy alto	-	-	-	1	-

Consideraciones de la tabla resumen de valoración

A la hora de valorar los activos, se muestra la valoración cualitativa basada en la valoración cuantitativa por el coste asociados a éstos. Los activos de mayor peso económico hacen referencia a los datos que se almacenan en la empresa, entre ellos el total de los desarrollos llevados a cabo por la compañía y por otro lado el conjunto de todo el personal con el conocimiento y la experiencia adquirida.

A la hora de concretar la dependencia entre los activos, se tiene en consideración que la dependencia es jerárquica, es decir el activo del nivel más bajo dependerá de todos sus activos superiores, por lo tanto no tendrá un valor superior:

- **Instalaciones**: No tienen dependencias
- **Hardware**: Depende directamente de la instalación donde está ubicado, de otro hardware, de la corriente eléctrica y de estar conectado a la red de internet.
- **Aplicaciones**: Depende directamente del hardware
- **Datos**: Depende del hardware y de las aplicaciones instaladas en el hardware
- **Red**: Depende de otro hardware y de la corriente eléctrica
- **Servicios**: Depende del hardware y de las aplicaciones
- **Equipamiento auxiliar**: Ciertos activos dependen de las instalaciones y de la corriente eléctrica
- **Personal**: No tiene dependencias

Entre las instalaciones, se han definido la sala para el CPD, las oficinas y la recepción. Se ha definido una instalación a parte para la recepción ya que es donde está implantado los mecanismos de seguridad física: cámara de vigilancia de acceso y el torno de acceso a la oficina, en la oficina por su parte no dispone de mecanismos de seguridad. Por otro lado cabe destacar que el acceso al CPD depende de una llave que tiene a disposición del responsable de sistemas.

El alcance de este SGSI consiste en reforzar la seguridad en los servicios y procesos internos en las tecnologías de la información de la compañía, mantener unos sistemas estables es vital para la compañía para poder ofrecer sistemas de confianza a sus clientes. Por esta razón aunque no es decisivo para dar un buen soporte a los clientes, se le presta cierta atención a la disponibilidad de los servicios más visibles por el cliente como el servicio web, el correo electrónico o la red telefónica, especialmente para el servicio de outsourcing poder tratar cualquier incidencia o petición de los clientes.

Se almacenan información confidencial de los clientes, entre esta información destacan las credenciales de acceso a sus sistemas que se guardan en los servidores de datos por lo que no asegurar estos datos implicaría un incumplimiento excepcionalmente grave de las obligaciones contractuales con el cliente.

En ciertos activos se valora la dimensión “Trazabilidad” con un 7, puesto que según la escala estándar propuesta por Magerit, en el apartado de seguridad, si hubiera algún tipo de incidente podría dificultar la investigación de incidentes graves.

La confidencial de ciertos activos como la cámara de vigilancia, el torno de acceso a la oficina o los datos relacionados con la administración, no se valoran con un valor menor a un 6 puesto que probablemente quebrantarían seriamente la ley o algún reglamento de protección de información personal.

Algunos activos como aquellos relacionados con la administración y gestión tienen un nivel de disponibilidad con un valor 5 ya que podría causar la interrupción de actividades propias de la organización con impacto en otras organizaciones. Otros activos de menos importancia tienen valor 3 porque únicamente causan la interrupción de actividades propias de la organización.

Amenazas contra los activos que proporcionan seguridad implicarían valores de seguridad igual a 7, ya que probablemente perjudicarían la eficacia o seguridad de la misión operativa.

La dimensión relacionada con la autenticidad en los activos tiene un valor 5 ya que infringirla seriamente leyes o regulaciones.

Por último, referente al personal, identifico que su disponibilidad afecta al desarrollo de la empresa, pero valoro al personal TIC y al de administración y finanzas con un 1 ya que podría impedir la operación efectiva de una parte de la organización, que asigno un valor igual a 3 al responsable de sistemas e infraestructura y al responsable de operaciones porque probablemente impediría la operación efectiva de una parte de la organización de forma algo más critica que el resto de personal.

5.2. Análisis de amenazas

Una vez realizada la tabla resumen con la valoración de los activos, se debe analizar la exposición de estos activos a amenazas y como pueden afectar a estos.

Estas amenazas se clasificaran dentro de las siguientes agrupaciones:

- Desastres Naturales: [N.'x']
    - Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta
- De origen industrial: [I.'x']
    - Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada
- Errores y fallos no intencionados: [E.'x']
    - Fallos no intencionales causados por las personas.
- Ataques intencionados: [A.'x']
    - Fallos deliberados causados por las personas.

Destacar que para definir tanto a que tipo de activo le afecta una amenaza, como la la dimensión del activo que afecta, se basará en la definición que realiza Magerit versión 3. Por ejemplo, según la definición de Magerit para el caso de amenaza por fuego por causa natural:

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] Soportes de información • [AUX] Equipamiento auxiliar • [L] Instalaciones	**Dimensiones**: 1. [D] Disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema	

En este caso de estudio, fuego de origen natural afectaría a las instalaciones, al hardware y al equipamiento auxiliar, y específicamente a la dimensión disponibilidad.

Se incluye el estudio realizado de las amenazas en el *Anexo VIII – Análisis de riesgos.*

5.3. Impacto potencial

Una vez obtenida la tabla, obtendremos la medida del daño sobre el activo derivado de la materialización de la amenaza. En este punto conocemos los valores de los activos según las dimensiones de seguridad y por otro lado el impacto de degradación, por lo tanto podemos conocer valores de referencia para poder priorizar las acciones a llevar a cabo.

Por tanto, este valor se calcula según:

```
Impacto potencial = Valor del activo (según dimensión) x Valor del impacto
```

Tabla resumen de impacto potencial

ACTIVO		VALOR	VALORACIÓN					% IMPACTO					% IMPACTO POTENCIAL				
ID	NOMBRE		A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
[L.1]	Sala CPD	Alto	5	9	9	7	7		50%	50%	100%		0	4,5	4,5	7	0
[L.2]	Oficinas	Alto	5	6	5	7	7		50%	50%	100%		0	3	2,5	7	0
[L.3]	Recepción	Medio	5	6	5	7	7		50%	50%	100%		0	3	2,5	7	0
[HW.1]	Firewall externo	Bajo	5	7	5	7	7		100%	20%	100%		0	7	1	7	0
[HW.2]	Servidores de datos	Medio	5	9	9	7	7		100%	20%	100%		0	9	1,8	7	0
[HW.3]	Servidor de nóminas/finanzas/administración	Bajo	5	7	9	5	7		100%	20%	100%		0	7	1,8	5	0
[HW.4]	Servidores de BBDD	Bajo	5	7	9	7	7		100%	20%	100%		0	7	1,8	7	0
[HW.5]	Servidor web	Bajo	5	7	5	5	7		100%	20%	100%		0	7	1	5	0
[HW.6]	Servidor de correo	Bajo	5	7	7	5	7		100%	20%	100%		0	7	1,4	5	0

[HW.7]	**Servidor DNS**	Bajo	5	7	5	5	7		100%	20%	100%		0	7	1	5	0
[HW.8]	**Servidores de desarrollo**	Medio	3	3	3	3	3		100%	20%	100%		0	3	0,6	3	0
[HW.9]	**Estaciones de trabajo**	Medio	3	3	1	1	3		100%	20%	100%		0	3	0,2	1	0
[HW.10]	**Portátiles de guardias**	Medio	5	5	5	3	3		100%	20%	100%		0	5	1	3	0
[HW.11]	**Cámara de vigilancia**	Muy bajo	5	6	5	7	7		100%	10%	100%		0	6	0,5	7	0
[HW.12]	**Firewal interno**	Bajo	5	7	5	7	7		100%	20%	100%		0	7	1	7	0
[HW.13]	**Servidor NIDS**	Bajo	5	3	9	3	7		100%	20%	100%		0	3	1,8	3	0
[HW.14]	**Impresoras**	Muy bajo	1	1	1	1	1		100%	20%	100%		0	1	0,2	1	0
[HW.15]	**Switches**	Muy bajo	1	1	1	1	1		100%	20%	100%		0	1	0,2	1	0
[HW.16]	**Torno de acceso a oficina**	Bajo	5	6	5	7	7		100%	10%	100%		0	6	0,5	7	0
[HW.17]	**Routers wifi**	Muy bajo	5	6	5	1	7		100%	20%	100%		0	6	1	1	0
[HW.18]	**VPN CISCO**	Bajo	5	9	9	5	7		100%	20%	100%		0	9	1,8	5	0
[SW.1]	**Aplicación web**	Medio	5	7	5	5	7	100%	100%	100%	100%		5	7	5	5	0
[SW.2]	**Aplicaciones de gestión**	Medio	5	7	9	5	7	100%	100%	100%	100%		5	7	9	5	0
[SW.3]	**Servidor de correo**	Bajo	5	7	7	5	7	100%	100%	100%	100%		5	7	7	5	0
[SW.4]	**Antivirus**	Bajo	5	3	3	5	3	100%	100%	100%	100%		5	3	3	5	0
[SW.5]	**Servidor de ficheros**	Bajo	5	9	9	7	7	100%	100%	100%	100%		5	9	9	7	0
[SW.6]	**Microsoft SQL Server 2000**	Bajo	5	7	9	7	7	100%	100%	100%	100%		5	7	9	7	0
[SW.7]	**Servidor de DNS**	Bajo	5	7	5	5	7	100%	100%	100%	100%		5	7	5	5	0
[SW.8]	**Microsoft Windows Server 2000**	Bajo	5	7	9	7	7	100%	100%	100%	100%		5	7	9	7	0
[SW.9]	**Microsoft Windows XP Professional**	Medio	3	3	1	1	3	100%	100%	100%	100%		3	3	1	1	0
[SW.10]	**Microsoft Office Professional**	Medio	3	3	1	1	1	100%	100%	100%	100%		3	3	1	1	0
[D.1]	**Bases de datos**	Alto	5	7	9	7	7	100%	100%	50%	100%		5	7	4,5	7	0
[D.2]	**Datos en servidor de datos**	Muy alto	5	9	9	5	7	100%	100%	50%	100%		5	9	4,5	5	0
[D.3]	**Backups**	Muy alto	5	9	9	5	7	100%	100%	50%	100%		5	9	4,5	5	0
[D.4]	**Datos administrativos y gestión**	Alto	5	8	9	5	7	100%	100%	50%	100%		5	8	4,5	5	0
[D.5]	**Logs**	Medio	5	7	9	5	7	100%	50%	100%	50%	100%	5	3,5	9	2,5	7
[COM.1]	**Red telefónica**	Bajo	5	3	1	7	3		50%	10%	50%		0	1,5	0,1	3,5	0
[COM.2]	**Líneas ADSL**	Bajo	5	7	9	5	7		50%	10%	50%		0	3,5	0,9	2,5	0
[COM.3]	**VPN Madrid**	Bajo	5	7	9	5	7		50%	10%	50%		0	3,5	0,9	2,5	0
[COM.4]	**Red Inalámbrica**	Muy bajo	5	7	9	1	7		50%	10%	50%		0	3,5	0,9	0,5	0
[S.1]	**Acceso remoto**	Bajo	5	7	7	5	7	100%	100%	50%	100%	100%	5	7	3,5	5	7
[S.2]	**Monitorización**	Bajo	5	5	7	5	7	100%	100%	50%	100%	100%	5	5	3,5	5	7
[S.3]	**Correo electrónico**	Bajo	5	7	7	5	7	100%	100%	50%	100%	100%	5	7	3,5	5	7
[S.4]	**Transferencia de ficheros**	Bajo	5	9	9	5	7	100%	100%	50%	100%	100%	5	9	4,5	5	7
[S.5]	**Gestión de acceso físico a oficinas**	Bajo	5	6	5	7	7	100%	100%	50%	100%	100%	5	6	2,5	7	7
[S.6]	**Web**	Medio	5	7	5	5	7	100%	100%	50%	100%	100%	5	7	2,5	5	7
[AUX.1]	**Armario con llave de entrada a sala CPD**	Muy bajo	-	6	-	7	-		100%	50%	100%			6		7	
[AUX.2]	**Armario con llave con documentos en papel**	Muy bajo	-	6	5	5	-		100%	50%	100%			6	2,5	5	
[AUX.3]	**Aire acondicionado**	Bajo	-	-	-	5	-			50%	100%					5	
[AUX.4]	**SAI para el CPD**	Medio	-	-	-	5	-			50%	100%					5	
[AUX.5]	**Corriente eléctrica**	Bajo	-	-	-	5	-			50%	100%					5	
[P.1]	**Responsable de operaciones**	Alto	-	-	-	3	-		10%	10%	100%					3	

[P.2]	Responsable de Sistemas e infraestrucura	Medio	-	-	-	3	-		10%	10%	100%					3	
[P.3]	Resto personal TIC	Muy alto	-	-	-	1	-		10%	10%	100%					1	
[P.4]	Personal de administración/finanzas	Muy alto	-	-	-	1	-		10%	10%	100%					1	

5.4. Nivel de riesgo aceptable y riego residual

Teniendo calculado el impacto potencial que puede afectar a los activos de la empresa la materialización de las amenazas, es necesario definir un límite para poder discernir el riesgo aceptable que la compañía podría asumir y por otro lado poder dedicar recursos para poder paliar este nivel de riesgo con salvaguardas. Para ello podemos calcular una tabla para conocer el riesgo a partir de la siguiente fórmula sobre su cálculo:

```
Riesgo = impacto potencial (según dimensión) x frecuencia
```

Tabla resumen de riesgo

ACTIVO		VALOR	FRECUENCIA		% IMPACTO POTENCIAL					RIESGO				
ID	NOMBRE				A	C	I	D	T	A	C	I	D	T
[L.1]	Sala CPD	Alto	B	0,1	0	4,5	4,5	7	0	0	0,45	0,45	0,7	0
[L.2]	Oficinas	Alto	N	1	0	3	2,5	7	0	0	3	2,5	7	0
[L.3]	Recepción	Medio	N	1	0	3	2,5	7	0	0	3	2,5	7	0
[HW.1]	Firewall externo	Bajo	A	10	0	7	1	7	0	0	70	10	70	0
[HW.2]	Servidores de datos	Medio	N	1	0	9	1,8	7	0	0	9	1,8	7	0
[HW.3]	Servidor de nóminas/finanzas/administración	Bajo	N	1	0	7	1,8	5	0	0	7	1,8	5	0
[HW.4]	Servidores de BBDD	Bajo	N	1	0	7	1,8	7	0	0	7	1,8	7	0
[HW.5]	Servidor web	Bajo	A	10	0	7	1	5	0	0	70	10	50	0
[HW.6]	Servidor de correo	Bajo	A	10	0	7	1,4	5	0	0	70	14	50	0
[HW.7]	Servidor DNS	Bajo	A	10	0	7	1	5	0	0	70	10	50	0
[HW.8]	Servidores de desarrollo	Medio	N	1	0	3	0,6	3	0	0	3	0,6	3	0
[HW.9]	Estaciones de trabajo	Medio	MA	100	0	3	0,2	1	0	0	300	20	100	0
[HW.10]	Portátiles de guardias	Medio	MA	100	0	5	1	3	0	0	500	100	300	0
[HW.11]	Cámara de vigilancia	Muy bajo	N	1	0	6	0,5	7	0	0	6	0,5	7	0
[HW.12]	Firewal interno	Bajo	N	1	0	7	1	7	0	0	7	1	7	0
[HW.13]	Servidor NIDS	Bajo	A	10	0	3	1,8	3	0	0	30	18	30	0
[HW.14]	Impresoras	Muy bajo	MA	100	0	1	0,2	1	0	0	100	20	100	0
[HW.15]	Switches	Muy bajo	N	1	0	1	0,2	1	0	0	1	0,2	1	0
[HW.16]	Torno de acceso a oficina	Bajo	N	1	0	6	0,5	7	0	0	6	0,5	7	0
[HW.17]	Routers wifi	Muy bajo	N	1	0	6	1	1	0	0	6	1	1	0
[HW.18]	VPN CISCO	Bajo	A	10	0	9	1,8	5	0	0	90	18	50	0

[SW.1]	**Aplicación web**	Medio	N	1	5	7	5	5	0	5	7	5	5	0
[SW.2]	**Aplicaciones de gestión**	Medio	N	1	5	7	9	5	0	5	7	9	5	0
[SW.3]	**Servidor de correo**	Bajo	N	1	5	7	7	5	0	5	7	7	5	0
[SW.4]	**Antivirus**	Bajo	N	1	5	3	3	5	0	5	3	3	5	0
[SW.5]	**Servidor de ficheros**	Bajo	N	1	5	9	9	7	0	5	9	9	7	0
[SW.6]	**Microsoft SQL Server 2000**	Bajo	N	1	5	7	9	7	0	5	7	9	7	0
[SW.7]	**Servidor de DNS**	Bajo	N	1	5	7	5	5	0	5	7	5	5	0
[SW.8]	**Microsoft Windows Server 2000**	Bajo	N	1	5	7	9	7	0	5	7	9	7	0
[SW.9]	**Microsoft Windows XP Professional**	Medio	MA	100	3	3	1	1	0	300	300	100	100	0
[SW.10]	**Microsoft Office Professional**	Medio	MA	100	3	3	1	1	0	300	300	100	100	0
[D.1]	**Bases de datos**	Alto	A	10	5	7	4,5	7	0	50	70	45	70	0
[D.2]	**Datos en servidor de datos**	Muy alto	A	10	5	9	4,5	5	0	50	90	45	50	0
[D.3]	**Backups**	Muy alto	A	10	5	9	4,5	5	0	50	90	45	50	0
[D.4]	**Datos administrativos y gestión**	Alto	A	10	5	8	4,5	5	0	50	80	45	50	0
[D.5]	**Logs**	Medio	N	1	5	3,5	9	2,5	7	5	3,5	9	2,5	7
[COM.1]	**Red telefónica**	Bajo	N	1	0	1,5	0,1	3,5	0	0	1,5	0,1	3,5	0
[COM.2]	**Líneas ADSL**	Bajo	N	1	0	3,5	0,9	2,5	0	0	3,5	0,9	2,5	0
[COM.3]	**VPN Madrid**	Bajo	N	1	0	3,5	0,9	2,5	0	0	3,5	0,9	2,5	0
[COM.4]	**Red Inalámbrica**	Muy bajo	N	1	0	3,5	0,9	0,5	0	0	3,5	0,9	0,5	0
[S.1]	**Acceso remoto**	Bajo	A	10	5	7	3,5	5	7	50	70	35	50	70
[S.2]	**Monitorización**	Bajo	A	10	5	5	3,5	5	7	50	50	35	50	70
[S.3]	**Correo electrónico**	Bajo	A	10	5	7	3,5	5	7	50	70	35	50	70
[S.4]	**Transferencia de ficheros**	Bajo	A	10	5	9	4,5	5	7	50	90	45	50	70
[S.5]	**Gestión de acceso físico a oficinas**	Bajo	A	10	5	6	2,5	7	7	50	60	25	70	70
[S.6]	**Web**	Medio	A	10	5	7	2,5	5	7	50	70	25	50	70
[AUX.1]	**Armario con llave de entrada a sala CPD**	Muy bajo	N	1	0	6	0	7	0	0	6	0	7	0
[AUX.2]	**Armario con llave con documentos en papel**	Muy bajo	N	1	0	6	2,5	5	0	0	6	2,5	5	0
[AUX.3]	**Aire acondicionado**	Bajo	N	1	0	0	0	5	0	0	0	0	5	0
[AUX.4]	**SAI para el CPD**	Medio	N	1	0	0	0	5	0	0	0	0	5	0
[AUX.5]	**Corriente eléctrica**	Bajo	N	1	0	0	0	5	0	0	0	0	5	0
[P.1]	**Responsable de operaciones**	Alto	A	10	0	0	0	3	0	0	0	0	30	0
[P.2]	**Responsable de Sistemas e infraestructura**	Medio	A	10	0	0	0	3	0	0	0	0	30	0
[P.3]	**Resto personal TIC**	Muy alto	A	10	0	0	0	1	0	0	0	0	10	0
[P.4]	**Personal de administración/finanzas**	Muy alto	A	10	0	0	0	1	0	0	0	0	10	0

Consideraciones de la tabla y definición de riesgo aceptable

Considerando el riesgo obtenido mediante la tabla, en primer lugar se debe definir el riesgo aceptable. Para ello se define un riesgo aceptable con valor 50 aceptado por la Dirección, por tanto, todo valor superior a éste debe ser tratado en consideración para poder resolver o mitigar su riesgo asociado tal y como se especifica en las celdas de color rojo. Según la criticidad y el valor del riesgo asociado se tomarán medidas con mayor emergencia.

Teniendo en cuenta este riesgo aceptable, se deben solventar deficiencias en:

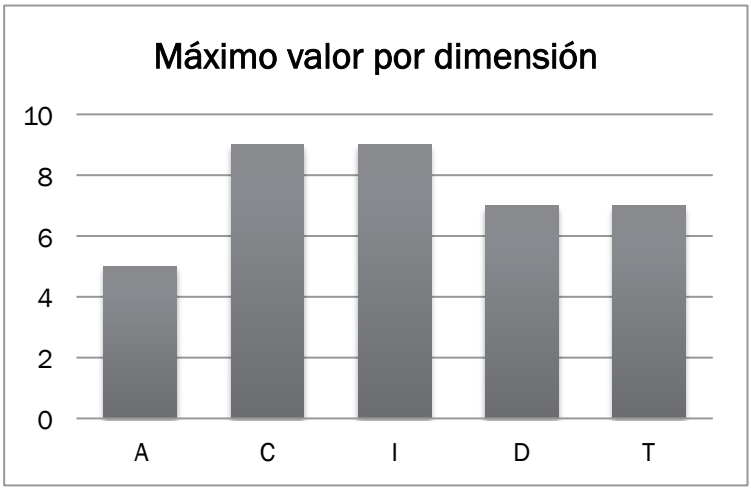
- Los activos relacionados directamente con el personal de la compañía como sus estaciones de trabajo y el software instalado
- La confidencialidad de los activos accesibles desde el exterior como el servidor web, DNS y el de correo
- La confidencialidad de los datos
- Asegurar la confidencialidad y trazabilidad en los servicios que ofrece ConTec S.L.

5.5. Resultados

Una vez realizado este estudio y obtenidos los resultados mediante las tablas de los anteriores apartados, se deberán tomar medidas con tal de mejorar las deficiencias de seguridad en la compañía y asegurar su continuidad.

Activos

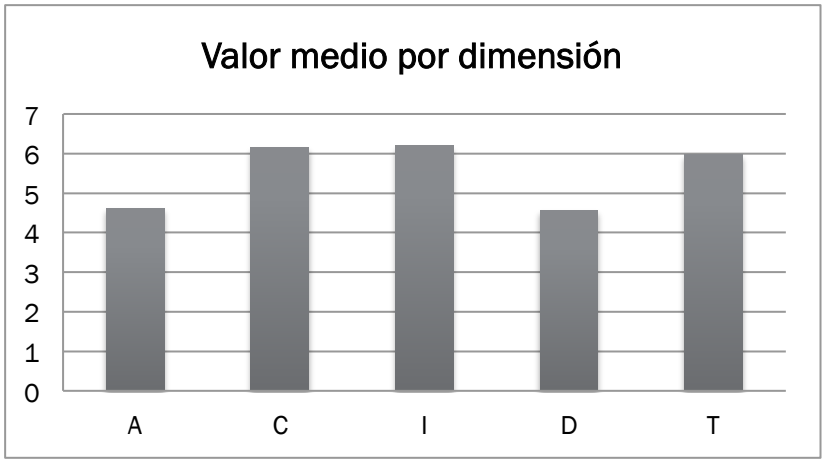
En primer lugar hemos conocido cuales son las dimensiones de la seguridad de la información más críticas para ConTec S.L. En la siguiente tabla se pueden observar cuales son los valores máximos asignados a los activos objeto de estudio:



Como se puede observar, los valores más elevados hacen referencia a la confidencialidad y a la integridad. Por un lado, la confidencialidad es una dimensión crítica por almacenar información de carácter personal y por otro lado información específica de cliente y específicamente credenciales para poder gestionar sus

sistemas. Por otro lado la integridad de los datos es también importante para el buen desarrollo de la compañía a pesar que de todos modos se realizan backups de los mismos, los cuales se almacenan exteriormente en un centro de datos de confianza. Al no ofrecer servicios críticos mediante su infraestructura, la disponibilidad no es decisiva pero sí importante para mantener la confianza del cliente.

En la siguiente tabla se puede observar el valor medio por dimensión asignado a los activos:



Siguiendo con las bases de la gráfica anterior, se puede observar que la trazabilidad también obtiene un papel importante, en caso de que no se llevara un control sobre el acceso a datos, posibles modificaciones o el robo de información. En definitiva, no poder rastrear a posteriori si alguien ha accedido o ha modificado cierta información podría incapacitar a la compañía a perseguir delitos y podría suponer un incumplimiento de obligaciones legales.

Amenazas

Sobre estos activos, las principales amenazas que pudieran sufrir y que ConTec S.L debe gestionar según la frecuencia de que sucedan destacan:

Amenazas con frecuencia diaria:

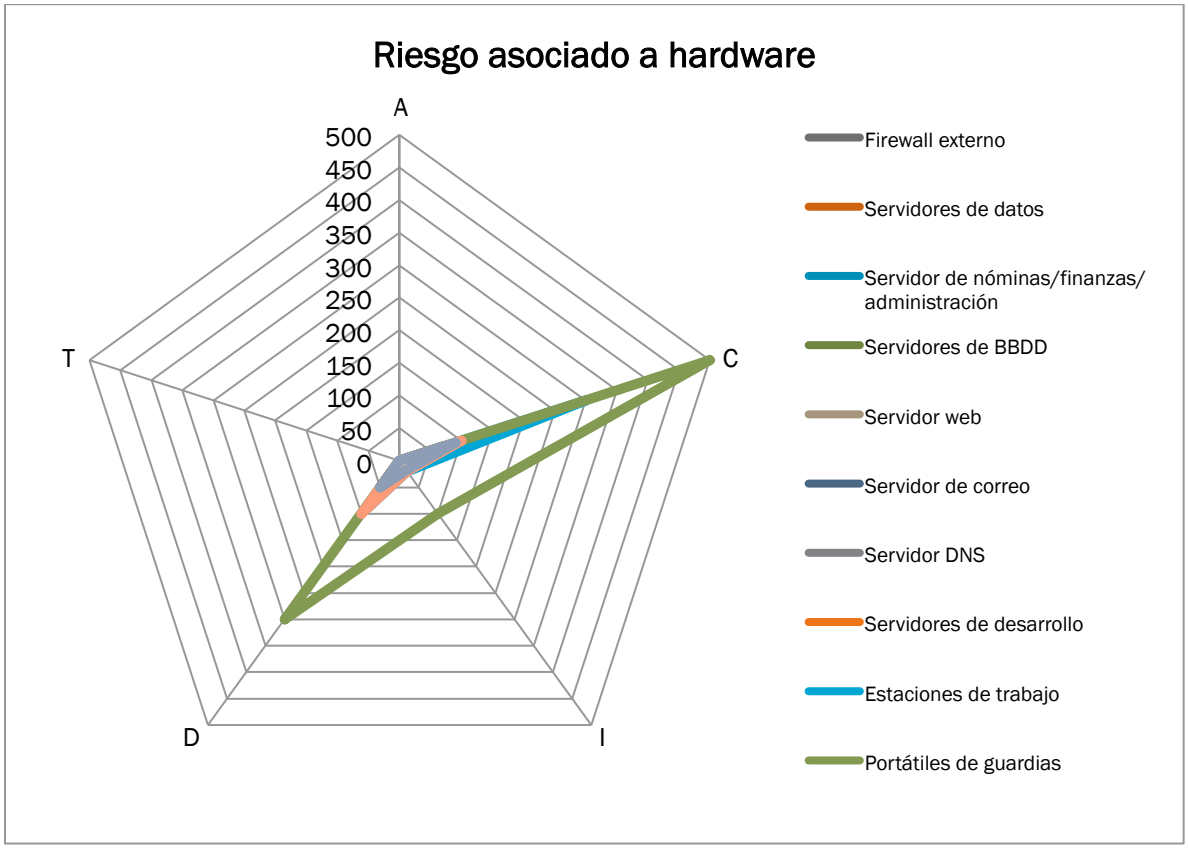
- Uso no previsto: ya que no hay restricciones de uso en las estaciones de trabajo

Amenazas con frecuencia mensual:

- Caída del sistema por agotamiento de recursos
- Errores de mantenimiento o actualización de equipos
- Errores de configuración
- Alteración o destrucción de información por error
- Acceso no autorizado
- Denegación de servicio
- Vulnerabilidades en los programas
- Alteración accidental de la información
- Errores de los usuarios
- Indisponibilidad de los usuario

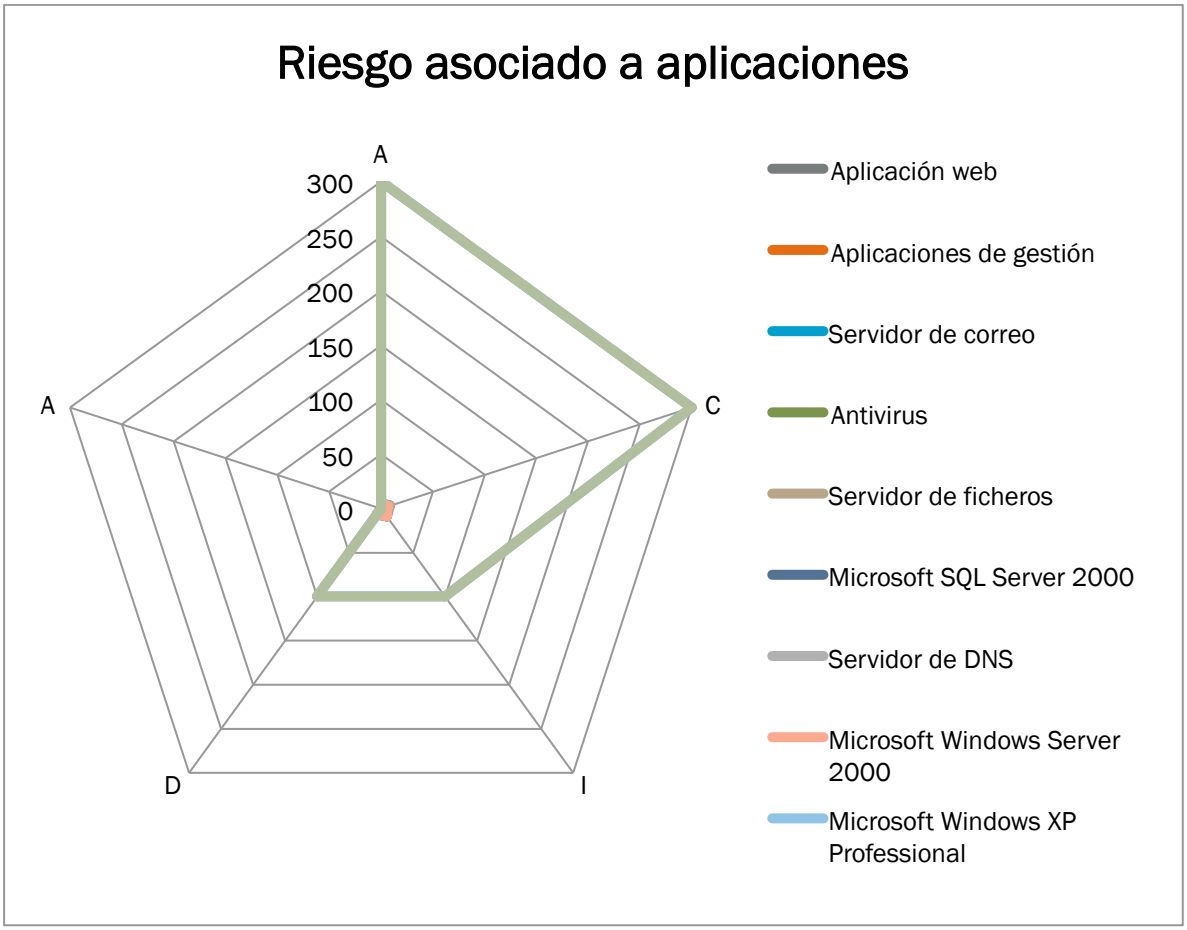
Riesgo

A continuación se indica mediante gráficas, el nivel de riesgo asociado a diferentes grupos de activos donde se tendrán que tomar medidas para solventar riesgos no aceptables por la compañía:



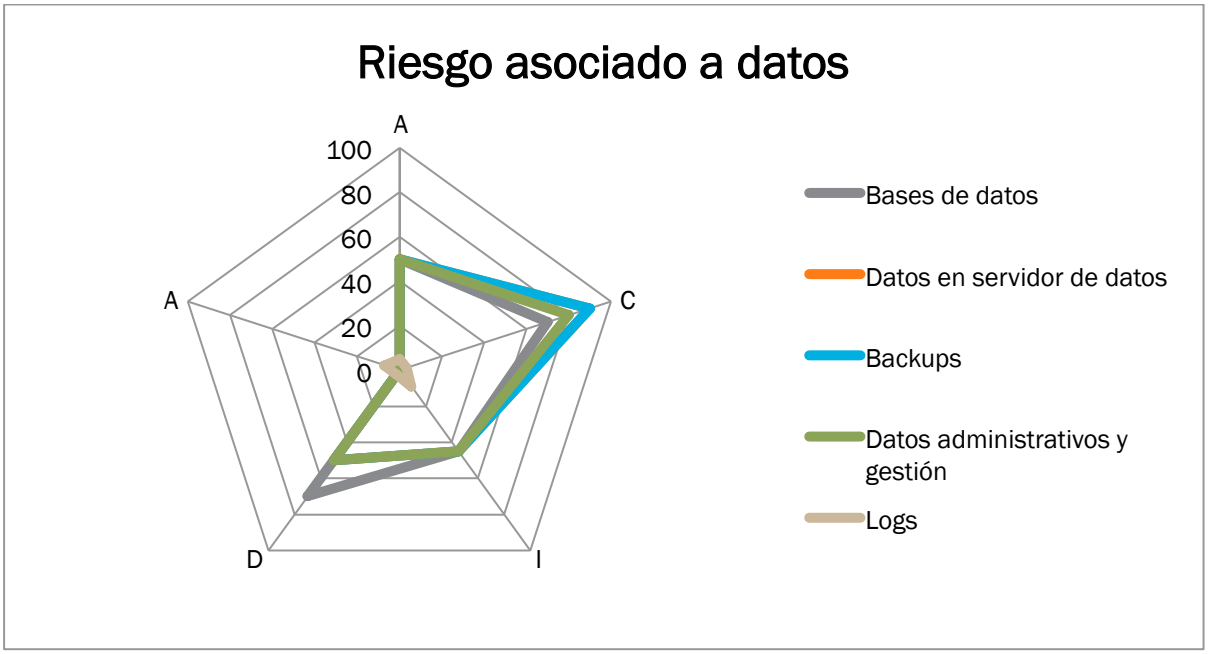
Como se puede observar en esta gráfica, los portátiles de guardia son un activo crítico a nivel de seguridad con el que ConTec S.L. debe prestar especial atención. Por un lado, a nivel de confidencialidad se almacena información crítica para la actividad de negocio de la empresa y por tanto se debe asegurar que la información no se dispone o se revela a personas no autorizadas, en esta tesitura también entra en juego la disponibilidad por si sucediera el extravío o robo del portátil. Los clientes tienen un SLA contratado con ConTec S.L. que se debe cumplir en horario no laboral.

La siguiente gráfica hace referencia al riesgo asociado a las aplicaciones:



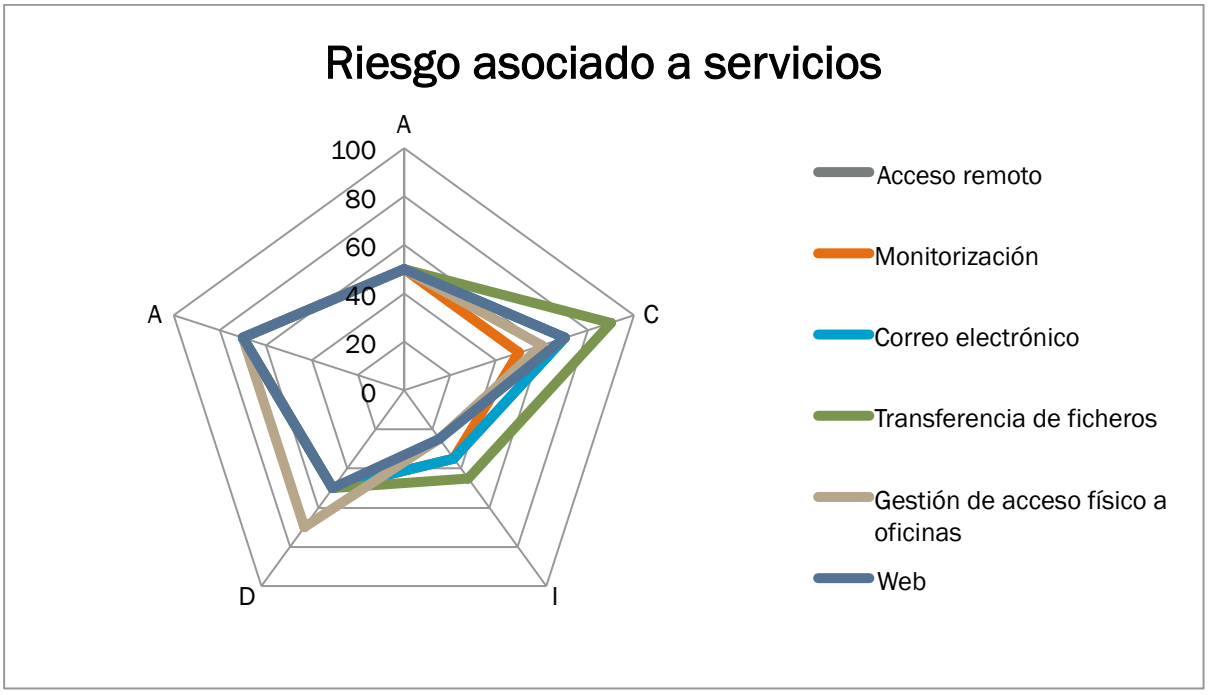
En el caso del software instalado destaca el software de las estaciones de trabajo de los empleados, esto es así puesto que los empleados no tienen restricciones de acceso a internet y tienen permisos de administración en sus estaciones respectivas, por lo que un empleado desprevenido o engañado por algún tipo de ataque como pudiera ser mediante ingeniería social podría comprometer la seguridad de la compañía.

La siguiente gráfica hace referencia al riesgo asociado a los datos:



Según los resultados obtenidos de esta gráfica se puede concretar que existe cierta igualdad en el riesgo asociado a los distintos tipos de datos excepto en los logs, esto es así puesto que los logs es más difícil que sean alterados accidentalmente.

La siguiente gráfica hace referencia al riesgo asociado a servicios:



A partir de la gráfica anterior se puede destacar la importancia de ciertos servicios y lo que implicarían fallos sobre ellos:

- La confidencialidad a la hora de transferir ficheros
- La trazabilidad de los servicios y poder rastrear si sucediera cualquier tipo de incidente.
- La disponibilidad de los servicios asociados a los activos que gestionan la seguridad física a las oficinas.

Síntesis

En definitiva y a modo de resumen, a continuación se indican destacados cuales son los activos con mayor posibilidad de riesgo:

- En primer lugar, los activos directamente relacionados con el uso diario por parte del personal, como son las estaciones de trabajo, portátiles de guardia o el software instalado en estos ordenadores son los que contienen más riesgos, esto es así puesto que los empleados no tienen restricciones de acceso a internet y tienen permisos de administrador en sus estaciones respectivas. Por su parte, la compañía ofrece formación en cuanto a sensibilización en temas de seguridad a todo el personal de ConTec S.L.
- Dentro del grupo anterior, destacan los portátiles de guardia con un mayor riesgo asociado ya que se extraen de la oficina para realizar las guardias, por lo que tiene mayor posibilidad de pérdida o robo, con los problemas de seguridad que ello implicaría.
- Los sistemas accesibles externamente como el servidor de correo o el servidor web sufren caídas por agotamiento de recursos.
- La disponibilidad de la base de datos es importante para la continuidad de los distintos servicios de la compañía.
- Se debe prestar atención a la seguridad en la transferencia de ficheros y asegurar su confidencialidad.
- Es importante que se pueda rastrear el origen o causante de cualquier incidente que se diera sobre cualquier servicio que proporciona ConTec S.L.

6. Propuestas de proyectos

6.1. Introducción

Una vez conocido el estado actual de la compañía en relación a la seguridad de la información y por otro lado, realizado el análisis de riesgo, es necesario definir diferentes propuestas de proyecto con el fin de mitigar el riesgo actual de la compañía y así evolucionar para cumplir la ISO hasta conseguir un nivel adecuado.

Durante este apartado se listaran diferentes proyectos que se proponen para llevar a cabo e implantarlos durante el tiempo estimado de 3 años para el plan de proyectos.

Para ello será importante concretar aspectos como la prioridad de los proyectos a la hora de ordenarlos según la implicación que tienen en el impacto sobre la compañía.

6.2. Planificación temporal

Una vez realizadas las propuestas de proyecto tal y como se indican en el *Anexo IX – Propuestas de proyecto* se deben organizar estos proyectos según su prioridad.

El plan de proyecto estimado tendrá una duración de 3 años, durante este tiempo se realizarán los distintos proyectos.

Para la planificación temporal se especifica en la tabla el responsable del proyecto según la siguiente leyenda:

Departamento de sistemas	
Comité de seguridad de la información	

En la siguiente tabla, se puede ver como quedan encuadrados según año los diferentes proyectos:

Proyectos	Duración	2013	2014	2015	2016
		Primer año	Segundo año	Tercer año	
Administración de estaciones de trabajo y portátiles de guardia	6 meses				
Securización de portátiles de guardia	1 mes				
Gestión del inventario de activos	1 mes				
Mejora en servicio de transferencia de ficheros	1 mes				
Política de seguridad de la información	1 mes				
Revisión de aspectos organizativos internos	1 mes				
Cumplimiento de requisitos legales y políticas de la compañía	3 meses				
Clasificación de la información	2 meses				
Revisión de política de control de accesos	1 mes				
Política de tratamiento de incidentes de seguridad	1 mes				
Política de mantenimiento de los sistemas de la información	2 meses				
Revisión de política de backups y gestión de datos	1 mes				
Revisión documentación relacionada con los RRHH	2 mes				
Plan de continuidad de negocio	6 meses				
Sistema balanceado para servidor web corporativo	1 mes				
Migración del servidor de correo	2 meses				
Política de gestión de logs	1 mes				
Gestión de auditorias de sistemas	1 mes				
Política de retirada de equipos y material	1 mes				
Nuevo sistema de acceso a CPD	1 semana				

6.3. Mejora y evolución del riesgo

Cada uno de los proyectos tiene como objetivo mitigar o mejorar el riesgo actual de la compañía y dirigir sus esfuerzos al cumplimiento de la ISO 27001 hasta el nivel esperado. Para ello se ha estudiado el riesgo no aceptable al que están sometidos actualmente los activos de ConTec S.L. para idear proyectos que los solventen. Estos proyectos no están únicamente ideados para paliar los riesgos mediante proyectos relacionados directamente con la gestión de la seguridad sobre ellos, sino que también se incluyen proyectos para mejorar el nivel de cumplimiento de los diferentes dominios de la ISO 27002.

Estos proyectos llevados a la práctica resultarán en una mejora importante tal y como se puede ver en los siguientes apartados.

Evaluación del riesgo posterior

En la siguiente tabla se puede observar como ha evolucionado el riesgo. Actualmente todo riesgo superior a 50 no es aceptable, pero con las medidas satisfechas una vez desarrollados los proyectos, el riesgo que podría materializarse sobre los activos disminuye de forma notoria, muy por debajo del límite.

La causa de esta disminución en el riesgo viene dada por la reducción en el impacto de las amenazas sobre las distintas dimensiones según activo, como también según la probabilidad de que las amenazas sucedan.

Por ejemplo, los proyectos relacionados con la administración de las estaciones de trabajo y de los portátiles de guardia, solventan los riesgos más elevados a los que se afrontaba la compañía, especialmente referente a los portátiles de guardia con medidas como el sistema de autenticación mediante tokens de seguridad, el cual técnico de guardia llevará consigo el token para identificarse, cifrado de disco duro y bios con autenticación.

Los proyectos de mejora de transferencia de ficheros, los controles de acceso, la gestión de los datos, backups y la clasificación de información permiten proteger la información de la organización, dotando de impactos menores a las dimensiones de autenticidad, confidencialidad, integridad y trazabilidad.

La siguiente tabla muestra los valores del riesgo anterior y posteriormente de llevar a cabo los proyectos propuestos:

ACTIVO		RIESGO					RIESGO POSTERIOR				
ID	NOMBRE	A	C	I	D	T	A	C	I	D	T
[L.1]	Sala CPD	0	0,45	0,45	0,7	0	0	0,09	0,45	0,7	0
[L.2]	Oficinas	0	3	2,5	7	0	0	0,12	0,1	0,7	0
[L.3]	Recepción	0	3	2,5	7	0	0	0,12	0,1	0,7	0
[HW.1]	Firewall externo	0	70	10	70	0	0	7	1	7	0
[HW.2]	Servidores de datos	0	9	1,8	7	0	0	9	1,8	7	0
[HW.3]	Servidor de nóminas/finanzas/administración	0	7	1,8	5	0	0	7	1,8	5	0
[HW.4]	Servidores de BBDD	0	7	1,8	7	0	0	7	1,8	7	0
[HW.5]	Servidor web	0	70	10	50	0	0	7	1	5	0
[HW.6]	Servidor de correo	0	70	14	50	0	0	7	1,4	5	0
[HW.7]	Servidor DNS	0	70	10	50	0	0	7	1	5	0
[HW.8]	Servidores de desarrollo	0	3	0,6	3	0	0	3	0,6	3	0
[HW.9]	Estaciones de trabajo	0	300	20	100	0	0	15	2	10	0
[HW.10]	Portátiles de guardias	0	500	100	300	0	0	25	10	30	0
[HW.11]	Cámara de vigilancia	0	6	0,5	7	0	0	0,6	0,05	0,7	0
[HW.12]	Firewal interno	0	7	1	7	0	0	7	1	7	0
[HW.13]	Servidor NIDS	0	30	18	30	0	0	3	1,8	3	0
[HW.14]	Impresoras	0	100	20	100	0	0	5	2	10	0
[HW.15]	Switches	0	1	0,2	1	0	0	1	0,2	1	0
[HW.16]	Torno de acceso a oficina	0	6	0,5	7	0	0	0,6	0,05	0,7	0
[HW.17]	Routers wifi	0	6	1	1	0	0	6	1	1	0
[HW.18]	VPN CISCO	0	90	18	50	0	0	9	1,8	5	0
[SW.1]	Aplicación web	5	7	5	5	0	5	3,5	2,5	2,5	0
[SW.2]	Aplicaciones de gestión	5	7	9	5	0	5	3,5	4,5	2,5	0
[SW.3]	Servidor de correo	5	7	7	5	0	5	3,5	3,5	2,5	0
[SW.4]	Antivirus	5	3	3	5	0	5	1,5	1,5	2,5	0
[SW.5]	Servidor de ficheros	5	9	9	7	0	5	4,5	4,5	3,5	0
[SW.6]	Microsoft SQL Server 2000	5	7	9	7	0	5	3,5	4,5	3,5	0
[SW.7]	Servidor de DNS	5	7	5	5	0	5	3,5	2,5	2,5	0
[SW.8]	Microsoft Windows Server 2000	5	7	9	7	0	5	3,5	4,5	3,5	0
[SW.9]	Microsoft Windows XP Professional	300	300	100	100	0	30	15	5	5	0
[SW.10]	Microsoft Office Professional	300	300	100	100	0	30	15	5	5	0
[D.1]	Bases de datos	50	70	45	70	0	5	7	1,8	1,4	0
[D.2]	Datos en servidor de datos	50	90	45	50	0	5	9	1,8	1	0
[D.3]	Backups	50	90	45	50	0	5	9	1,8	1	0
[D.4]	Datos administrativos y gestión	50	80	45	50	0	5	8	1,8	1	0
[D.5]	Logs	5	3,5	9	2,5	7	0,5	0,35	0,18	0,1	0,35
[COM.1]	Red telefónica	0	1,5	0,1	3,5	0	0	0,6	0,1	3,5	0
[COM.2]	Líneas ADSL	0	3,5	0,9	2,5	0	0	1,4	0,9	2,5	0
[COM.3]	VPN Madrid	0	3,5	0,9	2,5	0	0	1,4	0,9	2,5	0
[COM.4]	Red Inalámbrica	0	3,5	0,9	0,5	0	0	1,4	0,9	0,5	0
[S.1]	Acceso remoto	50	70	35	50	70	5	7	3,5	5	3,5
[S.2]	Monitorización	50	50	35	50	70	5	5	3,5	5	3,5
[S.3]	Correo electrónico	50	70	35	50	70	5	7	3,5	5	3,5

[S.4]	Transferencia de ficheros	50	90	45	50	70	5	9	4,5	5	3,5
[S.5]	Gestión de acceso físico a oficinas	50	60	25	70	70	5	6	2,5	7	3,5
[S.6]	Web	50	70	25	50	70	5	7	2,5	5	3,5
[AUX.1]	Armario con llave de entrada a sala CPD	0	6	0	7	0	0	0,12	0	0,7	0
[AUX.2]	Armario con llave con documentos en papel	0	6	2,5	5	0	0	0,12	0,1	0,5	0
[AUX.3]	Aire acondicionado	0	0	0	5	0	0	0	0	5	0
[AUX.4]	SAI para el CPD	0	0	0	5	0	0	0	0	5	0
[AUX.5]	Corriente eléctrica	0	0	0	5	0	0	0	0	5	0
[P.1]	Responsable de operaciones	0	0	0	30	0	0	0	0	30	0
[P.2]	Responsable de Sistemas e infraestrucura	0	0	0	30	0	0	0	0	30	0
[P.3]	Resto personal TIC	0	0	0	10	0	0	0	0	10	0
[P.4]	Personal de administración/finanzas	0	0	0	10	0	0	0	0	10	0

Evolución cumplimiento de la ISO 27001

A continuación se indican los proyectos planteados con tal de resolver las deficiencias encontradas en ConTec S.L. según los dominios de la ISO:

5 - Política de seguridad

ID	Nombre de proyecto	Objetivos de control
DOC-013	Política de seguridad de la información	5.1

6 - Aspectos organizativos de la seguridad de la información

ID	Nombre de proyecto	Objetivos de control
DOC-014	Revisión de aspectos organizativos internos	6.1

7 - Gestión de activos

ID	Nombre de proyecto	Objetivos de control
DOC-005	Gestión del inventario de activos	7.1
DOC-004	Clasificación de la información	7.2

8 - Seguridad ligada a los recursos humanos

ID	Nombre de proyecto	Objetivos de control
DOC-012	Revisión documentación relacionada con RRHH	8.1, 8.2, 8.3

9 - Seguridad física y del entorno

ID	Nombre de proyecto	Objetivos de control
INF-001	Nuevo sistema de acceso al CPD	9.1.2
IMP-002	Securización de portátiles de guardia	9.2.5
DOC-008	Política de retirada de equipos y material	9.2.6, 9.2.7

10 - Gestión de comunicaciones y operaciones

ID	Nombre de proyecto	Objetivos de control
IMP-001	Administración de estaciones de trabajo y portátiles de guardia	10.4, 10.7
IMP-005	Mejora en servicio de transferencia de ficheros	10.8
DOC-003	Revisión de política de backups y gestión de datos	10.5
DOC-001	Política de gestión de logs	10.10

11 - Control de acceso

ID	Nombre de proyecto	Objetivos de control
IMP-001	Administración de estaciones de trabajo y portátiles de guardia	11.3, 11.5
DOC-002	Revisión de política de control de accesos	11.1.1, 11.2, 11.4, 11.5, 11.6
IMP-002	Securización de portátiles de guardia	11.7

12 - Adquisición, desarrollo y mantenimiento de sistemas de la información

ID	Nombre de proyecto	Objetivos de control
DOC-006	Política de mantenimiento de los sistemas de la información	12.1, 12.3, 12.4, 12.6

13 - Gestión de incidentes en la seguridad de la información

ID	Nombre de proyecto	Objetivos de control
DOC-007	Política de tratamiento de incidentes de seguridad	13.2

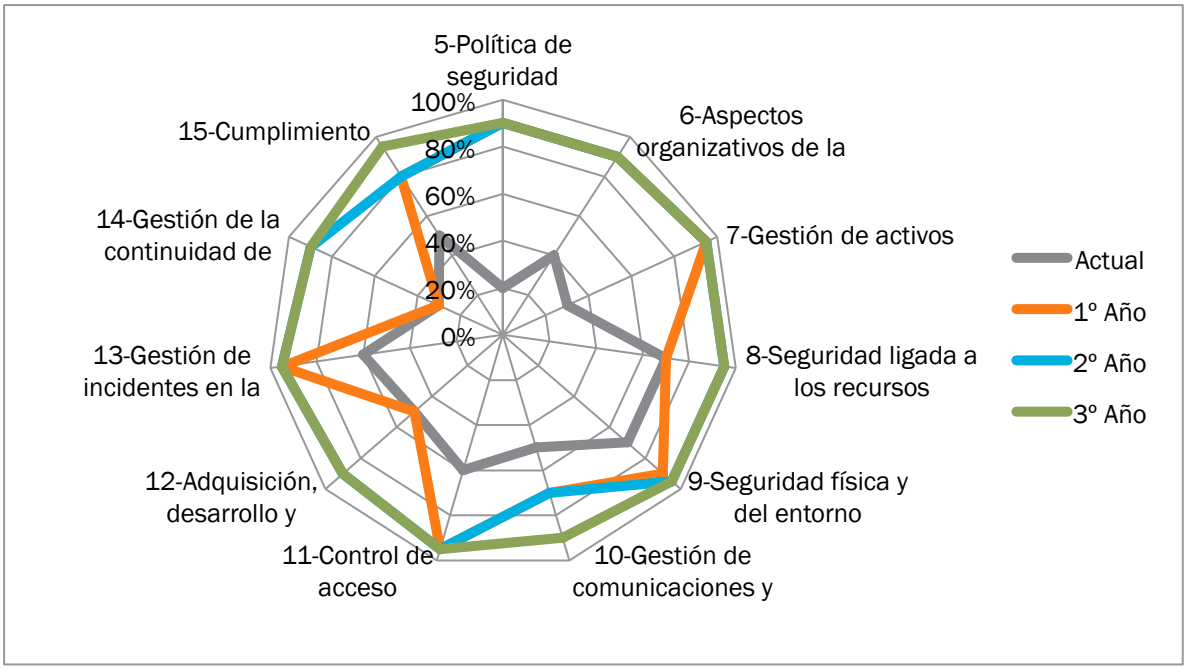
14 - Gestión de la continuidad de negocio

ID	Nombre de proyecto	Objetivos de control
DOC-011	Plan de continuidad de negocio	14.1

ID	Nombre de proyecto	Objetivos de control
DOC-009	Cumplimiento de requisitos legales y políticas de la compañía	15.1,15.2
DOC-010	Gestión de auditorias de sistemas	15.3

Gráfico de la evolución

Finalmente, este gráfico muestra la evolución del cumplimiento de la ISO según la planificación marcada durante los 3 años de proyecto:



De inicio se pueden destacar ciertos aspectos. Actualmente existen graves deficiencias en los dominios “Política de seguridad”, “Aspectos organizativos de la seguridad de la información”, “Gestión de activos” y “Gestión de la continuidad de negocio”, por lo que es necesario tomar medidas prioritarias para solventarlos. Por otro lado, ya se habían implantado mayores medidas para los dominios “Seguridad ligada a los recursos humano” y “Seguridad física y del entorno” en cuanto documentos, normas, procedimientos, controles y aspectos legales por lo que el trabajo a realizar es menor.

Por tanto, el objetivo del primer año consiste en solventar los dominios con un nivel más deficiente, para posteriormente perfilarlos los años siguientes años. La empresa ya desde su inicio tenía en cuenta la seguridad de la información pero sin estándares, normas o procedimientos correctamente establecidos, así como las responsabilidades directas, por lo que desde un inicio se definiría la política de seguridad y una revisión de los aspectos organizativos internos para definir responsabilidades. Posteriormente se centraría en el correcto cumplimiento de la legislación vigente y de políticas y normas de seguridad. Un proyecto importante a

tratar este primer año para poder realizar los siguientes de una forma más eficiente consiste en una buena definición de los activos, por lo que se definen procedimientos para mantener un inventario de activos actualizado y por otro lado detallando directrices para la clasificación de la información. Por último dos proyectos importantes consisten en la mejora en la gestión y normativa sobre controles de acceso y transferencia de ficheros de forma segura.

Las propuestas de proyecto del segundo año van orientadas a mejorar el mantenimiento de los sistemas, la gestión de datos y los backups en la parte técnica. En el área de gestión se determina un plan de continuidad de negocio y la revisión de la seguridad de la documentación de los RRHH.

Por último en el tercer año, se termina de pulir la gestión de comunicaciones y operaciones con una revisión de la política de gestión de logs, además de mejorar la seguridad física y del entorno con la implantación de nuevo control de acceso al CPD y la creación de procedimientos para gestionar las auditorias de sistemas.

Como se puede observar, al término de los 3 años, no se cumplen al 100% cada uno de los dominios de la ISO, esto es así porque a pesar de tomar medidas y realizar procedimientos y normas, aún sería necesario afinar algún detalle para cumplirlos completamente, por otro lado se deja la posibilidad de realizar nuevos análisis de riesgos para detectar nuevas insuficiencias. Aún así se considera necesario cumplir al menos en un 90% cada uno de los dominios aunque se conseguiría el objetivo de un 95% en los dominios “Gestión de activos”, “Seguridad ligada a los recursos humanos”, “Seguridad física y del entorno”, “Control de acceso”, “Gestión de incidentes en la seguridad de la información” y “Cumplimiento”.

6.4. Planificación económica

La siguiente tabla muestra el coste asociado a cada proyecto y el coste anual total:

2013		2014		2015	
ID	**Coste**	**ID**	**Coste**	**ID**	**Coste**
IMP-001	30.000€	**DOC-011**	30.000€	**INF-001**	1.000€
IMP-002	3.000€	**IMP-003**	3.000€	**DOC-001**	2.000€
DOC-005	500€	**IMP-004**	5.000€	**DOC-008**	1.000€
IMP-005	5.000€	**DOC-006**	8.000€	**DOC-010**	3.000€
DOC-009	10.000€	**DOC-012**	6.000€		
DOC-004	3.000€	**DOC-003**	3.000€		
DOC-007	3.000€				
DOC-002	2.000€				
DOC-014	3.000€				
DOC-013	3.000€				
Total:	**62.500€**	**Total:**	**55.000€**	**Total:**	**7.000€**

Tal y como se puede ver en la anterior tabla, la mayor parte del trabajo se centra en los dos primeros años, donde se desarrollarían los proyectos más críticos o más importantes

Finalmente, la suma del coste total de los proyectos repartidos en los 3 años ascendería a:

Año	Coste
1º Año	62.500€
2º Año	55.000€
3º Año	7.000€
Total:	**123.500€**

6.5. Conclusiones

El objetivo de esta etapa consiste en la realización de propuestas de proyecto con tal de afrontar y mejorar los resultados obtenidos del análisis de riesgos y del análisis diferencial respecto la ISO 27001 y 27002. Mediante estos dos análisis se obtuvieron de forma global el estado actual de ConTec S.L. en relación con la seguridad de la información.

La implantación de los distintos proyectos conduce a un cumplimiento casi en su totalidad de los 11 dominios de la ISO. Para conseguirlo se han ideado controles para poder mejorar la calidad y la eficiencia de los procesos.

Como se puede apreciar tanto en la planificación económica como en la temporal, el proceso de implementación de los proyectos está definido para 3 años aunque el mayor peso del proceso recae principalmente en los dos primeros años. Estos dos primeros años se enfocan en la disminución de los riesgos más elevados obtenidos del estudio del análisis de riesgos y de las mayores carencias dentro de la organización respecto los dominios de la ISO. Los proyectos del último año ofrecen medidas para pulir ciertas necesidades.

Cabe destacar que la mayoría de los proyectos son de índole estratégica y de gestión en los que se definen políticas, normas, procedimientos y directrices para asegurar la protección de la información, de los activos, y de la continuidad de negocio para proteger los procesos críticos frente a desastres. En cuanto los proyectos más técnicos tienen como objetivo solucionar las deficiencias obtenidas del resultado del análisis de riesgo.

Para poder completar todo este proceso con éxito es indispensable el compromiso de la dirección para proporcionar todos los recursos necesarios para poder implantar los proyectos.

7. Auditoria de cumplimiento

7.1. Introducción

Una vez conocidos los activos de la empresa y evaluadas las amenazas, se debe estudiar el cumplimiento de ConTec S.L respecto a la seguridad de la información utilizando la ISO/IEC 27002:2005 como marco de control.

7.2. Evaluación de la madurez

El objetivo de esta fase consiste en evaluar la madurez de la seguridad según los dominios definidos en la ISO/IEC 27002. Para cada uno de los dominios, se realiza una tabla de acuerdo con el nivel de madurez asociado a cada uno de los controles definidos. Estos niveles de madurez se dividen en:

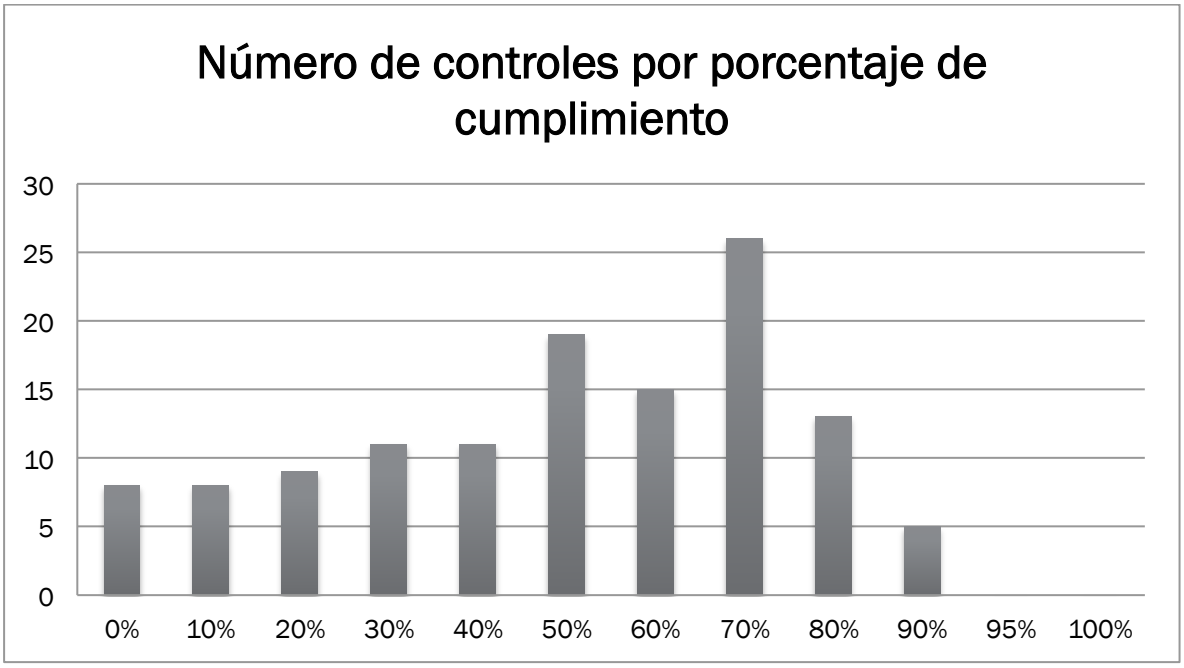
CMM	Efectividad	Descripción
L0 - No implementado / Inexistente	**0%**	No existen salvaguardas al control asociado.
L1 - Se ha hecho algo, manifiestamente insuficiente	**10%**	Las salvaguardas existen, pero no se gestionan. El éxito depende de la buena suerte. En este caso las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.
L2 - Reproducible, pero intuitivo	**50%**	La eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para incidentes más allá de una buena reacción por parte de los empleados. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo
L3 - Proceso definido	**90%**	Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor no planificado.
L4 - Gestionado y medible	**95%**	Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
L5 - Optimizado	**100%**	El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.
N.A. - No aplica		No es necesario aplicar ninguna salvaguarda.

7.3. Resumen de resultados

Una vez analizados cada uno de los controles del *Anexo X – Análisis de cumplimiento según dominio,* se pueden recalcar varias apreciaciones sobre los resultados obtenidos.

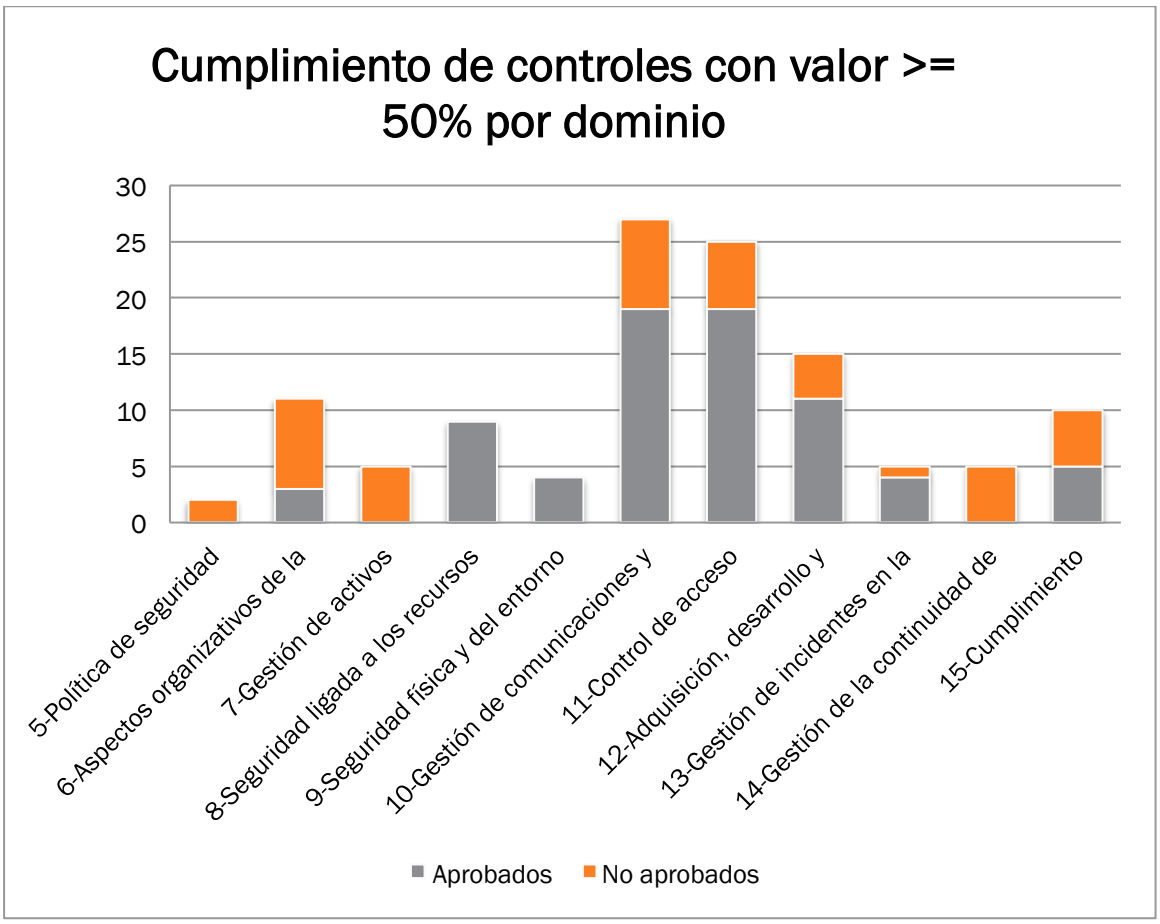
Número de controles por porcentaje de cumplimiento

A pesar que hay dominios en los que no se especifica ningún tipo de control o son muy deficientes, la mayoria de los procesos tienen asignados procedimientos, normas y controles para tratar la seguridad de la información. De todos modos, no es suficiente para cumplir con los requisitos necesarios por lo que se deben tomar medidas para mejorarlos y pasar de tener procesos relativamente documentados y medibles cualitativamente a técnicas estadísticas y cuantitativas mejor gestionables y comparables.



Cumplimiento de controles con valor >= 50% por dominio

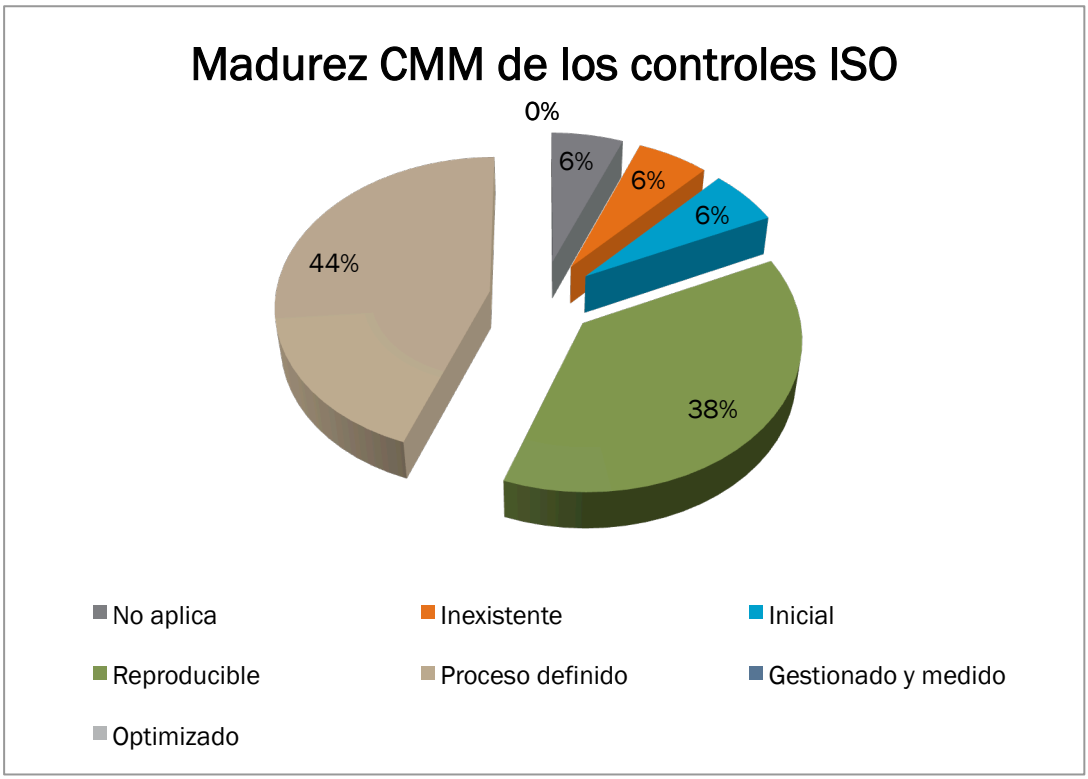
La siguiente gráfica muestra de forma representativa para cada dominio, aquellos en los que se han implantado medidas mínimas para la seguridad de la información y con salvaguardas que no dependan exclusivamente de la buena suerte o de la buena voluntad de los empleados, además de planes para incidentes más allá de una buena reacción por parte de los empleados.



Se pueden observar dominios donde no se han implementados medidas o controles para la seguridad de la información como en los dominios: “política de seguridad”, “gestión de activos” y “gestión de la continuidad de negocio”. Otros dominios como “Seguridad ligada a los recursos humanos” o “Seguridad física y el entorno” implementan medidas para cada uno de los controles.

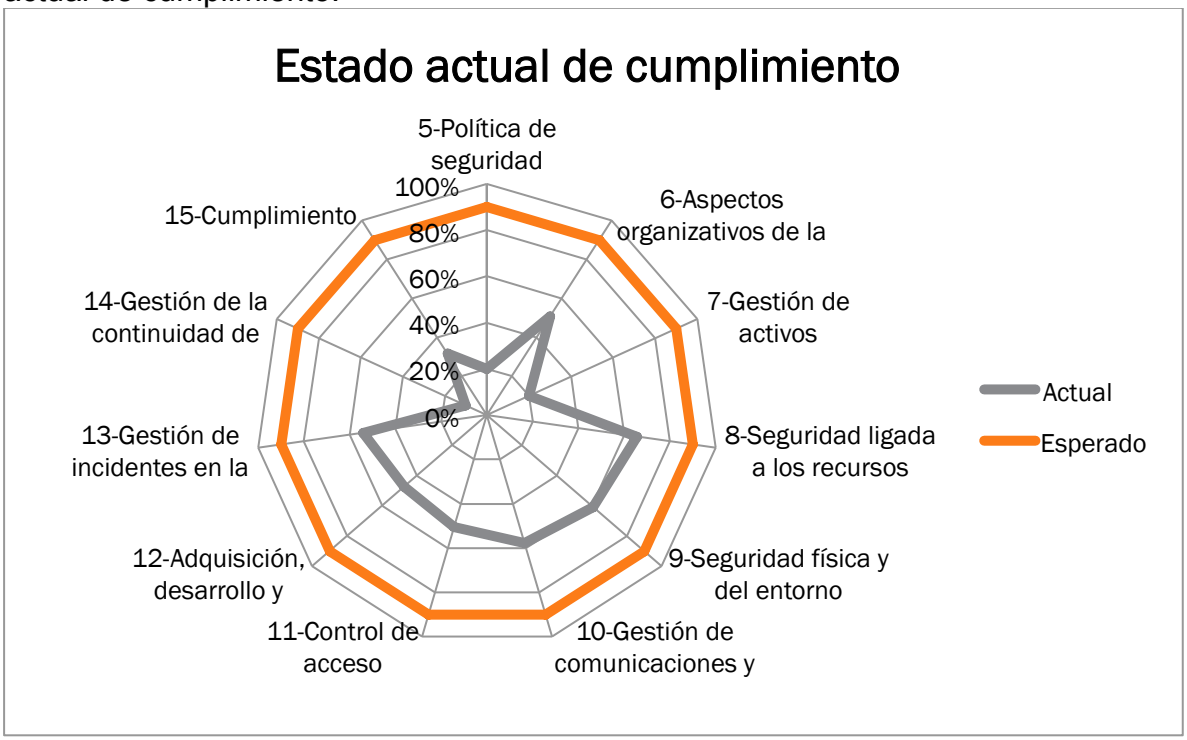
Nivel de madurez porcentual de los distintos controles

En la siguiente gráfica se puede observar como se reparten los controles según los distintos niveles de madurez y más concretamente entre los niveles “Reproducible” y “Proceso definido”. Actualmente no hay ningún control “Gestionado y medido” u “Optimizado”.



Nivel de cumplimiento según el nivel de cumplimiento por dominio ISO

A pesar que el objetivo a conseguir consiste en obtener un nivel del 90% en cada uno de los dominios de la ISO al cabo de 3 años, actualmente los controles asociados distan de este valor. En la siguiente gráfica se puede observar el estado actual de cumplimiento.



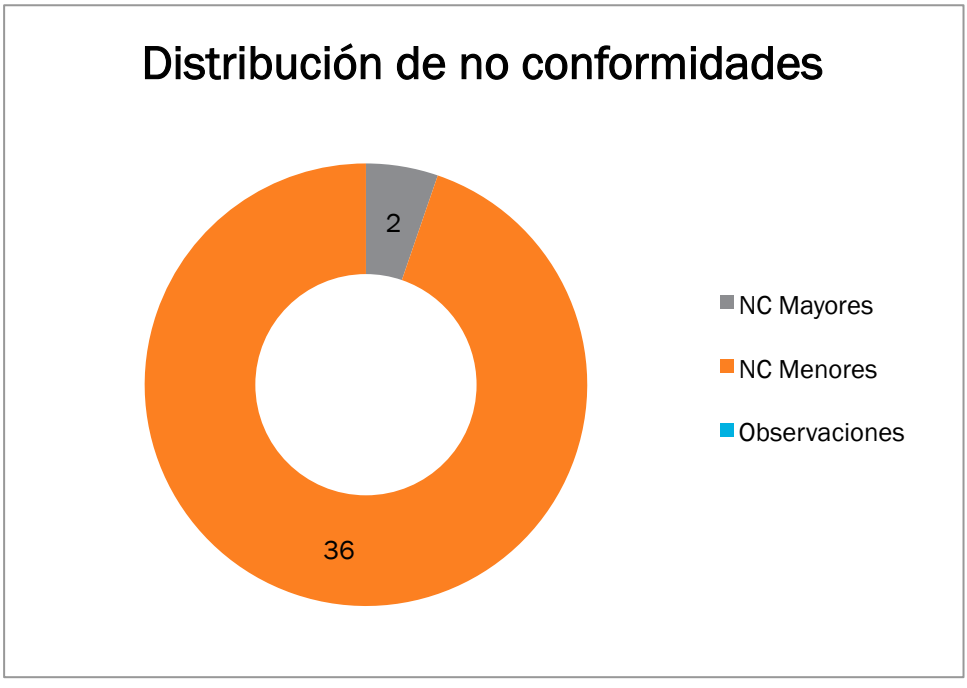
7.4. Informe de auditoría de cumplimiento

Se ha realizado una auditoría como se muestra en el *Anexo XI – Informe de auditoría.*

En este documento se estudian las no conformidades referentes a los distintos dominios de la ISO según el estado actual de la compañía. Para cada dominio se estudia el estado de cada uno de sus subdominios, obteniendo como resultado la siguiente tabla:

NORMA ISO 27001:2005	NC MAYORES	NC MENORES	OBSERVACIONES
5. Política de seguridad	0	1	0
6. Aspectos organizativos de la seguridad de la información	0	2	0
7. Gestión de activos	1	1	0
8. Seguridad ligada a los recursos humanos	0	3	0
9. Seguridad física y del entorno	0	2	0
10. Gestión de comunicaciones y operaciones	0	9	0
11. Control de acceso	0	7	0
12. Adquisición, desarrollo y mantenimiento de sistemas de información	0	6	0
13. Gestión de incidentes en la seguridad de la información	0	2	0
14. Gestión de la continuidad del negocio	1	0	0
15. Cumplimiento	0	3	0

Como se puede ver en la siguiente gráfica la mayor parte de las no conformidades son de nivel menor:



7.5. Conclusiones

Una vez realizado este estudio podemos conocer el estado actual del cumplimiento de los dominios con respecto a la ISO/IEC 27002:2005. Mediante los resultados obtenidos se puede diseñar un plan de acción para solventar las deficiencias actuales de la compañía.

Observando cada dominio por separado, se puede destacar que existen ciertos procedimientos o normas pero suelen ser desestructurados e insuficientes para cumplir con los requisitos necesarios. Es por ello que se deben tomar medidas para mejorarlos y desarrollar técnicas estadísticas y cuantitativas mejor gestionables y comparables a los actuales procesos medibles de forma cualitativa.

Es importante que la compañía destine todos los recursos necesarios para solventar las deficiencias en los dominios con nivel de cumplimiento menor como los referidos a la política de seguridad, a la gestión de activos o la gestión de la continuidad del negocio con tal de asegurar la continuidad de los procesos críticos de la compañía en caso de incidente grave.

El objetivo a cubrir a partir del análisis realizado y de los proyectos propuestos a lo largo de los siguientes 3 años consiste en la obtención de un nivel apropiado de cumplimiento de la ISO y así afianzar la seguridad de la información de la compañía.

8. Conclusiones

Este Plan Director de Seguridad enfocado a la sede principal de la compañía ConTec S.L en Barcelona, ha permitido mejorar los niveles de seguridad de la información a partir de conocer el estado actual, para finalmente desarrollar un plan de acción que ha facilitado un marco de referencia certificable en temas de seguridad de la información.

A pesar que la compañía disponía de ciertos procedimientos o normas, éstos son desestructurados e insuficientes para cumplir con los requisitos necesarios. Es por ello que se deben tomar medidas para mejorarlos y desarrollar técnicas estadísticas y cuantitativas mejor gestionables y comparables a los actuales procesos medibles de forma cualitativa.

Una vez realizado el estudio del estado actual y un análisis de riesgos con tal de estudiar cuales son las mayores amenazas a las que está expuesta ConTec S.L., se idearon un conjunto de proyectos con tal de afrontar y mejorar los resultados obtenidos. La implantación de estas propuestas de proyectos conducen a ConTec S.L. a un cumplimiento casi en su totalidad de los dominios de la ISO.

Para que todo este proyecto se lleve a cabo correctamente, es necesario el compromiso de la dirección para proporcionar todos los recursos necesarios para poder implantar los proyectos.

Como resumen, la realización de este plan ha permitido a ConTec S.L. obtener importantes beneficios, entre ellos:

- Definición clara de la situación actual de la compañía
- Definir los requisitos y objetivos de seguridad
- Definir el grado de cumplimiento de políticas, directivas, estándares y procedimientos de seguridad actuales
- Establecimiento de políticas, directivas, estándares y procedimientos de seguridad de la información
- Asegurar el cumplimiento de leyes y regulación vigente
- Análisis de las amenazas y riesgos asociados a la situación actual de la compañía para así poder gestionarlos de forma más efectiva
- Proposición de proyectos para mitigar los riesgos actuales de la organización a 3 años vista, evolucionando el cumplimiento ISO hasta niveles adecuados

9. Bibliografía

9.1. Referencias bibliográficas

- Sistema de gestió de la seguretat de la informació, Daniel Cruz Allende y Silvia Garre Gui. UOC, PID_00177790

9.2. Fuentes electrónicas

- MAGERIT
  http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=magerit

- PILAR
  http://www.pilar-tools.com/es/

- LOPD
  http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

- ISO 27001
  http://www.iso27000.es/

- Controles ISO 27002
  http://www.iso27000.es/download/ControlesISO27002-2005.pdf

- Normativa SGSI
  http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI/

- Códigos de buenas prácticas para la gestión de la seguridad de la información
  http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf

10. Anexos

10.1. Anexo I – Análisis diferencial

5. POLÍTICA DE SEGURIDAD	
5.1 Política de seguridad de la información	
5.1.1 Documento de la política de seguridad de la información	Aplica
5.1.2 Revisión de la política de seguridad de la información	Aplica
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1 Organización interna	
6.1.1 Compromiso de la dirección con la seguridad de la información	Aplica
6.1.2 Coordinación de la seguridad de la información	Aplica
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	Aplica
6.1.4 Proceso de autorización de recursos para el tratamiento de la información	Aplica
6.1.5 Acuerdo de confidencialidad	Aplica
6.1.6 Contacto con las autoridades	Aplica
6.1.7 Contacto con grupos de especial interés	Aplica
6.1.8 Revisión independiente de la seguridad de la información	Aplica
6.2 Terceros	
6.2.1 Identificación de los riesgos derivados del acceso de terceros	Aplica
6.2.2 Tratamiento de la seguridad en la relación con los clientes	Aplica
6.2.3 Tratamiento de la seguridad en contratos con terceros	Aplica
7. GESTIÓN DE ACTIVOS	
7.1 Responsabilidad sobre los activos	
7.1.1 Inventario de activos	Aplica
7.1.2 Propiedad de los activos	Aplica
7.1.3 Uso aceptable de los activos	Aplica
7.2 Clasificación de la información	
7.2.1 Directrices de clasificación	Aplica
7.2.2 Etiquetado y manipulado de la información	Aplica
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
8.1 Antes del empleo	
8.1.1 Funciones y responsabilidades	Aplica
8.1.2 Investigación de antecedentes	Aplica
8.1.3 Términos y condiciones de contratación	Aplica
8.2 Durante el empleo	
8.2.1 Responsabilidades de la dirección	Aplica
8.2.2 Concienciación, formación y capacitación en seguridad de la información	Aplica
8.2.3 Proceso disciplinario	Aplica
8.3 Cese del empleo o cambio de puesto de trabajo	
8.3.1 Responsabilidad del cese o cambio	Aplica
8.3.2 Devolución de activos	Aplica
8.3.3 Retirada de los derechos de acceso	Aplica
9. SEGURIDAD FÍSICA Y DEL ENTORNO	

9.1 Áreas seguras	
9.1.1 Perímetro de seguridad física	Aplica
9.1.2 Controles físicos de entrada	Aplica
9.1.3 Seguridad de oficinas, despachos e instalaciones	Aplica
9.1.4 Protección contra las amenazas externas y de origen ambiental	Aplica
9.1.5 Trabajo en áreas seguras	**N.A. - No aplica**
9.1.6 Áreas de acceso público y de carga y descarga	**N.A. - No aplica**
9.2 Seguridad de los equipos	
9.2.1 Emplazamiento y protección de equipos	Aplica
9.2.2 Instalaciones de suministro	Aplica
9.2.3 Seguridad del cableado	Aplica
9.2.4 Mantenimiento de los equipos	Aplica
9.2.5 Seguridad de los equipos fuera de las instalaciones	Aplica
9.2.6 Reutilización o retirada segura de equipos	Aplica
9.2.7 Retirada de materiales propiedad de la empresa	Aplica
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	
10.1 Responsabilidades y procedimientos de operación	
10.1.1 Documentación de los procedimientos de operación	Aplica
10.1.2 Gestión de cambios	Aplica
10.1.3 Segregación de tareas	Aplica
10.1.4 Separación de los recursos de desarrollo, prueba y operación	Aplica
10.2 Gestión de la provisión de servicios por terceros	
10.2.1 Provisión de servicios	Aplica
10.2.2 Supervisión y revisión de los servicios prestados por terceros	Aplica
10.2.3 Gestión del cambio en los servicios prestados por terceros	Aplica
10.3 Planificación y aceptación del sistema	
10.3.1 Gestión de capacidades	Aplica
10.3.2 Aceptación del sistema	Aplica
10.4 Protección contra el código malicioso y descargable	
10.4.1 Controles contra el código malicioso	Aplica
10.4.2 Controles contra el código descargado en el cliente	Aplica
10.5 Copias de seguridad	
10.5.1 Copias de seguridad de la información	Aplica
10.6 Gestión de la seguridad de las redes	
10.6.1 Controles de red	Aplica
10.6.2 Seguridad de los servicios de red	Aplica
10.7 Manipulación de los soportes	
10.7.1 Gestión de soportes extraíbles	Aplica
10.7.2 Retirada de soportes	Aplica
10.7.3 Procedimientos de manipulación de la información	Aplica
10.7.4 Seguridad de la documentación del sistema	Aplica
10.8 Intercambio de información	
10.8.1 Políticas y procedimientos de intercambio de información	Aplica
10.8.2 Acuerdos de intercambio	Aplica
10.8.3 Soportes físicos en tránsito	Aplica

10.8.4 Mensajería electrónica	Aplica
10.8.5 Sistemas de información empresariales	Aplica
10.9 Servicios de comercio electrónico	
10.9.1 Comercio electrónico	**N.A. - No aplica**
10.9.2 Transacciones en línea	**N.A. - No aplica**
10.9.3 Información públicamente disponible	**N.A. - No aplica**
10.10 Supervisión	
10.10.1 Registros de auditoría	Aplica
10.10.2 Supervisión del uso del sistema	Aplica
10.10.3 Protección de la información de los registros	Aplica
10.10.4 Registros de administración y operación	Aplica
10.10.5 Registro de fallos	Aplica
10.10.6 Sincronización del reloj	Aplica
11. CONTROL DE ACCESO	
11.1 Requisitos de negocio para el control de acceso	
11.1.1 Política de control de acceso	Aplica
11.2 Gestión de acceso de usuario	
11.2.1 Registro de usuario	Aplica
11.2.2 Gestión de privilegios	Aplica
11.2.3 Gestión de contraseñas de usuario	Aplica
11.2.4 Revisión de los derechos de acceso de usuario	Aplica
11.3 Responsabilidades de usuario	
11.3.1 Uso de contraseñas	Aplica
11.3.2 Equipo de usuario desatendido	Aplica
11.3.3 Política de puestos de trabajo despejados y pantalla limpia	Aplica
11.4 Control de acceso a la red	
11.4.1 Política de uso de los servicios de red	Aplica
11.4.2 Autenticación de usuario para conexiones externas	Aplica
11.4.3 Identificación de los equipos en red	Aplica
11.4.4 Protección de los puertos de diagnóstico y configuración remotos	Aplica
11.4.5 Segregación de las redes	Aplica
11.4.6 Control de la conexión a la red	Aplica
11.4.7 Control de encaminamiento a la red	Aplica
11.5 Control de acceso al sistema operativo	
11.5.1 Procedimientos seguros de inicio de sesión	Aplica
11.5.2 Identificación y autenticación de usuario	Aplica
11.5.3 Sistema de gestión de contraseñas	Aplica
11.5.4 Uso de los recursos del sistema	Aplica
11.5.5 Desconexión automática de la sesión	Aplica
11.5.6 Limitación del tiempo de conexión	Aplica
11.6 Control de acceso a las aplicaciones y a la información	
11.6.1 Restricción del acceso a la información	Aplica
11.6.2 Aislamiento de sistemas sensibles	Aplica
11.7 Ordenadores portátiles y teletrabajo	

11.7.1 Ordenadores portátiles y comunicaciones móviles	Aplica
11.7.2 Teletrabajo	Aplica
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	
12.1 Requisitos de seguridad de los sistemas de información	
12.1.1 Análisis y especificación de los requisitos de seguridad	Aplica
12.2 Tratamiento correcto de las aplicaciones	
12.2.1 Validación de los datos de entrada	Aplica
12.2.2 Control del procesamiento interno	Aplica
12.2.3 Integridad de los mensajes	Aplica
12.2.4 Validación de los datos de salida	Aplica
12.3 Controles criptográficos	
12.3.1 Política de uso de los controles criptográficos	Aplica
12.3.2 Gestión de claves	Aplica
12.4 Seguridad de los archivos de sistema	
12.4.1 Control del software en explotación	Aplica
12.4.2 Protección de los datos de prueba del sistema	Aplica
12.4.3 Control de acceso al código fuente de los programas	Aplica
12.5 Seguridad en los procesos de desarrollo y soporte	
12.5.1 Procedimientos de control de cambios	Aplica
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el SO	Aplica
12.5.3 Restricciones a los cambios en los paquetes de software	Aplica
12.5.4 Fugas de información	Aplica
12.5.5 Externalización del desarrollo de software	**N.A. - No aplica**
12.6 Gestión de la vulnerabilidad técnica	
12.6.1 Control de las vulnerabilidades técnicas	Aplica
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
13.1 Notificación de eventos y puntos débiles de seguridad de la información	
13.1.1 Notificación de los eventos de seguridad de la información	Aplica
13.1.2 Notificación de puntos débiles de seguridad	Aplica
13.2 Gestión de incidentes y mejoras de seguridad de la información	
13.2.1 Responsabilidades y procedimientos	Aplica
13.2.2 Aprendizaje de los incidentes de seguridad de la información	Aplica
13.2.3 Recopilación de evidencias	Aplica
14. GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	
14.1 Aspectos de seguridad de la información en la gestión de la continuidad de negocio	
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad de negocio	Aplica
14.1.2 Continuidad del negocio y evaluación de riesgos	Aplica
14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	Aplica
14.1.4 Marco de referencia para la planificación de la continuidad del negocio	Aplica
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad	Aplica
15. CUMPLIMIENTO	
15.1 Cumplimiento de los requisitos legales	
15.1.1 Identificación de la legislación aplicable	Aplica
15.1.2 Derechos de propiedad intelectual (DPI)	Aplica

15.1.3 Protección de los documentos de la organización	Aplica
15.1.4 Protección de datos y privacidad de la información de carácter personal	Aplica
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información	Aplica
15.1.6 Regulación de los controles criptográficos	Aplica
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	
15.2.1 Cumplimiento de las políticas y normas de seguridad	Aplica
15.2.2 Comprobación del cumplimiento técnico	Aplica
15.3 Consideraciones sobre las auditorías de los sistemas de la información	
15.3.1 Controles de auditoría de los sistemas de información	Aplica
15.3.2 Protección de las herramientas de auditoría de los sistemas de la información	Aplica

10.2. Anexo II - Política de seguridad

Objetivo

ConTec S.L reconoce la importancia de la seguridad de la información como requisito indispensable para el correcto desarrollo de la compañía.

La seguridad de la información se basa en la protección de:

- La integridad de los datos: se debe asegurar que la información no es alterada de forma no autorizada
- La confidencialidad de la datos: se debe asegurar que la información no se pone a disposición ni se revela a individuos no autorizados
- La disponibilidad de la datos: se debe asegurar que se pueda acceder a la información cuando se requiera.

Mediante este documento se establecerán las directrices generales, alineadas con los objetivos del negocio y la legislación aplicable, que el personal de la compañía debe conocer y cumplir independientemente del cargo que lleve a cabo con tal de garantizar la seguridad de los sistemas de información de ConTec S.L.

Esta política de seguridad se integrará en la normativa básica de la compañía.

Roles y responsabilidades

Responsabilidad de todo el personal

Todo el personal de ConTec S.L es responsable directo de la información con la que trata y deben asegurar su confidencialidad, integridad y disponibilidad.

Del mismo modo son responsables de mantener en buen estado todo el equipamiento que ConTec S.L. dispone para que lleven a cabo sus tareas. El material de oficina, como los equipos informáticos no pueden ser extraídos de la misma sin consentimiento expreso por parte de la dirección.

El personal es responsable de sus cuentas de usuario y debe protegerlas con contraseñas robustas y difícilmente adivinables.

Todos los datos almacenados y gestionados en ConTec S.L. deben cumplir los requisitos establecidos por la legislación vigente sobre Propiedad Intelectual y Protección de Datos de Carácter Personal por lo que los usuarios deben velar por su cumplimiento.

Responsabilidad de la dirección

La dirección cumple un papel crucial para asegurar la seguridad de la información y es la responsable de constituir y distribuir políticas, normativas y procedimientos de seguridad. Estos documentos serán revisados periódicamente con tal de mantenerlos actualizados. De estas revisiones se guardaran registros mediante actas de reunión firmadas.

Es responsabilidad de ConTec S.L. establecer objetivos anuales en relación a la seguridad de la información en la compañía.

Deberá desarrollar una política de gestión de incidentes de seguridad, además de planes de contingencia y continuidad para garantizar la continuidad de las operaciones de la compañía.

Además apoyará el despliegue de un plan de concienciación y formación en seguridad de la información del personal.

Responsabilidad de los administradores de sistemas

Los administradores de sistemas son responsables de asegurar que los sistemas informáticos sean correctamente gestionados, asegurando la confidencialidad, integridad y disponibilidad de los datos. Se mantendrá un registro de todos los equipos propiedad de la compañía.

Se implantarán y mantendrán controles de acceso y mecanismos de seguridad para el control de los usuarios.

Además de garantizar la inclusión de la seguridad en todo el ciclo de vida de los datos: creación, mantenimiento, conservación y destrucción, y en los procesos de gestión de hardware y software.

Deberán llevar a cabo las acciones oportunas para gestionar y solventar las vulnerabilidades de seguridad y los incidentes detectados.

Uso de los recursos de ConTec S.L.

Todo el material dispuesto al servicio del personal contratado es propiedad de ConTec S.L., por tanto sólo puede ser usado con fines relacionados con actividades exclusivamente laborales.

Está totalmente prohibido intentar acceder sin autorización a contenidos restringidos. La información se clasificará en niveles de disponibilidad: sin clasificar, difusión limitada, confidencial, reservado y secreto.

El personal no debe atentar contra el funcionamiento normal de ConTec S.L, al intentar destruir, modificar o difundir datos propiedad de la empresa de forma malintencionada o introducir malware en los equipos informáticos intencionadamente.

Tampoco está permitida la instalación de software pirata o sin la licencia correspondiente.

No está permitido la conexión a la red por medios distintos a los establecidos o utilizar internet, el correo electrónico o software con fines ajenos a la actividad laboral.

ConTec S.L. velará para asegurar el uso correcto de sus recursos y mantendrá sistemas para controlarlo. Si se detectan deficiencias o incumplimientos de las normas de conducta establecidas, ConTec S.L se reserva el derecho a adoptar las medidas legalmente oportunas que amparen la protección de sus derechos y abrir procesos disciplinarios a los usuarios que lo incumplan.

Actuación en caso de indecentes de seguridad

El personal debe comunicar inmediatamente al personal responsable cualquier tipo de incidente de seguridad que detectara para poder solventarlo con la máxima brevedad posible.

10.3. Anexo III - Procedimiento de auditorías internas

Objetivo

Establecer por escrito la forma como se planifican, efectúan, documentan y registran las actividades requeridas para realizar las auditorías internas al Sistema de Gestión de la Seguridad de la información, en las distintas áreas de la empresa que así lo requieran.

Alcance

Este procedimiento es aplicable al Sistema de Gestión de la Seguridad de la información de ConTec S.L., para verificar por medio de Auditorías Internas, si este se ha implementado y se mantiene de manera eficaz.

Criterios para la selección de auditores

Los Auditores internos del Sistema de Gestión de la Seguridad de la información deben cumplir con determinadas cualidades. Entre las que se encuentran cualidades personales, conocimientos y habilidades, de manera que las auditorías realizadas por éstos sean lo más confiable posibles.

Estas cualidades se describen a continuación:

- Atributos Personales relacionados con ética, diplomacia, observador, perceptivo, versatilidad, tenacidad, decisión y seguridad.
- Conocimientos y habilidades relacionados con principios, procedimientos, técnicas de auditoría, documentos de Sistema de Gestión de la Seguridad de la información, normas legales y reglamentos.
- Conocimiento de la terminología, los principios de la gestión de la Seguridad de la información y su aplicación.
- Conocimiento de herramientas de la gestión de la Seguridad de la información y su aplicación.
- Técnicas para recopilar información y establecer la variedad y suficiencia de la misma.
- Conocimiento de la terminología, características técnicas de los procesos, productos y practicas especificas.
- Entrenamiento y experiencia en la realización de auditorías.
- El auditor líder debe tener conocimientos y habilidades adicionales en el liderazgo de la auditoría, además debe ser capaz de planificar la auditoría y hacer uso eficaz de los recursos durante la auditoría, representar al equipo auditor en las comunicaciones con el auditado, organizar y dirigir a los miembros del equipo auditor, proporcionar dirección y orientación a los auditores en formación, conducir al equipo auditor para llegar a las conclusiones de la auditoría, prevenir y resolver conflictos, preparar y completar el informe de la auditoría.

Es especialmente interesante que los auditores internos puedan acreditar dicha experiencia con certificaciones como CISA (Certified Information Systems Auditor).

Metodología

Planificación de las auditorías

Las auditorías internas de ConTec S.L. son planificadas, organizadas y coordinadas por el Comité de Seguridad de la Información. Dicho Comité efectúa y registra a comienzos de cada año, una programación general de las áreas y procedimientos a auditar, estimando el mes de ejecución. Una copia de este programa es enviada a cada área involucrada, la cual dispone de un mes para hacer objeciones y observaciones a dicho programa.

La confirmación de la fecha definitiva de cada auditoría se realiza de común acuerdo entre el Comité y el área a auditar, la cual queda registrada en el respectivo plan de auditoría.

El registro de las fechas efectivas de ejecución se indica en el mismo programa de auditoría como control interno de la ejecución de las auditorías. La copia del programa de auditoría con las fechas de ejecución sólo serán entregadas a petición del interesado.

Se realizará un mínimo de una auditoría por área al año aunque es posible que se aumente el número según el área o si se han detectado irregularidades.

Preparación de la Auditoría

El Comité de Seguridad de la Información constituye el equipo auditor, al menos 7 días hábiles antes de la fecha programada para la auditoría, designa al auditor-jefe e informa el alcance y objetivos de la auditoría. El equipo auditor sea externo al área de trabajo a auditar.

El auditor jefe envía al Jefe del área auditada, con al menos 5 días hábiles de anticipación, el Plan de Auditoría Interna, el que debe contener como mínimo:

- Objetivos y alcance de la auditoría
- Fecha
- Integrantes del equipo auditor
- Documentos de Referencia
- Detalle de las actividades de la auditoría (reunión inicial, entrevistas, revisión de documentos, emisión de informe y reunión final).

Si el Jefe del área auditada no hace observaciones al plan de auditoría dentro de los dos días hábiles siguientes de recibido éste, se dará por aceptado y aprobado.

El auditor jefe puede solicitar además, para su información y estudio, documentación relacionada con la auditoría, la que deberá ser enviada por el jefe del área auditada

a menos que exista algún motivo justificado para no hacerlo.

Ejecución de la Auditoría

La auditoría comienza con una reunión inicial del equipo auditor con el responsable del área de trabajo a auditar, en la cual se da a conocer formalmente la metodología y alcance de la auditoría.

Durante la auditoría un representante del área de trabajo a auditar debe acompañar al equipo auditor para facilitar el proceso, así como para confirmar el total entendimiento y alcance de las no conformidades u observaciones registradas. Los auditores deben recolectar evidencia a través de entrevistas, examen de documentos y observación de las actividades y condiciones en el área de interés.

Cuando un auditor detecta una no conformidad en el sistema, toda la evidencia de ésta debe ser documentada en la redacción de la no conformidad registrada en el informe, indicando además, el punto de una norma o procedimiento que no se cumplió y la evidencia objetiva donde se detectó la falla.

Una vez terminada la recolección de evidencias, el equipo auditor se debe reunir para elaborar el informe de auditoría interna. Se deben emitir dos originales del informe, uno de los cuales será entregado al jefe del área auditada en la reunión final. El otro ejemplar es entregado por el auditor jefe al Comité de Seguridad de la Información.

En dicha reunión, los auditados tienen la posibilidad de solicitar aclaración de alguna no conformidad detectada y si se da el caso, eliminar alguna de ellas con la argumentación y evidencia objetiva correspondiente.

Los informes deben ser firmados por el auditor jefe y el jefe del área auditada. Al momento de firmar, el Jefe del área auditada formaliza en el informe su compromiso de entrega de las Acciones Correctivas en una fecha específica.

Cuando la No Conformidad se refiere a la validez de las operaciones o resultados del área, el Jefe del área debe iniciar de inmediato las acciones correctivas necesarias y notificar por escrito, en caso que se vea afectado algún servicio que se haya realizado o se esté realizando.

Informes de auditoría interna

El informe de auditoría debe contener al menos la siguiente información:

- Título y código del informe.
- Área auditada y Fecha de la auditoría
- Identificación del equipo auditor.
- Documentos de referencia
- Objetivos de la auditoría
- Personas entrevistadas
- Descripción de las no conformidades

- Observaciones (si procede)
- Fecha de entrega de Acciones Correctivas
- Firmas del Jefe del área auditada y del auditor jefe

10.4. Anexo IV - Gestión de indicadores

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

En los siguientes apartados se enumeraran algunos indicadores propios según los 11 dominios que define la ISO/IEC 27002.

Política de seguridad

- Grado de adopción de las políticas de la organización mediante revisiones por parte de la dirección, auditorías u otras autoevaluaciones
- Número de políticas modificadas o creadas en el último periodo
- Porcentaje de los controles de la ISO/IEC 27001 aplicables, para los cuales se ha escrito, aprobado y comunicado políticas
- Número de revisiones realizadas a la política de seguridad

Organización de la seguridad de la información

- Porcentaje de los trabajadores de la Dirección que tienen asociadas y aceptadas responsabilidades en el sistema de seguridad de la información.
- Número de incidencias en los acuerdos de confidencialidad con los empleados
- Número de incidencias en los acuerdos de confidencialidad con los clientes
- Número de auditorias realizadas, respecto a las planificadas
- Porcentaje de terceros formalmente certificados conforme a la ISO/IEC 27001 u otros estándares de seguridad apropiados.
- Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y consideradas seguras.

Gestión de activos

- Grado de despliegue del inventario de activos
- Porcentaje de los activos identificados como críticos para los que se tienen desarrollados planes de tratamiento de riesgos y se mantienen dentro de un rango aceptable establecido.
- Clasificación de los datos sensibles por su distribución en los sistemas

Seguridad relativa al personal

- Porcentaje de personal nuevo, que ha sido investigado y han pasado las pruebas de acuerdo a las políticas de la compañía antes de empezar a trabajar
- Número de cursos de formación, concienciación o capacitación en seguridad de la información impartidos a los empleados.
- Tiempo medio de retirada de los derechos de acceso a un trabajador cesado o que cambia de puesto de trabajo
- Número de incidencias causadas por los empleados durante el empleo
- Número de activos no devueltos por los empleados que cambian de puesto de trabajo o cesan del empleo

- Número de dispositivos perdidos fuera de la oficina

Seguridad física y del entorno

- Número de revisiones periódicas de seguridad física de las instalaciones
- Número de mantenimientos a los equipos de la compañía
- Número de material retirado de la compañía

Gestión de comunicaciones y operaciones

- Porcentaje de implementación de actualizaciones de sistemas
- Porcentaje de implementación de soluciones a vulnerabilidades de sistemas
- Porcentaje de solicitudes atendidas de cambios en los servicios prestados por terceros
- Cumplimiento y efectividad de los acuerdos de nivel de servicio (SLA)
- Efectividad de proveedores de servicios
- Porcentaje de proyectos implementados
- Porcentaje de backups críticos exitosos e importantes
- Número de sistemas sin backups
- Porcentaje de recuperaciones exitosas de sistemas críticos e importantes
- Número de incidentes de seguridad de red
- Número de falsos positivos contra positivos críticos
- Evaluación de medidas de seguridad adoptadas en el intercambio de activos de información relevante, crítica o sensible
- Número de incidentes de seguridad resueltos correctamente.

Control de acceso

- Existencia, revisión y adecuación de políticas de control de accesos
- Porcentaje de trabajadores cuyas responsabilidades en seguridad de la información se encuentran aceptadas
- Evaluación de logs y estadísticas del software y hardware, relacionando vulnerabilidades aprovechadas e intentos de acceso, con ataques bloqueados.
- Existencia y efectividad de controles de acceso a los sistemas operativos de las plataformas informáticas

Seguridad en la adquisición, desarrollo y mantenimiento de sistemas de información

- Porcentaje de sistemas en los que los controles de validación de datos han sido vulnerados
- Porcentaje de procesos de cambios realizados conforme a la normativa existente al respecto, en relación al total de cambios solicitados y realizados

Gestión de incidencias de seguridad de la información

- Número de peticiones de soporte a los helpdesk en temas relacionados con la seguridad de la información
- Porcentaje de incidentes de seguridad que generaron costes superiores al umbral aceptable

Gestión de la continuidad de negocio

- Efectividad en la implementación de los planes de continuidad de negocio
- Grado de despliegue de los planes de continuidad del negocio

Conformidad

- Número de requerimientos legales agrupados y analizados por estado y nivel de riesgo
- Porcentaje de requisitos externos claves cumplidos a través de auditorias
- Efectividad de las auditorías o revisiones normativas
- Número de recomendaciones de auditoría agrupadas y analizadas
- Porcentaje de hallazgos de auditoría que han sido resueltos y cerrados respecto del total que se abrió en el mismo período
- Plazos de tiempo en resolver las recomendaciones
- Grado de despliegue del análisis de riesgos
- Tendencia en el número de riesgos relacionados con la seguridad de información según nivel de severidad
- Gastos de la seguridad de la información respecto al presupuesto asignado

10.5. Anexo V - Procedimiento de revisión por dirección

Objetivo

El objeto de este procedimiento consiste en la revisión por parte de la dirección en cuanto a las cuestiones más importantes en relación al sistema de gestión de seguridad de la información.

La dirección revisará anualmente el SGSI implantado para asegurar su efectividad y conveniencia cumpliendo los objetivos definidos y asegurando las necesidades de ConTec S.L.

Se deben llevar a cabo revisiones anuales en las que además se debe incluir la posibilidad de poder realizar cambios en el SGSI, la política de seguridad y los objetivos de seguridad de la información.

Para poder llevar a cabo una revisión eficaz, se reunirá toda la información necesaria para posteriormente obtener unos resultados con los que tomar las medidas oportunas. Estos resultados deben documentarse claramente y mantener registros sobre ellos.

Una vez con los resultados finales, se pueden consensuar acciones dirigidas a la mejora de la organización, en función de los recursos disponibles.

A continuación se especifican las entrada de información necesaria y las salidas obtenidas una vez analizada toda la información.

Entradas

Previa a la revisión, se deben recopilar suficiente información para poder hacer una revisión efectiva.

Esta información debe incluir:

- Resultados de mediciones realizadas, auditorías y revisiones del SGSI,
- Consideraciones propuestas y recomendaciones de mejora
- Material que se podría utilizar para mejorar el desempeño y efectividad del SGSI
- Estado de acciones preventivas y correctivas
- Vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa
- Acciones de seguimiento de las revisiones por la dirección previas
- Cualquier cambio que pudiera afectar el SGSI

Salidas

Los datos de entrada anteriores se analizan teniendo en cuenta los objetivos y la política de la organización con tal de buscar acciones correctivas y/o preventivas.

El resultado obtenido debe incluir decisiones o acciones relacionadas con:

- La mejora de la eficacia del SGSI
- La actualización de la evaluación del riesgo y el plan de tratamiento del riesgo
- Modificar los procedimientos o controles que sean necesarios por cambios sucedidos en la compañía como por ejemplo nuevos contratos, nuevos requisitos comerciales o de seguridad y requisitos reguladores o legales.
- Mejorar la gestión de los recursos asignados a la gestión del SGSI.

El resultado obtenido en este proceso es la evaluación del funcionamiento del SGSI.

10.6. Anexo VI - Gestión de roles y responsabilidades

Para poder llevar a cabo una buena implantación del SGSI, es necesario crear una infraestructura interna con responsabilidades directamente relacionadas con aspectos de la seguridad de la información. Esta infraestructura debe estar aprobada y apoyada por la Dirección.

Comité de dirección

Estará constituido por el director de la compañía, el director de administración y finanzas, el director comercial y el director de operaciones. Las funciones en materia de seguridad de la información de éste son las siguientes:

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

Comité de seguridad de la información

Las decisiones en materia de seguridad de la información son tomadas de forma consensuada por un grupo formado por diferentes responsables dentro de la compañía, en este caso será formado por los mismos integrantes que el Comité de Dirección al ser una compañía pequeña, junto con el responsable de Sistemas e Infraestructura como Responsable de seguridad de la información.

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

- Implantar las directrices del Comité de Dirección.
- Asignar roles y funciones en materia de seguridad.
- Presentar a aprobación al Comité de Dirección las políticas, normas y responsabilidades en materia de seguridad de la información.

- Validar el mapa de riesgos y las acciones de mitigación propuestas por el responsable de seguridad de la información (RSI).

- Validar el Plan de seguridad de la información o Plan director de seguridad de la información y presentarlo a aprobación al Comité de Dirección. Además de supervisar y hacer el seguimiento de su implantación.

- Supervisar y aprobar el desarrollo y mantenimiento del Plan de continuidad de negocio.

- Velar por el cumplimiento de la legislación que en materia de seguridad sea de aplicación.

- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.

- Revisar las incidencias más destacadas.

- Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

Responsable de seguridad del la información

El responsable de Sistemas e Infraestructura tomaría el puesto de Responsable de seguridad de la información (RSI), y formaría parte del Comité de Seguridad de la información. Sus tareas se corresponden a:

- Implantar las directrices del Comité de Seguridad de la Información de la compañía.

- Elaborar, promover y mantener una política de seguridad de la información, y proponer anualmente objetivos en materia de seguridad de la información.

- Desarrollar y mantener el documento de Organización de la seguridad de la información en colaboración con el departamento de Administración y Finanzas.

- Desarrollar, con el soporte de las unidades correspondientes, el marco normativo de seguridad y controlar su cumplimiento.

- Actuar como punto focal en materia de seguridad de la información dentro de la compañía a fin de gestionar la seguridad de la información de forma global.

- Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo.

- Controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de aplicaciones.

- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas.

- Coordinar acciones con las áreas de negocio para elaborar y gestionar un Plan de continuidad de negocio de la compañía, basado en el análisis de riesgo y la criticidad de los procesos de negocio.

- Velar por el cumplimiento legal coordinando las actuaciones necesarias con las unidades responsables.

- Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad y hacer el seguimiento de los incidentes de seguridad.

- Elaborar y mantener un plan de concienciación y formación en seguridad de la información del personal, en colaboración con la unidad responsable de la formación en la compañía.

- Coordinar la implantación de herramientas y controles de seguridad de la información y definir el cuadro de mando de la seguridad. Debe analizar y mantener actualizado dicho cuadro de mando.

Departamentos de Tecnologías de la Información y Comunicaciones (TIC)

Los trabajadores de los departamentos de Desarrollo, Outsourcing y Sistemas e infraestructuras, deben cumplir los siguientes puntos:

- Cumplir con las políticas, normas y procedimientos en materia de seguridad de la información. Colaborar con el RSI en su definición.

- Implantar en los sistemas de información los controles de seguridad prescritos, las acciones correctoras establecidas y gestionar las vulnerabilidades detectadas.

- Requerir la participación del RSI en nuevos proyectos de desarrollo o adaptación/implantación de productos de mercado, especialmente cuando puedan ser críticos en términos de confidencialidad, privacidad, integridad, continuidad, autenticidad, no repudio y trazabilidad, o puedan tener un impacto mediático importante.

- Requerir la participación del RSI en la implantación o gestión de los cambios de hardware y software

- Garantizar la inclusión de la seguridad en todo el ciclo de vida de los datos: creación, mantenimiento, conservación y destrucción, y en los procesos de gestión de hardware y software.

- Adoptar medidas para proteger la información según su clasificación por parte del responsable de la información.

- Colaborar con el RSI en la identificación de riesgos y la propuesta de soluciones, y colaborar en las revisiones o auditorías de seguridad que se lleven a cabo.

Departamento de RRHH

Tienen las funciones siguientes:

- Informar a las unidades gestoras de recursos de información sobre cambios movimientos de personal para poder realizar una buena gestión de recursos: altas, bajas definitivas y temporales, cambios de categoría y/o funciones, cambios organizativos, etc.

- Trabajar conjuntamente con el RSI en el desarrollo de la política de seguridad de la información en los temas referentes al personal.

- Aplicar procedimientos disciplinarios en caso de vulneración del marco normativo.

Personal en general

Tienen las funciones siguientes:

- Mantener la confidencialidad de la información.

- Hacer un buen uso de los equipos y de la información a la cual tienen acceso y protegerla de accesos no autorizados.

- Respetar las normas y procedimientos vigentes en materia de seguridad de la información, y velar por que terceras partes en prestación de servicios también la respeten.

- Utilizar adecuadamente las credenciales de acceso a los sistemas de información.

- Respetar la legislación vigente en materia de protección de datos de carácter personal y cualquier otra que sea de aplicación.

- Notificar, por la vía establecida, insuficiencias, anomalías o incidentes de seguridad y situaciones sospechosas que pudieran poner en peligro la seguridad de la información.

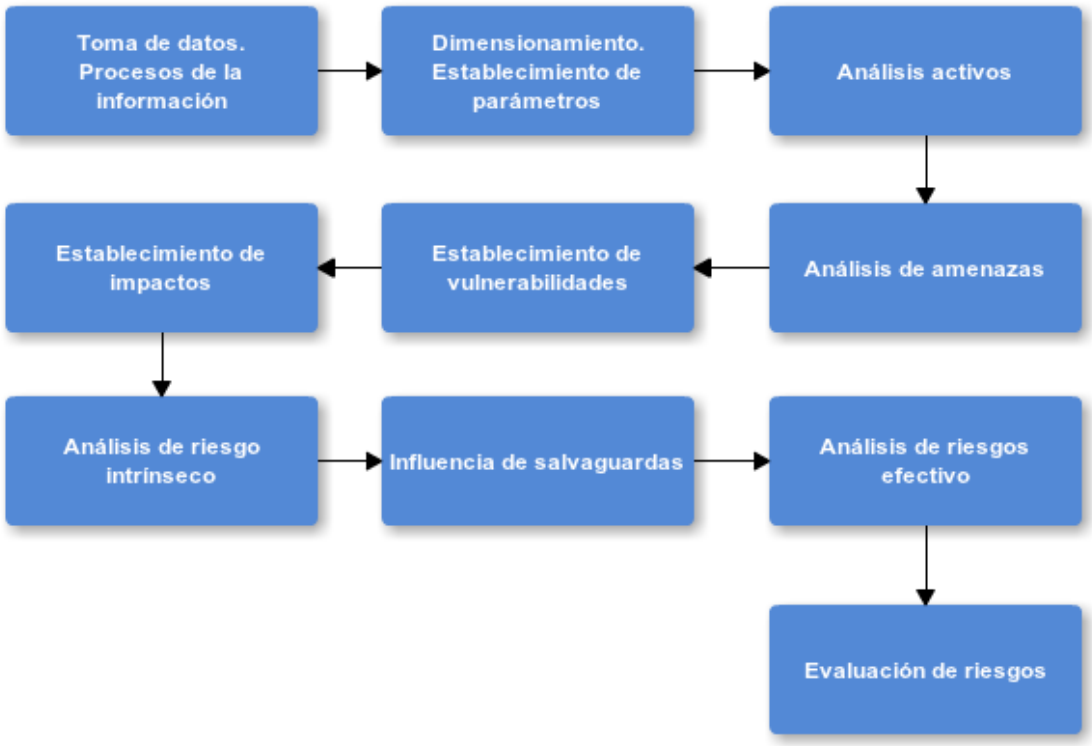
10.7. Anexo VII - Metodología de análisis de riesgos

La realización de un análisis de los riesgos asociado a los activos de información de una compañía es la piedra angular de un SGSI. Es la herramienta que permite identificar las amenazas a las que se encuentran expuestos estos activos, para luego evaluar la frecuencia de que pudieran suceder y finalmente valorar el impacto que supondría esta materialización.

Para ello es importante definir una metodología que cumpla los requisitos pertinentes. En este caso se utilizará la metodología MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT, actualmente en la versión 3, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Fases

MAGERIT sigue un proceso hasta elaborar e identificar todos los riesgos de una organización. El siguiente gráfico muestra la evolución de las fases:



Toma de datos y procesos de información

En esta fase debe definirse el alcance que se ha de estudiar, además de analizar los procesos que lleva a cabo la organización. Hay que tener presente la granularidad, es decir el nivel de detalle al que se quiere llegar.

Establecimiento de parámetros

En esta fase se establecen los parámetros que se utilizarán durante el proceso de análisis de riesgos. Los parámetros que deben identificarse con los siguientes:

Valor de los activos

La valoración de activos es una tarea compleja en el proceso de evaluación de riesgos. En esta tarea se debe otorgar un valor a cada activo y de esta manera comparar este valor, con el coste de las medidas de protección que se deberían aplicar al activo. Únicamente tendría sentido aplicar la medida, si su coste es menor al del activo.

Existen dos formas de valoración de activos, cuantitativamente o cualitativamente. Esta valoración se basará en la siguiente escala utilizando la propuesta por la metodología MAGERIT junto con una valoración cuantitativa:

Valoración	Valor
Muy alto	500.000€
Alto	100.000€
Medio	30.000€
Bajo	3.000€
Muy bajo	500€

Mediante esta tabla, podemos realizar valorar cada activo de forma cualitativa, mediante la columna “Valoración”, y por otro lado cuantitativamente según la columna “Valor”.

Por otro lado, se debe tener en cuenta la relación jerárquica de los activos. El siguiente paso consiste en identificar y valorar las dependencias entre ellos.

Vulnerabilidades

En MAGERIT, una vulnerabilidad se refiere a la frecuencia con la que la compañía puede sufrir una amenaza. En la siguiente tabla se define la clasificación de vulnerabilidades:

Frecuencia		Valor	Rango
MA	Muy frecuente	100	A diario
A	Frecuente	10	Mensualmente
N	Normal	1	Una vez al año
B	Poco frecuente	1/10	Cada varios años
MB	Muy poco frecuente	1/100	Siglos

Impacto

El impacto es el tanto por ciento del valor del activo que se pierde en el caso de que suceda un incidente sobre él. En la siguiente tabla se definen los niveles de impacto y el porcentaje de valor que se puede perder en cada caso:

Impacto	Valor
Muy alto	100%
Alto	50%
Medio	20%
Bajo	10%
Muy bajo	1%

Efectividad del control de seguridad

Este parámetro identifica la influencia que tendrán las medidas de protección ante los riesgos que se detecten. La siguiente tabla define la clasificación por efectividad del control:

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

*No se ha realizado un estudio sobre la efectividad de las medidas de protección antes los riesgos en este proyecto.

Análisis de activos

Se deben identificar los activos de la compañía y que son necesarios para llevar a cabo sus actividades. Entre los activos a estudiar se pueden identificar:

- Instalaciones
- Hardware
- Aplicaciones
- Datos
- Red
- Servicios
- Equipamiento auxiliar
- Personal

Análisis de amenazas

MAGERIT clasifica las amenazas que afectan a la compañía según:

- Accidentes: Situaciones no provocadas voluntariamente y que no pueden evitarse
- Errores: Situaciones que son cometidas involuntariamente por desconocimiento, descuido o por terceros

- Amenazas intencionales presenciales: Situaciones provocadas por el personal de la compañía de forma voluntaria
- Amenazas intencionales remotas: Situaciones provocadas por terceras personas

Establecimiento de las vulnerabilidades

A pesar de que no es necesario listar las vulnerabilidades, si que es necesario tenerlas en cuenta para poder estimar la frecuencia de ocurrencia de una determinada amenaza sobre un activo.

Valoración de impacto

A la hora de valorar impactos, se debe considerar:

- El resultado de la agresión de una amenaza sobre un activo
- El efecto sobre cada activo para poder agrupar los impactos en cadena según la relación de activos
- El valor económico representativo de las pérdidas producidas en cada activo
- Las pérdidas cuantitativas o cualitativas

```
Impacto potencial = Valor del activo (según dimensión) x Valor del impacto
```

Análisis intrínseco

Esta fase define el estudio de la situación actual, es decir, aquí ya se puede calcular los riegos actuales a los que está sometida la compañía. Para ellos se puede calcular con la siguiente fórmula:

```
Riesgo = impacto potencial (según dimensión) x frecuencia
```

Influencia de las salvaguardas

En esta fase se debe escoger la mejor solución de seguridad para reducir los riesgos actuales. Para ello existen dos tipos de controles:

- Preventivos: Reducen las vulnerabilidades
- Correctivos: Reducen el impacto de la amenaza

Análisis de riesgos

En esta fase se estudia la forma en la que reducirían los riesgos siguiendo las salvaguardas que se han propuesto

Gestión de riesgos

En esta fase se toman decisiones por parte de la organización sobre las medidas de seguridad a tomar a partir de los resultados de los apartados anteriores. Se pueden tomar 3 tipos de decisiones en cuanto a la hora de gestionar los riesgos:

- Reducirlos
- Transferirlos
- Aceptarlos

Finalmente se elabora un plan de acción.

10.8. Anexo VIII – Análisis de riesgos

Tabla resumen de amenazas

Para hacer un estudio más detallado, se hará una división de los activos en los siguientes grupos para estudiar la forma en que le influye la materialización de las amenazas:

- Instalaciones (CPD)
- Instalaciones (Oficinas)
- Hardware de la red interna (Servidores y comunicación)
- Hardware de la DMZ (Servidores y comunicación)
- Hardware relacionado con la seguridad física
- Hardware de puestos de trabajo
- Aplicaciones para servidores
- Aplicaciones para estaciones de trabajo
- Datos
- Logs
- Red
- Servicios
- Equipamiento auxiliar de oficina
- Equipamiento auxiliar en el CPD
- Personal

A continuación se muestra el contenido de las distintas tablas:

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
INSTALACIONES (CPD)								
[L.1]	Sala CPD	B	0,1		50%	50%	100%	
Amenazas								
[N.1]	Fuego	MB	0,01				100	
[N.2]	Daños por agua	MB	0,01				50	
[I.1]	Fuego	MB	0,01				100	
[I.2]	Daños por agua	B	0,1				50	
[A.7]	Uso no previsto	B	0,1		50	50	20	
[A.11]	Acceso no autorizado	B	0,1		50	50		
[A.26]	Ataque destructivo	MB	0,01				100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
INSTALACIONES (OFICINAS)								
[L.2]	Oficinas	N	1		50%	50%	100%	
[L.3]	Recepción							

Amenazas	Amenazas							
[N.1]	Fuego	MB	0,01				100	
[N.2]	Daños por agua	MB	0,01				50	
[I.1]	Fuego	MB	0,01				100	
[I.2]	Daños por agua	B	0,1				50	
[A.7]	Uso no previsto	N	1		50	50	10	
[A.11]	Acceso no autorizado	B	0,1		10	10		
[A.26]	Ataque destructivo	MB	0,01				100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
HARDWARE (SERVIDORES Y COMUNICACIONES) RED INTERNA								
[HW.2]	Servidores de datos	N	1		100%	20%	100%	
[HW.3]	Servidor de nóminas/finanzas/administración							
[HW.4]	Servidores de BBDD							
[HW.8]	Servidores de desarrollo							
[HW.12]	Firewal interno							
[HW.15]	Switches							
[HW.17]	Routers wifi							
Amenazas								
[N.1]	Fuego	MB	0,01				100	
[N.2]	Daños por agua	MB	0,01				100	
[I.1]	Fuego	B	0,1				100	
[I.2]	Daños por agua	B	0,1				100	
[I.5]	Avería de origen físico o lógico	N	1				100	
[I.6]	Corte del suministro eléctrico	N	1				50	
[I.7]	Condiciones inadecuadas de temperatura y humedad	N	1				100	
[E.23]	Errores de mantenimiento / actualización de equipos	N	1				100	
[E.24]	Caída del sistema por agotamiento de recursos	N	1				50	
[E.25]	Pérdida de equipos	MB	0,01		100		100	
[A.6]	Abuso de privilegio de acceso	B	0,1		100		100	
[A.7]	Uso no previsto	B	0,1		100	10	100	
[A.11]	Acceso no autorizado	B	0,1		50	20		
[A.23]	Manipulación de los equipos	B	0,1		50		50	
[A.24]	Denegación de servicio	B	0,1				100	
[A.25]	Robo	MB	0,01		100		100	
[A.26]	Ataque destructivo	MB	0,01				100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
HARDWARE (SERVIDORES Y COMUNICACIONES) (DMZ)								
[HW.1]	Firewall externo	A	10		100%	20%	100%	
[HW.5]	Servidor web							
[HW.6]	Servidor de correo							
[HW.7]	Servidor DNS							
[HW.13]	Servidor NIDS							
[HW.18]	VPN CISCO							
Amenazas								
[N.1]	Fuego	MB	0,01				100	
[N.2]	Daños por agua	MB	0,01				100	
[I.1]	Fuego	B	0,1				100	
[I.2]	Daños por agua	B	0,1				100	
[I.5]	Avería de origen físico o lógico	N	1				100	
[I.6]	Corte del suministro eléctrico	N	1				50	
[I.7]	Condiciones inadecuadas de temperatura y humedad	N	1				100	
[E.23]	Errores de mantenimiento / actualización de equipos	N	1				100	
[E.24]	Caída del sistema por agotamiento de recursos	A	10				50	
[E.25]	Pérdida de equipos	MB	0,01		100		100	
[A.6]	Abuso de privilegio de acceso	B	0,1		100		100	
[A.7]	Uso no previsto	B	0,1		100	10	100	
[A.11]	Acceso no autorizado	N	1		50	20		
[A.23]	Manipulación de los equipos	B	0,1		50		50	
[A.24]	Denegación de servicio	N	1				100	
[A.25]	Robo	MB	0,01		100		100	
[A.26]	Ataque destructivo	MB	0,01				100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
HARDWARE SEGURIDAD								
[HW.11]	Cámara de vigilancia	N	1		100%	10%	100%	
[HW.16]	Torno de acceso a oficina							
Amenazas								
[N.1]	Fuego	MB	0,01				100	
[N.2]	Daños por agua	MB	0,01				100	
[I.1]	Fuego	B	0,1				100	
[I.2]	Daños por agua	B	0,1				100	

[I.5]	Avería de origen físico o lógico	N	1				100	
[I.6]	Corte del suministro eléctrico	N	1				50	
[I.7]	Condiciones inadecuadas de temperatura y humedad	B	0,1				100	
[E.23]	Errores de mantenimiento / actualización de equipos	N	1				100	
[E.24]	Caída del sistema por agotamiento de recursos	B	0,1				50	
[E.25]	Pérdida de equipos	MB	0,01		100		100	
[A.6]	Abuso de privilegio de acceso	B	0,1		100		100	
[A.7]	Uso no previsto	B	0,1		100	10	100	
[A.11]	Acceso no autorizado	B	0,1		50	10		
[A.23]	Manipulación de los equipos	B	0,1		50		50	
[A.24]	Denegación de servicio	B	0,1				100	
[A.25]	Robo	MB	0,01		100		100	
[A.26]	Ataque destructivo	MB	0,01				100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
HARDWARE (PUESTOS DE TRABAJO)								
[HW.9]	Estaciones de trabajo	MA	100		100%	20%	100%	
[HW.10]	Portátiles de guardias							
[HW.14]	Impresoras							
Amenazas								
[N.1]	Fuego	MB	0,01				100	
[N.2]	Daños por agua	MB	0,01				100	
[I.1]	Fuego	B	0,1				100	
[I.2]	Daños por agua	B	0,1				100	
[I.5]	Avería de origen físico o lógico	N	1				100	
[I.6]	Corte del suministro eléctrico	N	1				50	
[I.7]	Condiciones inadecuadas de temperatura y humedad	B	0,1				100	
[E.23]	Errores de mantenimiento / actualización de equipos	A	10				50	
[E.24]	Caída del sistema por agotamiento de recursos	A	10				50	
[E.25]	Pérdida de equipos	B	0,1		100		100	
[A.6]	Abuso de privilegio de acceso	N	1		100		100	
[A.7]	Uso no previsto	MA	100		100	10	100	
[A.11]	Acceso no autorizado	A	10		50	20		
[A.23]	Manipulación de los equipos	N	1		50		50	
[A.24]	Denegación de servicio	A	10				100	
[A.25]	Robo	B	0,1		100		100	
[A.26]	Ataque destructivo	MB	0,01				100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
APLICACIONES (SERVIDORES)								
[SW.1]	Aplicación web	N	1	100%	100%	100%	100%	
[SW.2]	Aplicaciones de gestión							
[SW.3]	Servidor de correo							
[SW.4]	Antivirus							
[SW.5]	Servidor de ficheros							
[SW.6]	Microsoft SQL Server 2000							
[SW.7]	Servidor de DNS							
[SW.8]	Microsoft Windows Server 2000							
Amenazas								
[E.1]	Errores de los usuarios	N	1		10	10	1	
[E.2]	Errores del administrador	N	1		10	20	20	
[E.4]	Errores de configuración	N	1		10	10	50	
[E.8]	Difusión de software dañino	B	0,1		10	10	10	
[E.15]	Alteración accidental de la información	N	1			1		
[E.18]	Destrucción de información	N	1				50	
[E.19]	Fuga de información	B	0,1		50			
[E.20]	Vulnerabilidad de los programas	N	1		20	20	1	
[E.21]	Errores de mantenimiento/actualización de programas	N	1			1	1	
[A.5]	Suplantación de la identidad del usuario	B	0,1	100	50	50		
[A.6]	Abuso de privilegios de acceso	B	0,1		50	10	10	
[A.7]	Uso no previsto	B	0,1		10	10	100	
[A.8]	Difusión de software dañino	B	0,1		100	100	100	
[A.11]	Acceso no autorizado	N	1		50	10		
[A.15]	Modificación deliberada de la información	N	1			50		
[A.18]	Destrucción de información	B	0,1				50	
[A.19]	Divulgación de información	B	0,1		50			
[A.22]	Manipulación de programas	B	0,1		100	100	100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
APLICACIONES (ESTACIONES DE TRABAJO)								
[SW.9]	Microsoft Windows XP Professional	MA	100	100%	100%	100%	100%	
[SW.10]	Microsoft Office Professional							
Amenazas								
[E.1]	Errores de los usuarios	A	10		10	10	1	

[E.2]	Errores del administrador	N	1		10	20	20	
[E.4]	Errores de configuración	A	10		10	10	50	
[E.8]	Difusión de software dañino	N	1		10	10	10	
[E.15]	Alteración accidental de la información	A	10			1		
[E.18]	Destrucción de información	A	10				50	
[E.19]	Fuga de información	N	1		50			
[E.20]	Vulnerabilidad de los programas	A	10		20	20	1	
[E.21]	Errores de mantenimiento/actualización de programas	A	10			1	1	
[A.5]	Suplantación de la identidad del usuario	N	1	100	50	50		
[A.6]	Abuso de privilegios de acceso	B	0,1		50	10	10	
[A.7]	Uso no previsto	MA	100		10	10	100	
[A.8]	Difusión de software dañino	N	1		100	100	100	
[A.11]	Acceso no autorizado	N	1		50	10		
[A.15]	Modificación deliberada de la información	B	0,1			50		
[A.18]	Destrucción de información	B	0,1				50	
[A.19]	Divulgación de información	B	0,1		50			
[A.22]	Manipulación de programas	B	0,1		100	100	100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
DATOS								
[D.1]	Bases de datos	A	10	100%	100%	50%	50%	
[D.2]	Datos en servidor de datos							
[D.3]	Backups							
[D.4]	Datos administrativos y gestión							
Amenazas								
[E.1]	Errores de los usuarios	A	10		10	10	10	
[E.2]	Errores del administrador	A	10		10	20	20	
[E.4]	Errores de configuración	N	1			10		
[E.15]	Alteración accidental de la información	A	10			1		
[E.18]	Destrucción de información	N	1				1	
[E.19]	Fugas de información	B	0,1		10			
[A.4]	Manipulación de la configuración	B	0,1	100	50	10		
[A.5]	Suplantación de la identidad del usuario	B	0,1	100	50	10		
[A.15]	Modificación deliberada de la información	B	0,1			50		
[A.18]	Destrucción de la información	B	0,1				50	
[A.19]	Divulgación de información	B	0,1		100			

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
LOGS								
[D.5]	Logs	N	1	100%	50%	100%	50%	100%
Amenazas								
[E.2]	Errores del administrador	N	1		10	20	10	
[E.3]	Errores de monitorización	N	1					50
[E.4]	Errores de configuración	N	1			10		
[E.15]	Alteración accidental de la información	N	1			10		
[E.18]	Destrucción de información	B	0,1				50	
[E.19]	Fugas de información	B	0,1		1			
[A.3]	Manipulación de los registros de logs	B	0,1			100		100
[A.4]	Manipulación de la configuración	B	0,1	100	50	10		
[A.13]	Repudio	B	0,1					100
[A.15]	Modificación deliberada de la información	B	0,1			50		
[A.18]	Destrucción de la información	B	0,1				50	
[A.19]	Divulgación de información	B	0,1		50			

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
RED								
[COM.1]	Red telefónica	N	1		50%	10%	50%	
[COM.2]	Líneas ADSL							
[COM.3]	VPN Madrid							
[COM.4]	Red Inalámbrica							
Amenazas								
[E.2]	Errores del administrador	B	0,1		10	1	50	
[E9]	Errores de [re]-encaminamiento	B	0,1		1			
[E.10]	Errores de secuencia	B	0,1			10		
[E.14]	Escapes de información	B	0,1		1			
[E.24]	Caída del sistema por agotamiento de recursos	N	1				50	
[A.6]	Abuso de privilegios de acceso	B	0,1		50	10		
[A.9]	Reencaminamiento de mensajes	B	0,1		10			
[A.10]	Alteración de secuencia	B	0,1			10		
[A.11]	Acceso no autorizado	B	0,1		50	10		
[A.12]	Análisis de tráfico	B	0,1		20			
[A.14]	Interceptación información (escucha)	B	0,1		20			
[A.24]	Denegación de servicio	B	0,1				50	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
SERVICIOS								
[S.1]	Acceso remoto	A	10	100%	100%	50%	100%	100%
[S.2]	Monitorización							
[S.3]	Correo electrónico							
[S.4]	Transferencia de ficheros							
[S.5]	Gestión de acceso físico a oficinas							
[S.6]	Web							
Amenazas								
[E.1]	Errores de los usuarios	A	10		10	1	1	
[E.2]	Errores del administrador	N	1		10	20	20	
[E.15]	Alteración accidental de la información	N	1			10		
[E.18]	Destrucción de la información	N	1				50	
[E.19]	Fugas de la información	B	0,1		10			
[A.5]	Suplantación de la identidad del usuario	B	0,1	100	50	10		
[A.6]	Abuso de privilegios de acceso	B	0,1		10	50	10	
[A.7]	Uso no previsto	B	0,1		10	10	100	
[A.10]	Alteración de secuencia	B	0,1			10		
[A.11]	Acceso no autorizado	B	0,1			10		
[A.13]	Repudio	B	0,1					100
[A.15]	Modificación deliberada de la información	B	0,1			50		
[A.18]	Destrucción de la información	B	0,1				10	
[A.19]	Divulgación de información	B	0,1		100			
[A.24]	Denegación de servicio	N	1				100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
EQUIPAMIENTO AUXILIAR (OFICINA)								
[AUX.1]	Armario con llave de entrada a sala CPD	N	1		100%	50%	100%	
[AUX.2]	Armario con llave con documentos en papel							
Amenazas								
[N.1]	Fuego	MB	0,01				100	
[N.2]	Daños por agua	MB	0,01				100	
[I.1]	Fuego	B	0,1				100	
[I.2]	Daños por agua	B	0,1				100	
[I.7]	Condiciones inadecuadas de temperatura y humedad	MB	0,01				1	
[E.25]	Pérdida de equipos	N	1				100	
[A.7]	Uso no previsto	N	1		100	50	50	

[A.11]	Acceso no autorizado	N	1		100	50		
[A.25]	Robo	B	0,1				100	
[A.26]	Ataque destructivo	MB	0,01				100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
EQUIPAMIENTO AUXILIAR (CPD)								
[AUX.3]	Aire acondicionado	N	1			50%	100%	
[AUX.4]	SAI para el CPD							
[AUX.5]	Corriente eléctrica							
Amenazas								
[N.1]	Fuego	MB	0,01				100	
[N.2]	Daños por agua	MB	0,01				100	
[I.1]	Fuego	B	0,1				100	
[I.2]	Daños por agua	B	0,1				100	
[I.5]	Avería de origen físico o lógico	N	1				100	
[I.6]	Corte del suministro eléctrico	N	1				100	
[I.7]	Condiciones inadecuadas de temperatura y humedad	N	1				100	
[I.9]	Interrupción de otros servicios y suministros esenciales	N	1				100	
[E.23]	Errores de mantenimiento / actualización de equipos	N	1				50	
[E.25]	Pérdida de equipos	MB	0,01				100	
[A.7]	Uso no previsto	MB	0,01			50	50	
[A.11]	Acceso no autorizado	MB	0,01			20		
[A.23]	Manipulación de los equipos	MB	0,01				50	
[A.25]	Robo	MB	0,01				100	
[A.26]	Ataque destructivo	MB	0,01				100	

ACTIVO		FRECUENCIA		ASPECTOS CRÍTICOS				
				A	C	I	D	T
PERSONAL								
[P.1]	Responsable de operaciones	A	10		10%	10%	100%	
[P.2]	Responsable de Sistemas e infraestrucura							
[P.3]	Personal TIC							
[P.4]	Personal de administración/finanzas							
Amenazas								
[E.7]	Deficiencias en la organización	N	1				10	
[E.19]	Fugas de información	N	1		10			
[E.28]	Indisponibilidad del personal	A	10				100	
[A.29]	Extorsión	MB	0,01		10	10	10	
[A.30]	Ingeniería social	N	1		10	10	10	

10.9. Anexo IX - Propuestas de proyectos

A continuación se detallan las propuestas de proyectos. Para cada una de ellas se especifica la prioridad de ejecución, el responsable, su objetivo, descripción, cual es la motivación del proyecto, los controles para verificar la evolución, tiempo y costes.

Los proyectos que se consideran importantes para la mejora de la seguridad de la información de la compañía son:

Administración de estaciones de trabajo y portátiles de guardia	**IMP-001**
Prioridad	Alta
Responsables de proyecto	Departamento de sistemas
Objetivo • Mejora de la seguridad en el puesto de trabajo y de las estaciones de trabajo y portátiles de guardia utilizados por los empleados	
Descripción • Actualmente las estaciones de trabajo y portátiles de guardia están mínimamente administrados por el soporte técnico. Se implantaran medidas para aumentar la seguridad de estos activos con tal de minimizar los riesgos asociados, gestionando cuentas de usuarios con menor nivel de privilegios, sistema de cambio de contraseñas, sistemas de actualización de software, antivirus, anti-spyware, instalación de únicamente software de confianza, política de uso de software extraíble, políticas de puestos de trabajo despejado y pantalla limpia... Se incluyen cursos de formación sobre concienciación en seguridad informática.	
Motivación • Mejora los resultados obtenidos en el análisis de riesgos • Mejora los puntos de la ISO 27002: 10.4, 10.7, 11.3, 11.5	
Controles • Estadísticas de vulnerabilidades y tiempo medio de parcheo de vulnerabilidades • Número de malware detectado y bloqueado • Número y costes asociados a incidentes por malware • Porcentaje del personal con responsabilidades aceptadas en seguridad de la información • Porcentaje de dispositivos cifrados • Número de cursos de formación	
Tiempo de implementación	6 meses
Coste	30.000€

Securización de portátiles de guardia	IMP-002
Prioridad	Alta
Responsables de proyecto	Departamento de sistemas

Objetivo

- La seguridad referente a los portátiles de guardia es de gran importancia en caso de robo o extravío. La información contenida en los portátiles puede ser aprovechada por personas ajenas por lo que es importante implantar sistemas para asegurar la protección de los datos.

Descripción

- Con el objetivo de asegurar la protección de los portátiles de guardia, se desarrollará una política formal de uso de los portátiles y por otro lado, el departamento de sistemas aplicará sobre éstos diversas acciones, entre ellas, un sistema de autenticación mediante tokens de seguridad, el cual técnico de guardia llevará consigo el token para identificarse, cifrado de disco duro y bios con autenticación.

Motivación

- Mejora los resultados obtenidos en el análisis de riesgos
- Mejora los puntos de la ISO 27002: 9.2.5, 11.7

Controles

- Porcentaje de autenticaciones correctas/fallidas con token
- Número de incidencias con los portátiles de guardia
- Porcentaje de discos duros cifrados y bios con autenticación

Tiempo de implementación	1 mes
Coste	3.000€

Nuevo sistema de acceso a CPD	INF-001
Prioridad	Baja
Responsables de proyecto	Departamento de sistemas
Objetivo • Implantación de un sistema de control de acceso por tarjeta que mejore el sistema actual	
Descripción • Actualmente se usa una llave que resguarda el responsable de sistemas para acceder al CPD. La seguridad de acceso al CPD se optimizará mediante un sistema de control de acceso por tarjeta, de esta manera se podrá mantener un control sobre los accesos a la sala. Ese sistema debe tener además una validación con identificación numérica. Cada empleado con acceso al CPD tendrá su número de identificación propio.	
Motivación • Mejora los puntos de la ISO 27002: 9.1.2	
Controles • Número de averías del sistema de control de acceso • Porcentaje de accesos permitidos/denegados al CPD • Número de incidencias de acceso al CPD	
Tiempo de implementación	1 semana
Coste	1.000€ (incluye compra del sistema de control de acceso)

Sistema balanceado para servidor web corporativo	IMP-003
Prioridad	Media
Responsables de proyecto	Departamento de sistemas
Objetivo • Se ha mantenido el servidor web que se implantó al comienzo de la compañía. El servidor web actual no cumple las expectativas esperadas, por lo que se desea implantar uno nuevo con mayores garantías.	
Descripción • Haciendo uso de 2 servidores no utilizados actualmente por la compañía, se instalarán en ambos el sitio web corporativo actualizado. Por otro lado se implantará un servidor que balanceará las peticiones a alguno de los servidores según la carga que tengan en ese momento. Mediante este sistema se consigue mejorar la disponibilidad en el caso que alguno de estos servidores falla.	
Motivación • Mejora los resultados obtenidos en el análisis de riesgos	
Controles • Número de caídas del sistema y tiempos sin dar servicio	
Tiempo de implementación	1 mes
Coste	3.000€

Migración del servidor de correo	IMP-004
Prioridad	Media
Responsables de proyecto	Departamento de sistemas
Objetivo • Se ha mantenido el servidor de correo que se implantó al comienzo de la compañía. El servidor de correo actual no cumple las expectativas esperadas, por lo que se desea implantar uno nuevo con mayores garantías.	
Descripción • Se plantea la migración del servicio de correo a un nuevo servidor de correo más estable y con mejores prestaciones.	
Motivación • Mejora los resultados obtenidos en el análisis de riesgos	
Controles • Número de caídas del sistema y tiempos sin dar servicio	
Tiempo de implementación	2 meses
Coste	5.000€ (incluye la compra del nuevo servidor)

Política de gestión de logs	DOC-001
Prioridad	Baja
Responsables de proyecto	Comité de seguridad de la información
Objetivo • El objetivo de esto proyecto consiste en la de mantener un sistema apto para detectar actividades de procesamiento de la información no autorizadas.	
Descripción • Se deben definir las reglas para mantener un sistema que monitorice los eventos de seguridad de la información que se vayan registrando. Esta monitorización debe garantizar la identificación de los problemas que causen sobre los sistemas informáticos. Para ello se deben cumplir todos los requisitos legales para la monitorización y registro de actividades. Por último, esta política debe asegurar la efectividad de los controles adoptados y la conformidad del modelo de política de acceso.	
Motivación • Mejora los resultados obtenidos en el análisis de riesgos • Mejora los puntos de la ISO 27002: 10.10	
Controles • Porcentaje de sistemas con logs de seguridad correctamente configurados y que son transferidos de forma seguridad a un servidor centralizado	
Tiempo de implementación	1 mes
Coste	2.000€

Mejora en servicio de transferencia de ficheros	IMP-005
Prioridad	Alta
Responsables de proyecto	Departamento de sistemas
Objetivo • Mantener la seguridad de la información y de las aplicaciones que se transfieren dentro de la compañía.	
Descripción • Se debe crear una política de intercambio según acuerdos de transferencias, además de procedimientos y normas para proteger la información y los dispositivos físicos que la almacenan para posteriormente implantar el servicio.	
Motivación • Mejora los resultados obtenidos en el análisis de riesgos • Mejora los puntos de la ISO 27002: 10.8	
Controles • Porcentaje de sistemas donde se ha implementado correctamente el servicio de transferencia de ficheros seguro	
Tiempo de implementación	1 mes
Coste	5.000 €

Revisión de política de control de accesos	DOC-002
Prioridad	Alta
Responsables de proyecto	Comité de seguridad de la información
Objetivo • Controlar el acceso a la información	
Descripción • Se debe realizar una política de control de acceso a la información en base a las necesidades de seguridad y de negocio de la compañía. Para ello se deben definir controles para asegurar la protección de la red, los sistemas operativos, aplicaciones y especialmente de la información, de tal manera que se restringirá el acceso a todo el personal o persona ajena que no deba poder acceder al activo.	
Motivación • Mejora los resultados obtenidos en el análisis de riesgos • Mejora los puntos de la ISO 27002: 11.1.1, 11.2, 11.4, 11.5, 11.6	
Controles • Porcentaje de sistemas y software con sistema de control de acceso basado en roles. • Estadísticas de paquetes bloqueados por algún control de acceso • Número de intentos y nombre de sistema a los que ha sido bloqueado el acceso	

Tiempo de implementación	1 mes
Coste	2.000 €

Revisión de política de backups y gestión de datos	**DOC-003**
Prioridad	Media
Responsables de proyecto	Comité de seguridad de la información
Objetivo • Mantener la integridad y disponibilidad de la información que la compañía identifica como transcendente para la continuidad de negocio de la compañía.	
Descripción • Se deben definir procedimientos para realizar copias de seguridad y por otro lado testearlas por si sucede cualquier incidente de seguridad. Por otro lado, se gestionará la separación de los datos para restringir el acceso únicamente al personal autorizado y mantener su confidencialidad. Para ello se dispondrán los datos en distintos sistemas según la clasificación de la información.	
Motivación • Mejora los resultados obtenidos en el análisis de riesgos • Mejora los puntos de la ISO 27002: 10.5	
Controles • Porcentaje de backups que se han realizado con éxito • Porcentaje de pruebas de backups realizadas con éxito y tiempo necesario para la prueba de recuperación • Porcentaje de backups que están cifrados	
Tiempo de implementación	1 mes
Coste	3.000 €

Clasificación de la información	DOC-004
Prioridad	Alta
Responsables de proyecto	Comité de seguridad de la información
Objetivo • Asegurar que la información se protege de forma adecuada.	
Descripción • Se establecerá un esquema de clasificación de la información según su valor, requisitos legales y criticidad. Según el baremo, se establecerán distintos niveles de protección.	
Motivación • Mejora los puntos de la ISO 27002: 7.2	
Controles • Porcentaje de activos clasificados • Porcentaje de activos clasificados según categoría	
Tiempo de implementación	2 meses
Coste	3.000€

Gestión del inventario de activos	DOC-005
Prioridad	Alta
Responsables de proyecto	Departamento de sistemas
Objetivo • Obtener un inventario actualizado de los activos	
Descripción • Actualmente se mantiene un inventario de activos no actualizados y sin identificación correcta, al finalizar este proyecto se habrá definido una política de gestión del inventario con tal de mantenerlo actualizado y correctamente identificado, incluyendo la propiedad de cada uno de los activos y la normativa de uso.	
Motivación • Mejora los puntos de la ISO 27002: 7.1	
Controles • Número de activos añadidos/actualizados/eliminados del inventario	
Tiempo de implementación	1 semana
Coste	500 €

Política de mantenimiento de los sistemas de la información	DOC-006
Prioridad	Medio
Responsables de proyecto	Comité de seguridad de la información

Objetivo

- Garantizar que la seguridad es requisito básico de los sistemas de la información, se implantarán todas las medidas necesarias para asegurarlo.

Descripción

- Se establecerán procedimientos y responsabilidades a la hora de gestionar el mantenimiento y seguridad de los sistemas de la información. Específicamente en los siguientes campos:
  - Análisis y especificación de los requisitos de seguridad
  - Seguridad de las aplicaciones del sistema
  - Controles criptográficos
  - Seguridad de los ficheros de los sistemas
  - Seguridad en los procesos de desarrollo y soporte
  - Gestión de las vulnerabilidades técnicas

Motivación

- Mejora los puntos de la ISO 27002: 12.1, 12.3, 12.4, 12.6

Controles

- Porcentaje de sistemas que cumplen los requisitos básicos de seguridad
- Porcentaje de sistemas con información sensible con controles criptográficos
- Informe sobre seguridad de las aplicaciones en desarrollo
- Tiempo de parcheo de vulnerabilidades

Tiempo de implementación	2 meses
Coste	8.000 €

Política de tratamiento de incidentes de seguridad	DOC-007
Prioridad	Alta
Responsables de proyecto	Comité de seguridad de la información

Objetivo

- Garantizar que se aplica una correcta gestión en los incidentes de seguridad que suceden en los sistemas de la información de la compañía.

Descripción

- Se establecerán procedimientos y responsabilidades a la hora de gestionar sucesos o fallos de seguridad de una forma efectiva. Para ello se ordenan los incidentes por criticidad, una respuesta rápida es vital para contrarrestar y limitar el impacto del incidente.

Motivación • Mejora los puntos de la ISO 27002: 13.2	
Controles • Número de incidentes, gravedad de cada uno y coste de resolución • Número de incidentes que ha causado costes mayores al máximo aceptable	
Tiempo de implementación	1 mes
Coste	3.000 €

Política de retirada de equipos y material	**DOC-008**
Prioridad	Baja
Responsables de proyecto	Comité de seguridad de la información
Objetivo • Garantizar que la seguridad de la información no se ve comprometida por la retirada de equipos o material propiedad de la compañía	
Descripción • Se establecerán procedimientos para revisar cualquier elemento de los equipos o material que se retiran con dispositivos de almacenamiento con tal de garantizar que no almacenan ningún tipo de dato sensible. Además, se especificará una guía sobre almacenamiento y borrado seguro de la información. Por otro lado se redefinirá la política para evitar que se saquen equipos, información o software fuera del local sin autorización.	
Motivación • Mejora los puntos de la ISO 27002: 9.2.6, 9.2.7	
Controles • Porcentaje de equipos y sistemas que han sido analizados antes de su retirada • Número de equipos que han sido sacados de la oficina sin autorización	
Tiempo de implementación	1 mes
Coste	1.000 €

Cumplimiento de requisitos legales y políticas de la compañía	**DOC-009**
Prioridad	Alta
Responsables de proyecto	Comité de seguridad de la información
Objetivo • Garantizar la conformidad de los sistemas de la información con los requisitos legales existentes, y las políticas y estándares de seguridad de la compañía.	

Descripción

- Se establecerán documentos actualizados para mantener de forma explícita todos los requisitos legales, regulatorios y contractuales importantes para los sistemas de la información. Entre estos se deberá cumplir:
  - Derechos de propiedad intelectual
  - Salvaguarda de los registros de la compañía
  - Protección de los datos y de la privacidad de la información personal
  - Prevención en el mal uso de los recursos de tratamiento de la información
  - Regulación de los controles criptográficos
- Además se establecerán procedimientos para revisar regularmente la seguridad de los sistemas de la información según las políticas de seguridad de la compañía. Además se auditarán los sistemas de acuerdo a la implantación llevada a cabo y los controles de seguridad documentados.

Motivación

- Mejora los puntos de la ISO 27002: 15.1, 15.2

Controles

- Número de cuestiones de cumplimiento legal estudiadas
- Número de cuestiones de política interna estudiadas

Tiempo de implementación	3 meses
Coste	10.000 €

Gestión de auditorias de sistemas	**DOC-010**
Prioridad	Baja
Responsables de proyecto	Comité de seguridad de la información

Objetivo

- Maximizar la efectividad en el proceso de auditorías de sistemas.

Descripción

- Se establecerán controles y planificaciones para la realización de auditorias con el fin de minimizar el riesgo a interrupciones que afecten las actividades de la compañía, estas auditorias serán realizadas por personas independientes a las actividades auditadas. Se acordará y controlará el alcance de las verificaciones, limitándola a accesos de solo lectura. Todos los accesos serán registrados y supervisados para poder realizar su seguimiento

Motivación

- Mejora los puntos de la ISO 27002: 15.3.1

Controles

- Número de cuestiones de auditoría estudiadas
- Número de fallos de seguridad detectados por auditorías
- Tiempo de resolución de los fallos de seguridad

Tiempo de implementación	1 mes
Coste	3.000€

Plan de continuidad de negocio	DOC-011
Prioridad	Media
Responsables de proyecto	Comité de seguridad de la información
Objetivo • Creación de un plan de continuidad de negocio con tal de reaccionar a la interrupción de actividades de negocio y proteger los procesos críticos.	
Descripción • Con tal de poder hacer frente a cualquier desastre que pueda afectar a la compañía, es necesario diseñar un plan completo para asegurar la continuidad de negocio. Mediante este plan se reducirá a niveles aceptables la interrupción causada por un desastre o fallo de seguridad mediante controles preventivos y de recuperación. • La gestión de la continuidad de negocio debe incluir controles para la identificación y reducción de riesgos, limitar la forma en la que pueden afectar cualquier desastre y asegurar la reanudación de las actividades críticas a tiempo. • El plan se revisará cada dos años, pero se irán realizando pruebas para asegurar su efectividad y verificar que se está preparado a adversidades.	
Motivación • Mejora los puntos de la ISO 27002: 14	
Controles • Número de eventos que pueden causar interrupciones con la probabilidad e impacto asociado con sus consecuencias para la seguridad de la información • Porcentaje de departamentos con planes de continuidad de negocio documentados y probados	
Tiempo de implementación	6 meses
Coste	30.000€

Revisión documentación relacionada con los RRHH	DOC-012
Prioridad	Media
Responsables de proyecto	Comité de seguridad de la información
Objetivo • Revisión de la documentación que hace referencia a las funciones y responsabilidades de los empleados antes, durante y al finalizar su contrato.	
Descripción • Un factor vital para la seguridad de la información viene principalmente dada por el uso que hacen de ella los empleados. Desde la contratación se deben especificar las funciones y responsabilidades, además de analizar los empleados que sean aptos. • Se establecerá un proceso disciplinario para gestionar las brechas de seguridad, además de asegurar un adecuado nivel de concienciación y educación en seguridad durante su etapa en la compañía. • Una vez finalizado el contrato, se eliminarán todos los derechos de acceso y deberá devolver todo el material de ConTec S.L, verificándolo con el del inventario. • Por último, se tomarán medidas para la seguridad de la documentación relacionada	

con RRHH para que no pueda ser obtenida por personas ajenas a este departamento sin el consentimiento oportuno.
Motivación • Mejora los puntos de la ISO 27002: 8.1, 8.2, 8.3
Controles • Porcentaje de empleados que han sido estudiados antes de ser contratados según la política de la compañía • Porcentaje de actividades a las que ha asistido los empleados sobre concienciación en seguridad. • Número de incidencias causadas por empleados • Tiempos necesarios para deshabilitar cada uno de los accesos a los distintos servicios a los que se le da permiso a los empleados.

Tiempo de implementación	2 mes
Coste	6.000€

Política de seguridad de la información	**DOC-013**
Prioridad	Alta
Responsables de proyecto	Comité de seguridad de la información
Objetivo • Creación de la política de seguridad de la información según los requisitos de negocio de la compañía.	
Descripción • Se debe definir una política de seguridad de la información apoyada por la dirección que posteriormente será comunicada a todos los empleados. Este documento debe abarcar entre otra información: los objetivos de la política, el alcance, la definición de responsabilidades, mecanismos para evaluar y gestionar el riesgo y principios, normas y requisitos para el correcto funcionamiento de la compañía. • La política de seguridad se revisará con tal de asegurar su efectividad según periodos de tiempo establecidos o si hay cambios importantes. Se tendrán en cuenta los resultados de las revisiones anteriores.	
Motivación • Mejora los puntos de la ISO 27002: 5.1	
Controles • Porcentaje de dominios de la política de seguridad según la ISO 27002 a los que se han desarrollado políticas, normas o procedimientos. • Porcentaje de adopción de la política de seguridad en la compañía.	
Tiempo de implementación	1 mes
Coste	3.000€

Revisión de aspectos organizativos internos	DOC-014
Prioridad	Alta
Responsables de proyecto	Comité de seguridad de la información
Objetivo • Depurar los aspectos organizativos internos respecto a la seguridad de la información.	
Descripción • Una vez que la dirección ha aceptado el compromiso de acuerdo a la seguridad de la información, se revisará la coordinación de la seguridad de la información depurando las responsabilidades. • Se establecerán contactos con fuentes especializadas de consulta en seguridad de la información para mantenerse informado sobre vulnerabilidades de seguridad, las novedades en el mercado y la industria, además de la evolución sobre normas o métodos de evaluación. • Se establecerán procedimientos para la revisión de la gestión de la seguridad de la información de forma independiente cada cierto tiempo.	
Motivación • Mejora los puntos de la ISO 27002: 6.1	
Controles • Número de incidencias resultantes de revisiones independientes de la gestión de la seguridad de la información • Número de contacto con fuentes especializadas de consulta sobre seguridad de la información. • Porcentaje de empleados con roles y responsabilidades en seguridad	
Tiempo de implementación	1 mes
Coste	3.000€

10.10. Anexo X - Análisis de cumplimiento según dominio

A continuación se realiza un estudio del cumplimiento de cada uno de los controles de los distintos dominios de la ISO.

Política de seguridad

5. POLÍTICA DE SEGURIDAD	20%
5.1 Política de seguridad de la información	**20%**
5.1.1 Documento de la política de seguridad de la información	30%
5.1.2 Revisión de la política de seguridad de la información	10%

Actualmente, ConTec S.L. no cuenta con un marco normativo de seguridad que regule las líneas maestras sobre la forma de trabajar en la compañía en materia de seguridad.

A pesar de haber elaborado documentación en forma de manual o instrucciones sobre ciertos apartados de seguridad, éstos no tienen una estructura homogénea, nomenclatura o terminología en común, por lo que dificulta la interpretación y gestión. No dispone de una línea clara de procedimientos o líneas de actuaciones globales alineados con los objetivos de negocio para poder constituir una política de seguridad.

Aspectos organizativos de la seguridad de la información

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	51%
6.1 Organización interna	**31%**
6.1.1 Compromiso de la dirección con la seguridad de la información	40%
6.1.2 Coordinación de la seguridad de la información	30%
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	30%
6.1.4 Proceso de autorización de recursos para el tratamiento de la información	30%
6.1.5 Acuerdo de confidencialidad	70%
6.1.6 Contacto con las autoridades	0%
6.1.7 Contacto con grupos de especial interés	40%
6.1.8 Revisión independiente de la seguridad de la información	10%
6.2 Terceros	**70%**
6.2.1 Identificación de los riesgos derivados del acceso de terceros	40%
6.2.2 Tratamiento de la seguridad en la relación con los clientes	80%
6.2.3 Tratamiento de la seguridad en contratos con terceros	90%

Hasta ahora, ConTec S.L. no ha centrado sus esfuerzos en establecer una estructura organizativa para gestionar la seguridad de la información, por lo que tampoco existen responsabilidades y funciones claras y concretas.

A pesar de ello, tanto en tecnología como en recursos humanos, se tiene presente la seguridad de la información. Aún así se debería concretar una estructura organizativa interna con responsabilidades directas sobre la seguridad de la información, que pueda asegurar que se implante correctamente un SGSI.

Los empleados firman acuerdos de confidencialidad y no divulgación al firmar el contrato de trabajo.

Los acuerdos con terceras partes cubren los requisitos de seguridad necesarios, de tal manera que no existen desentendimientos entre ambos.

No existen procedimientos sobre autoridades con las que contactar, ni de la información que debe ser reportada en caso de vulnerar alguna ley o incidente.

Gestión de activos

7. GESTIÓN DE ACTIVOS	20%
7.1 Responsabilidad sobre los activos	**30%**
7.1.1 Inventario de activos	30%
7.1.2 Propiedad de los activos	40%
7.1.3 Uso aceptable de los activos	30%
7.2 Clasificación de la información	**10%**
7.2.1 Directrices de clasificación	10%
7.2.2 Etiquetado y manipulado de la información	10%

En el apartado de activos, se mantiene un inventario de los sistemas de la compañía. El inventario de los sistemas no incluye todos los datos necesarios como el tipo de activo, formato, ubicación, información de respaldo, información de licencia y el valor dentro del negocio. Tampoco se especifica procedimientos de mantenimiento y actualización del inventario.

No existe documentación formal del uso correcto de los ordenadores usados directamente por los empleados. Existe un pequeño manual de uso correcto del correo electrónico.

La información tiene grados variables de sensibilidad y criticidad pero no existe ningún sistema de clasificación de esta información y se confía en el buen hacer de los trabajadores.

Seguridad relativa a los recursos humanos

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	66%
8.1 Antes del empleo	**70%**
8.1.1 Funciones y responsabilidades	50%
8.1.2 Investigación de antecedentes	70%
8.1.3 Términos y condiciones de contratación	90%
8.2 Durante el empleo	**63%**
8.2.1 Responsabilidades de la dirección	70%
8.2.2 Concienciación, formación y capacitación en seguridad de la información	70%
8.2.3 Proceso disciplinario	50%
8.3 Cese del empleo o cambio de puesto de trabajo	**63%**
8.3.1 Responsabilidad del cese o cambio	70%
8.3.2 Devolución de activos	70%
8.3.3 Retirada de los derechos de acceso	50%

A pesar que ConTec S.L no ha dirigido sus esfuerzos hacia la seguridad de la información, el departamento de formación realiza cursos de concienciación y formación en la seguridad de la información.

Antes de pactar el contrato de trabajo, el trabajador debe firmar de acuerdo a sus roles y responsabilidades, una serie de políticas de confidencialidad y no divulgación, para evitar posibles fugas de información.

Una vez que un trabajador finaliza su contrato o cambia de trabajo, se llevan a cabo acciones para eliminar los derechos de acceso, correo electrónico y cambio de contraseñas clave al que el trabajador tenía acceso.

Seguridad física y del entorno

9. SEGURIDAD FÍSICA Y DEL ENTORNO	61%
9.1 Áreas seguras	**70%**
9.1.1 Perímetro de seguridad física	70%
9.1.2 Controles físicos de entrada	80%
9.1.3 Seguridad de oficinas, despachos e instalaciones	70%
9.1.4 Protección contra las amenazas externas y de origen ambiental	60%
9.1.5 Trabajo en áreas seguras	N.A. - No aplica
9.1.6 Áreas de acceso público y de carga y descarga	N.A. - No aplica
9.2 Seguridad de los equipos	**51%**
9.2.1 Emplazamiento y protección de equipos	70%
9.2.2 Instalaciones de suministro	70%
9.2.3 Seguridad del cableado	70%

9.2.4 Mantenimiento de los equipos	60%
9.2.5 Seguridad de los equipos fuera de las instalaciones	30%
9.2.6 Reutilización o retirada segura de equipos	30%
9.2.7 Retirada de materiales propiedad de la empresa	30%

La sede de Barcelona está alojada en un tercer piso de un edificio de oficinas. Este edificio dispone de detectores de incendio y de dos salidas de emergencia. El edificio dispone de conserje.

El CPD de la oficina está situado en una habitación separada con único método de acceso mediante llave, la cual está al resguardo del responsable de sistemas de la información. La sala dispone de un sistema de aire acondicionado para mantener un control de temperatura y humedad.

Existen sistemas para proteger los equipos contra fallos de energía u otras anomalías eléctricas. Los PCs y portátiles están atados con cables de seguridad para evitar su robo. Los cables están soterrados.

Respecto al acceso físico a las oficinas, dispone de una recepción en horario de oficina. Para el acceso al interior de la oficina, es necesario que cada empleado lleve consigo una tarjeta de identificación necesaria para abrir el torno que da acceso al interior. En la entrada a la oficina hay implantado un sistema de grabación de imagen. Una vez dentro de la oficina no existe ningún otro tipo de control.

No hay documentación formal sobre la reutilización o retirada segura de equipos.

Gestión de comunicaciones y operaciones

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	58%
10.1 Responsabilidades y procedimientos de operación	**43%**
10.1.1 Documentación de los procedimientos de operación	40%
10.1.2 Gestión de cambios	60%
10.1.3 Segregación de tareas	20%
10.1.4 Separación de los recursos de desarrollo, prueba y operación	50%
10.2 Gestión de la provisión de servicios por terceros	**90%**
10.2.1 Provisión de servicios	90%
10.2.2 Supervisión y revisión de los servicios prestados por terceros	90%
10.2.3 Gestión del cambio en los servicios prestados por terceros	90%
10.3 Planificación y aceptación del sistema	**35%**
10.3.1 Gestión de capacidades	50%
10.3.2 Aceptación del sistema	20%
10.4 Protección contra el código malicioso y descargable	**60%**
10.4.1 Controles contra el código malicioso	60%
10.4.2 Controles contra el código descargado en el cliente	N.A. - No aplica
10.5 Copias de seguridad	**80%**
10.5.1 Copias de seguridad de la información	80%
10.6 Gestión de la seguridad de las redes	**70%**

10.6.1 Controles de red	70%
10.6.2 Seguridad de los servicios de red	70%
10.7 Manipulación de los soportes	**25%**
10.7.1 Gestión de soportes extraíbles	0%
10.7.2 Retirada de soportes	10%
10.7.3 Procedimientos de manipulación de la información	50%
10.7.4 Seguridad de la documentación del sistema	40%
10.8 Intercambio de información	**48%**
10.8.1 Políticas y procedimientos de intercambio de información	60%
10.8.2 Acuerdos de intercambio	60%
10.8.3 Soportes físicos en tránsito	N.A. - No aplica
10.8.4 Mensajería electrónica	20%
10.8.5 Sistemas de información empresariales	50%
10.9 Servicios de comercio electrónico	
10.9.1 Comercio electrónico	N.A. - No aplica
10.9.2 Transacciones en línea	N.A. - No aplica
10.9.3 Información públicamente disponible	N.A. - No aplica
10.10 Supervisión	**70%**
10.10.1 Registros de auditoría	70%
10.10.2 Supervisión del uso del sistema	70%
10.10.3 Protección de la información de los registros	80%
10.10.4 Registros de administración y operación	80%
10.10.5 Registro de fallos	80%
10.10.6 Sincronización del reloj	40%

ConTec S.L. se toma en serio la seguridad de los sistemas de comunicación y de las comunicaciones. Los siguientes puntos reflejan aspectos en la seguridad en la gestión de comunicaciones y operaciones dentro de la compañía.

- A nivel de red, su infraestructura está dividida en varios niveles, siempre teniendo en cuenta la seguridad de la red, mediante firewalls, NIDS y HIDS.
- Se realizan backups de los datos críticos que almacena fuera de la oficina, específicamente en el CPD del proveedor de servicios de comunicación que tiene contratado.
- Tiene implantado un sistema de monitorización de sistemas.
- A nivel de posibles fallos eléctricos, la compañía dispone de un sistema SAI, el cual le dispondría de energía durante un periodo máximo de 2 horas.
- A nivel de un posible corte en el servicio de la línea de internet, ConTec S.L. tiene contratada dos líneas ADSL de distinta compañía.
- Las líneas de energía y telecomunicaciones están soterradas, estas líneas están separadas evitando interferencias.
- Los cables están marcados para minimizar errores.
- Se mantiene un registro de gestión de cambios que se llevan a cabo en los sistemas.
- No hay procedimiento seguro para la extracción segura de soportes extraíbles.
- No se ha implantado ningún tipo de segregación de tareas para reducir el riesgo de un uso incorrecto de los sistemas.

- No hay un procedimiento formal sobre la sincronización de los relojes de los sistemas.

Control de acceso

11. CONTROL DE ACCESO	51%
11.1 Requisitos de negocio para el control de acceso	**50%**
11.1.1 Política de control de acceso	50%
11.2 Gestión de acceso de usuario	**53%**
11.2.1 Registro de usuario	50%
11.2.2 Gestión de privilegios	40%
11.2.3 Gestión de contraseñas de usuario	60%
11.2.4 Revisión de los derechos de acceso de usuario	60%
11.3 Responsabilidades de usuario	**23%**
11.3.1 Uso de contraseñas	50%
11.3.2 Equipo de usuario desatendido	20%
11.3.3 Política de puestos de trabajo despejados y pantalla limpia	0%
11.4 Control de acceso a la red	**73%**
11.4.1 Política de uso de los servicios de red	70%
11.4.2 Autenticación de usuario para conexiones externas	80%
11.4.3 Identificación de los equipos en red	70%
11.4.4 Protección de los puertos de diagnóstico y configuración remotos	50%
11.4.5 Segregación de las redes	80%
11.4.6 Control de la conexión a la red	80%
11.4.7 Control de encaminamiento a la red	80%
11.5 Control de acceso al sistema operativo	**30%**
11.5.1 Procedimientos seguros de inicio de sesión	60%
11.5.2 Identificación y autenticación de usuario	70%
11.5.3 Sistema de gestión de contraseñas	50%
11.5.4 Uso de los recursos del sistema	0%
11.5.5 Desconexión automática de la sesión	0%
11.5.6 Limitación del tiempo de conexión	0%
11.6 Control de acceso a las aplicaciones y a la información	**75%**
11.6.1 Restricción del acceso a la información	80%
11.6.2 Aislamiento de sistemas sensibles	70%
11.7 Ordenadores portátiles y teletrabajo	**50%**
11.7.1 Ordenadores portátiles y comunicaciones móviles	50%
11.7.2 Teletrabajo	50%

Se tiene especial atención a la seguridad en los accesos en los servidores, por lo tanto sólo está permitido a los trabajadores habilitados. Cada trabajador tiene sus credenciales de acceso.

Existen políticas de control de acceso para los trabajadores de los departamentos de administración, finanzas, contabilidad, marketing y recursos humanos.

En los programas de gestión, administración, finanzas y contabilidad se registran los accesos de los trabajadores asociados.

Por el contrario no hay procedimientos para equipos desatendidos, puestos de trabajo limpios, pantalla despejada, ni limitaciones de tiempo en las sesiones.

Adquisición, desarrollo y mantenimiento de sistemas de información

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	47%
12.1 Requisitos de seguridad de los sistemas de información	**40%**
12.1.1 Análisis y especificación de los requisitos de seguridad	40%
12.2 Tratamiento correcto de las aplicaciones	**68%**
12.2.1 Validación de los datos de entrada	60%
12.2.2 Control del procesamiento interno	60%
12.2.3 Integridad de los mensajes	70%
12.2.4 Validación de los datos de salida	80%
12.3 Controles criptográficos	**60%**
12.3.1 Política de uso de los controles criptográficos	50%
12.3.2 Gestión de claves	70%
12.4 Seguridad de los archivos de sistema	**43%**
12.4.1 Control del software en explotación	20%
12.4.2 Protección de los datos de prueba del sistema	40%
12.4.3 Control de acceso al código fuente de los programas	70%
12.5 Seguridad en los procesos de desarrollo y soporte	**50%**
12.5.1 Procedimientos de control de cambios	60%
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el SO	40%
12.5.3 Restricciones a los cambios en los paquetes de software	50%
12.5.4 Fugas de información	50%
12.5.5 Externalización del desarrollo de software	N.A. - No aplica
12.6 Gestión de la vulnerabilidad técnica	**70%**
12.6.1 Control de las vulnerabilidades técnicas	70%

Tanto en sistemas como en el área de desarrollo, la seguridad se considera un pilar importante.

En el área de desarrollo tienen en consideración aspectos de seguridad durante todo el ciclo de vida en el desarrollo de software.

Para conseguirlo, los trabajadores disponen de material, manuales y cursos de formación para el desarrollo seguro de aplicaciones. Existen implantados sistemas de detección que ayudan a pulir fallos en el desarrollo.

No se mantienen procedimientos para controlar el software en explotación.

Gestión de incidencias de seguridad de la información

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	54%
13.1 Notificación de eventos y puntos débiles de seguridad de la información	**65%**
13.1.1 Notificación de los eventos de seguridad de la información	70%
13.1.2 Notificación de puntos débiles de seguridad	60%
13.2 Gestión de incidentes y mejoras de seguridad de la información	**43%**
13.2.1 Responsabilidades y procedimientos	50%
13.2.2 Aprendizaje de los incidentes de seguridad de la información	50%
13.2.3 Recopilación de evidencias	30%

ConTec S.L tiene implantados sistemas de monitorización ante fallos en sus sistemas, por lo que estos fallos se reportan rápidamente al responsable del área de sistemas que gestionará la incidencia. No tienen documentadas todas las guías de actuación ante incidencias que han sufrido, aunque se van añadiendo a una base de datos de incidencias.

Gestión de la continuidad de negocio

14. GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	10%
14.1 Aspectos de seguridad de la información en la gestión de la continuidad de negocio	**10%**
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad de negocio	30%
14.1.2 Continuidad del negocio y evaluación de riesgos	0%
14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	10%
14.1.4 Marco de referencia para la planificación de la continuidad del negocio	0%
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad	10%

A pesar de mantener algún pequñeo manual de recuperación ante desastre en los procesos críticos para así reducir los tiempo de interrupción que puedan resultar de desastres naturales, accidentes, fallos en los equipos o acciones deliberadas, estos manuales no están correctamente documentados y aceptados formalmente por los responsables.

No hay un plan estratégico para determinar un enfoque global de la continuidad del negocio. Los eventos que pueden causar interrupciones a los procesos de negocio deben ser identificados, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información. Se debería desarrollar un

plan de mantenimiento para asegurar la disponibilidad para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas, tras la interrupción o la falla de los procesos críticos.

Existen instrucciones para asegurar la seguridad del personal y la protección de las instalaciones de procesamiento y de la propiedad de la organización. Se han realizado varios simulacros de incendio.

Cumplimiento

15. CUMPLIMIENTO	32%
15.1 Cumplimiento de los requisitos legales	**60%**
15.1.1 Identificación de la legislación aplicable	70%
15.1.2 Derechos de propiedad intelectual (DPI)	60%
15.1.3 Protección de los documentos de la organización	70%
15.1.4 Protección de datos y privacidad de la información de carácter personal	80%
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información	60%
15.1.6 Regulación de los controles criptográficos	20%
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	**20%**
15.2.1 Cumplimiento de las políticas y normas de seguridad	20%
15.2.2 Comprobación del cumplimiento técnico	20%
15.3 Consideraciones sobre las auditorías de los sistemas de la información	**15%**
15.3.1 Controles de auditoría de los sistemas de información	20%
15.3.2 Protección de las herramientas de auditoría de los sistemas de la información	10%

ConTec S.L. cumple con la ley de Protección de Datos de Carácter Personal.

Por el contrario, no se comprueba si los trabajadores del departamento de desarrollo se instalan software autorizado y productos bajo licencia. Los trabajadores pueden instalarse software de fuentes no confiables.

Tampoco se llevan a cabo auditorías de sistemas por parte de terceros.

10.11. Anexo XI – Informe de auditoría

Datos de la auditoría de certificación

Empresa y razón social
ConTec S.L.

Fecha y lugar de realización
La auditoria se ha realizado entre el 10 y el 24 de Mayo de 2013 en las oficinas del cliente.

Alcance de la certificación

El alcance del sistema de gestión de seguridad de la información consiste en reforzar la seguridad en los servicios y procesos internos en las tecnologías de la información de la compañía al ser uno de los principales responsables del tratamiento y conservación de la información

Tipo de Auditoría de certificación

- ☒ Inicial
- ❑ Seguimiento.
- ❑ Renovación
- ❑ Ampliación
- ❑ Extraordinaria (Precisar el motivo)

Norma aplicable

- ❑ ISO 27001:2005

Resultados de la auditoría

NORMA ISO 27001:2005	NC MAYORES	NC MENORES	OBSERVACIONES
5. Política de seguridad	0	1	0
6. Aspectos organizativos de la seguridad de la información	0	2	0
7. Gestión de activos	1	1	0
8. Seguridad ligada a los recursos humanos	0	3	0
9. Seguridad física y del entorno	0	2	0
10. Gestión de comunicaciones y operaciones	0	9	0
11. Control de acceso	0	7	0
12. Adquisición, desarrollo y mantenimiento de sistemas de información	0	6	0
13. Gestión de incidentes en la seguridad de la información	0	2	0
14. Gestión de la continuidad del negocio	1	0	0
15. Cumplimiento	0	3	0

- Número total de no conformidades mayores: 2
- Número total de no conformidades menores: 36
- Número total de observaciones: 0

Valoración del SGSI de la organización

Evaluación del análisis y gestión de riesgos

REQUISITOS DOCUMENTALES	Pto ISO 27001	REVISADO	NC MAYOR	NC MENOR	OBSERVACIÓN
Metodología análisis de riesgos	4.2.1 4.3.1	Sí	0	1	0
Criterios de aceptación del riesgo	4.2.1	Sí	0	1	0
Análisis y evaluación del riesgo	4.2.1 4.3.1	Sí	0	1	0
Gestión del riesgo	4.2.1	Sí	0	1	0
Aprobación del riesgo residual	4.2.1	Sí	0	1	0
Plan de tratamiento de riesgos	4.2.2 4.3.1	Sí	0	1	0
Revisión de niveles de riesgo residual y aceptable	4.2.3	Sí	0	1	0

Fichas de no conformidad

Dominio	4. Sistema de gestión de seguridad de la información		
No-Conformidad:	**NC/1**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**7**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Metodología análisis de riesgos

- Existe documentación pero no existe una estructura homogénea, nomenclatura o terminología en común, por lo que dificulta la interpretación y gestión

[NC Menor] Criterios de aceptación del riesgo

- Existe documentación pero no existe una estructura homogénea, nomenclatura o terminología en común, por lo que dificulta la interpretación y gestión

[NC Menor] Análisis y evaluación del riesgo

- Existe documentación pero no existe una estructura homogénea, nomenclatura o terminología en común, por lo que dificulta la interpretación y gestión

[NC Menor] Gestión del riesgo

- Existe documentación pero no existe una estructura homogénea, nomenclatura o terminología en común, por lo que dificulta la interpretación y gestión

[NC Menor] Aprobación del riesgo residual

- Existe documentación pero no existe una estructura homogénea, nomenclatura o terminología en común, por lo que dificulta la interpretación y gestión

[NC Menor] Plan de tratamiento de riesgos

- Existe documentación pero no existe una estructura homogénea, nomenclatura o terminología en común, por lo que dificulta la interpretación y gestión

[NC Menor] Revisión de niveles de riesgo residual y aceptable

- Existe documentación pero no existe una estructura homogénea, nomenclatura o terminología en común, por lo que dificulta la interpretación y gestión

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

• Establecer procedimientos formalmente documentados debidamente estructurados, y con una nomenclatura y terminología en común del sistema de gestión de seguridad de la información. Estos documentos deben ser revisados y actualizados conforme sea necesario, manteniéndolos legibles y fácilmente identificables	**Responsable implantación:**
	Fecha prevista implantación: 1 / 6 / 2013
	Representante empresa:
	Firma:

Dominio	5. Política de seguridad		
No-Conformidad:	**NC/2**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**1**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Política de seguridad de la información:

- A pesar de haber elaborado documentación en forma de manual o instrucciones sobre ciertos apartados de seguridad, éstos no tienen una estructura homogénea, nomenclatura o terminología en común, por lo que dificulta la interpretación y gestión. No dispone de una línea clara de procedimientos o líneas de actuaciones globales alineados con los objetivos de negocio para poder constituir una política de seguridad.

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (DOC-013: Política de seguridad de la información): • Creación de la política de seguridad de la información según los requisitos de negocio de la compañía, junto con una política de revisión con tal de asegurar su efectividad según periodos de tiempo establecidos.	**Responsable implantación:** **Fecha prevista implantación:** 1 / 7 / 2013 **Representante empresa:** **Firma:**

Dominio	6. Aspectos organizativos de la seguridad de la información		
No-Conformidad:	**NC/3**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**2**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Organización interna:

- No existe una estructura organizativa interna correctamente definida con responsabilidades directas sobre la seguridad de la información que pueda asegurar que se implante correctamente un SGSI

[NC Menor] Terceros

- No existen procedimientos sobre autoridades con las que contactar, ni de la información que debe ser reportada en caso de vulnerar alguna ley o incidente

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (DOC-014: Revisión de aspectos organizativos internos): • Revisión de la coordinación en aspectos relacionados con la seguridad de la información depurando las responsabilidades. • Establecimiento de contactos con fuentes especializadas de consulta en seguridad de la información	**Responsable implantación:** **Fecha prevista implantación:** 1 / 8 / 2013 **Representante empresa:**

• Establecimiento de procedimientos para la revisión de la gestión de la seguridad de la información de forma independiente.	**Firma:**

Dominio	7. Gestión de activos		
No-Conformidad:	**NC/4**	**Fecha:**	20/05/13
NC Mayor:	**1**	**NC menor:**	**1**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Mayor] Clasificación de la información

- No existe ningún sistema de clasificación de la información

[NC Menor] Responsabilidad sobre los activos

- Se mantiene un inventario de activos pero es insuficiente, sin procedimientos de mantenimiento ni actualización. Tampoco existe ningún sistema formal del uso correcto de los ordenadores usados directamente por los empleados

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (DOC-005: Gestión del inventario de activos): • Política de gestión del inventario con tal de mantenerlo actualizado y correctamente identificado, incluyendo la propiedad de cada uno de los activos y la normativa de uso Acciones recomendadas incluidas en el documento (DOC-004: Clasificación de la información): • Establecer un esquema de clasificación de la información según su valor, requisitos legales y criticidad. Según el baremo, se establecerán distintos niveles de protección.	**Responsable implantación:** **Fecha prevista implantación:** 1 / 12 / 2013 **Representante empresa:** **Firma:**

Dominio	8. Seguridad relativa a los recursos humanos		
No-Conformidad:	**NC/5**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**3**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Antes del empleo

- No existe documentación formal sobre las responsabilidades de los empleados según la política de seguridad de la compañía

[NC Menor] Durante el empleo

- No existe un proceso disciplinario formal y establecido con tal de prevenir que empleados, contratistas o terceros puedan violar las políticas de seguridad de la compañía.

NC Menor] Cese del empleo o cambio de puesto de trabajo

- No existe procedimiento formal y establecido sobre la política de retirada de derechos de acceso al termino del contrato de un empleado

Nombre representante de la empresa:	Nombre del Auditor:	Nombre del Auditor Jefe:
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (DOC-012: Revisión documentación relacionada con RRHH) • Se establecerá un proceso disciplinario para gestionar las brechas de seguridad, además de asegurar un adecuado nivel de concienciación y educación en seguridad durante la etapa en la compañía. • Eliminación de todos los derechos de acceso y retorno de todo el material usado por parte de los empleados que finalizan contrato.	**Responsable implantación:** **Fecha prevista implantación:** 1 / 10/ 2014 **Representante empresa:** **Firma:**

Dominio	9. Seguridad física y del entorno		
No-Conformidad:	**NC/6**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**2**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Áreas seguras

- Acceso al CPD de la oficina únicamente con llave

[NC Menor] Seguridad de los equipos

- No existe una política de seguridad con respecto a los equipos fuera de las instalaciones, ni implementaciones seguras de los equipos en caso de pérdida o robo. Tampoco hay normas sobre reutilización o retirada segura de equipos.

Nombre representante de la empresa:	Nombre del Auditor:	Nombre del Auditor Jefe:
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (INF-011: Nuevo sistema de acceso al CPD) • Implantación de un sistema de control de acceso por tarjeta que mejore el sistema actual Acciones recomendadas incluidas en el documento (IMP-002: Securización de portátiles de guardia) • Establecer una política de seguridad y mejora de las medidas de seguridad referentes a los portátiles de guardia Acciones recomendadas incluidas en el documento (DOC-008: Política de retirada de equipos y material) • Establecer procedimientos de revisión de equipos o dispositivos antes de retirarlos. Se especifica una guía sobre almacenamiento y borrado seguro de la información.	**Responsable implantación:** **Fecha prevista implantación:** 1 / 2/ 2014 **Representante empresa:** **Firma:**

Dominio	10. Gestión de comunicaciones y operaciones		
No-Conformidad:	**NC/7**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**9**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Responsabilidades y procedimientos de operación

- La documentación referente a los procedimientos de operación no está correctamente documentada y no existen procedimientos sobre la segregación de tareas.

[NC Menor] Gestión de la provisión de servicios por terceros

- Se deberían establecer controles cuantitativos sobre la gestión de la provisión de servicios por terceros.

[NC Menor] Planificación y aceptación del sistema

- No se tienen definidos claramente criterios de aceptación en los nuevos sistemas.

[NC Menor] Protección contra el código malicioso y descargable

- No se revisa regularmente el software en búsqueda de software malicioso, ni existen procedimientos y responsabilidades de administración para la utilización de la protección antivirus.

[NC Menor] Copias de seguridad

- No se realizan pruebas sobre la copias de seguridad en caso de incidente.

[NC Menor] Gestión de la seguridad de las redes

- Se deberían implantar controles cuantitativos sobre la gestión de la seguridad de la red**.**

[NC Menor] Manipulación de los soportes

- No existe un procedimiento de extracción segura de soportes extraíbles.

[NC Menor] Intercambio de información

- No existe procedimiento o política formal de intercambio de información

[NC Menor] Supervisión

- No hay procedimientos para mantener sincronizados los relojes de los sistemas de información

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (IMP-001: Administración de estaciones de trabajo y portátiles de guardia): • Mejora de la seguridad en los puestos de trabajo Acciones recomendadas incluidas en el documento (IMP-005: Mejora en servicio de transferencia de ficheros): • Creación de una política de intercambio seguro , además de procedimientos y normas para proteger la información y los dispositivos físicos que la almacenen. Acciones recomendadas incluidas en el documento (DOC-003: Revisión de política de backups y gestión de datos): • Definición de procedimientos para la realización de copias de seguridad y de pruebas para testearlas por si sucede algún incidente de seguridad. Se gestionarán la separación de datos para restringir el acceso únicamente a personal autorizado. Acciones recomendadas incluidas en el documento (DOC-001: Política de gestión de logs): • Se definen reglas para mantener un sistema de monitorización de eventos de seguridad y de sincronización de reloj.	**Responsable implantación:** **Fecha prevista implantación:** 1/ 8/ 2013 **Representante empresa:** **Firma:**

Dominio	11. Control de acceso		
No-Conformidad:	**NC/8**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**7**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Requisitos de negocio para el control de acceso

- No existe una política de control de acceso establecida, documentada y revisada

[NC Menor] Gestión de acceso de usuario

- No existen procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas

[NC Menor] Responsabilidades de usuario

- No existe una política de puestos de trabajo despejado y pantalla limpia

[NC Menor] Control de acceso a la red

- No existen procedimientos formales para la protección de los puertos de diagnóstico y configuración remotos.

[NC Menor] Control de acceso al sistema operativo

- Se debería establecer un procedimiento formal sobre la desconexión automática de la sesión o limitación del tiempo de conexión

[NC Menor] Control de acceso a las aplicaciones y a la información

- Los activos con información sensible deberían ser aislados

[NC Menor] Ordenadores portátiles y teletrabajo

- Medidas de seguridad insuficiente en los portátiles de guardia

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (DOC-002: Revisión de política de control de acceso):

- Definición de controles para asegurar la protección de la red, los sistemas operativos, aplicaciones y especialmente de la información, de tal manera que se restringe el acceso a todo el personal que no deba poder acceder al activo.

Acciones recomendadas incluidas en el documento (IMP-001: Administración de estaciones de trabajo y portátiles de guardia):

- Mejora de la seguridad en los puestos de trabajo

Acciones recomendadas incluidas en el documento (IMP-002: Securización de portátiles de guardia)

- Establecer una política de seguridad y mejora de las medidas de seguridad referentes a los portátiles de guardia

Responsable implantación:

Fecha prevista implantación: 1/ 8 / 2013

Representante empresa:

Firma:

Dominio	12. Adquisición, desarrollo y mantenimiento de sistemas de información		
No-Conformidad:	**NC/9**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**6**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Requisitos de seguridad de los sistemas de información

- No se identifican completamente todos los requisitos de seguridad para sistemas nuevos o mejoras en los existentes

[NC Menor] Tratamiento correcto de las aplicaciones

- Se deben aplicar controles cuantitativos sobre las validaciones de los datos de entrada y salida

[NC Menor] Controles criptográficos

- Se debería mantener una política de cambios de credenciales

[NC Menor] Seguridad de los archivos del sistema

- No se tienen implementado procedimientos para controlar el software en explotación, de los sistemas así como su documentación

[NC Menor] Seguridad en los procesos de desarrollo y soporte

- No existe procedimiento formal para revisar las aplicaciones cuando se efectúan cambios o actualizaciones en el sistema

[NC Menor] Gestión de la vulnerabilidad técnica

- Falta por definir una línea de tiempo para reaccionar ante vulnerabilidades técnicas, definiendo el riesgo y las acciones a tomar

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (DOC-006: Política de mantenimiento de los sistemas de la información): • Establecer procedimientos y responsabilidades a la hora de gestionar el mantenimiento y seguridad de los sistemas de la información.	**Responsable implantación:** **Fecha prevista implantación:** 1/ 1 / 2014 **Representante empresa:** **Firma:**

Dominio	13. Gestión de incidentes en la seguridad de la información		
No-Conformidad:	**NC/10**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**2**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Notificación de eventos y puntos débiles de seguridad la información

- No se dispone de un procedimiento formal para que los empleados puedan reportar cualquier fallo encontrado o sospechas sobre la seguridad de alguno de los activos.

[NC Menor] Gestión de incidentes y mejoras de seguridad de la información

- No tienen documentadas todas las guías de actuación ante incidentes que han sufrido, aunque se van añadiendo a una base de datos de incidencias

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (DOC-007: Política de tratamiento de incidentes de seguridad): • Establecer procedimientos y responsabilidades a la hora de gestionar sucesos o fallos de seguridad de una forma efectiva	**Responsable implantación:** **Fecha prevista implantación:** 1/ 3 / 2014 **Representante empresa:** **Firma:**

Dominio	14.Gestión de la continuidad de negocio		
No-Conformidad:	**NC/11**	**Fecha:**	20/05/13
NC Mayor:	**1**	**NC menor:**	**0**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Mayor] Aspectos de seguridad de la información en la gestión de la continuidad de negocio

- Existen ciertos manuales de recuperación frente a desastres, aún así no hay un plan estratégico para determinar un enfoque global con tal de asegurar la continuidad del negocio

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (DOC-011: Plan de continuidad de negocio): • Creación de un plan para asegurar la continuidad de negocio reduciendo a niveles aceptables la interrupción causada por un desastre o fallo de seguridad mediante controles preventivos y de recuperación.	**Responsable implantación:** **Fecha prevista implantación:** 1/ 6 / 2014 **Representante empresa:** **Firma:**

Dominio	15. Cumplimiento		
No-Conformidad:	**NC/12**	**Fecha:**	20/05/13
NC Mayor:	**0**	**NC menor:**	**3**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

[NC Menor] Cumplimiento de los requisitos legales

- No se comprueba si los trabajadores del departamento de desarrollo se instalan software autorizado y productos bajo licencia.

[NC Menor] Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

- No existen procedimientos formales para la revisión regular , de forma planeada y documentada sobre la conformidad técnica

[NC Menor] Consideraciones sobre las auditorías de los sistemas de la información

- No se llevan a cabo auditorias externas

Nombre representante de la empresa:	**Nombre del Auditor:**	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acciones recomendadas incluidas en el documento (DOC-009: Cumplimiento de requisitos legales y políticas de la compañía): • Establecimiento de documentos actualizados para mantener de forma explícita todos los requisitos legales, regulatorios y contractuales importantes para los sistemas de la información. Se establecerán procedimientos para revisar la seguridad de los sistemas según las políticas de seguridad de la compañía.	**Responsable implantación:** **Fecha prevista implantación:** 1/ 10 / 2013 **Representante empresa:**

Acciones recomendadas incluidas en el documento (DOC-010: Gestión de auditorías de sistemas): • Establecimiento de controles para la realización de auditorías externas con el fin de minimizar el riesgo a interrupciones que afecten la actividad de la compañía	**Firma:**