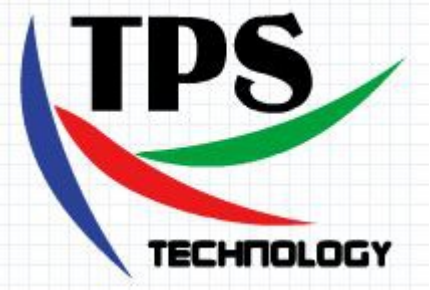
Màster Interuniversitari en Seguretat de les TIC (MISTIC)

Plan Director de Seguridad



Autor: José Consuegra del Pino

Tutor: Arsenio Tortajada Gallego

Universitat Oberta de Catalunya

Realizado durante Curso: 01-2013

Dedicatoria y Agradecimientos

Quisiera dedicar la realización de este trabajo a mi esposa Isabel por su infinita paciencia y por su apoyo incondicional a todo lo que hago.

Agradecer a mis compañeros de trabajo Sergio Dijort y Fran Català su apoyo moral durante todos estos meses.

Resumen

El proyecto expuesto en este documento forma parte del Trabajo Final del “Máster Inter-universitario en Seguridad de las Tecnologías de la información y la Comunicación” y tiene como objeto el desarrollo de un análisis para la implantación de un Sistema de Gestión de Seguridad de la Información dentro de una organización.

Un Sistema de Gestión de la Seguridad de la Información es un conjunto de políticas de administración de la información que conlleva el elaborar, mantener y mejorar un esquema documental, un proceso de gestión de la seguridad y unos procedimientos que permitan gestionar todo el conjunto.

El SGSI se ha de integrar en la organización de manera que se convierta en una parte fundamental de la gestión de ésta. Un SGSI correctamente implantado permite establecer procedimientos que aseguren la Confidencialidad, Disponibilidad e Integridad de la información que se gestiona en el organización.

En el desarrollo de este trabajo se han seguido las directrices establecidas en la norma ISO 27001, que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI mediante el “ciclo de Deming” o “PDCA” que establece cuatro fases de actuación (Plan-Do-Check-Act).

La organización sobre la que se ha realizado este trabajo es una empresa real que presta servicios en el ámbito de las telecomunicaciones aunque su nombre real no aparece en el trabajo por deseo expreso de la dirección de la empresa que ha dado su apoyo a la realización de este trabajo bajo esa condición.

Summary

The project exposed in this document is part of the End-Of-Master Work of the “Inter-University Master of Security in Information Technology and Communications” and has the aim of developing an analysis to implant an Information Security Management System in an organization.

An Information Security Management System is a set of information administration policies which involves to elaborate, maintain and improve a documentation schema, a security management process and procedures to manage the whole set.

The ISMS has to be integrated in the organization to allow it become in an essential part of its management. A correctly implanted ISMS allows to establish procedures to ensure the confidentiality, availability and integrity of the information managed by the organization.

In the development of this work we have followed the guidelines set in ISO 27001, which specify the requirements for establishing, implementing, maintaining and improving an ISMS through the "Deming cycle" or "PDCA" that establishes four phases of action (Plan-Do-Check-Act).

The organization on which this work has been performed is a real-world company who provides services in the area of telecommunications although his real name has not been revealed in this document because an express company directive, who has given its support to the realization of this work under that condition.

Índice de contenido

Índice de ilustraciones

Índice de tablas

Introducción

Justificación

En el mundo actual es indudable que la información es un bien con un valor intrínseco de gran magnitud.

Las organizaciones gestionan cantidades ingentes de información de muchos tipos y sensibilidades, gracias a las Tecnologías de la información.

Debido a la importancia de la información que gestionan se ha perfilado la necesidad de establecer mecanismos para garantizar la Seguridad de la Información, ya sea por requerimientos legales (LOPD), por evitar que la información pueda ser revelada a un competidor, o por exigencias contractuales con un cliente o un proveedor, etc.

En cualquier caso, por muchos motivos, es preciso que las organizaciones cuenten con un proceso de Seguridad de la información que esté completamente integrado dentro de su esquema gestión.

Este proceso es el conocido como Sistema de Gestión de Seguridad de la Información (SGSI).

Un SGSI correctamente implementado permite minimizar la materialización de las amenazas sobre los activos de información, así como minimizar el impacto sobre éstos en caso de que las amenazas se materialicen. Todo ello, dentro del marco de un proceso de mejora continua del SGSI que garantiza que está en continua revisión a fin de mejorar la eficiencia y el desempeño de éste.

Un SGSI correctamente implantado permite asegurar que la información:

a) Solamente será revelada a las personas autorizadas (Confidencialidad)

b) Sea consistente y completa (Integridad)

c) Será accedida por las personas autorizadas cuando éstas lo necesiten (Disponibilidad)

Objetivos

Llevar a cabo un análisis para la implantación de un SGSI en la organización “TPS Technology”.

Este análisis se desarrollará dentro de las directrices establecidas en la norma ISO-27001 y tendrá como resultados:

- Un análisis de contexto y de la situación inicial de la seguridad de la información en la organización.
- Elaboración del esquema documental del SGSI requerido por la norma.
- Confección de un Análisis de Riesgos de los activos de la organización.
- Elaboración de Propuestas de proyectos sobre el Análisis de Riesgos realizado e identificación de los proyectos cuya relación inversión-tiempo-beneficio sea más favorable.
- Análisis de situación actual a través de una auditoría de cumplimiento.

Enfoque

El análisis se lleva a cabo desde la perspectiva de una persona que conoce la organización en profundidad. Además, tiene un conocimiento amplio de sus procedimientos, prioridades y limitaciones.

Método

Para la implantación del SGSI se seguirá el modelo PDCA que a su vez sigue la norma ISO-27001

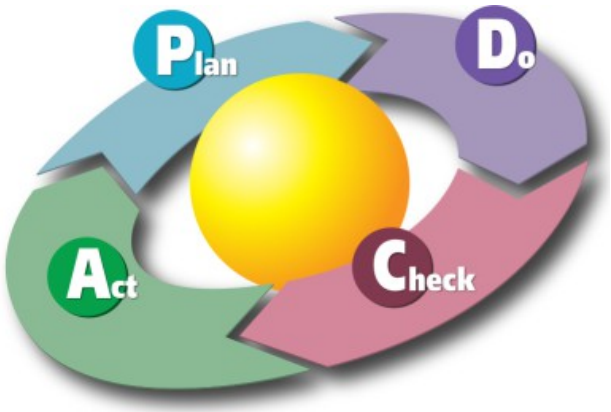


Ilustración 1: Ciclo de Deming

- **Plan**: Establecer el SGSI (definición de la política, objetivos, procesos y procedimientos relevantes).
- **Do**: Implementar y operar el SGSI.
- **Check**: Monitorizar y revisar el SGSI (Evaluar y medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas).
- **Act**: Mantener y mejorar el SGSI (tomar acciones correctivas y preventivas basadas en los resultados de la auditoría interna del SGSI y de la revisión por la dirección u otras fuentes relevantes).

Este modelo cíclico de mejora continua establece el proceso del SGSI y permite alcanzar los objetivos establecidos en diferentes iteraciones, de tal manera que cada iteración supone una ampliación gradual del SGSI, incorporando mejoras y lecciones aprendidas en las iteraciones anteriores.

Planificación del Trabajo

El trabajo desarrollado se ha hecho siguiendo el plan de entregas establecido en el calendario de la asignatura:

Fase	Fecha de Entrega
[1] Situación Actual: Contextualización, objetivos y análisis diferencial	15 de Marzo de 2013
[2] Sistema de Gestión Documental	28 de Marzo de 2013
[3] Análisis de Riesgos	19 de Abril de 2013
[4] Propuestas de Proyectos	10 de Mayo de 2013
[5] Auditoría de cumplimiento de ISO/IEC 27002:2005	24 de Mayo de 2013
[6] Presentación de Resultados y entrega de Informes	7 Junio de 2013

Situación Inicial: Contextualización, objetivos y análisis diferencial

Enfoque y selección de la empresa

La empresa TPS Technology tiene su ámbito de negocio en la Definición, Implementación y Mantenimiento de Tecnologías de la Información y la Comunicación.

El tipo de cliente al que se orienta son las medianas y grandes empresas de ámbito nacional e internacional.

El capital humano de TPS Technology está formado por 40 personas entre personal técnico, Directivos, personal de “BackOffice” y Comercial.

La actividad de la compañía se desempeña principalmente en las oficinas ubicadas en la ciudad de Castelldefels.

El Catálogo general de Servicios ofrecidos por la empresa se divide en tres ámbitos:

- Mantenimiento y Desarrollo de Software
- Administración, e Implantación de Bases de Datos
- Administración e Implantación de Sistemas operativos

Estos servicios se ofrecen mayoritariamente mediante conexiones VPN desde las oficinas de la compañía a las redes del cliente.

Si se considera necesario, los técnicos se desplazan a las dependencias del cliente para realizar trabajos puntuales o desarrollar proyectos.

Diagrama Organizativo

A continuación se presenta un diagrama que presenta las diferentes divisiones de la compañía:

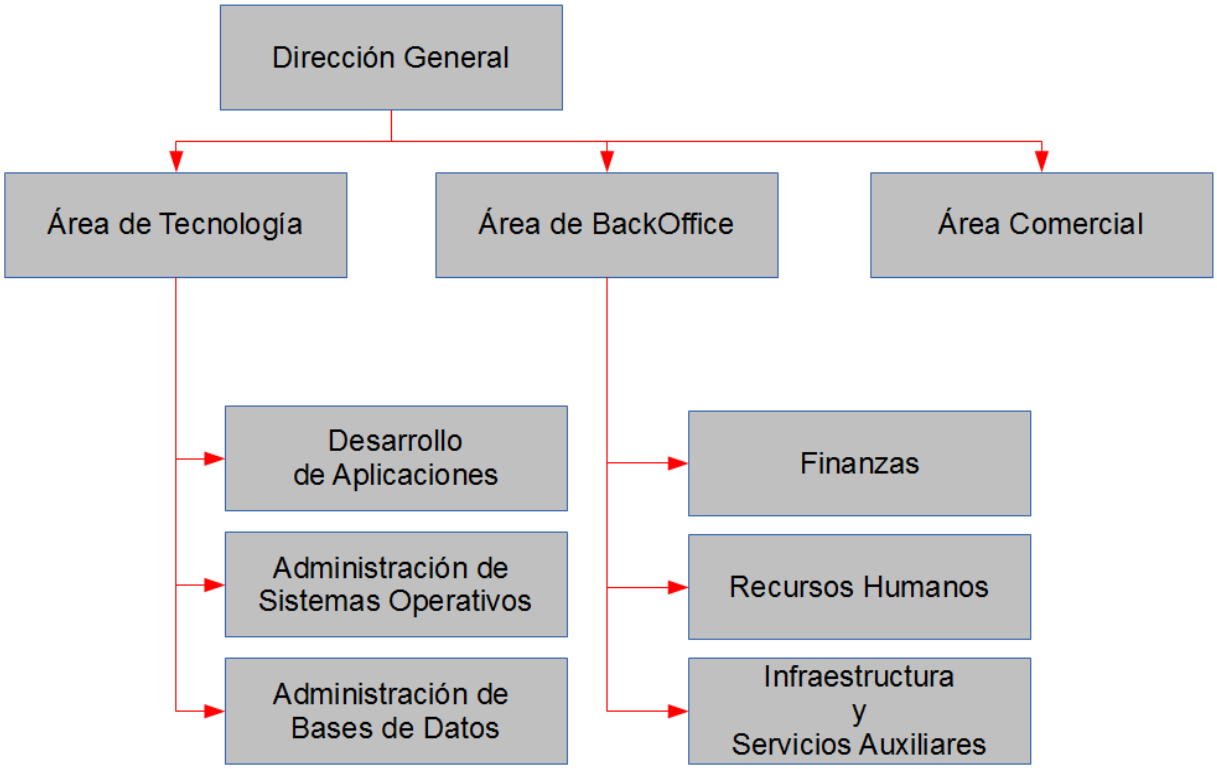


Ilustración 2: Diagrama Organizativo

Cada una de las Áreas y Sub-Áreas tiene asignado un responsable a su cargo.

A continuación se detallan cada una de las Áreas y Sub-Áreas que se muestran en el diagrama:

Dirección General

Área ejecutiva de la compañía desde la que se toman las decisiones estratégicas y las que pueden suponer un impacto global en la organización.

Área de Tecnología

Es el área donde se desempeña la actividad que constituye el núcleo del negocio de la compañía. Está compuesta de las siguientes Sub-Áreas:

Desarrollo de Aplicaciones

La actividad principal de este área es la de realizar proyectos de Desarrollo de aplicaciones informáticas y el mantenimiento de éstas.

Para ello, cuenta con un equipo de Jefes de Proyecto, Analistas y Programadores especializados en desarrollar aplicaciones para diferentes plataformas (cliente-servidor, dispositivos móviles, etc).

Las aplicaciones se desarrollan tanto para uso interno como para terceros (clientes).

El área de Desarrollo de aplicaciones está formada por el Responsable del Área, tres jefes de equipo (Analistas), y 6 desarrolladores de aplicaciones (2 por cada uno de los tres equipos).

Administración de Sistemas Operativos

Este área está integrada por personal cualificado en la Administración de sistemas operativos y servicios asociados a éstos, como pueden ser directorios de Usuarios, Cortafuegos, Monitores de Sistemas y Servicios, Gestores de Procesos, Antivirus, Sistemas de detección de Intrusos, etc.

El equipo de profesionales lo forman Administradores especializados en sistemas operativos de las familias Microsoft Windows, Unix (en sus diversas variantes), así como en los servicios descritos en el párrafo anterior.

Al igual que en el Área de Desarrollo de Aplicaciones, se administran tanto Sistemas Operativos de los clientes como los sistemas operativos de la compañía.

El área de Administración de Sistemas operativos cuenta actualmente con 10 personas, que son, el responsable del área y nueve personas más que están a su cargo.

Administración de Bases de Datos

Los profesionales que integran este Área llevan a cabo tareas asociadas a la implantación y mantenimiento de Sistemas Gestores de Bases de Datos, concretamente Oracle y Microsoft SQL Server.

El catálogo de Servicios que se desempeñan incluye la instalación, monitorización, gestión de seguridad, gestión de almacenamiento, ajustes de rendimiento y resolución de incidencias, entre otros más específicos.

El área de Administración de base de datos está liderada por un responsable de área que tiene a su cargo a siete personas más.

Área de BackOffice

El Área de BackOffice gestiona servicios esenciales para el funcionamiento de la compañía así como para el cumplimiento de las normativas vigentes.

Está compuesta de las Sub-Áreas siguientes:

Finanzas

Se encarga de gestionar los recursos económicos y financieros de la empresa.

El personal que forma este área tiene formación en gestión administrativa y financiera.

Entre sus funciones se encuentra la gestión de clientes, proveedores, facturación, compras, gestión del patrimonio de la empresa, vehículos, amortizaciones, etc.

Finanzas está formado actualmente por tres personas.

Recursos Humanos

El Sub-Área de Recursos Humanos se encarga de llevar a cabo las gestiones relacionadas con el Personal de la Empresa.

Las personas que integran Recursos Humanos llevan a cabo tareas de Selección de Personal, formación y desarrollo profesional, gestión de nóminas, prevención de riesgos laborales, etc.

Actualmente RRHH cuenta con dos personas para desempeñar las funciones descritas.

Servicios Auxiliares

Las funciones que se llevan a cabo en este área son las siguientes:

- Mantenimiento de las instalaciones de la compañía (limpieza, reparaciones menores de electricidad, fontanería, calefacción y Aire Acondicionado).
- Gestión del material (ordenadores, impresoras, fotocopiadoras, material de oficina, etc).
- Gestión de viajes. Los desplazamientos que tiene que llevar a cabo el personal de la empresa se organizan y se contratan desde este departamento.

El área de Servicios auxiliares está formada actualmente por dos personas.

Área Comercial

El Área Comercial es la encargada de ampliar el horizonte empresarial de la compañía.

Está formada por profesionales autónomos especializados en el trato con los clientes y en la negociación de contratos comerciales con éstos.

Su función principal es la de ampliar el negocio de la compañía, tanto en número de clientes como en el número y volumen de los contratos firmados con ellos.

Descripción de las Oficinas

A continuación se muestra un plano de las oficinas donde la compañía desempeña su actividad:

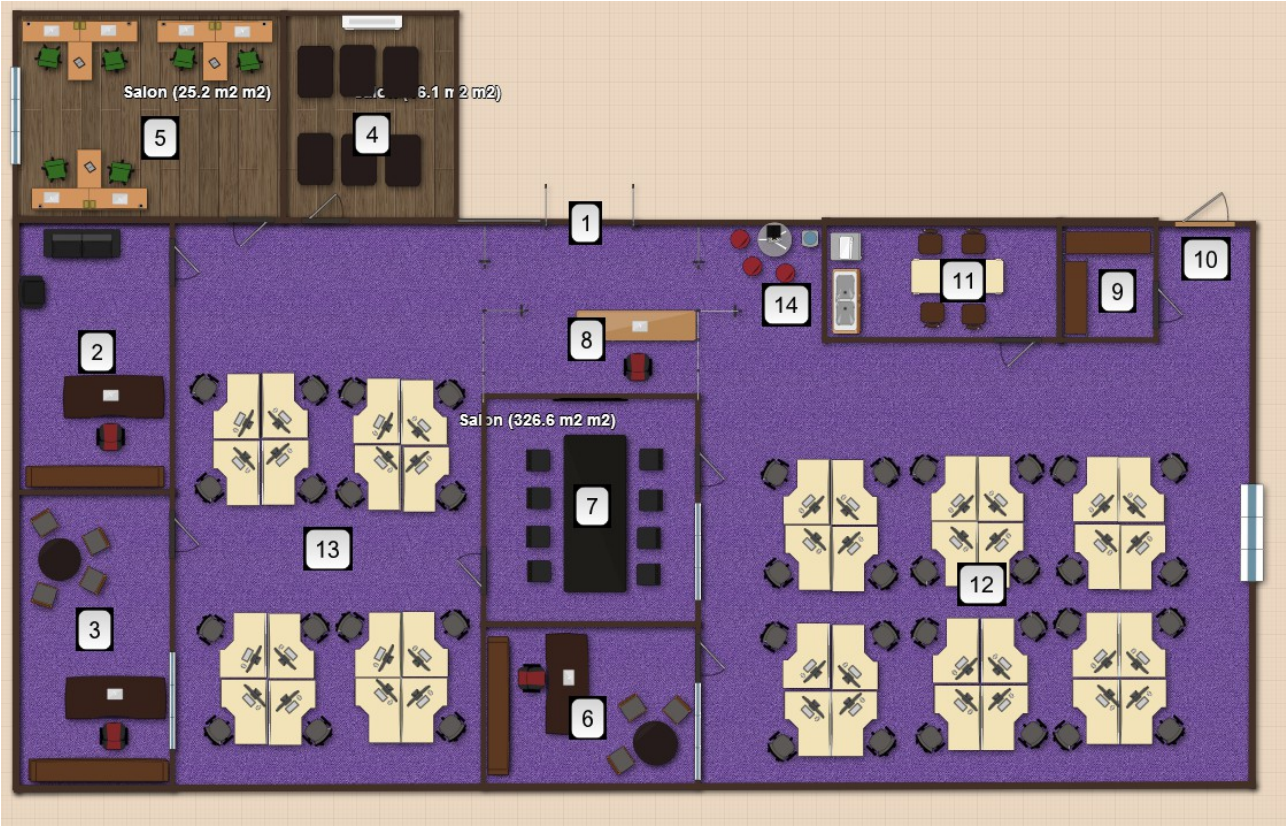


Ilustración 3: Descripción de las oficinas

1) Puerta de acceso a las oficinas

Los empleados validan su acceso a las oficinas a través de una tarjeta magnética que les identifica de manera unívoca.

Las visitas solicitan el acceso a las oficinas utilizando un timbre con video teléfono. La persona de recepción valida y registra el acceso de los visitantes.

2) Despacho del Director General:

El despacho del Director General cuenta con aislamiento acústico en las paredes.

La puerta del acceso al despacho se cierra con llave cuando el Director General no se encuentra en él.

3) Despacho del Director de BackOffice:

Al igual que el despacho del Director General, el despacho del Director de BackOffice cuenta con aislamiento acústico en las paredes. De la misma manera, la puerta del despacho queda cerrada con llave en ausencia del Director de BackOffice.

4) Sala de Servidores (CPD):

La sala de servidores alberga los servidores de la organización así como la infraestructura de comunicaciones (centralita, Internet, conexiones de red...).

Los dispositivos y los servidores están ubicados dentro de armarios especiales (Racks).

La sala cuenta con un SAI que asegura la alimentación en caso de corte de suministro eléctrico durante al menos 1 hora.

La sala cuenta además, con un equipo de refrigeración propio y un extintor.

El acceso a la sala se valida con un código de acceso que sólo conocen los Administradores de la sala y que se cambia periódicamente.

5) Sala de BackOffice:

La sala de BackOffice es el lugar de trabajo de las personas que integran el Área de BackOffice (RRHH, Finanzas y Servicios).

La sala cuenta con una puerta, aunque ésta no tiene cerradura.

6) Despacho del Director de Tecnología:

Al igual que los despachos del Director General y del Director de BackOffice, el despacho del Director de Tecnología cuenta con aislamiento acústico y la puerta queda cerrada cuando no se encuentra dentro.

7) Sala de Reuniones:

Esta sala se utiliza como sala de Reuniones. Es el lugar habitual donde se realizan presentaciones a los clientes, formación a los empleados, y reuniones de trabajo en general.

La sala está equipada con equipos audiovisuales (una TV de plasma de gran tamaño, un proyector, y un equipo de captación omnidireccional destinado a llevar a cabo conferencias telefónicas con asistentes remotos).

8) Recepción:

Es el lugar donde se verifica y registra el acceso de los visitantes a las dependencias de la organización.

Cuenta con dos butacas donde las visitas pueden esperar mientras la persona a la que visitan sale a recibirles.

La persona de recepción es la encargada de validar la identidad de los visitantes y registrar el acceso de éstos a las oficinas. Se proporciona a los visitantes una tarjeta identificativa que deben mantener visible en todo momento mientras permanezcan en las oficinas.

9) Archivo:

Es una dependencia destinada al almacenamiento documentación, software, discos duros, dispositivos extraíbles y cualquier dispositivo o soporte que pueda contener información sensible.

La puerta del archivo está cerrada con llave. La llave está en poder del responsable de RRHH y el Responsable de Finanzas.

10) Salida de Emergencia:

Se trata de una puerta que solamente se puede abrir desde dentro de las oficinas y que conecta directamente con el exterior.

El uso de esta puerta está solamente permitido en caso de emergencia.

11) Comedor:

Es una estancia donde los empleados disponen de los utensilios necesarios para poder consumir alimentos que traen desde sus casas o que hayan comprado en un comercio.

Dispone de una nevera, un horno microondas y un pequeño fregadero, además de una mesa y varias sillas.

12) Sala de Administradores:

Se trata del lugar de trabajo de los administradores de Sistemas y de Bases de Datos.

Cada una de las personas que trabajan en esta estancia disponen de un puesto de trabajo individual compuesto de una mesa, una silla, un ordenador conectado a la red corporativa, un teléfono fijo (cuyo número es una extensión de la centralita) y una cajonera con llave.

En esta sala hay dos mesas de trabajo reservadas para las necesidades de los comerciales que, de manera ocasional, pueden necesitar de un puesto para poder trabajar en la oficina (aunque es una situación poco frecuente, puesto que no están en plantilla y tienen sus propios despachos fuera de las dependencias de la compañía).

13) Sala de Desarrolladores:

Es la sala donde los Desarrolladores de Aplicaciones llevan a cabo su trabajo.

El puesto de trabajo de cada uno de los desarrolladores sigue la misma política que en el caso de los Administradores de Sistemas y de Bases de Datos (mesa, silla, ordenador, teléfono, cajonera con llave, etc).

14) “Coffee corner”:

Se trata de un espacio ubicado dentro de la sala de producción de los Administradores de Sistemas y Bases de Datos, equipado con un dispensador de agua, una máquina de café, y unas sillas.

La finalidad de este espacio es ser un lugar de descanso y reunión del personal dentro de la oficina.

Infraestructura de Red y Sistemas

A continuación se muestra un diagrama general de los elementos que forman la Red de la organización:

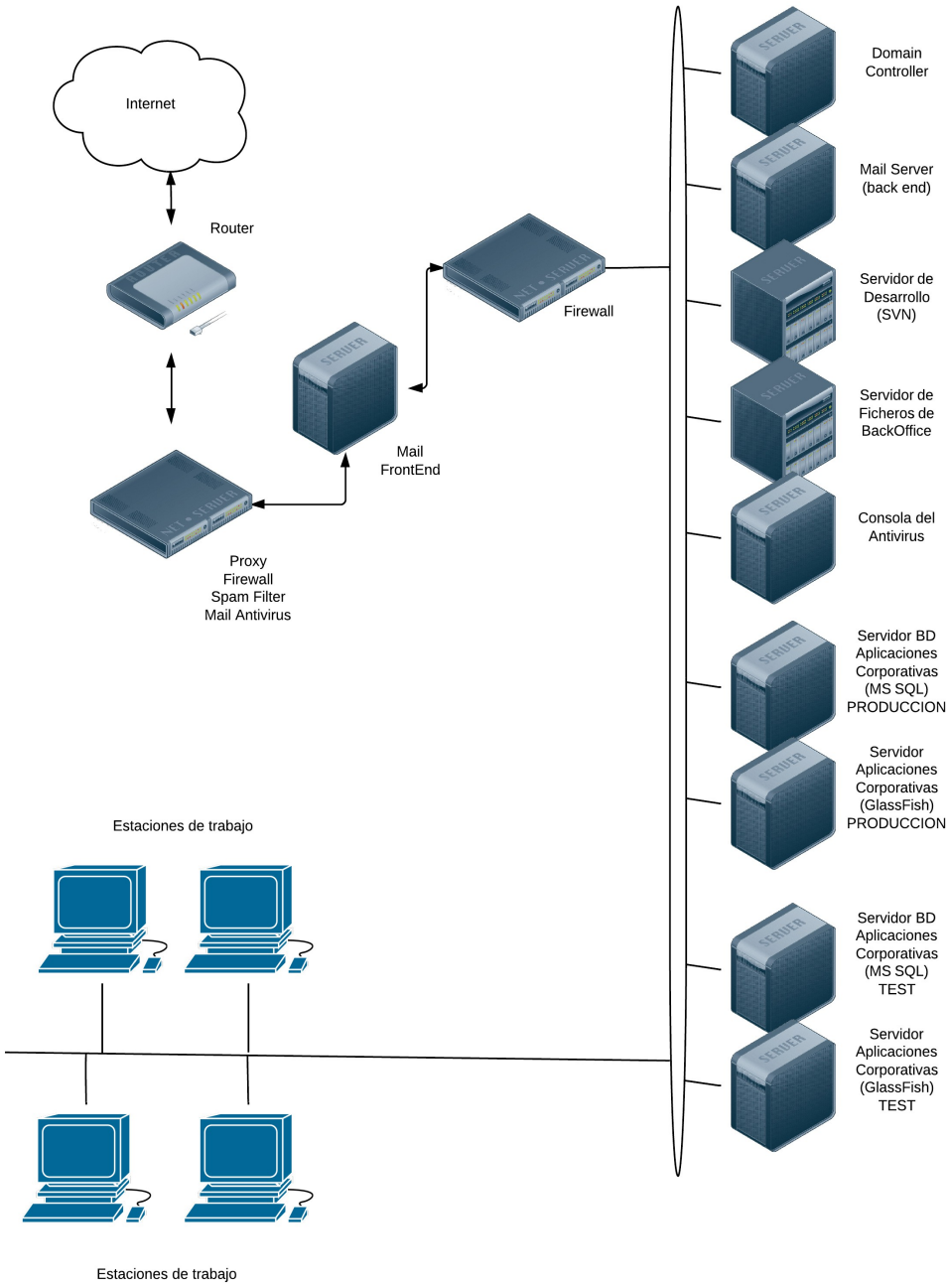


Ilustración 4: Diagrama de Sistemas

La gestión de los recursos de la red se lleva a cabo bajo un dominio de Microsoft Windows.

Todos los servidores excepto los “firewalls” funcionan bajo Microsoft Windows 2008. Los “firewalls” ejecutan una versión de linux adaptada para funcionar como “firewall” y proporcionar diversos servicios (Se trata de “Endian”. Más información en: http://www.endian.com/en/community/overview/).

El sistema operativo de los terminales de los equipos del Área de Tecnología es Microsoft Windows 7 Professional. Todos ellos tienen licencia y antivirus (Symantec) y se actualizan diariamente desde un Servidor Windows Update ubicado en el Servidor de la consola del Antivirus.

El detalle de los servidores es este:

- **Domain Controller:** Controlador de Dominio de la Red. Alberga el Directorio Activo y gestiona todas las credenciales así como los accesos a los recursos de la Red.
- **Mail Server Front-End:** Ubicado dentro de la DMZ, proporciona un acceso seguro por web desde el exterior al servidor de correo de Back-End. El Servidor de Front-End ejecuta Microsoft Internet Information Server y la aplicación “Outlook Web Access”.
- **Mail Server Back-End:** Ejecuta el servidor de Correo Microsoft Exchange Server, que alberga todos los datos del correo electrónico, calendarios, carpetas compartidas... todos los servicios que proporciona esta herramienta. Se integra dentro del Dominio y, por consiguiente, todas las credenciales de acceso se validan a través del Domain Controller.
- **Servidor de Desarrollo:** Gestiona el código fuente que los desarrolladores generan. Ejecuta el servidor de versiones “Subversion” (SVN) que ayuda a centralizar el código, gestionar versiones, resolver conflictos entre varios desarrolladores cuando modifican fragmentos de código de un mismo bloque, etc.
- **Servidor de Ficheros de BackOffice:** Es un servidor de Ficheros bajo Windows que comparte un juego de carpetas a los usuarios de las diferentes Sub-Áreas de BackOffice. Al igual que en el resto de los recursos bajo el dominio, las credenciales de acceso a cada una de las carpetas se gestionan desde el Domain Controller. El objetivo de este servidor es albergar la documentación de las diferentes sub-áreas (RRHH, Finanzas, Servicios).
- **Consola del Antivirus:** Centraliza la administración de los antivirus instalados tanto en los servidores como en las estaciones de trabajo. Desde la consola se monitoriza en todo momento las versiones de las bases de datos de firmas que hay instaladas en cada una de las máquinas, y se visualizan en tiempo real si se ha detectado alguna amenaza en alguno de los clientes monitorizados. También contiene el servidor de Windows Update cuya función es proporcionar una fuente centralizada de suministro de los parches actualizados de cada una las máquinas Windows que integran el dominio.
- **Servidor de BD de aplicaciones Corporativas (Prod):** Ejecuta el Sistema de Gestión de Base de Datos Microsoft SQL Server 2012 que soporta las aplicaciones corporativas. La gestión de los usuarios de Base de Datos se lleva dentro del propio SGBD.
- **Servidor de Aplicaciones Corporativas (Prod):** Ejecuta un servidor de contenedores oc4j (GlassFish) que ejecuta aplicaciones construidas sobre plataforma j2ee.
- **Servidor de BD de aplicaciones Corporativas (Test):** Instancia donde realizar pruebas en un entorno similar al productivo de las modificaciones que se llevan a cabo en las aplicaciones corporativas.
- **Servidor de Aplicaciones Corporativas (Test):** Idem al anterior, aunque referido al servidor de aplicaciones java.

- **Firewall/AntiSpam/Mail Antivirus/Proxy:** Este servidor establece la frontera entre la DMZ e Internet. El servidor ejecuta el software “Endian”, que es una versión de Linux convenientemente modificada y con un juego de servicios y aplicaciones configuradas para servir de firewall, proxy, y de filtro de spam/antivirus de los correos.
- **Firewall:** Un segundo servidor “Endian” cuyas reglas de “firewall” están configuradas para delimitar la frontera entre la red interna y la DMZ.

Objetivos del Plan Director

El motivo de la elaboración del Plan Director es el de definir un plan de acciones con el fin de cumplir con los objetivos que se establecerán en el SGSI.

El ámbito del plan director abarca la totalidad de la empresa, con lo que las medidas que se establezcan se orientarán a aspectos funcionales, técnicos y organizativos.

Más en detalle, los objetivos deseados desde la Dirección General de la empresa son los siguientes:

- Establecer la seguridad de la información como un proceso más en la empresa.
- Convertir la seguridad de la información en la prioridad principal en la gestión diaria de los sistemas.
- Al hilo de los objetivos anteriores descritos, establecer el marco organizativo, técnico y funcional para poder certificar a la empresa en la ISO 27001:2005

Análisis Diferencial de la situación inicial respecto a las ISO 27001 y 27002

Introducción

En este apartado se lleva a cabo un análisis diferencial de la implementación de los diferentes controles de la normativas ISO-27001 y 27002 en el que se encontraba la organización antes de iniciar las acciones para implementar el SGSI formalmente.

Este análisis nos permitirá establecer un punto de partida en el que poder determinar los logros y avances que materializarán a lo largo del desarrollo del proyecto.

Para llevar a cabo este análisis se ha utilizado el modelo de madurez de la capacidad (CMM) cuya escala se define en el siguiente cuadro:

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

Tabla 1: Valoraciones del modelo CMM

Las valoraciones de los resultados de cada uno de los dominios se llevan a cabo realizando un promedio de los controles de éstos.

Diferencial respecto a los controles de ISO 27001

El grado de cumplimiento de los controles definidos en la ISO 27001 es, prácticamente inexistente, como muestran las cifras que se detallan a continuación.

Por dominios, las cifras de cumplimiento son las siguientes:

Dominio	% de Efectividad	# NC Mayores	# NC Menores	Control OK
4.- SGSI	1%	56	0	0
5.- Gestión de la Responsabilidad	8%	19	0	1
6.- Auditoría Interna Del SGSI	0%	6	0	0
7.- Revisión por la Dirección del SGSI	0%	15	0	0
8.- Mejora del SGSI	0%	13	0	0

Tabla 2: Gap Analysis. Cumplimiento de 27001

El recuento de controles totales ajustados al modelo CMM son los siguientes:

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	101
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	8
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	0
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	0
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	0
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	1
L6	N/A	No aplica		0

Tabla 3: Gap Analysis. CMM de 27001

El detalle de los controles analizados en este apartado se encuentra en el Anexo 1:

jconsuegra_TFM_062013_Anexo1_Analisis_Diferencial_27001.xls

Diferencial respecto a los controles de ISO 27002

El grado de cumplimiento de los controles definidos en la ISO 27002 es bajo (un promedio de un 15%), como muestran las cifras que se detallan a continuación.

Por dominios, las cifras de cumplimiento son las siguientes:

Dominio	% de Efectividad	# NC Mayores	# NC Menores	Control OK
5.- Política De Seguridad	0%	2	0	0
6.- Aspectos Organizativos de la SI	14%	9	0	2
7.- Gestión de activos	18%	4	1	0
8.- Seguridad ligada A RRHH	22%	7	3	2
9.- Seguridad física Y del entorno	30%	9	0	3
10.- Comunic. y Operaciones	19%	23	5	2
11.- Control De acceso	33%	15	3	7
12.- Adquisición, Desarrollo y Mantenimiento De los SI	25%	9	5	0
13.- Gestión de Incidentes deSI	0%	5	0	0
14.- Continuidad Del negocio	0%	5	0	0
15.- Cumplimiento	7%	9	1	0

Tabla 4: Gap Analysis. Cumplimiento de 27002

El recuento de controles totales ajustados al modelo CMM son los siguientes:

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	64
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	33
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	7
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	8
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	14
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	2
L6	N/A	No aplica		5

Tabla 5: Gap Analysis. CMM de 27002

En la siguiente gráfica de red se muestra gráficamente el nivel de cumplimiento por Dominios:

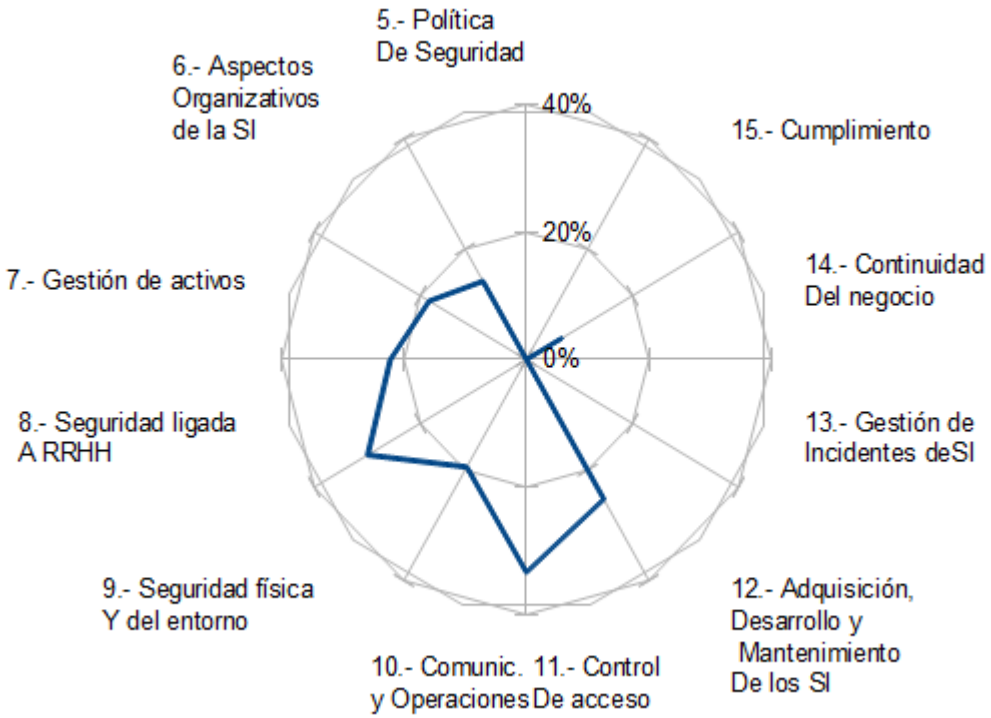


Ilustración 5: Gráfica de Red de cumplimiento por dominios de 27002

El detalle de los controles analizados en este apartado se encuentra en el Anexo 2:
jconsuegra_TFM_062013_Anexo2_Analisis_Diferencial_27002.xls

Esquema Documental del SGSI

	POLITICA DE SEGURIDAD	**Código:**	PR-POLSEG-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	1

Histórico de Versiones			
Versión	Fecha	Editor	Cambios
1.0	01/03/2013	J.Consuegra	Edición Inicial

Política de Seguridad

Principios Generales

Los principios generales de la política del Sistema de Gestión de Seguridad de la Información (SGSI) son los siguientes:

- El Sistema de Gestión de Seguridad de la Información debe velar esencialmente por la preservación de la confidencialidad, integridad y disponibilidad, de todos los activos de información físicos y electrónicos propiedad de TPS Technology S.L., de sus clientes, empleados, asociados de negocio y demás partes interesadas.
- Los Objetivos en Seguridad de la Información deben estar de acuerdo a las obligaciones contractuales y legales, la rentabilidad de los activos, el estado de la tecnología y los criterios organizativos vigentes.
- Se debe aplicar una Gestión de los Riesgos con un criterio de evaluación del riesgo alineado con la estrategia de la organización y aprobado por la Dirección
- Se deben aplicar los principios de mejora continua en la reducción del riesgo, los procesos y la implementación de controles, anteponiendo la prevención a la corrección.
- La política debe ser conocida y cumplida por todo el personal que trabaja en y para la organización, así como las partes interesadas (terceros o clientes) que puedan tener afectación en la seguridad de la información, independiente de su nivel jerárquico u organizativo.
- Quien con conocimiento manifiesto de la presente política de seguridad omita su cumplimiento o actúe de manera negligente contra cualquiera de sus preceptos podrá quedar sujeto a acciones disciplinarias, llegando si procede al despido y al emprendimiento de las acciones legales contra él que la compañía considere oportunas.
- La compañía proporcionará todos los medios humanos y recursos económicos y técnicos a su alcance para establecer, adecuar y mejorar de manera permanente un plan de Continuidad del Negocio que tenga como objetivo asegurar la operatividad de las actividad productiva en caso de producirse un desastre con posibles consecuencias mayores.

TPS TECHNOLOGY	**POLITICA DE SEGURIDAD**	**Código:**	PR-POLSEG-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	2

Responsabilidades en el SGSI

Se definen en este apartado las responsabilidades Generales y Específicas respecto a la gestión de la seguridad de la Información.

El establecimiento del SGSI conllevará la creación de un Área de Seguridad de la Información, dependiente directamente de la dirección general y totalmente independiente del resto de Áreas de la compañía. De esta manera, el organigrama de la empresa quedaría así:

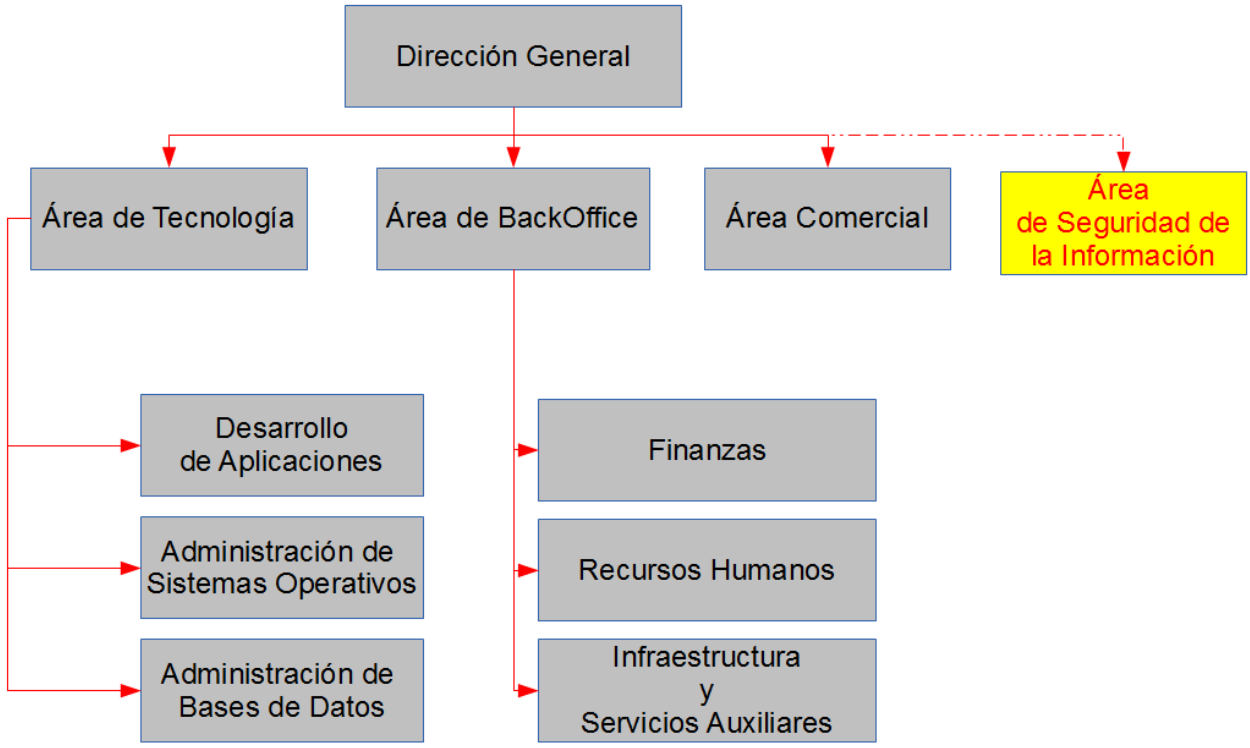


Ilustración 6: Diagrama Organizativo modificado

La dirección, formación, análisis del desempeño y establecimiento de procedimientos y procesos relacionados con la seguridad de la información serán responsabilidad directa del Área de Seguridad de la Información.

El Área de Seguridad de la Información, con la aprobación de la dirección, tendrá autoridad para solicitar los recursos de soporte técnico, y de cualquier tipo que considere necesario a las Áreas de Tecnología y de BackOffice (herramientas, privilegios de acceso a los sistemas, procedimientos, etc).

Las investigación de las violaciones de la seguridad serán competencia del Área de Seguridad de la información.

Las medidas de carácter disciplinario o legal serán competencia del Sub-Área de Recursos Humanos (dependiente del Área de Back-Office).

	POLITICA DE SEGURIDAD	**Código:**	PR-POLSEG-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	3

Referencias Documentales

Los principios generales se desarrollan en Políticas Especificas del Sistema de Gestión de Seguridad de la Información debidamente documentados en los respectivos documentos que los constituyen.

	POLITICA DE SEGURIDAD	**Código:**	PR-POLSEG-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	4

Política del SGSI (documento para los empleados)

La Misión de TPS Technology es:

- Añadir valor a sus clientes, colaboradores y accionistas, a través de la oferta en el mercado de Servicios Expertos en Desarrollo de Aplicaciones Informáticas, Administración de Bases de Datos y Administración en sistemas con claros beneficios para todas las partes involucradas.
- Constituirse en una empresa líder en el Mercado Europeo de Servicios en Tecnologías de la Información, a través de la excelencia en el servicio a sus clientes.

En consecuencia, definimos la **POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)** en los siguientes principios generales:

- El Sistema de Gestión de Seguridad de la Información debe velar esencialmente por la preservación de la confidencialidad, integridad y disponibilidad, de todos los activos de información físicos y electrónicos propiedad de TPS Technology, de sus clientes, empleados, asociados de negocio y demás partes interesadas.
- Los Objetivos en Seguridad de la Información deben estar de acuerdo a las obligaciones contractuales y legales, la rentabilidad de los activos, el estado de la tecnología y los criterios organizativos vigentes.
- Se debe aplicar una Gestión de los Riesgos con un criterio de evaluación del riesgo alineado con la estrategia de la organización y aprobado por la Dirección
- Se deben aplicar los principios de mejora continua en la reducción del riesgo, los procesos y la implementación de controles, anteponiendo la prevención a la corrección.
- La política debe ser conocida y cumplida por todo el personal que trabaja en y para la organización, así como las partes interesadas (terceros o clientes) que puedan afectar la seguridad de la información, independientemente de su nivel jerárquico u organizativo.

Los principios generales se desarrollan en Políticas Especificas del Sistema de Gestión de Seguridad de la Información debidamente documentado en los documentos que los constituyen.

Firmado y Aprobado
por la Dirección de
TPS Technology

	PROCEDIMIENTO DE AUDITORIAS INTERNAS	**Código:**	PR-AUDINT-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	1

Histórico de Versiones			
Versión	Fecha	Editor	Cambios
1.0	01/03/2013	J.Consuegra	Edición Inicial

Procedimiento de Auditorías Internas

Objeto

Se define en este procedimiento las consideraciones a tener en cuenta a la hora de realizar auditorías internas.

Ámbito

Se incluye los sistemas de Gestión de Seguridad de la Información de TPS Technology S.L.

El propietario de este proceso es el Responsable del Área de Seguridad de la Información y se considera de tipo Estratégico.

Planificación

Todo el Sistema de Gestión de Seguridad de Información es auditado completamente por lo menos una vez al año. Estas auditorías se pueden hacer de forma conjunta o por separado, lo cual queda a juicio del responsable del Área de Seguridad de la Información. También deberá comprobarse periódicamente el cumplimiento técnico de las normas y controles de seguridad aplicados a los sistemas de información.

Pueden, asimismo, llevarse a cabo auditorías extraordinarias no programadas cuando se detecten anomalías o deficiencias en el Sistema de Gestión, en una actividad, proceso o Área, o bien si ha sido anteriormente requerido por una auditoría previa, o en caso de producirse cambios significativos que afecten a la Seguridad de la Información y las medidas o controles adoptados.

Estas Auditorías se ejecutan en todos sus aspectos conforme a lo descrito en este procedimiento, con la salvedad de que no constan en el Plan de Auditorías.

En el caso de la Seguridad de la Información, los objetivos de control, controles y políticas deberán someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

Las auditorías de Seguridad de la Información deberán proveer a los responsables de procesos un mecanismo de comprobación conforme a que los procedimientos de seguridad de su área de responsabilidad se realizan correctamente de acuerdo a lo definido.

Durante la revisión por la Dirección debe plasmarse en el acta la planificación de auditorías del año próximo.

TPS TECHNOLOGY	**PROCEDIMIENTO DE AUDITORIAS INTERNAS**	**Código:**	PR-AUDINT-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	2

Responsables

Dirección General

- Aprobación del programa de auditorías internas.

Representante de la dirección

- Conocer el procedimiento de auditorías Internas
- Revisión del plan de Auditorías; Realizar modificaciones y actualizaciones de éste
- Inclusión de los Informes de Auditorías en la revisión por la dirección

Responsable de Seguridad de la Información

- Elaboración y actualización del procedimiento de auditorías internas
- Planificación de las Auditorías Internas
- Revisión de los informes de las Auditorías Internas
- Determinación de medidas para acometer las no conformidades.

	PROCEDIMIENTO DE AUDITORIAS INTERNAS	**Código:**	PR-AUDINT-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	3

Equipo Auditor

El equipo auditor interno podrá delegar las funciones a un equipo externo para un mayor grado de independencia, o por graves faltas derivadas de nuevas funciones o actividades de la empresa. Deberá asegurarse que el auditor nunca auditará su propio trabajo.

Se aplicarán acuerdos de confidencialidad específicos al equipo auditor externo que requieran del acceso a estos registros.

Las personas que forman el equipo auditor deberán cumplir los siguientes requisitos:

Educación

- Diplomado o Licenciado

Formación

- Haber aprobado el curso como Auditor de SGSI o tener conocimientos y habilidades en auditorías internas de SGSI.
- Conocimiento demostrable de la norma ISO-27001:2005

Experiencia

- Mínimo un año en la Organización o experiencia en auditorias internas.
- Conocimiento de la cultura de la organización así como su tamaño y estructura.

Habilidades

- Dominar la estructuración y preparación de Informes
- Objetivo e Imparcial
- Buen comunicador
- Buen entrevistador
- Puntual y responsable
- Habilidad en revisión de registros y datos

Compromiso

- Comprometido con el SGSI y con las actividades de auditoría interna.

	PROCEDIMIENTO DE AUDITORIAS INTERNAS	**Código:**	PR-AUDINT-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	4

Programación

El Responsable del Área de Seguridad de la Información debe contactar con el área a auditar y el equipo auditor para concertar las fechas de auditoría.

Debe solicitarse al equipo auditor la presentación de un Programa de Auditoría donde se ha de especificar como mínimo:

- Fechas y horarios
- Departamentos
- Procesos
- Requerimientos
- Emplazamientos

Es responsabilidad del auditor preparar la auditoría (formularios, documentación, etc.).

El Área de Seguridad de la Información debe enviar la documentación requerida por el equipo auditor para la revisión de la documentación y la preparación de la auditoría interna.

De la misma manera, el Área de Seguridad de la Información debe enviar copia del programa de auditoría a los propietarios de los procesos con antelación suficiente a fin de asegurar su disponibilidad.

Ejecución

El Equipo Auditor debe llevar a cabo la auditoría en las fechas concertadas.

Los auditores dispondrán una breve reunión de apertura al inicio de la auditoría con los interesados para comentar el método de la auditoria y ajustar horarios; asimismo también dispondrán una reunión de final donde expondrán los resultados.

Durante la ejecución, el personal de la compañía deberá colaborar con los auditores y responder a las cuestiones planteadas por el equipo auditor así como presentar las evidencias solicitadas.

La revisión del cumplimiento técnico de los controles de seguridad aplicados a los sistemas de información deberá hacerse únicamente por personas competentes y autorizadas o bien bajo la supervisión de dichas personas. Durante la auditoría se dará la posibilidad de hacer uso de herramientas de software adecuadas que automaticen o permitan hacer un análisis de mayor precisión, generando informes o cualquier forma de resultado que permita una interpretación.

Los requisitos de las actividades de auditoría que impliquen comprobaciones en los sistemas de producción deberán ser cuidadosamente planificados y acordados para minimizar el registro de interrupciones en los procesos de negocio.

Cuando se empleen herramientas de auditoría para verificar el funcionamiento o la aplicación de controles a los sistemas de información, se deberán proteger estas herramientas para evitar cualquier peligro o uso indebido.

	PROCEDIMIENTO DE AUDITORIAS INTERNAS	**Código:**	PR-AUDINT-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	5

Informe de Auditoría

Cuando el equipo Auditor considere finalizada su tarea, deberá presentar un Informe con los resultados obtenidos de la auditoría.

El informe deberá incluir:

- Nombre del equipo auditor y/o auditor líder
- Fecha de la auditoría
- Procesos auditados
- Responsables de las actividades o procesos
- Objetivos, alcances y criterios
- Hora de inicio y duración de la auditoría
- Hallazgos y no conformidades encontradas
- Oportunidades de mejora
- Requerimiento de acciones correctoras.
- Nombre, cargo y firma de la persona responsable del auditado
- Firma de los Auditores

El informe de auditoría debe emitirse en un plazo máximo de cinco días hábiles después de su ejecución.

Dirección debe exigir la entrega de este informe.

TPS TECHNOLOGY	**PROCEDIMIENTO DE REVISION POR LA DIRECCION**	**Código:**	PR-REVDIR-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	1

Histórico de Versiones			
Versión	Fecha	Editor	Cambios
1.0	01/03/2013	J.Consuegra	Edición Inicial

Procedimiento de Revisión por la Dirección

Objeto

En este proceso se pretende definir la forma de revisión por parte de la dirección del correcto seguimiento y control de los sistemas de gestión de TPS Technology S.L.

Ámbito

Se incluye los sistemas de Gestión de Seguridad de la Información de TPS Technology S.L.

Se excluye a todo tipo de procesos o procedimientos que por su simplicidad o ciclo de actividad rutinario o constante su revisión periódica entorpecería la eficiencia de estas acciones.

El propietario de este proceso es la Dirección y se considera de tipo Estratégico.

Ficha de Proceso

Recursos	Descripción	Responsables
Sala de Reuniones	Se describe el proceso de revisión, por parte de la dirección, de la adecuación y eficacia del sistema de gestión de seguridad de información	Propietario: Dirección Roles: Dirección, Gestor de Seguridad de la Información, Propietarios de Procesos y Personal
Entradas	**Interacciones**	**Salidas**
Resultado de Auditorías Satisfacción de los clientes Reclamaciones e Incidencias Técnicas, productos o procedimientos que pueden ser utilizados para mejorar el SGSI. Vulnerabilidades y amenazas que no se han canalizado adecuadamente en revisiones previas. Resultados de la medición de la efectividad. Cambios que puedan afectar al sistema. Indicadores de los procesos y servicios. Estado de las acciones. Actas de reuniones previas Recomendaciones y propuestas de mejora	Proceso de Mejora Continua Proceso de Monitorización, Evaluación y Reporting	Acta de Reunión Objetivos para los indicadores Planes Asignación y/o necesidades de recursos Modificaciones a procesos, instrucciones o formatos.
Indicadores	**Riesgos**	**Documentos**
Resultado en las Auditorías	SGSI no adecuado a la normativa (resultado de auditorías)	Acta de Reunión

Tabla 6: Ficha de Proceso de Revisión por la dirección

	PROCEDIMIENTO DE REVISION POR LA DIRECCION	Código:	PR-REVDIR-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	2

Diagrama de Flujo

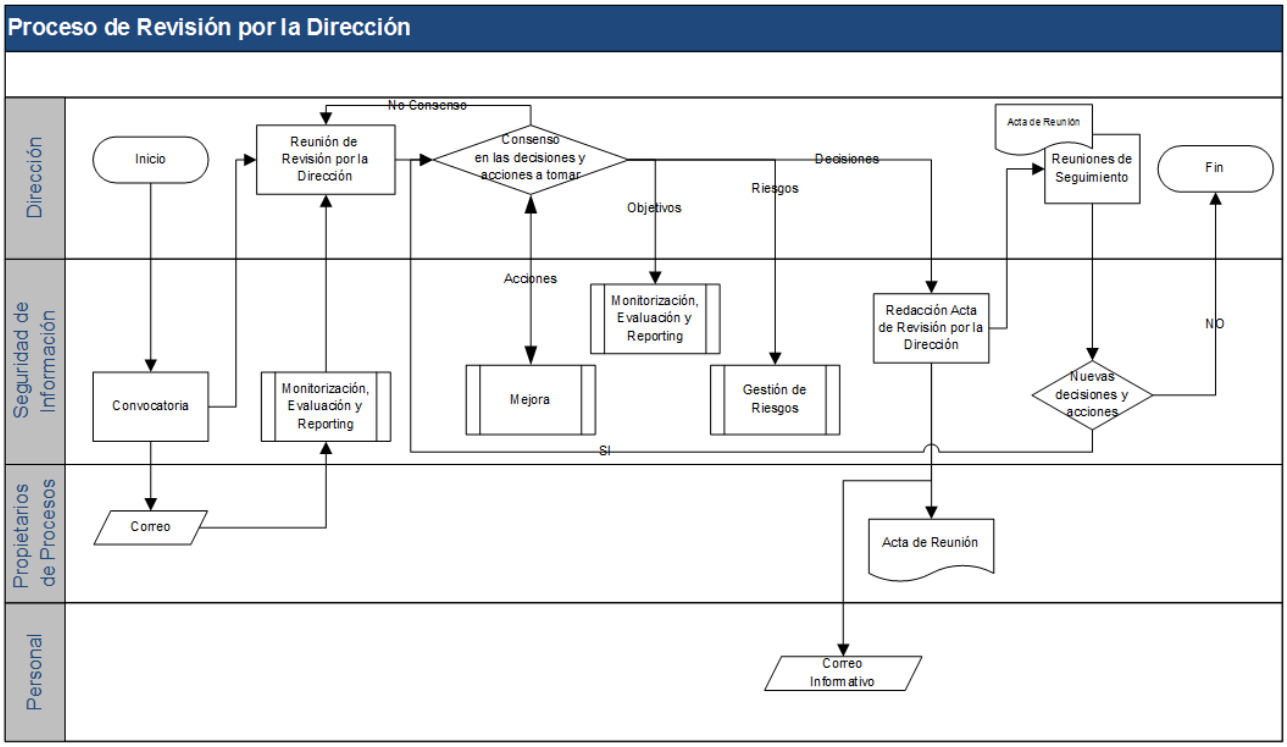


Ilustración 7: Diagrama de Flujo del proceso de Revisión por la dirección

Descripción del Procedimiento

Las reuniones de revisión se deberán realizar como mínimo una vez al año o cuando sea necesario para reaccionar apropiadamente a los resultados de estas revisiones.

Las revisiones de los sistemas de gestión de seguridad de la información se podrán realizar de manera independiente o conjunta, de acuerdo a como se especifique en la convocatoria y acta de reunión.

TPS TECHNOLOGY	**GESTIÓN DE ROLES Y RESPONSABILIDADES**	**Código:**	PR-ROLRESP-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	1

Histórico de Versiones			
Versión	Fecha	Editor	Cambios
1.0	01/03/2013	J.Consuegra	Edición Inicial

Gestión de Roles y Responsabilidades

Miembros permanentes del comité de Seguridad de la Información

El comité de seguridad de la información de la compañía debe contar con un comité de personas alineadas en todo momento con la política y los objetivos del SGSI.

Las figuras que forman este comité serán:

Responsable de Seguridad de la Información

Esta figura será un miembro de la plantilla de la empresa. Este rol, en las fases iniciales del proyecto de implantación del SGSI, consumirá la mayor parte de su tiempo de trabajo, ya que tiene que desempeñar las siguientes tareas:

- Elaborar, promover y mantener la política de seguridad de la compañía.
- Desarrollar, colaborando con los responsables de las áreas del negocio, el marco normativo de seguridad. Asegurar que estas normativas se cumplen.
- Ser la cabeza visible de la seguridad de la información en la compañía, coordinando acciones con el resto de áreas haciendo posible que la política de seguridad se extienda en todos los ámbitos de ésta.
- Controlar la gestión de Riesgos en la organización así como analizar los riesgos que pueden conllevar los cambios que se introducen o que se pretendan introducir en la organización.
- Llevar a cabo puntos de control periódicos sobre el estado de la seguridad de la información en la organización a fin de actualizar el plan de seguridad de la información en base a las conclusiones obtenidas en los controles.
- Velar por el cumplimiento de las normativas aplicables a la compañía (LOPD, LSSI, etc) y coordinar las acciones que se deriven en aras de asegurar este cumplimiento.
- Ser la “ventana única” de la compañía donde se reporta y se hace seguimiento del tratamiento de las incidencias de seguridad.
- Elaborar y mantener un plan de formación y concienciación sobre la seguridad de la información y hacerlo extensivo a todo el personal que trabaja para la compañía.
- Impulsar la elaboración, mantenimiento y pruebas del Plan de Continuidad del negocio.

	GESTIÓN DE ROLES Y RESPONSABILIDADES	Código:	PR-ROLRESP-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	2

Responsable ejecutivo

Este rol lo ha de desempeñar necesariamente una persona con capacidad ejecutiva en la compañía, de manera que las decisiones del comité de seguridad queden respaldadas por la Dirección y, de esta manera, las acciones que de ellas se deriven se traten como directrices estratégicas y reciban los recursos y el personal necesarios para su desarrollo.

Sus responsabilidades serán:

- Certificar que las decisiones del comité de Seguridad están alineadas con la Estrategia empresarial.
- Valorar las decisiones del comité de Seguridad desde el punto de vista del Negocio.
- Analizar la viabilidad económica de las acciones derivadas de las decisiones del comité de seguridad. Determinar que las acciones acordadas son económicamente asumibles por la empresa y que la relación coste-beneficio es aceptable para los objetivos estratégicos.
- Aportar el punto de vista de la Dirección frente a la aceptación de riesgos residuales.

Responsable técnico de Seguridad de la Información

El perfil del Responsable técnico de Seguridad de la Información es el de una persona que tenga un conocimiento detallado del funcionamiento de los Sistemas de Información de la compañía.

Las atribuciones del Responsable técnico de Seguridad de la Información son:

- Asegurar la viabilidad técnica de los controles acordados en el comité de Seguridad de la Información.
- Definir las bases técnicas del plan de continuidad del negocio.
- Coordinación de la implantación en los sistemas de Información de la compañía de las herramientas necesarias para llevar a cabo los controles de seguridad sobre éstos.
- Asegurar el cumplimiento de todas las normativas, instrucciones y políticas definidas por el comité de seguridad.
- Asistir al Responsable de Seguridad de la Información en la valoración de los riesgos en la implantación de nuevos sistemas o procedimientos así como en las modificaciones que se lleven a cabo sobre éstos.
- Supervisar que la Gestión de Cambios se está llevando a cabo de manera adecuada en el Área de Tecnología.

	GESTIÓN DE ROLES Y RESPONSABILIDADES	Código:	PR-ROLRESP-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	3

Responsable de Seguridad Física

El Responsable de Seguridad Física es la persona encargada de definir y proporcionar los medios necesarios para tratar los riesgos relacionados con la seguridad perimetral de los centros donde se gestione información de la compañía.

Sus atribuciones principales son:

- Proporcionar los medios necesarios para la protección física de la información, tanto frente a desastres como frente a accesos no deseados.
- Colaborar en la definición del Plan de Continuidad del negocio.
- Implementar medidas de recuperación de los activos de acuerdo con el Plan de Continuidad de Negocio.
- Implantar y asegurar el funcionamiento de los procedimientos de seguridad física definidos en la Política de Seguridad.
- Reportar al Responsable de Seguridad de la información cualquier incidente, defecto o merma en el desempeño de las medidas de seguridad física.

Delegado del Área de Tecnología

Su función principal es la de ser el representante de los técnicos que forman el Área de Tecnología en las reuniones del comité de Seguridad.

Otras de sus funciones son:

- Transmitir la percepción del personal sobre las acciones llevadas a cabo por el comité de seguridad.
- Detectar oportunidades de mejora en la seguridad de la información (optimización de procedimientos, procesos, herramientas...).
- Asistir al Responsable técnico de Seguridad de la Información en la implementación de las herramientas y controles acordados en el comité de Seguridad de la Información.

Delegado del Área de Back-Office

Las funciones del delegado del Área de Back-Office son análogas a las descritas sobre el Delegado del Área de Tecnología.

TPS TECHNOLOGY	**METODOLOGÍA DE ANÁLISIS DE RIESGOS**	**Código:**	PR-METANARIE-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	1

Histórico de Versiones			
Versión	Fecha	Editor	Cambios
1.0	01/03/2013	J.Consuegra	Edición Inicial

Metodología de Análisis de Riesgos

Descripción del procedimiento

Identificación de Activos

La identificación de Activos es crucial en el proceso de Gestión de Riesgos. Los activos a proteger han de tener asignado un propietario en la compañía. El propietario de los activos es la persona que en primera instancia utilizan el activo y las que llevarán a cabo la implementación final de las medidas de tratamiento de riesgos que afectan a ese activo.

Los tipos de activos identificables en base al análisis de riesgos en la Seguridad de la Información son:

- Físicos: Referido a activos de Hardware, tales como ordenadores, teléfonos móviles, Tablets, Impresoras, etc.
- Lógicos: Se refiere a activos de Software, como los sistemas operativos, utilidades, aplicaciones desarrolladas por la compañía, procesos batch, etc.
- Personal: Los diferentes roles que intervienen en el funcionamiento de la compañía (Director, Responsable de Seguridad Física, Desarrolladores, Administradores...).
- Entorno e Infraestructura: Elementos de inmovilizado de la organización necesarios para que ésta pueda desempeñar su actividad (ej. cableado, suministro eléctrico, climatización...).
- Intangibles: Elementos no materiales pero determinantes para la organización (credibilidad, confianza de los clientes, experiencia, “know-how”).

Identificación de Vulnerabilidades

La identificación de vulnerabilidades de Seguridad de Información puede provenir de distintas fuentes:

- Requerimientos legales, regulatorios y contractuales aplicables a la organización, los productos realizados o empleados, los servicios prestados o consumidos, etc.
- Identificación de lecciones aprendidas y de experiencias en relación a seguridad de información de otras organizaciones y de la misma organización.
- Informes, consejos, o noticias relevantes a la seguridad de la información con impacto posible en la organización.
- El personal de la organización tiene la responsabilidad de identificar y canalizar los las vulnerabilidades identificadas al Responsable de Seguridad de Información.
- El personal tiene la obligación de comunicar los riesgos incluso si éstos fueran identificados por partes externas.

TPS TECHNOLOGY	**METODOLOGÍA DE ANÁLISIS DE RIESGOS**	**Código:**	PR-METANARIE-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	2

El miembro de la compañía que haya identificado vulnerabilidades en la seguridad de la información deberá comunicarlo al Responsable de Seguridad de la Información con el propósito de la evaluación y registro de la vulnerabilidad identificada.

Registro de Riesgos

Se registrarán todos aquellos riesgos que tengan una probabilidad no nula de ocurrir en el período de un año y que, de materializarse, tendrían un efecto negativo en activos de información de la organización.

El registro de riesgos se hará en el documento “Mapa de riesgos” que está bajo la responsabilidad del Responsable de Seguridad de la Información y con el soporte de la persona o personas que hubieran identificado la vulnerabilidad.

En el momento del registro de riesgos se identificarán:

- Activo o tipo de activo afectado y su propietario
- Vulnerabilidad del activo
- Amenazas que pueden explotar la vulnerabilidad identificada
- Probabilidad o frecuencia con la que las amenazas podrían materializarse
- Impacto esperado en caso de materializarse la amenaza
- Alternativas de tratamiento si se conocen.

En el momento de la identificación de los riesgos, es importante que se identifique otras posibles vulnerabilidades o activos que pudieran verse afectados, en caso de que se materializase la amenaza.

Evaluación de Riesgos y Tratamientos Posibles

La evaluación de riesgos en la organización se hace de en dos dimensiones: Probabilidad o Frecuencia e Impacto. Para ellos se aplica la siguiente clasificación:

Probabilidad del riesgo o frecuencia de incidencias

- **Baja**: Existe la probabilidad de se materialice el riesgo una vez al año o menos
- **Moderada**: Existe la probabilidad de que se materialice el riesgo unas dos a tres veces durante un año
- **Alta**: Existe la probabilidad de que se materialice el riesgo cuatro o más veces durante un año

	METODOLOGÍA DE ANÁLISIS DE RIESGOS	Código:	PR-METANARIE-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	3

Impacto del riesgo para el negocio

1. Leves

- Pérdidas monetarias no significativas (especificar).
- Tiempo necesario para realizar de nuevo el trabajo inferior a un día de un recurso.
- Percepción de baja calidad en los servicios por personal interno de la organización.
- Pérdidas de la disponibilidad de servicios inferior a una hora de trabajo o dentro de los límites en los acuerdos contractuales o legales.
- Dificultades e incomodidades para realizar las labores dentro de la organización
- Fugas de datos no controladas de información internamente en la organización (no incluidos datos personales)

2. Moderados

- Pérdidas monetarias poco significativas (especificar).
- Tiempo necesario para realizar de nuevo el trabajo inferior una semana de un recurso
- Objetivos secundarios de proyecto o servicio no satisfechos
- Pérdidas de la disponibilidad de servicios inferior a 4 horas de trabajo o superior a los límites en los acuerdos contractuales o legales sin riesgos de multas o penalizaciones.
- Percepción de baja calidad en los servicios por usuarios-clave secundarios o proveedores
- Fugas de datos no controladas de información de la organización (no incluidos datos personales)

3. Graves.

- Pérdidas monetarias significativas para la organización (especificar).
- Tiempo necesario para realizar de nuevo el trabajo equivalente o superior a una semana de un recurso.
- Imposibilidad de reconstruir la información perdida.
- Pérdidas de la disponibilidad de servicios superior a 4 horas de trabajo o superior a los límites en los acuerdos contractuales o legales con riesgos de multas o penalizaciones.
- Objetivos principales de proyecto o servicios no satisfechos (SLAs no cumplidos)
- Percepción de baja calidad en los servicios por usuarios-clave primarios de proyectos o servicios
- Riesgo de seguridad personal
- Fugas de datos no controladas de información de clientes o datos personales

	METODOLOGÍA DE ANÁLISIS DE RIESGOS	**Código:**	PR-METANARIE-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	4

Categorización de los Riesgos

Los riesgos se dividirán en Alto, Medio o Bajo de acuerdo a la siguiente tabla y código de colores:

		Impacto / Pérdidas		
		Leves	Moderadas	Graves
Probabilidad	Alta	**Medio**	**Alto**	**Alto**
	Moderada	**Bajo**	**Medio**	**Alto**
	Baja	**Bajo**	**Bajo**	**Medio**

Tabla 7: Categorización de los Riesgos

Para definir la probabilidad y el impacto de los riesgos, el Responsable de Seguridad de la Información tomará en considerará el criterio de la persona que identifica la vulnerabilidad.

Definición del tratamiento de los riesgos

El Responsable de Seguridad de la Información propondrá los tratamientos necesarios para reducir los riesgos a niveles aceptables. Propondrá un plan de tratamiento basado en Acciones correctivas, preventivas o de mejora, en las que se establecerán los responsables de la implementación de las medidas.

El plan de tratamiento deberá procurar una o más medidas que:

1. Prevengan o eviten que se materialicen los riesgos
2. Reduzcan la probabilidad de que se materialicen los riesgos
3. Detecten la materialización de riesgos y permitan tratar sus consecuencias
4. Repriman o reduzcan las consecuencias una vez que se materialicen
5. Permitan la corrección y recuperación una vez que se materialicen
6. Transfieran los riesgos a otras entidades mejor preparadas
7. Acepten los riesgos residuales, entendiendo que no se hará un tratamiento adicional

La aplicación de estas medidas dará más prioridad de aplicación del inicio al fin de la lista anterior (la 1 antes que la 7).

Tras la aplicación de las medidas de tratamiento de riegos debe quedar un riesgo residual (o la eliminación del riesgo) que también será evaluado.

Si la aplicación de tratamientos realizados no redujera el riesgo a un nivel aceptable se repetirá el proceso o se solicitará a la organización que acepte expresamente la decisión tomada.

	METODOLOGÍA DE ANÁLISIS DE RIESGOS	Código:	PR-METANARIE-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	5

Revisión de evaluación de los riesgos

La dirección llevará a cabo una revisión mensual de los riesgos identificados en categorías **Medio** o **Bajo** en el período anterior.

Dirección revisará la evaluación y las posibles medidas de tratamiento de los riesgos identificados que no sean aceptados (ver el apartado siguiente “criterio de aceptación de riesgos”).

Dirección acordará también un plan para el tratamiento de los riesgos y aprobará que se establezcan responsables de la implementación de las medidas.

Si durante el período se identifican riesgos de categoría **Alto**, o bien se requieran revisiones especiales para la toma de decisiones que no puedan esperar, éstos serán revisados en la mayor brevedad posible.

La actividad de revisión tiene por objetivos:

- Asegurar que la valoración del riesgo se ajusta a la realidad del negocio.
- Autorizar las medidas de tratamiento en consonancia con la valoración del riesgo, las pérdidas en los activos de la organización y la probabilidad de incurrir en estas pérdidas.
- Priorizar adecuadamente la forma en cómo serán tratados los riesgos.
- Aceptar los riesgos residuales tras la aplicación de controles y medidas de tratamiento.
- Aceptar el estado general de riesgo en referencia a la seguridad de la información de la organización

Importante: Tras aprobar el plan de tratamiento de riesgos, se actualizará la declaración de aplicabilidad.

Criterio de aceptación de riesgos

La gestión de riesgos procurará la identificación de todos los riesgos relacionados con la seguridad de la información vinculados a la operación de la compañía, así como de dar tratamiento a los riesgos identificados, evitando de esta manera que la organización opere con riesgos de tipo **Alto** o **Medio** si el tratamiento para eliminarlos o reducirlos a nivel **Bajo** es viable.

Materialización de Riesgos durante del ejercicio

La materialización de riesgos se registrará como una incidencia (generalmente de seguridad) a través del proceso de Gestión de Reclamaciones e Incidencias.

Durante la gestión de la incidencia o de la ejecución de las acciones para corregir su efecto se podrían identificar vulnerabilidades nuevas. Estas serían transmitidas al proceso de Gestión de Riesgos para que sean incorporadas y tratadas en el mapa de riesgos de la organización.

	GESTIÓN DE INDICADORES	**Código:**	PR-GESIND-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	1 de 12

Histórico de Versiones			
Versión	Fecha	Editor	Cambios
1.0	01/03/2013	J.Consuegra	Edición Inicial

Gestión de Indicadores

En el cuadro siguiente se detallan los indicadores definidos para medir eficacia del SGSI relacionados con cada uno de los controles de la norma:

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
5. POLÍTICA DE SEGURIDAD **5.1. Política de Seguridad de la Información**					
5.1.1	Documento de Política de Seguridad de la Información	Número de revisiones por la dirección	>= 1 por año	Se obtiene del registro de revisiones por la dirección Constata las revisiones del SGSI que se llevan a cabo por la dirección durante un ejercicio.	Anual
5.1.2	Revisión de la política de Seguridad de la Información.				
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.	Número de No-Conformidades detectadas por la auditoría.	< 1por auditoría	Obtenido de los registros de auditorías Permite evaluar el desempeño del apartado de Aspectos organizativos de la SI. La fuente de este indicador es el informe del resultado de la Revisión independiente de la Seguridad de la Información.	Según el plan de Auditorías
6.1.2	Coordinación de la seguridad de la información.				
6.1.3	Asignación de responsabilidades relativas al seguimiento de la información.				
6.1.4	Proceso de autorización de recursos para el tratamiento de la información.				
6.1.5	Acuerdos de Confidencialidad				
6.1.6	Contacto con las Autoridades				
6.1.7	Contacto con grupos especializados de interés para la				

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
	organización.				
6.1.8	Revisión independiente de la seguridad de la información.				
6.2 Terceros					
6.2.1	Identificación de los riesgos derivados del acceso de terceros.	Número de riesgos identificados en un ejercicio	<= número de riesgos determinados en la revisión del plan anterior	Obtenido del registro de cambios en el mapa de riesgos. Este indicador permite determinar si el plan de tratamiento de riesgos en esta sección está teniendo un desempeño óptimo. La tendencia natural de este indicador debería ser a la baja, ya que a medida que se materializa el plan de tratamiento de riesgos, éstos deberían ser cada vez menos.	Anual
6.2.2	Tratamiento de la seguridad en la relación con los clientes.	No se define			
6.2.3	Tratamiento de la seguridad en contratos con terceros.	# de Revisiones de Riesgos realizadas	>= 1 por año	Obtenido del registro de cambios en el mapa de riesgos. Este indicador se materializa sólo en compras no habituales (ej. Cuando se compra un servidor nuevo para la compañía). El indicador permite comparar por ejercicios cuántas veces se ha revisado el mapa de riesgos por motivo de una adquisición relevante para la compañía.	Anual
7. GESTIÓN DE ACTIVOS **7.1. Responsabilidad sobre los activos.**					
7.1.1	Inventario de Activos	Número de elementos en el inventario de activos	N/A	Obtenido del inventario de activos. Permite conocer la extensión del mapa de activos para los que se está gestionando riesgos, de manera que se pueda comparar el número de estos en cada ejercicio.	Anual
7.1.2	Propiedad de los Activos	Número de activos gestionado por cada responsable	N/A	Obtenido del inventario de activos. Por ejercicio, nos muestra cuántos activos gestiona cada responsable. La utilidad de este es conocer	Anual
7.1.3	Uso aceptable de los activos	Número de incidencias relacionadas con faltas a la normativa definida sobre el uso aceptable de los activos	< Número de Incidencias del año anterior	Obtenido del registro de incidencias. Evaluación del cumplimiento de la política de uso aceptable de los activos	Anual
7.2 Clasificación de la información					
7.2.1	Directrices de clasificación	Número de incidencias	< Número de Incidencias del	Obtenido del registro de incidencias.	Anual

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
7.2.2	Etiquetado y manipulado de información	relacionadas con las directrices de clasificación de la información	año anterior	Permite conocer cuántas incidencias se han producido en un ejercicio respecto a este apartado. El propósito es verificar la eficacia de las directrices de clasificación y etiquetado.	
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS **8.1. Antes del Empleo**					
8.1.1	Funciones y Responsabilidades	Número de incidencias relacionadas con la Seguridad ligada a los RRHH.	< 5 por año	Obtenido del registro de incidencias. Determinar la eficacia de las políticas y normativas definidas en la seguridad ligada los RRHH.	Anual
8.1.2	Investigación de Antecedentes				
8.1.3	Términos y condiciones de contratación				
8.2 Durante el empleo					
8.2.1	Responsabilidades de la Dirección	No se define			
8.2.2	Concienciación, formación y capacitación en Seguridad de la información	Número de incidencias de Seguridad causadas por falta de formación del personal en SI.	< Número de Incidencias del año anterior	Obtenido del registro de incidencias. Determinar la eficacia de las acciones formativas y de concienciación.	Anual
8.2.3	Proceso Disciplinario	Número de procesos disciplinarios llevados a cabo por actuaciones que afectan al SI	< Número de Incidencias del año anterior	Obtenido de los expedientes de los trabajadores. Compromiso y determinación del personal en el seguimiento de buenas prácticas sobre seguridad de la información	Anual
8.3 Cese del empleo o cambio de puesto de trabajo					
8.3.1	Responsabilidad del cese o cambio	a) % de activos no devueltos tras un cese o cambio de actividad b) Número de incidencias por no retirada de accesos a una persona que ha cesado o cambiado de actividad.	a) < 10% b) < Número de Incidencias del año anterior	Tanto para (a) como (b), se trata de determinar el cumplimiento de los procedimientos asociados al cese de empleo o cambio de puesto de trabajo. El modo de calcular (a) es a través la recopilación de evidencias de la devolución de los activos. El modo de calcular (b) es a través del registro de incidencias de SI que mantiene el responsable de Seguridad de la Información.	Anual
8.3.2	Devolución de Activos				
8.3.3	Retirada de los derechos de Acceso				
9. SEGURIDAD FÍSICA Y DEL ENTORNO **9.1. Áreas seguras**					
9.1.1	Perímetro de seguridad física	Número de incidencias relacionadas con la seguridad física	< Número de Incidencias del año anterior	El modo de calcular este indicador es a través del registro de incidencias de SI que mantiene el responsable de Seguridad de la Información.	Anual
9.1.2	Controles físicos de entrada				
9.1.3	Seguridad de oficinas, despachos e instalaciones				

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
9.1.4	Protección contra las amenazas externas de origen ambiental				
9.1.5	Trabajo en áreas seguras				
9.1.6	Áreas de acceso público y de carga y descarga.				
9.2 Seguridad de los equipos					
9.2.1	Emplazamiento y protección de equipos.	Número de incidencias de disponibilidad imputadas a la seguridad de los equipos en las oficinas.	< 3 por año	El modo de calcular este indicador es a través del registro de incidencias de SI que mantiene el responsable de Seguridad de la Información.	Anual
9.2.2	Instalaciones de Suministro				
9.2.3	Seguridad del cableado				
9.2.4	Mantenimiento de los equipos				
9.2.5	Seguridad de los equipos fuera de las instalaciones	Número de incidencias de seguridad en equipos ubicados fuera de las instalaciones.	< Número de Incidencias del año anterior	El modo de calcular este indicador es a través del registro de incidencias de SI que mantiene el responsable de Seguridad de la Información.	Anual
9.2.6	Reutilización o retirada segura de los equipos	a) % de equipos reutilizados a los que se ha aplicado correctamente los procedimientos de reutilización segura b) % de equipos retirados a los que se ha aplicado correctamente el procedimiento de retirada segura	a) < 10% b) < Número de Incidencias del año anterior	El modo de calcular estos indicadores es el de recoger evidencias de que los procedimientos se llevan a cabo correctamente.	Anual
9.2.7	Traslado de materiales propiedad de la empresa.	% de envíos que han llegado a su destino sin sufrir daños ni extravío.	< 5%	Se calcula a través de los registros de las empresas de transporte contratadas para llevar a cabo los traslados.	Anual
10. GESTION DE COMUNICACIONES Y OPERACIONES. 10.1. Responsabilidades y Procedimientos de Operación.					
10.1.1	Documentación de los procedimientos de operación	Número procedimientos de operación no documentados detectados	< 5	Se alimenta del Registro de Incidencias del SGSI	Anual
10.1.2	Gestión de cambios	Número de cambios realizados	N/A	Se extrae del Registro de Cambios	Anual

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
10.1.3	Segregación de tareas	Número de construidos realizados y probados por una misma persona.	> 95%	Se extrae del Registro de Cambios. Permite conocer cuántos fallos de este control han habido en un ejercicio.	Anual
10.1.4	Separación de los recursos de desarrollo, prueba y operación.	No se define			
10.2 Gestión de la provisión de Servicios por terceros					
10.2.1	Provisión de Servicios	Número de incidencias de disponibilidad de los servicios proporcionados por terceros	< 5 por año	Se calcula a través del Registro de Incidencias	Anual
10.2.2	Supervisión y revisión de Servicios prestados por terceros	Número de incumplimientos de SLAs	< 5 por año	Se extrae del registro de incidencias en conjunción con el detalle de la resolución de cada una de éstas y con los acuerdos de servicio a los que se ha llegado con los diferentes proveedores.	Anual
10.2.3	Gestión del cambio en servicios prestados por terceros	Número de cambios realizados en servicios prestados por terceros	N/A	Se extrae del registro de cambios	Anual
10.3 Planificación y Aceptación del Sistema					
10.3.1	Gestión de capacidades	Promedio de ocupación de los recursos de los sistemas	< 60%	Se obtiene del subsistema de reporting del sistema de monitorización de los sistemas.	Semanal
10.3.2	Aceptación del Sistema	% de sistemas incorporados según procedimiento.	> 95%	Se obtiene del registro de cambios vs la recopilación de evidencias de que se ha seguido el procedimiento de aceptación.	Anual
10.4 Protección contra el código malicioso y descargable					
10.4.1	Controles contra el código malicioso	Número de virus/malware detectados en los sistemas.	N/A	Se obtiene de los registros de la consola del antivirus Permite evaluar la idoneidad de los controles que se llevan a cabo, así como del desempeño del software antivirus.	Semanal
10.4.2	Controles contra el código descargado en el cliente	Número de programas no autorizados detectados en los sistemas.	< 2 por semana	Se obtiene de los registros de la consola del software de auditoría de los sistemas.	Semanal
10.5 Copias de Seguridad					
10.5.1	Copias de Seguridad de la Información	a) % de backups correctos b) % de pruebas de recuperación	a) > 95% a) > 95%	Tanto (a) como (b) se obtienen de los registros de las copias de seguridad.	Semanal

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
		de backups correctos			
10.6 Gestión de la seguridad de las redes					
10.6.1	Controles de Red	Número de intrusiones detectadas	0 por semana	Se obtiene de los logs del IDS así como de los registros de incidencias relacionadas con la SI	Semanal
10.6.2	Seguridad de los servicios de Red				
10.7 Manipulación de los soportes					
10.7.1	Gestión de soportes extraibles	Número de incidencias relacionadas con la gestión de soportes extraíbles	< 3 por año	Se obtiene del registro de incidencias del SI	Anual
10.7.2	Retirada de soportes	% de cintas retiradas correctamente	> 95%	Se calcula a través de evidencias del correcto retiro de las cintas.	Anual
10.7.3	Procedimientos de manipulación de información	Número de incidencias relacionadas con la gestión de soportes extraíbles.	< 3 por año	Se obtiene del registro de incidencias del SI	Anual
10.7.4	Seguridad de la documentación del sistema.	Número de accesos no autorizados a la documentación del sistema.	0 por año	Se obtiene del registro de incidencias del SI	Anual
10.8 Intercambio de Información.					
10.8.1	Políticas y procedimientos de intercambio de información.	Número de incumplimientos de la política y procedimientos de intercambio de información.	< 3 por año	Se obtiene del registro de incidencias del SI	Anual
10.8.2	Acuerdos de intercambio	Número de incidencias de SI en las transacciones de compra	< 3 por año	Se obtiene del registro de incidencias del SI	Anual
10.8.3	Soportes físicos en tránsito	% de cintas entregadas con éxito	> 95%	Se obtiene de los certificados de la empresa que lleva a cabo el transporte	Anual
10.8.4	Mensajería electrónica	Número de incidencias de SI en la mensajería electrónica	< 3 por año	Se obtiene del registro de incidencias del SI	Anual
10.8.5	Sistemas de información empresariales	Número de incidencias de SI en los sistemas de información empresariales	< 12 por año	Se obtiene del registro de incidencias del SI	Anual

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
10.9 Servicios de Comercio Electrónico					
10.9.1	Comercio Electrónico	No Aplica			
10.9.2	Transacciones en línea				
10.9.3	Información públicamente disponible.	No se define			
10.10 Supervisión					
10.10.1	Registros de Auditoría	% de sistemas que implementan registros de auditoría	> 95%	Se obtiene de las evidencias de la existencia de los registros de auditoría	Anual
10.10.2	Supervisión del uso del Sistema	Número de No-conformidades en los sistemas supervisados	0	Se obtiene de los Resultados de auditorías internas.	Según planificación de auditorías
10.10.3	Protección de la información de los registros	Número de incidencias sobre acceso no autorizado a los registros de auditorías.	0	Se obtiene del registro de incidencias del SI	Anual
10.10.4	Registros de administración y operación	% de sistemas que monitorizan los accesos de los administradores y operadores	> 95%	Obtenido de las evidencias de los accesos de los administradores y los operadores	Anual
10.10.5	Registro de fallos	% de aplicaciones que registran sus fallos.	>75%	Obtenido de las evidencias de que las aplicaciones registran los errores	Anual
10.10.6	Sincronización del reloj.	% de servidores con el reloj sincronizado	> 95%	Se puede obtener directamente haciendo consultas al sistema NTP.	Semanal
11. CONTROL DE ACCESO **11.1. Requisitos de Negocio para el control de Acceso**					
11.1.1	Política de control de acceso	Número de incumplimientos de la política de control de acceso	< 3 por año	Se obtiene del registro de incidencias del SI	Anual
11.2 Gestión de Acceso de Usuario					
11.2.1	Registro de usuario	Número de incumplimientos de la política de control de acceso	< 3 por año	Se obtiene del registro de incidencias del SI	Anual
11.2.2	Gestión de privilegios				
11.2.3	Gestión de contraseñas de usuario.				
11.2.4	Revisión de los derechos de acceso de usuario.	Número de revisiones de derechos de	>= 1 por año	Se obtiene de los registros de las revisiones de derechos de acceso de usuario.	Anual

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
		acceso de usuario.			
11.3 Responsabilidades de Usuario					
11.3.1	Uso de contraseñas	Número de no-conformidades en la cláusula de Responsabilidades de usuario	0	Se obtiene de los registros de las auditorías	Según planificación de las auditorías
11.3.2	Equipo de usuario desatendido				
11.3.3	Política de puesto de trabajo despejado y pantalla limpia				
11.4 Control de Acceso a la red					
11.4.1	Política de uso de los servicios de red	Número de incumplimientos de la política de control de acceso a la red.	< 3 por año	Se obtiene del registro de incidencias del SI	Anual
11.4.2	Autenticación del usuario para conexiones externas	Número de incumplimientos de la política de Gestión de Accesos	< 3 por año	Se obtiene de los registros de las auditorías	Según planificación de las auditorías
11.4.3	Identificación de los equipos en las redes	% de equipos que cumplen la política de identificación de los equipos en las redes	100%	Obtenido de la consola de gestión de la red (servidor del DHCP).	Semanal
11.4.4	Diagnóstico remoto y protección de los puertos de configuración.	Número de incumplimientos de la política de control de acceso a la red.	0	Se obtiene de los registros de las auditorías	Según planificación de las auditorías
11.4.5	Segregación de las redes				
11.4.6	Control de la conexión a la red.				
11.4.7	Control de encaminamiento (routing) de red				
11.5 Control de Acceso al Sistema Operativo					
11.5.1	Procedimientos seguros de inicio de sesión.	Número de incidencias de SI asociadas al control de acceso al sistema operativo.	< 5 por año	Se obtiene del registro de incidencias de SI	Anual
11.5.2	Identificación y autenticación de usuario.				
11.5.3	Sistema de gestión de contraseñas.	Número de no-conformidades en el Sistema de gestión de contraseñas y sesiones definido	0	Se obtiene de los registros de las auditorías	Según planificación de las auditorías

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
11.5.4	Uso de los recursos del sistema.	a) Número de instalaciones de software en servidores que han acabado con resultados erróneos. b) Número de programas no autorizados instalados en equipos personales.	a) < 3 por año b) < 2 por revisión	a) Obtenido del Registro de cambios b) Obtenido del Registro de incidencias del SI (reportado en las revisiones periódicas de los equipos personales). Permiten medir la ocurrencia de incumplimientos en las políticas respecto al software.	a) Anual b) Según periodicidad de las revisiones.
11.5.5	Desconexión automática de sesión	Número de no-conformidades en el Sistema de gestión de contraseñas y sesiones definido	0	Se obtiene de los registros de las auditorías	Según planificación de las auditorías
11.5.6	Limitación del tiempo de conexión.				
11.6 Control de acceso a las aplicaciones y a la información					
11.6.1	Restricción del acceso a la información.	Número de incidencias de SI relacionadas con el control de acceso a las aplicaciones y a la información	< 5 por año	Se obtiene del registro de incidencias.	Anual
11.6.2	Aislamiento de sistemas sensibles.				
11.7 Gestión de Acceso de Usuario					
11.7.1	Ordenadores portátiles y comunicaciones móviles.	Número de incumplimientos graves de la política de seguridad en equipos personales	< 3 por año	Se obtiene de las evidencias obtenidas de la ejecución de los procesos disciplinarios. Permite conocer el grado de cumplimiento de la política.	Anual
11.7.2	Teletrabajo	No 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.	Número de no-conformidades sobre requisitos de seguridad de los SI	0 por cada auditoría	Se obtiene de los registros de las auditorías	Según planificación de auditorías
12.2 Tratamiento correcto de las aplicaciones					
12.2.1	Validación de los datos de entrada.	Número de no-conformidades sobre requisitos de tratamiento correcto de las aplicaciones.	0 por cada auditoría	Se obtiene de los registros de las auditorías	Según planificación de auditorías
12.2.2	Control del procesamiento interno				
12.2.3	Integridad de los mensajes.				
12.2.4	Validación de los datos de salida.				
12.3 Controles criptográficos					

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
12.3.1	Política de uso de los controles criptográficos.	Número de no-conformidades sobre los Controles criptográficos	0 por auditoría	Se obtiene de los registros de las auditorías	Según planificación de auditorías
12.3.2	Gestión de claves.				
12.4 Seguridad de los archivos de Sistema					
12.4.1	Control del software en explotación.	Número de no-conformidades sobre la seguridad de los archivos de sistema detectadas	0 por auditoría	Se obtiene de los registros de las auditorías	Según planificación de auditorías
12.4.2	Protección de los datos de prueba del sistema.				
12.4.3	Control de acceso al código fuente de los programas.	Número de incidencias producidas por accesos no autorizados a los códigos fuente de los programas.	< 2 por año	Obtenida del Registro de incidencias del SI	Anual
12.5 Seguridad en los procesos de desarrollo y soporte					
12.5.1	Procedimientos de control de cambios.	Tiempo medio de resolución de cambios	< tiempo que el año anterior	Obtenido del detalle de los registros de cambios. El propósito es determinar la agilidad del procedimiento.	Anual
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	% de cambios sobre los que se efectúa la revisión	> 90%	Se obtiene a partir de las evidencias de que se han llevado a cabo las revisiones técnicas y a partir del registro de cambios	Anual
12.5.3	Restricciones a los cambios en los paquetes de software.	No aplica.			
12.5.4	Fugas de información.	Número Incidencias que han provocado o han podido provocar fugas de información	0 por año	Se obtiene a partir del registro de incidencias del SI	Anual
12.5.5	Externalización del desarrollo de software.	No aplica.			
12.6 Gestión del a vulnerabilidad técnica					
12.6.1	Control de las vulnerabilidades técnicas.	% de vulnerabilidades encontradas que han sido evaluadas en el mapa de riesgos	> 95%	Calculado a partir de las fuentes de información de vulnerabilidades técnicas y del registro de revisiones del mapa de riesgos.	Anual
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.					

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
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	% de incidentes en la seguridad de la información detectados que han sido notificados de manera conveniente	> 95%	Se calcula a través de las Reclamaciones e Incidencias registradas.	Anual
13.1.2	Notificación de puntos débiles de seguridad.				
13.2 Gestión de incidentes y mejoras de la Seguridad de la Información					
13.2.1	Responsabilidades y procedimientos.	Tiempo medio de resolución de incidencias	< que el año anterior.	Se obtiene a partir del detalle de reclamaciones e incidencias	Anual
13.2.2	Aprendizaje de los incidentes de seguridad de la información.	Número de entradas almacenadas en la base de conocimiento.	N/A	Obtenido a partir de la documentación que forma la base de conocimiento. Permite conocer el volumen de información que se ha incorporado a ésta.	Anual
13.2.3	Recopilación de evidencias.	% de incidentes de SI con repercusiones legales de los que se ha recopilado evidencias	> 95%	Obtenido del Registro de Incidencias de SI y de las evidencias recopiladas. Nos da información sobre el grado de concienciación del personal sobre la obtención de evidencias de cara a posibles procesos legales.	Anual
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO **14.1. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio**					
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Número de no-conformidades en la gestión de la continuidad del negocio	0 por auditoría	Se obtiene de los registros de las auditorías	Según planificación de auditorías
14.1.2	Continuidad del negocio y evaluación de riesgos.				
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.				
14.1.4	Marco de referencia para la planificación de la continuidad del negocio.				
14.1.5	Pruebas, mantenimiento y re-evaluación de planes de continuidad.	% de sistemas disponibles en las pruebas del plan de	> 95%	Obtenido de los registros de las pruebas del plan de continuidad del negocio. Permite constatar que se está llevando a	Según periodicidad de las pruebas del PCN.

Ref.	Cláusula/Control	Indicador	Umbral de Tolerancia	Descripción	Frecuencia
		continuidad del negocio		cabo un mantenimiento correcto del plan de continuidad del negocio.	
15. CUMPLIMIENTO **15.1. Cumplimiento de los requisitos legales**					
15.1.1	Identificación de la legislación aplicable.	Número de no-conformidades en el cumplimiento de requisitos legales.	0 por auditoría	Obtenido de los registros de las auditorías	Según planificación de auditorías
15.1.2	Derechos de propiedad intelectual (DPI).				
15.1.3	Protección de los documentos de la organización.				
15.1.4	Protección de datos y privacidad de la información de carácter personal.				
15.1.5	Prevención del uso indebido de recursos de tratamiento de la información.				
15.1.6	Regulación de los controles criptográficos.				
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico					
15.2.1	Cumplimiento de las políticas y normas de seguridad.	Número de no-conformidades en el cumplimiento de políticas y normas de seguridad.	0 por auditoría	Obtenido de los registros de las auditorías	Según planificación de auditorías
15.2.2	Comprobación del cumplimiento técnico.				
15.3 Consideraciones sobre las auditorías de los sistemas de información.					
15.3.1	Controles de auditoría de los sistemas de información.	No se define			
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	Número de accesos no autorizados a las herramientas y registros para la auditoría de la aplicación de controles de seguridad.	0 por año	Se obtiene del registro de incidencias del SI	Anual

	DECLARACIÓN DE APLICABILIDAD	**Código:**	PR-SOA-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	1

Histórico de Versiones			
Versión	Fecha	Editor	Cambios
1.0	01/03/2013	J.Consuegra	Edición Inicial

Declaración de Aplicabilidad

Objeto

En este apartado se resumen los controles de seguridad que aplica o planea aplicar la organización en el marco de la implementación del sistema de gestión de seguridad de la información.

Los controles aquí detallados se numerarán de acuerdo al Anexo A de la norma ISO/IEC 27001:2005. Esta es la norma que se aplica de referencia para la implementación del Sistema de Gestión de la Seguridad de la Información.

En la siguiente tabla describe la forma de aplicación de los controles a través de las columnas que tendrán la siguiente interpretación:

- **REF:** Número de referencia respecto a la numeración de las normas (ISO27001 e ISO27002)
- **Cláusula/Control:** Descripción de la cláusula o control que se está midiendo.
- **Aplicación:** La manera en cómo la cláusula o control ha sido aplicado en la implantación o bien la justificación de porqué no ha sido aplicada. Se incluye el estado en función de:
    - **Alcanzado:** Control ya resuelto
    - **Alcanzado/Verificar:** Ya está resuelto, el proyecto verificará y propondrá ajuste si es necesario.
    - **Proyecto actual:** El proyecto actual contempla su desarrollo
    - **En RTP:** Controlado directamente en el Risk Treatment Plan
- **Proceso:** El proceso o procedimiento dentro del manual de seguridad donde se ve reflejado
- **Results/Indicad:** Resultados o indicadores que se utilizan para medir o comprobar la implementación del control (cuando sea posible y viable). Entre los resultados también se entienden los registros o evidencias de la aplicación del control. En algunos casos en los que el control solo se puede verificar si está o no está, es posible que no exista información de resultados o indicadores de aplicación del control, estos controles deberán ser revisados por auditorías del sistema o auditorías técnicas.

Ámbito

Se incluye los sistemas de Gestión de Seguridad de la Información de TPS Technology S.L.

El propietario de este proceso es el Responsable del Área de Seguridad de la Información y se considera de tipo Estratégico.

TPS TECHNOLOGY	**DECLARACIÓN DE APLICABILIDAD**	**Código:**	PR-SOA-01
		Versión:	1
		Vigente:	01/03/2013
		Página:	2 de 17

Ficha de Proceso

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
5. POLÍTICA DE SEGURIDAD **5.1. Política de Seguridad de la Información**					
5.1.1	Documento de Política de Seguridad de la Información	Aplica	Se dicta la política de seguridad de la información y las políticas subsidiarias. Revisadas y firmadas por la dirección de la organización.	- Documento de Política de Seguridad de la Información	No se define
5.1.2	Revisión de la política de Seguridad de la Información.	Aplica	Revisión anual planificada y revisión como parte de acciones correctivas o preventivas aplicadas.	- Documento de Revisión por la dirección. - Informe de la revisión por la dirección	Revisión por la dirección (mínimo anual).
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	Proyecto autorizado por la dirección. Inversión de recursos, tiempos y formaciones.	- Documento de Política de Seguridad de la Información - Revisión por la dirección - Registro de Riesgos	No se define
6.1.2	Coordinación de la seguridad de la información.	Aplica	Definir un Área encargada de la gestión de la seguridad de la información, el proceso de gestión de riesgos, y procesos que aseguran la sistemática de actuación frente a las vulnerabilidades e incidentes de seguridad.	- Inventario de Activos (define el responsable de cada activo). - Revisión por la dirección (Planificación del seguimiento de Actividades).	- Evaluación periódica de los riesgos de Seguridad de la Información
6.1.3	Asignación de responsabilidades relativas al seguimiento de la información.	Aplica	Se mantiene un inventario detallado de activos. Para cada activo se detalla un responsable o propietario. Se definen roles y responsabilidades para los procesos definidos. En el documento de Riesgos (RSI) se vinculan los procesos e instrucciones relacionados con el tratamiento de los riesgos.	- Riesgos - Organigrama de la compañía - Manual de Seguridad de la información	- Evaluación periódica de los riesgos de Seguridad de la Información - Evaluaciones Periódicas del personal.
6.1.4	Proceso de autorización de recursos para el tratamiento de la información.	Aplica	La introducción de cambios en los activos se gestionará a través de un proceso de cambios que medirá el impacto de la introducción o cambio. El proceso enlaza con la gestión de riesgos para que estos se actualicen.	- Riesgos - Gestión de Cambios	Número de Cambios realizados en infraestructura, software y hardware.

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
6.1.5	Acuerdos de Confidencialidad	Aplica	Se establecen acuerdos para: - General para todos los trabajadores - Protección de datos de carácter personal (LOPD) - Acuerdos de confidencialidad con los clientes.	- LOPD - Procesos de Gestión de Personal. - Procesos de Gestión de Clientes	No se define
6.1.6	Contacto con las Autoridades	Aplica	Se define la instrucción de contactos de emergencia incluyendo: Policía, Bomberos, etc. Se hace disponible esta información en la organización	- Plan de Continuidad del Negocio - Agenda de contactos	No se define
6.1.7	Contacto con grupos especializados de interés para la organización.	Aplica	Foros y listas de correo de seguridad de la información, de desarrolladores de bases de datos Oracle y Microsoft, de programación Java, php y .net, de Sistemas operativos Windows y Linux.	- Proceso de Formación - Inventario de Grupos de Interés	No se define
6.1.8	Revisión independiente de la seguridad de la información.	Aplica	Auditorías internas de seguridad.	- Procedimiento de Auditorías Internas - Planificación de Auditorías - Revisión por la dirección	Cumplimiento del plan de auditorías
6.2 Terceros					
6.2.1	Identificación de los riesgos derivados del acceso de terceros.	Aplica	Se establece una supervisión de riesgos con los proveedores de servicios de la empresa (entre ellos, los comerciales).	- Gestión de Accesos - Gestión de Riesgos - Confidencialidad en Outsourcing	Revisión y evaluación periódica de riesgos de Seguridad de la Información
6.2.2	Tratamiento de la seguridad en la relación con los clientes.	Aplica	Actualmente los clientes no tienen acceso a las aplicaciones albergadas en servidores de la oficina, aunque en un futuro no se descarta la posibilidad de ubicar un servidor de aplicaciones en la DMZ para que éstos puedan acceder a las aplicaciones que pueda albergar.	- Gestión de Accesos - LOPD	Revisión Mensual de Accesos.
6.2.3	Tratamiento de la seguridad en contratos con terceros.	Aplica	Cuando se realizan compras a terceros se hace una revisión de riesgos para identificar qué impacto tienen éstas en el SGSI.	- Compras de Productos y Servicios - Confidencialidad en Outsourcing	Revisiones de Riesgos realizadas (sólo para compras no habituales).
7. GESTIÓN DE ACTIVOS **7.1. Responsabilidad sobre los activos.**					
7.1.1	Inventario de Activos	Aplica	Se mantiene un inventario de Activos definido por el proceso de Gestión de cambios. El registro de Riesgos relaciona los riesgos con tipos de Activos. La información se detalla en función de los requerimientos de uso. El Sub-Área de recursos humanos mantiene un registro de personas y de sus capacitaciones.	- Inventario de Activos - Gestión de Cambios - Riesgos - Personas	No conformidades en la revisión de Activos.
7.1.2	Propiedad de los Activos	Aplica	El inventario de activos identifica el Propietario de los activos y el Responsable, siendo el propietario la persona encargada de establecer los controles de seguridad que serán aplicados al activo. El responsable es la persona a quién se le ha encargado el activo para su uso y protección.	- Riesgos - Inventario de Activos - Gestión de Cambios - Control de Documentos - Gestión de Accesos	No se define

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
7.1.3	Uso aceptable de los activos	Aplica	Se especifica en gestión de accesos. Se definen usos aceptables para herramientas de administración y equipos personales.	- Gestión de Accesos - Seguridad en equipos personales.	No se define
7.2 Clasificación de la información					
7.2.1	Directrices de clasificación	Aplica	Se establece la clasificación en cuatro tipos: • Pública o desclasificada • Propietaria • Confidencial de cliente • Confidencial de TPS	- Documentos y Registros	No se define
7.2.2	Etiquetado y manipulado de información	Aplica	Se establecen directrices de etiquetado de soportes físicos y electrónicos, así como para el almacenamiento que garanticen las condiciones de confidencialidad y disponibilidad más adecuadas.	- Documentos y Registros	Número de Incidencias sobre soportes documentales.
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS **8.1. Antes del Empleo**					
8.1.1	Funciones y Responsabilidades	Aplica	Se establecen perfiles de trabajo para cada miembro de la organización. Se establece el perfil previo a la contratación y se evalúa al candidato de acuerdo al perfil definido.	- Contratación	No se define
8.1.2	Investigación de Antecedentes	Aplica	Se incluye en la fase de selección y contratación la verificación y comprobación del CV con las referencias.	- Contratación	No se define
8.1.3	Términos y condiciones de contratación	Aplica	Al momento de contratación y de acuerdo al perfil de la persona se presentará al solicitante los términos de contratación generales y de seguridad aplicables: Contrato de confidencialidad, Usuarios Autorizados de LOPD, etc	- Contratación - Confidencialidad de Outsourcing - Expediente del trabajador	Las faltas a la normativa quedan registradas en el expediente del trabajador
8.2 Durante el empleo					
8.2.1	Responsabilidades de la Dirección	Aplica	Especificación de políticas de Seguridad de Información, involucrar al personal en el funcionamiento del SGSI, evaluación del desempeño del personal	- Formación - Ficha de Evaluación - Manual de acogida	Evaluación continua del Personal.
8.2.2	Concienciación, formación y capacitación en Seguridad de la información	Aplica	Formación del personal llevada a cabo desde la acogida en temas de Seguridad de Información, en el conocimiento del SGSI. Evaluación del desempeño del personal.	- Formación - Ficha de Evaluación - Manual de acogida	Evaluación continua del Personal.
8.2.3	Proceso Disciplinario	Aplica	Se dicta el proceso disciplinario de conformidad con el Contrato de Trabajo, y las leyes vigentes (LOPD, LPI, etc).	- Proceso Disciplinario - Personas - Expediente del trabajador	Evaluación continua del Personal. Revisión por la dirección de incidencias de seguridad de la información
8.3 Cese del empleo o cambio de puesto de trabajo					
8.3.1	Responsabilidad del cese o cambio	Aplica	Se establece como parte del proceso de contratación (ciclo de vida del empleado). Se recogen en el contrato de confidencialidad.	- Contratación - Confidencialidad - Contrato de empleados	No se define

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
8.3.2	Devolución de Activos	Aplica	Se recoge en instrucciones precisas en el proceso de contratación. Los cambios en los inventarios de activos se coordinan a través de gestión de activos.	- Contratación - Gestión de Activos	No conformidades en la revisión de Activos
8.3.3	Retirada de los derechos de Acceso	Aplica	Se recoge en instrucciones precisas en el proceso de contratación. Se establecen procedimientos claros para el registro y administración de accesos en el proceso e instrucción de gestión de accesos.	- Contratación - Gestión de Accesos	Resultados de supervisión de accesos de acuerdo al proceso de gestión de accesos.
9. SEGURIDAD FÍSICA Y DEL ENTORNO **9.1. Áreas seguras**					
9.1.1	Perímetro de seguridad física	Aplica	Los controles de seguridad física se recogen en la instrucción de gestión de acceso. Son aplicables distintos niveles: barreras físicas de entrada a la oficina, seguridad adicional de acceso al CPD de la oficina, seguridad para información física (armarios con llaves/claves).	- Gestión de Accesos	Las auditorías tendrán en cuenta la comprobación de estos requisitos.
9.1.2	Controles físicos de entrada	Aplica	Los controles de acceso físicos se recogen en la instrucción de gestión de acceso. Para cada activo se definen controles físicos, técnicos y organizacionales. Se dicta la política de gestión de accesos de conformidad con la política del SGSI donde se regula el uso de controles de acceso.	- Gestión de Accesos	Las auditorías tendrán en cuenta la comprobación de estos requisitos.
9.1.3	Seguridad de oficinas, despachos e instalaciones	Aplica	Se dicta la política de uso de las oficinas conforme a la política de gestión de accesos y del SGSI donde se dictan las medidas de seguridad en uso de la oficina.	- Gestión de Accesos	Las auditorías tendrán en cuenta la comprobación de estos requisitos.
9.1.4	Protección contra las amenazas externas de origen ambiental	Aplica	Para cada tipo de efecto que podría causar amenaza externa identificada se define un plan de respuesta.	- Plan de Continuidad del Negocio	Pruebas realizadas de los planes de continuidad.
9.1.5	Trabajo en áreas seguras	Aplica	Se define como área segura la sala de la oficina donde se encuentra el CPD.	- Gestión de Accesos	Supervisión y Auditoría del cumplimiento de las normas.
9.1.6	Áreas de acceso público y de carga y descarga.	**NO Aplica**	NO APLICA. Las oficinas no cuentan con un punto de carga y descarga.	No Aplica	No Aplica.
9.2 Seguridad de los equipos					
9.2.1	Emplazamiento y protección de equipos.	Aplica	Los servidores de producción se alojan en el CPD de la oficina, dentro de Racks Cerrados. El uso de equipos personales se encuentra regulado por la política de uso de equipos personales.	- Gestión de Accesos - Seguridad de Equipos Personales	No se define
9.2.2	Instalaciones de Suministro	Aplica	Se establece en el plan de continuidad para este tipo de riesgos	- Planes de contingencia	Se levantan incidencias cuando sucedan este tipo de situaciones para verificar la efectividad de las medidas

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
9.2.3	Seguridad del cableado	Aplica	El cableado interno se encuentra canalizado por conducciones específicas del suelo técnico instalado en las oficinas. Se define una política de infraestructura para tal fin.	- Manual de operaciones	Se comprueba en las auditorías
9.2.4	Mantenimiento de los equipos	Aplica	El mantenimiento de los equipos se realiza de acuerdo a los procesos de gestión de activos. El inventario de infraestructuras define las fechas de realización de labores de mantenimiento.	- Gestión de infraestructuras. - Gestión de Software y Hardware.	Se comprueba en las auditorías
9.2.5	Seguridad de los equipos fuera de las instalaciones	Aplica	Se define como parte de la política de uso de equipos personales, las medidas de seguridad para equipos fuera de las oficinas.	- Seguridad de equipos personales. - Gestión de Software y Hardware	Se comprueba en las auditorías
9.2.6	Reutilización o retirada segura de los equipos	Aplica	Se define un procedimiento para la reutilización y retiro de equipos. El proceso de gestión de software/hardware solicita a gestión de cambios que se apliquen las medidas definidas.	- Seguridad de equipos personales. - Gestión de Software y Hardware.	Se verifica en la gestión de cambios.
9.2.7	Traslado de materiales propiedad de la empresa.	Aplica	Se define la política de seguridad de equipos personales y en ella el apartado de seguridad de equipos fuera de las instalaciones y el sub apartado de seguridad en el transporte de equipos.	- Seguridad de equipos personales. - Gestión de Software y Hardware.	No se define.
10. GESTION DE COMUNICACIONES Y OPERACIONES. 10.1. Responsabilidades y Procedimientos de Operación.					
10.1.1	Documentación de los procedimientos de operación	Aplica	Se mantiene la documentación del sistema de gestión.	- Mapa de procesos - Manual del SGSI - Documentos Internos y Externos	Resultados de Auditorías del Sistema de Gestión
10.1.2	Gestión de cambios	Aplica	Se clasifican los cambios en dos tipos; Internos y Externos. Los Internos son los cambios sobre Infraestructura, Software, Hardware, que se llevan a cabo sobre propiedades de TPS Technology. Los Externos son los cambios que se llevan a cabo sobre los activos de los clientes motivados por proyectos de Software, de Sistemas o de Bases de Datos.	- Gestión de Infraestructuras - Gestión de Software / Hardware - Gestión de cambios - Implantación y Administración de Sistemas - Implantación y Administración de Bases de Datos - Desarrollo y Mantenimiento de Software	Registros de Cambios.
10.1.3	Segregación de tareas	Aplica	Se recomienda en los procesos de gestión de cambios que las personas que construyen los cambios no sean las mismas que desplieguen el cambio construido. Se recomienda su aplicación para que la persona que desarrolla el cambio no sea la misma que lo pruebe.	- Gestión de cambios - Implantación y Administración de Sistemas - Implantación y Administración de Bases de Datos - Desarrollo y Mantenimiento de Software	No se define
10.1.4	Separación de los recursos de desarrollo, prueba y operación.	Aplica	Se establece la separación entornos de desarrollo, pre-producción y producción. Como norma general, el entorno de desarrollo se encuentra en las estaciones de trabajo de los Administradores y desarrolladores.	- Manual de operaciones de sistemas - Implantación y Administración de Sistemas	No se define

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
			Los entornos de pre-producción y producción se encuentran en los servidores de la compañía	- Implantación y Administración de Bases de Datos - Desarrollo y Mantenimiento de Software	
10.2 Gestión de la provisión de Servicios por terceros					
10.2.1	Provisión de Servicios	Aplica	Se consideran servicios provistos por terceros el hosting de la página web corporativa, los servicios proporcionados por los comerciales, servicios de telecomunicaciones, garantías y soporte de Hardware y Software	- Manual de operaciones de sistemas - Manual de operaciones del proveedor de hosting	Incidencias de disponibilidad de la página web. Incidencias de disponibilidad de las comunicaciones Incidencias resueltas por cada uno de los proveedores de soporte.
10.2.2	Supervisión y revisión de Servicios prestados por terceros	Aplica	Se hace el registro de todas las incidencias de proveedores por incumplimiento de SLAs. Se hace la evaluación periódica de proveedores.	- Evaluación de Proveedores	Resultados de Evaluación de los proveedores.
10.2.3	Gestión del cambio en servicios prestados por terceros	Aplica	Se gestionan los cambios en la infraestructura del proveedor de hosting a través de su proceso de gestión de cambios.	- Manual de operaciones de sistemas - Manual de operaciones del proveedor de hosting	Indicadores de gestión de cambios.
10.3 Planificación y Aceptación del Sistema					
10.3.1	Gestión de capacidades	Aplica	Se monitorizan los sistemas a través de la herramienta ATENEA (de desarrollo propio) que se ejecuta en el servidor de producción de la empresa. Se define la instrucción de monitorización y control de servicios	- Gestión de Software / Hardware - Manual de Operaciones de ATENEA - Manual de Operaciones de sistemas	Número de Incidencias producidas por pérdida de capacidad de los servicios
10.3.2	Aceptación del Sistema	Aplica	Se establece una política de incorporación y aceptación de sistemas nuevos.	- Gestión de Software / Hardware - Gestión de cambios - Manual de Operaciones de Sistemas.	Indicadores de Gestión de Cambios.
10.4 Protección contra el código malicioso y descargable					
10.4.1	Controles contra el código malicioso	Aplica	Se establece la política de seguridad de equipos personales en la que se previene el uso de programas no autorizados por la organización. Se regula el uso de software antivirus y su actualización.	- Seguridad de equipos personales	Incidencias de seguridad Revisiones preventivas de equipos para comprobar el seguimiento de la política de seguridad.
10.4.2	Controles contra el código descargado en el cliente	Aplica	Se establece la política de seguridad de equipos personales en la que se previene la descarga y utilización de códigos descargables.	- Seguridad de equipos personales	Incidencias de Seguridad
10.5 Copias de Seguridad					
10.5.1	Copias de Seguridad de la Información	Aplica	Se realizan copias de seguridad de forma periódica sobre la información en el CPD de las oficinas y sobre la información en el proveedor	- Gestión de Software / Hardware - Manual de operaciones	Se mantiene un registro de la verificación de

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
			de hosting de la web. Se comprueba periódicamente el funcionamiento y la capacidad de recuperación de las copias de seguridad.	de backups - Manual de operaciones del proveedor de hosting	los backups.
10.6 Gestión de la seguridad de las redes					
10.6.1	Controles de Red	Aplica	La red local de la oficina se protege con firewalls. Se establece filtrado por MAC desde la gestión del switch para evitar la conexión no autorizada de equipos ajenos.	- Gestión de infraestructuras.	No se define
10.6.2	Seguridad de los servicios de Red	Aplica	Se establece política de redes y comunicaciones.	- Manual de operaciones.	No se define
10.7 Manipulación de los soportes					
10.7.1	Gestión de soportes extraibles	Aplica	Se establece como soporte extraíble, las cintas de los backups que se extraen semanalmente de la oficina para garantiza la recuperación en caso de desastre. Se definen controles específicos para uso, conservación, y un criterio para la exteriorización de cintas. La información en las cintas se cifra con la herramienta que hace los backups.	- Manual de operaciones de Backups	Comprobaciones del funcionamiento de los Backups
10.7.2	Retirada de soportes	Aplica	Se define un procedimiento de retiro de cintas para evitar que se desechen con información	- Manual de operaciones de Backups	No se define
10.7.3	Procedimientos de manipulación de información	Aplica	Se define una tabla donde se resumen los controles aplicados a los backups realizados en la oficina. Los controles de seguridad aplicados a los backups realizados por el proveedor de hosting de la página web se especifican en el contrato de servicio.	- Manual de operaciones de Backups. - Gestión de Software / Hardware. - Manual de operaciones del proveedor de hosting	Comprobaciones del funcionamiento de los Backups
10.7.4	Seguridad de la documentación del sistema.	Aplica	Se definen los controles aplicados tanto físicos, técnicos y organizacionales en la gestión de accesos.	- Gestión de Accesos - Documentos Internos y Externos	Las auditorías buscarán no-conformidades en la aplicación de controles
10.8 Intercambio de Información.					
10.8.1	Políticas y procedimientos de intercambio de información.	Aplica	Se especifican términos para el uso de equipos fuera de la oficina Y la forma de conectarse a los servidores.	- Seguridad en equipos personales	No se define
10.8.2	Acuerdos de intercambio	Aplica	Se establecen medidas de seguridad en las transacciones de compra.	- Compras de productos y Servicios - Compras especiales	Las auditorías comprueban la eficiencia de los controles.
10.8.3	Soportes físicos en tránsito	Aplica	Aplicado al transporte de las cintas de los backups. Se especifican los controles y medidas de seguridad aplicadas al transporte y manipulación de las cintas. El transporte es siempre delegado a la misma persona. El almacenamiento recoge medidas de seguridad	- Gestión de Software / Hardware. - Manual de operaciones de Backups	No se define

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
			para evitar el acceso no autorizado.		
10.8.4	Mensajería electrónica	Aplica	El servidor de correo es Microsoft Exchange 2003. El acceso externo al correo se lleva a cabo a través de un Front-End (OWA). La instrucción de seguridad de equipos personales define el software de comunicaciones autorizado, se selecciona software que permite comunicaciones cifradas exclusivamente.	- Gestión de Software / Hardware. - Seguridad en equipos personales	No se define
10.8.5	Sistemas de información empresariales	Aplica	Se definen las directrices para sistemas de información de uso común (CONSERIT, ATENEA, etc), y procesos de operaciones conforme a las directrices. Las vulnerabilidades de los sistemas se mantienen en el registro de riesgos de la organización, el resumen de controles aplicados se mantiene en gestión de accesos.	- Mapa de Riesgos - Gestión de Software / Hardware - Manual de operaciones de sistemas - Gestión de Accesos	Revisión periódica de Riesgos. Registro de controles aplicados.
10.9 Servicios de Comercio Electrónico					
10.9.1	Comercio Electrónico	**NO Aplica**	El comercio electrónico no está en el catálogo de servicios de la empresa.	No Aplica	No Aplica
10.9.2	Transacciones en línea	**NO Aplica**	No se llevan a cabo transacciones económicas, contractuales o solicitudes de pedidos en línea.	No Aplica	No Aplica
10.9.3	Información públicamente disponible.	Aplica	Se mantiene como información públicamente disponible la página web de la organización. Se define la política general del sitio web. Los cambios en la información de la página web de la organización se controlan por gestión de cambios.	- LOPD - Manual de operaciones de sistemas. - Gestión de Cambios	No se define
10.10 Supervisión					
10.10.1	Registros de Auditoría	Aplica	Se recomienda la implementación de registros de auditorías en el desarrollo de sistemas. Se registran los accesos externos a las redes. Se registran las conexiones al Front-End de correo. Se establecen registros de auditorías a los backups de la oficina.	- Manual de operaciones. - Manual de operaciones de Backups - LOPD	No se define
10.10.2	Supervisión del uso del Sistema	Aplica	Se supervisa: * Control de los accesos a activos, * Aplicación de controles definidos a el uso de equipos personales, * Monitorización de los sistemas, desempeño y uso de recursos a través de ATENEA * planificación de las auditorías a los sistemas de gestión de Seguridad de la Información	- Plan de auditorías - LOPD - Manual de operaciones de ATENEA - Gestión de Accesos	Resultados de auditorías.
10.10.3	Protección de la información de los registros	Aplica	Los registros de auditorías solo serán accesibles por el personal de administración del sistema. No se permitirá su borrado fuera de los términos de tiempo definidos para cada sistema. Los registros de control de acceso a LOPD son por 2 años, aunque no estén disponibles de forma online.	- LOPD	No se define
10.10.4	Registros de administración y operación	Aplica	Se hace la supervisión de los servidores de la oficina y de la disponibilidad de servicios a través de ATENEA	- Manual de operaciones de ATENEA	Informes de disponibilidad de ATENEA.

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
10.10.5	Registro de fallos	Aplica	En las aplicaciones desarrolladas por la compañía debe existir un registro de los errores de la aplicación.	- Desarrollo de Aplicaciones	Número de errores reportados en los logs de las aplicaciones
10.10.6	Sincronización del reloj.	Aplica	Se implementan en los sistemas servicios de sincronización de los relojes contra el controlador de dominio. Este, a su vez, se sincroniza con un “Time Server” en internet a través del protocolo NTP.	- Manual de Operaciones	No se define
11. CONTROL DE ACCESO **11.1. Requisitos de Negocio para el control de Acceso**					
11.1.1	Política de control de acceso	Aplica	Se desarrolla la política de control de accesos de conformidad con la política de seguridad y en atención a la legislación aplicable.	- Gestión de Accesos - Política de Seguridad	No se define
11.2 Gestión de Acceso de Usuario					
11.2.1	Registro de usuario	Aplica	Se establece para cada tipo de activo un repositorio donde hacer el registro de los usuarios para inventariar todos los accesos otorgados a cada activo.	- Gestión de Accesos	Supervisión del registro de usuarios para comprobar su adecuación
11.2.2	Gestión de privilegios	Aplica	Se establece una gestión de privilegios para cada tipo de activo de acuerdo a los procedimientos de administración de ese activo.	- Gestión de Accesos	Adecuación a las medidas definidas a cada activo.
11.2.3	Gestión de contraseñas de usuario.	Aplica	Se establece para cada tipo de activo de acuerdo a la evaluación de riesgos asociada.	- Gestión de Accesos	Adecuación a las medidas definidas a cada activo.
11.2.4	Revisión de los derechos de acceso de usuario.	Aplica	Se establece la segregación de funciones respecto a la gestión de accesos y se lleva a cabo supervisión para asegurar la continua adecuación.	- Gestión de Accesos	Supervisión del registro de usuarios para comprobar su adecuación
11.3 Responsabilidades de Usuario					
11.3.1	Uso de contraseñas	Aplica	Se define la política de seguridad de contraseñas para usuarios de servidores de las oficinas.	- Manual de operaciones.	No se define
11.3.2	Equipo de usuario desatendido	Aplica	En la política de seguridad de equipos personales se establecen medidas de protección para equipos desatendidos en las oficinas y fuera de ellas.	- Seguridad de equipos personales.	No se define
11.3.3	Política de puesto de trabajo despejado y pantalla limpia	Aplica	Se indica en la política de uso de las oficinas de la organización.	- Gestión de Accesos	Supervisión del seguimiento de la politica
11.4 Control de Acceso a la red					
11.4.1	Política de uso de los servicios de red	Aplica	Se dicta la política de redes y comunicaciones de conformidad con la política de control de accesos.	- Manual de Operaciones. - Gestión de Accesos	No se define
11.4.2	Autenticación del usuario para conexiones externas	Aplica	Los mecanismos de conexión definidos para las redes de la oficina de TPS se establece a través de conexiones VPN La especificación de estos accesos se regla en la instrucción de gestión de accesos.	- Gestión de Accesos	No se define

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
11.4.3	Identificación de los equipos en las redes	Aplica	Se documenta la forma de identificar los equipos en el manual de Operaciones	- Manual de Operaciones. - Gestión de Accesos	No se define
11.4.4	Diagnóstico remoto y protección de los puertos de configuración.	Aplica	La administración remota de los enrutadores está deshabilitada.	- Manual de Operaciones	No se define
11.4.5	Segregación de las redes	Aplica	Hay dos entornos de red separados por un firewall. Uno de ellos es la DMZ, que es donde se encuentra el Front-End de correo. El otro es la red de la empresa, donde se encuentran los servidores y las estaciones de trabajo.	- Manual de Operaciones	No se define
11.4.6	Control de la conexión a la red.	Aplica	Se configuran los proxy-firewall (endian) para dar servicio y monitorizar las conexiones salientes de la organización hacia Internet y a las VPN de los clientes	- Manual de Operaciones	No se define
11.4.7	Control de encaminamiento (routing) de red	Aplica	Se aplica al proxy-firewall que separa la DMZ de Internet, para filtrar las conexiones entrantes al front-end de correo.	- Manual de Operaciones - Gestión de Accesos	No se define
11.5 Control de Acceso al Sistema Operativo					
11.5.1	Procedimientos seguros de inicio de sesión.	Aplica	Se aplican controles en los servidores de la compañía para realizar seguimiento de las operaciones realizadas en el servidor.	- Manual de Operaciones	No se define
11.5.2	Identificación y autenticación de usuario.	Aplica	Equipos personales: Los usuarios acceden a ellos con sus usuarios de dominio. Solamente tienen permiso para instalar aplicaciones los administradores de sistemas a cargo de los equipos de la compañía. Servidores**:** Los usuarios acceden a los recursos de los servidores con su usuario de dominio pudiendo acceder solamente a los recursos asignados a su perfil. Bases de Datos: La gestión de los usuarios de BD se lleva a cabo localmente en cada instancia, siendo el administrador de ésta el que concede o revoca los permisos al usuario.	- Manual de Operaciones. - Seguridad en equipos personales. - Implementación y Administración de Bases de Datos	No se define
11.5.3	Sistema de gestión de contraseñas.	Aplica	Forma parte de los controles enumerados en el control de accesos	- Gestión de Accesos	No se define
11.5.4	Uso de los recursos del sistema.	Aplica	En base a la clasificación de riesgos se lleva a cabo a estos niveles: Servidores de Producción: La instalación de Software se lleva a cabo bajo el proceso de Gestión de Cambios Equipos Personales: La instalación de Software se regula en la política de Seguridad de equipos personales.	- Mapa de Riesgos. - Seguridad en equipos personales. - Manual de Operaciones de Sistemas	No se define

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
11.5.5	Desconexión automática de sesión	Aplica	Se detalla en la gestión de Accesos	- Gestión de Accesos	No se define
11.5.6	Limitación del tiempo de conexión.	Aplica	Se detalla en la gestión de Accesos	- Gestión de Accesos	No se define
11.6 Control de acceso a las aplicaciones y a la información					
11.6.1	Restricción del acceso a la información.	Aplica	Se hace de acuerdo a la política de gestión de accesos	- Gestión de Accesos	Se lleva a cabo la supervisión de los accesos para verificar la adecuación de estos al perfil del usuario.
11.6.2	Aislamiento de sistemas sensibles.	Aplica	Se aplica al servidor de correo y al servidor de aplicaciones de producción. La evaluación de riesgos sobre este control forma parte de la política de incorporación de nuevos sistemas.	- Manual de operaciones de sistemas	No se define
11.7 Gestión de Acceso de Usuario					
11.7.1	Ordenadores portátiles y comunicaciones móviles.	Aplica	Se dicta la política de uso de equipos personales para definir los controles técnicos, físicos y organizacionales a aplicar en estos equipos. Se considera una falta grave en el Proceso disciplinario cuando no se haga seguimiento a la política de seguridad.	- Seguridad en equipos personales. - Proceso disciplinario - Expediente del trabajador	En caso de no cumplimiento se abrirá un expediente al trabajador de acuerdo con el proceso disciplinario
11.7.2	Teletrabajo	Aplica	Definido en la Política de Uso de equipos personales.	- Seguridad en equipos personales.	En caso de no cumplimiento se abrirá un expediente al trabajador de acuerdo con el proceso disciplinario
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	Se propone la plantilla básica para documentación de requerimientos y pruebas del sistema. Para desarrollo de software de uso interno (CONSERIT y ATENEA) se deberán documentar los requerimientos. Para proyectos que se desarrollen a clientes se deberá hacer la identificación de requerimientos si estos no vinieran especificados claramente por parte del cliente.	- Implementación y Administración de Sistemas - Implementación y Administración de Bases de Datos - Desarrollo y Mantenimiento de Software - Gestión de cambios.	Controles de eficiencia de Cambios
12.2 Tratamiento correcto de las aplicaciones					
12.2.1	Validación de los datos de entrada.	Aplica	Se contempla en la instrucción de desarrollo y mantenimiento de software, que debe ser empleada por todas las personas que realicen desarrollo de software para la organización	- Desarrollo y Mantenimiento de Software	No se define
12.2.2	Control del procesamiento interno	Aplica	Se contempla en la instrucción de desarrollo y mantenimiento de software, que debe ser empleada por todas las personas que realicen	- Desarrollo y Mantenimiento de Software	No se define

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
			desarrollo de software para la organización		
12.2.3	Integridad de los mensajes.	Aplica	Se contempla en la instrucción de desarrollo y mantenimiento de software, que debe ser empleada por todas las personas que realicen desarrollo de software para la organización	- Desarrollo y Mantenimiento de Software	No se define
12.2.4	Validación de los datos de salida.	Aplica	Se contempla en la instrucción de desarrollo y mantenimiento de software, que debe ser empleada por todas las personas que realicen desarrollo de software para la organización	- Desarrollo y Mantenimiento de Software	No se define
12.3 Controles criptográficos					
12.3.1	Política de uso de los controles criptográficos.	Aplica	Se dicta la política de uso de controles criptográficos de conformidad con la política de seguridad de la organización. Para los proyectos donde se requiera el uso de controles criptográficos se identificarán los controles y la forma de aplicación	- Política de uso de controles criptográficos - Implementación y Administración de Sistemas - Implementación y Administración de Bases de Datos - Desarrollo y Mantenimiento de Software	Registros en la política de uso de controles criptográficos
12.3.2	Gestión de claves.	Aplica	Se dicta la instrucción de gestión de claves criptográficas de conformidad con la política de uso de controles criptográficos para especificar los procedimientos de gestión de claves y reacción frente a eventos.	- Gestión de claves criptográficas	Detalle de las medidas de gestión de claves en la instrucción.
12.4 Seguridad de los archivos de Sistema					
12.4.1	Control del software en explotación.	Aplica	El control es aplicado al desarrollo de CONSERIT y ATENEA. Se define la instrucción de operaciones de sistemas y el proceso de gestión de cambios para controlar la implantación de mejoras en estas aplicaciones	- Gestión de cambios - Manual de operaciones de sistemas	Indicadores de eficiencia en los cambios.
12.4.2	Protección de los datos de prueba del sistema.	Aplica	El control se aplica para el desarrollo de sistemas internos (CONSERIT y ATENEA) y para el caso en que se desarrolle software a la medida. La plantilla de requerimientos y pruebas documenta los escenarios de prueba utilizados.	- Manual de operaciones de sistemas - Desarrollo y Mantenimiento de Software - Requerimientos y pruebas	Registro de pruebas. Indicadores de eficiencia en los cambios.
12.4.3	Control de acceso al código fuente de los programas.	Aplica	Conforme a la política de gestión de accesos, solo las personas autorizadas tendrán acceso al código o la información de proyectos o sistemas. Se definen controles específicos para cada activo restringiendo su acceso por perfiles.	- Gestión de Accesos	No se define
12.5 Seguridad en los procesos de desarrollo y soporte					
12.5.1	Procedimientos de control de cambios.	Aplica	Se establece el proceso de control de cambios para activos para los cambios a CONSERIT y ATENEA. Para el desarrollo que se haga a clientes se definirá un proceso ajustado de control de cambios en las especificaciones del proyecto.	- Implementación y Administración de Sistemas - Implementación y Administración de Bases de Datos - Desarrollo y Mantenimiento de Software - Control de cambios - Manual de operaciones	Indicadores de eficiencia en los cambios.

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
				de sistemas	
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Aplica	El control se aplica a los sistemas y servicios relacionados con el funcionamiento de CONSERIT y ATENEA. La revisión técnica, si fuera necesaria para el caso de clientes, se aplicará por parte de su personal experto.	- Control de cambios - Manual de operaciones de sistemas	Indicadores de eficiencia en los cambios.
12.5.3	Restricciones a los cambios en los paquetes de software.	Aplica	NO Aplica. No se llevan a cabo modificaciones en paquetes de software adquiridos a terceros.	NO Aplica.	No Aplica.
12.5.4	Fugas de información.	Aplica	Se implementan, como mecanismos de control contra fugas de información, la restricción del acceso a activos de información, la instalación de software de protección contra troyanos y spyware	- Gestión de Accesos - Seguridad en equipos personales.	Verificaciones realizadas en los equipos.
12.5.5	Externalización del desarrollo de software.	Aplica	NO Aplica. TPS technology no subcontrata el desarrollo de software.	NO Aplica.	No Aplica.
12.6 Gestión del a vulnerabilidad técnica					
12.6.1	Control de las vulnerabilidades técnicas.	Aplica	Se aplica el control en todos los sistemas que soportan la operación * Herramientas de Oracle utilizadas * Herramientas de Microsoft utilizadas * Herramientas Open Source utilizadas. Se identifican a partir de incidencias y grupos de interés. Se agregan y valoran en el mapa de riesgos de la organización.	- Riesgos - Mapa de Riesgos. - Gestión de cambios.	Registro de Riesgos analizados.
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	Se realiza de acuerdo al proceso de gestión de incidencias. En caso de tratarse de un fallo en el sistema de gestión o en la operación, la incidencia podrá derivar en acciones correctivas, preventivas o de mejora	- Gestión de Reclamaciones e Incidencias	Registro de Incidencias. Indicadores de gestión de incidencias.
13.1.2	Notificación de puntos débiles de seguridad.	Aplica	Los puntos débiles se identificarán como incidencias y en su tratamiento se incluirán las medidas tomadas en la gestión de Riesgos. La notificación de vulnerabilidades es un aspecto clave y está contemplado como una obligación en el acuerdo de confidencialidad y el el proceso disciplinario.	- Gestión de Reclamaciones e Incidencias - Formación - Acciones correctivas y preventivas. - Acuerdo de confidencialidad - Proceso disciplinario	Registro de Incidencias. Indicadores de gestión de incidencias
13.2 Gestión de incidentes y mejoras de la Seguridad de la Información					
13.2.1	Responsabilidades y procedimientos.	Aplica	El tratamiento de incidencias se hace de acuerdo al proceso de gestión de incidencias y reclamaciones. La gestión del conocimiento se almacena en el proceso e instrucciones específicas.	- Gestión de reclamaciones e incidencias - Manual de operaciones de sistemas	Registro de Incidencias. Indicadores de gestión de incidencias
13.2.2	Aprendizaje de los incidentes de seguridad de la información.	Aplica	El proceso de análisis y resolución de incidencias tiene dos partes: Reactiva: referida a la búsqueda e implementación de acciones correctivas, Proactiva: Referida a la búsqueda e	- Incidencias	Indicadores de gestión de incidencias

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
			implementación de acciones preventivas. Adicionalmente si se identifican riesgos son comunicados a gestión de riesgos para que se evalúen y se actúe en consecuencia.		
13.2.3	Recopilación de evidencias.	Aplica	Se consideran los aspectos legales en la recopilación de evidencias en incidencias de seguridad. La LOPD establece 3 años antes de la caducidad de infracciones muy graves, (Art. 47) El RD 1720/07 establece la conservación de evidencias de registro de accesos de 2 años (Art. 103)	- Gestión de reclamaciones e incidencias - Documento de seguridad (LOPD).	No se define
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO **14.1. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio**					
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Aplica	Se define el proceso de gestión de continuidad del negocio y las directrices de continuidad del negocio de conformidad con la política de seguridad de la información.	- Gestión de continuidad - Continuidad del negocio - Política del SGSI	Planes definidos en la instrucción de continuidad del negocio
14.1.2	Continuidad del negocio y evaluación de riesgos.	Aplica	Se define en el proceso la forma de abordar los riesgos de continuidad de negocio y las interfaces con el proceso de gestión de riesgos	- Gestión de continuidad - Continuidad del negocio - Gestión de Riesgos - Mapa de Riesgos	Riesgos identificados y evaluados en el mapa de riesgos
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	Aplica	Se definen e implantan los planes de continuidad del negocio de acuerdo al orden de prioridades, en los términos presentados en la instrucción de continuidad del negocio	- Gestión de continuidad - Continuidad del negocio - Contactos de Emergencia	Planes definidos en la instrucción de continuidad del negocio
14.1.4	Marco de referencia para la planificación de la continuidad del negocio.	Aplica	Se dictan las directrices de continuidad del negocio para gobernar los aspectos generales de la continuidad y específicos de cada plan.	- Gestión de continuidad - Plantilla del Plan de continuidad	No se define
14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad.	Aplica	Se realizan pruebas periódicas en los plazos y términos acordados de los planes de continuidad definidos.	- Gestión de continuidad - Pruebas de los Planes de continuidad	Se establecen registros de las pruebas de los planes
15. CUMPLIMIENTO **15.1. Cumplimiento de los requisitos legales**					
15.1.1	Identificación de la legislación aplicable.	Aplica	Se identifica la legislación aplicable y se establece un contrato de soporte con la legislación aplicable al área de negocio de TPS Technology	- Política del SGSI - Documentos Internos y Externos - Tratamiento de requisitos legales. - Listado legislativo.	El listado legislativo muestra los cambios en la legislación y su impacto en el SGSI.
15.1.2	Derechos de propiedad intelectual (DPI).	Aplica	Se identifica la legislación aplicable en el listado legislativo. Términos contractuales en las licencias adquiridas, se hace un inventario de software licenciado para asegurar la idoneidad de su uso. Se dicta la política de cumplimiento	- Seguridad en equipos personales. - Listado legislativo.	Inventario de activos. Software licenciado.

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
			de derechos de propiedad intelectual de conformidad con la política de seguridad de la información.		
15.1.3	Protección de los documentos de la organización.	Aplica	La documentación del SGSI se encuentran disponibles en el servidor de ficheros en formato PDF. Los formatos editables solo están disponibles para los responsables de los sistemas. Se clasifica la documentación en función de su importancia. Se establecen copias de seguridad sobre información electrónica y se comprueba la efectividad de los controles. Se protegen en armarios cerrados la documentación física sensible de pérdida, autenticidad y confidencialidad.	- Documentos Internos y Externos - Control de los registros del Sistema - Manual de Operaciones de los backups. - Gestión de Accesos	Categorización de los documentos. Almacenamiento de los documentos en base a las reglas definidas. Gestión de versiones de los documentos.
15.1.4	Protección de datos y privacidad de la información de carácter personal.	Aplica	Se establece el documento de seguridad de conformidad con la legislación de protección de datos personales.	- Documento de seguridad (LOPD).	Se mantiene la documentación actualizada de ficheros en el Registro de Protección de Datos Personales
15.1.5	Prevención del uso indebido de recursos de tratamiento de la información.	Aplica	La dirección dicta y acuerda la política de SGSI, se establecen los acuerdos de confidencialidad de conformidad con la política, tanto para el personal interno como para el outsourcing. Se establece un proceso disciplinario trazado con la legislación vigente aplicable. Se pactan los términos de confidencialidad con clientes actuales y potenciales a través de las ofertas de servicios. El proceso de contratación en la fase de retención y compromiso hace la evaluación y seguimiento de la política y los acuerdos de confidencialidad	- Política del SGSI - Contratación - Proceso Disciplinario - Acuerdo de Confidencialidad - Confidencialidad para Outsourcing. - Expediente del trabajador.	Las evidencias de incumplimiento se recogerían en forma de incidencia y contribuirán al desarrollo del expediente del trabajador
15.1.6	Regulación de los controles criptográficos.	Aplica	Se dicta la política de uso de controles criptográficos de conformidad con la política de seguridad de la información y con los requerimientos contractuales de clientes y legales. Se establece una instrucción para detallar la gestión de claves de cifrado. Ambas, política e instrucción son transversales a la organización. El uso y aplicación de controles criptográficos requiere de la evaluación de riesgos y autorización por parte de la dirección. El listado legislativo y la instrucción de gestión de accesos recogen las referencias requerimientos de controles criptográficos	- Política de uso de controles criptográficos. - Gestión de claves criptográficas. - Gestión de accesos - Listado legislativo	Se mantiene un registro detallado de los controles aplicados, los procedimientos de gestión y legislación aplicable.
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	La dirección dicta y acuerda la política de SGSI, y de ella se desarrollan políticas específicas. Se establece un proceso disciplinario. Se pacta un calendario de auditorías para comprobar el cumplimiento de las políticas definidas. Se define la revisión por la dirección del SGSI	- Política del SGSI - Revisión por la dirección - Auditorías de Sistemas - Plan de Auditorías	Informes de auditoría y de revisión por la dirección

Ref.	Cláusula / Control	Aplica / No Aplica	Aplicación	Procesos / Documentos	Results / Indicadores
			como mínimo una vez al año en la que se revisa la adecuación de las políticas y el desempeño del SGSI		
15.2.2	Comprobación del cumplimiento técnico.	Aplica	Se establece la aplicación de auditorías técnicas con regularidad anual como mínimo o cuando se produzcan circunstancias que lo requieran. Se audita sobre la base de los riesgos de la organización y los controles aplicados.	- Auditorías de Sistemas - Plan de Auditorías	Resultado de las Auditorías.
15.3 Consideraciones sobre las auditorías de los sistemas de información.					
15.3.1	Controles de auditoría de los sistemas de información.	Aplica	El proceso de auditorías del sistema exige la planificación previa y concreta de los elementos a ser auditados para minimizar el riesgo de impacto en los sistemas productivos de la organización.	- Auditorías - Plan de Auditorías	No se define
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	Aplica	Las herramientas y registros para la auditoría de la aplicación de controles de seguridad estarán protegidos de accesos indebidos. Solo el usuario responsable del sistema tendrá acceso a esta información. Se aplicarán acuerdos de confidencialidad específicos cuando terceros requieran del acceso a estos.	- Auditorías de Sistemas - Instrucción de Operaciones	Acuerdos de confidencialidad de Auditores.

Análisis de Riesgos

Definición de Nivel de Riesgo Aceptable

De acuerdo con la dirección, se ha establecido que los controles a aplicar deben permitir que los riesgos analizados y valorados queden en nivel “Medio” o “Bajo” de acuerdo con el siguiente esquema establecido dentro de la definición de la metodología de Análisis de Riesgos:

		Impacto / Pérdidas		
		Leves	Moderadas	Graves
Probabilidad	Alta	**Medio**	**Alto**	**Alto**
	Moderada	**Bajo**	**Medio**	**Alto**
	Baja	**Bajo**	**Bajo**	**Medio**

Tabla 8: Riesgo Aceptable. Categorización de los riesgos

Los riesgos residuales de nivel “Alto” han de ser aceptados de manera explícita por la dirección

Como norma general, la dirección, en las revisiones periódicas de la matriz de riesgos, priorizará el tratamiento de los riesgos aceptados con valor “Medio” respecto a los riesgos calificados como “Bajo”.

Detalle del Análisis de Riesgos

Identificación de los Activos

En este apartado se realiza una lectura analítica del mapa de riesgos elaborado que se presenta en el siguiente apartado de este documento.

En el presente análisis de riesgos se han identificado 74 activos de la empresa clasificados en cinco Tipos con sus correspondientes Subtipos:

- **Físicos:** Activos de Hardware
  - **Equipos del Personal:** Equipos y útiles físicos que necesarios para que el personal de la empresa desarrolle su actividad.
  - **Equipamiento de comunicaciones:** Electrónica y dispositivos que soportan la infraestructura de las redes y comunicaciones de la compañía.
  - **Servidores:** Ordenadores que albergan servicios compartidos entre todo el personal de la empresa (aplicaciones, bases de datos, ficheros, seguridad, etc).
- **Lógicos:** Activos de Software
  - **Software de Desarrollo Interno:** Software desarrollado y mantenido por el personal del Área de Desarrollo de Aplicaciones de la organización.
  - **Software de Desarrollo Externo:** Software desarrollado por terceros y licenciado para su uso en la organización.
  - **Documentación y Datos:** Información útil para la organización almacenada en cualquier soporte (electrónico, papel,...)
- **Personal:** Los diferentes roles que intervienen en el funcionamiento de la compañía
  - **Directivos:** Corresponde al personal que forma la cúpula directiva de la compañía y que toma las decisiones sobre estrategia empresarial responsabilidad ejecutiva
  - **Mandos Intermedios:** Personal con responsabilidad sobre gestión de un área concreta de la empresa (Responsables de Área).
  - **Personal de Base:** Personal administrativo, técnicos jefes de equipo de desarrollo.
  - **Personal Externo:** Personal que tienen relación con la organización sin formar parte de ella (proveedores, clientes, autónomos, etc).
- **Entorno e Infraestructura:** Elementos de inmovilizado de la organización necesarios para que ésta pueda desempeñar su actividad.
  - **Seguridad Física:** Activos de seguridad física, tales como puertas, áreas de trabajo, áreas seguras...
  - **Suministros:** Activos relacionados con los servicios necesarios para el funcionamiento de las infraestructuras y los elementos físicos.
  - **Comunicaciones:** Proveen las conexiones de la organización con el exterior, tanto voz como datos.

- **Intangibles:** Elementos no materiales
    - **Externos a la organización:** Elementos cuya entidad no se gestiona desde dentro de la organización.
    - **Internos a la organización:** Elementos intangibles que se gestionan en el seno de la organización.

El detalle de los activos identificados y la clasificación de éstos se encuentra en el documento del “Anexo 3 – Análisis de Riesgos” en la hoja “Identificación de Activos”.

Evaluación de Riesgos

El detalle del Análisis de Riesgos se encuentra en el documento del “Anexo 3 – Análisis de Riesgos” en la hoja “Riesgos”.

Identificación del Riesgo

En este apartado se ubican los activos, vulnerabilidades, amenazas y riesgos que se van a evaluar. Se especifican los siguientes apartados:

- **ID**: A cada uno de los riesgos se le asigna un identificador para facilitar su seguimiento
- **Tipo y Subtipo de Activo**: Clasificación del activo definida en “Identificación de Activos”
- **Activo**: Una descripción del activo analizado.
- **Propietario**: Persona que se establece como propietaria del activo.
- **Vulnerabilidad**: Situaciones o aspectos que facilitan la materialización de las amenazas.
- **Amenaza**: Situación de la que se ha de proteger el activo.
- **Riesgo**: Qué consecuencias perniciosas pueden ocurrir sobre Activo en caso de que se materialice la amenaza sobre la vulnerabilidad identificada.

Fuentes y características de las amenazas

Las amenazas se pueden clasificar por la fuente de la que provienen éstas y por las características a las que éstas pueden afectar en caso de que se materialicen.

En el análisis de Riesgos se tienen en cuenta estás clasificaciones y se estima oportuno detallarlas.

Las Fuentes de las amenazas son:

- **Natural**: Fenómenos naturales (ej: rayo, inundación, incendio).
- **Humana**: Actos malintencionados, incumplimientos de las normativas de seguridad, negligencias, o falta de controles adecuados.
- **Entorno**: Averías o defectos en dispositivos, redes o software.

Las posibles características afectadas en caso de materialización de amenazas son:

- **Disponibilidad**: El acceso a la información no es posible.
- **Confidencialidad**: La información se revela a personas no autorizadas
- **Integridad**: La información es modificada o manipulada por personas o procesos no autorizados.

En el caso de materialización de una amenaza, se puede dar el caso de que quede afectada más de una característica del activo (Disponibilidad, Confidencialidad, Integridad).

Valoración de los riesgos (Impacto/Pérdidas)

La valoración del riesgo se lleva a cabo considerando la Probabilidad/Frecuencia de que la amenaza se materialice y la evaluación del impacto o las pérdidas que puede producir.

Para simplificar la tarea de valorar los riesgos, se han establecido las escalas siguientes para la Probabilidad/Frecuencia y la Evaluación de Impacto / Pérdidas (ya especificadas en la metodología de evaluación de Riesgos):

Probabilidad/Frecuencia

- **Alta:** Existe la probabilidad de que se materialice el riesgo cuatro o más veces durante un año.
- **Moderada:** Existe la probabilidad de que se materialice el riesgo de dos a tres veces durante un año.
- **Baja:** Existe la probabilidad de se materialice el riesgo una vez al año o menos

Evaluación

- **Graves:**
  - Pérdidas monetarias significativas para la organización (especificar).
  - Tiempo necesario para realizar de nuevo el trabajo equivalente o superior a una semana de un recurso.
  - Imposibilidad de reconstruir la información perdida.
  - Pérdidas de la disponibilidad de servicios superior a 4 horas de trabajo o superior a los límites en los acuerdos contractuales o legales con riesgos de multas o penalizaciones.
  - Objetivos principales de proyecto o servicios no satisfechos (SLAs no cumplidos)
  - Percepción de baja calidad en los servicios por usuarios-clave primarios de proyectos o servicios
  - Riesgo de seguridad personal
  - Fugas de datos no controladas de información de clientes o datos personales

- **Moderadas:**
  - Pérdidas monetarias poco significativas (especificar).
  - Tiempo necesario para realizar de nuevo el trabajo inferior una semana de un recurso
  - Objetivos secundarios de proyecto o servicio no satisfechos
  - Pérdidas de la disponibilidad de servicios inferior a 4 horas de trabajo o superior a los límites en los acuerdos contractuales o legales sin riesgos de multas o penalizaciones.
  - Percepción de baja calidad en los servicios por usuarios-clave secundarios o proveedores
  - Fugas de datos no controladas de información de la organización (no incluidos datos personales)
- **Leves:**
  - Pérdidas monetarias no significativas (especificar).
  - Tiempo necesario para realizar de nuevo el trabajo inferior a un día de un recurso.
  - Percepción de baja calidad en los servicios por personal interno de la organización.
  - Pérdidas de la disponibilidad de servicios inferior a una hora de trabajo o dentro de los límites en los acuerdos contractuales o legales.
  - Dificultades e incomodidades para realizar las labores dentro de la organización
  - Fugas de datos no controladas de información internamente en la organización (no incluidos datos personales)

En la siguiente tabla se muestra cuál es el riesgo resultante del cálculo entre las diferentes escalas de Probabilidad/Frecuencia y Evaluación de Impacto / Pérdidas:

		Impacto / Pérdidas		
		Leves	Moderadas	Graves
Probabilidad / Frecuencia	Alta	**Medio**	**Alto**	**Alto**
	Moderada	**Bajo**	**Medio**	**Alto**
	Baja	**Bajo**	**Bajo**	**Medio**

Tabla 9: Valoración de los Riesgos

Riesgos residuales

En este apartado se proponen los tratamientos necesarios para reducir los riesgos identificados a niveles aceptables.

Este tratamiento se basa en acciones correctivas, preventivas o de mejora.

Para ello, en el apartado “Medidas de Control” se establece el tipo de tratamiento que se va a llevar a establecer para cada uno de los riesgos, el Control que se le aplicará y la probabilidad/Frecuencia resultante de aplicar las medidas de control especificadas.

Los tipos de Tratamiento son los siguientes:

1. **Prevenir:** Que prevengan o eviten que se materialicen los riesgos
2. **Reducir:** Que reduzcan la probabilidad de que se materialicen los riesgos
3. **Detectar:** Que detecten la materialización de riesgos y permitan tratar sus consecuencias
4. **Reprimir:** Que repriman o reduzcan las consecuencias una vez que se materialicen
5. **Corregir:** Que permitan la corrección y recuperación una vez que se materialicen
6. **Transferir:** Que transfieran los riesgos a otras entidades mejor preparadas
7. **Aceptar:** Que se acepten los riesgos residuales, entendiendo que no se hará un tratamiento adicional

Esta lista está ordenada en base a aplicabilidad, esto es, que el tipo de tratamiento “Prevenir” debería, en lo posible, anteponerse a los demás tratamientos, Reducir a los cinco siguientes y de esta manera sucesivamente.

En el apartado “Impacto/Pérdidas” se especificará en la descripción cómo se estima el impacto/pérdidas de la materialización de los riesgos una vez aplicadas las medidas de control, especificando en la columna “Evaluación” la valoración según la escala definida con el mismo nombre en el apartado anterior de este documento “Valoración de los riesgos (Impacto/Pérdidas)”

Finalmente, en el campo “Riesgo” se calcula el Riesgo resultante de la aplicación de las medidas de control según el cruce de Probabilidad/Frecuencia con la Evaluación de impacto/Pérdidas ya mostrada en la Tabla 9: Valoración de los Riesgos.

Resumen de Resultados

En este apartado se hace un resumen de los resultados obtenidos en la realización del análisis de riesgos (detallado en el documento del “Anexo 3 – Análisis de Riesgos”).

Análisis de Gravedad, Fuentes e Impactos de los Riesgos.

En los siguientes gráficos se muestran las diferencias entre las valoraciones de los Riesgos analizados y las valoraciones en los Riesgos Residuales:

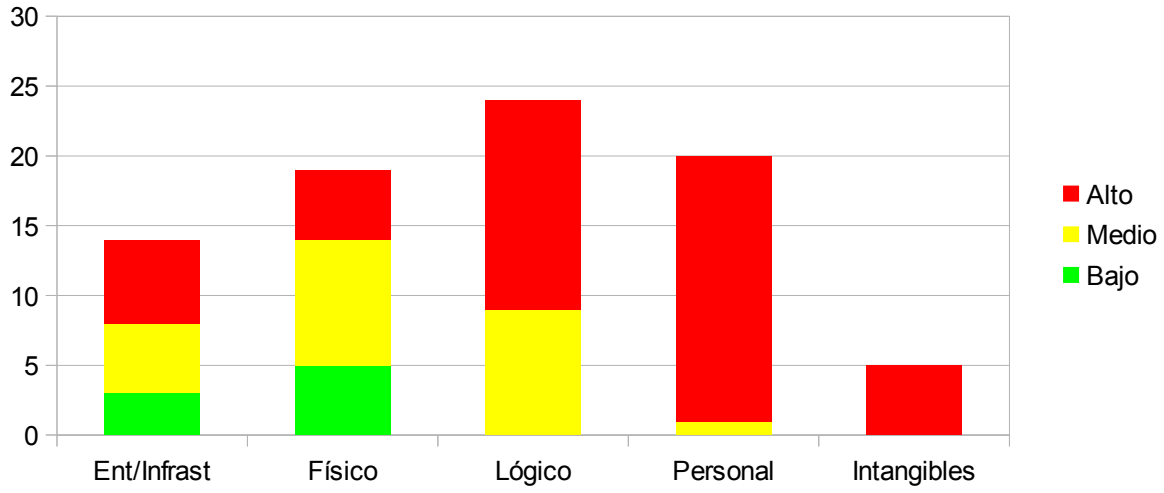


Ilustración 8: Valoración Riesgos Analizados

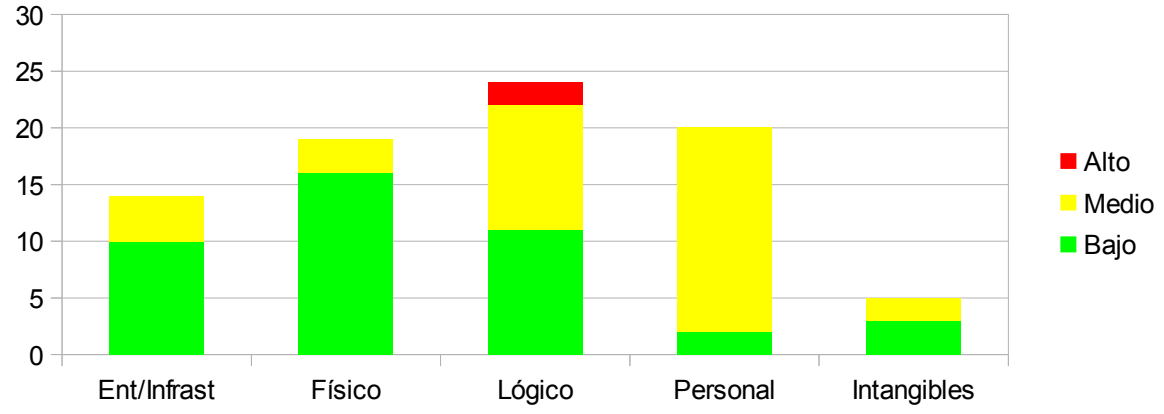


Ilustración 9: Valoración Riesgos Residuales

Se aprecia claramente que la aplicación de las medidas de control reduce el riesgo de manera ostensible.

Excepto en el caso del personal, en todos los tipos predominan los riesgos valorados como “Bajo”. Esto es debido a que el control del riesgo de fugas de información que se da en el tipo de riesgos de “Personal”, consistente en la suscripción de un contrato de confidencialidad entre la empresa y la persona, permite reducir la frecuencia de materialización de la amenaza, aunque no el impacto/pérdidas de ésta.

En la siguiente gráfica podemos ver un resumen de los orígenes de las fuentes de los riesgos clasificadas por tipo de Activo:

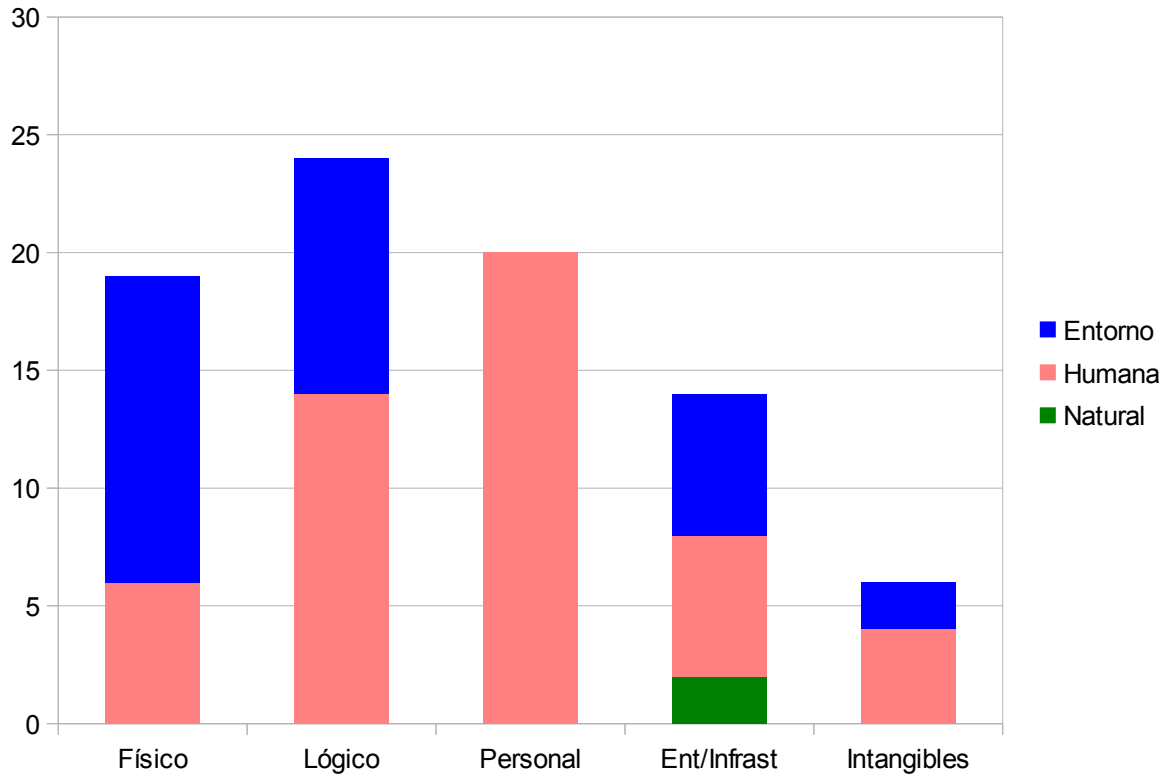


Ilustración 10: Fuentes de los Riesgos por tipo de Activo

Como es lógico, la mayor parte de las amenazas tienen su origen en factores humanos, quedando las amenazas del entorno en segundo lugar y de manera marginal las amenazas por causas naturales (que afectan exclusivamente a las infraestructuras).

En la siguiente gráfica se observa la clasificación del Impacto de los Riesgos por tipo de Activo:

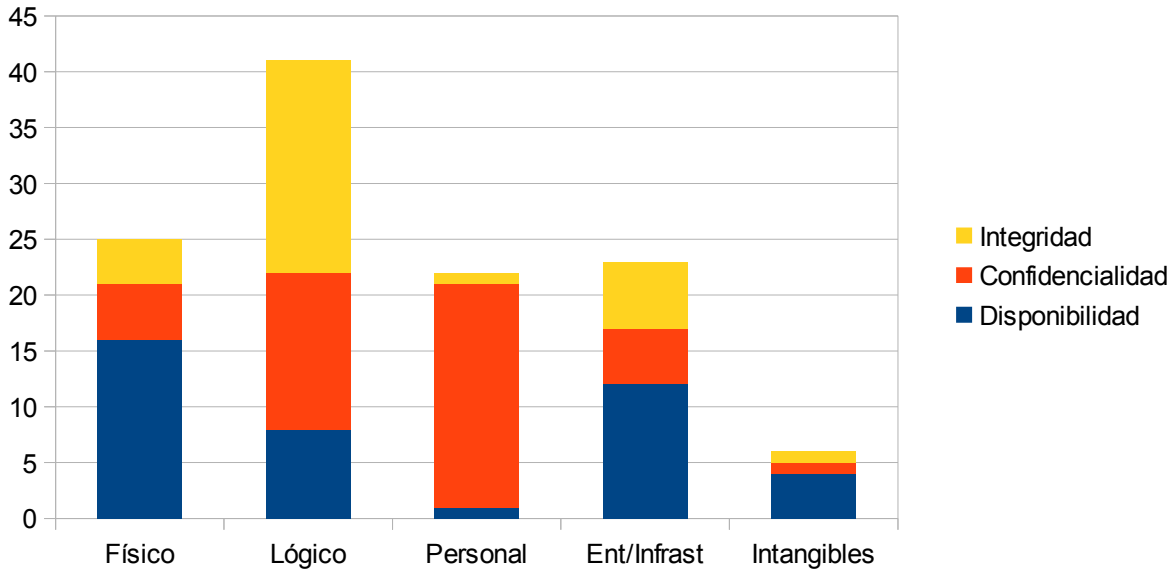


Ilustración 11: Impacto de los Riesgos por tipo de Activo

En la lectura de esta gráfica se ha de tener en cuenta que la materialización de un mismo riesgo podría impactar en más de uno de los elementos que se muestran (Integridad, Confidencialidad, Disponibilidad), e incluso en los tres elementos a la vez.

Principales Amenazas

En el siguiente esquema podemos ver un gráfico que muestra las principales amenazas. El gráfico se acompaña con las cifras con los que se ha elaborado:

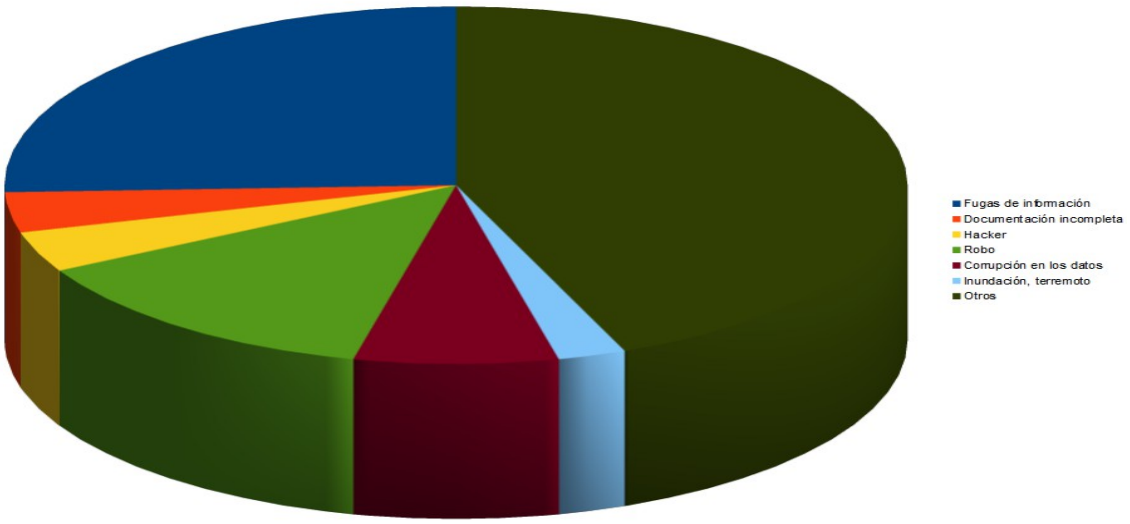


Ilustración 12: Principales Amenazas

Amenaza	# Riesgos en los que aparece	%
Fugas de información	21	26%
Documentación incompleta	3	4%
Hacker	3	4%
Robo	11	13%
Corrupción en los datos	6	7%
Inundación, terremoto	2	2%
Otros	36	44%

Tabla 10: Principales Amenazas

Se observa que las principales amenazas identificadas son las fugas de información y los robos.

Las fugas de información están ligadas de manera mayoritaria a riesgos relacionados con el personal. 16 de los 21 riesgos de fugas de información identificados están ligados al personal; Los 5 restantes están ligados a activos lógicos.

Las amenazas de Robos se reparten entre los grupos de activos de Personal, Infraestructura y activos físicos.

Principales Riesgos

En el siguiente esquema podemos ver un gráfico que muestra los principales riesgos. El gráfico se acompaña con las cifras con los que se ha elaborado:

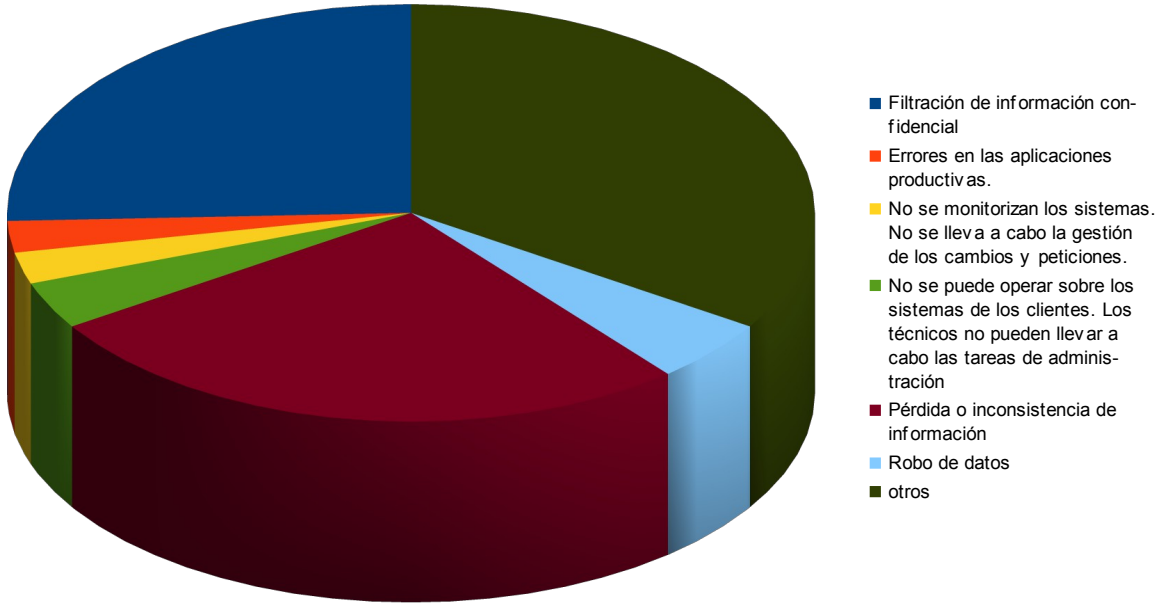


Ilustración 13: Principales Riesgos

Riesgo	# Riesgos de apariciones	%
Filtración de información confidencial	21	26%
Errores en las aplicaciones productivas.	2	2%
No se monitorizan los sistemas. No se lleva a cabo la gestión de los cambios y peticiones.	2	2%
No se puede operar sobre los sistemas de los clientes. Los técnicos no pueden llevar a cabo las tareas de administración	3	4%
Pérdida o inconsistencia de información	22	27%
Robo de datos	4	5%
otros	28	34%

Tabla 11: Principales Riesgos

Los dos principales riesgos detectados son la filtración de información confidencial y la pérdida o inconsistencia de información. Ambos riesgos suponen el 52% de los riesgos detectados.

- La filtración de información confidencial está ligada en la mayoría de las ocasiones al Personal (17 de las 21 contabilizadas). Para este caso, la acción definida para tratar este riesgo es el establecimiento de un contrato de confidencialidad entre la organización y las personas que tienen relación con ésta.
- La pérdida o inconsistencia de información está asociada mayoritariamente a los activos lógicos (software de desarrollo Interno o Externo) en 10 de las 22 ocasiones. En 7 ocasiones está asociada a activos de infraestructura y en 4 a activos físicos (hardware). Para estos casos, el tratamiento depende de si el software es de desarrollo Interno o Externo.
    - Si es de desarrollo Interno, la acción definida para reducir el impacto/pérdidas es la copia de seguridad diaria de los datos.
    - Si es desarrollo externo, las acciones son diversas en función del tipo de software. En el caso software que gestiona datos, la copia de seguridad diaria de éstos. En otras aplicaciones, dependiendo de la naturaleza de éstas, se estimarán unas medidas de control orientadas a instalar solamente versiones probadas del software y, en última instancia, la aceptación por parte de la dirección en de los riesgos inherentes a emplear esas aplicaciones.
- En el apartado “Otros”, destacar que supone el 34% de los riesgos detectados (concretamente 28). De estos 28 riesgos, 11 de ellos (que supone el 13% del total) se deben a la vulnerabilidad de “Avería en el equipo” (resultando en diferentes riesgos en función de a qué esté destinado el equipo). Este 13% de las amenazas se tratará en su conjunto a través de la medida de control consistente en la instalación de un sistema de alta disponibilidad (“cluster” de virtualización).

Proyectos

Planificación de proyectos

El siguiente gráfico muestra una planificación de los eventos más significativos que relacionados con el SGSI durante tres años desde el inicio de la implantación del SGSI:

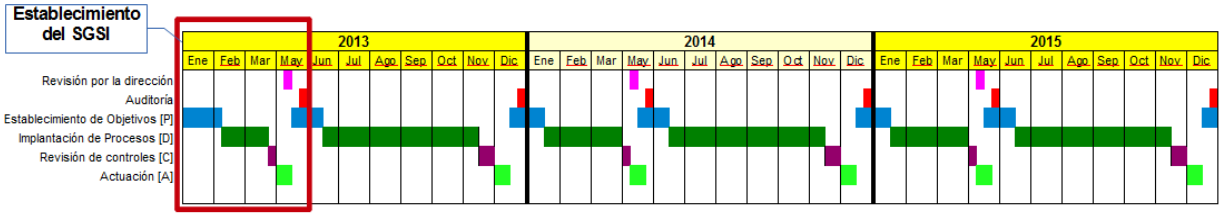


Ilustración 14: Planificación de Proyectos

Se planifican dos auditorías anuales a efectos de establecer una revisión independiente del SGSI (ver el procedimiento de auditorías internas).

Se planifica igualmente una revisión anual por la dirección del SGSI. Esta revisión es una revisión de mínimos, siendo posible que hayan más revisiones por la dirección en el caso de que se produzca una variación importante en el plan de riesgos o en los activos de la compañía.

La fase de establecimiento del SGSI engloba la primera iteración del ciclo PDCA, finalizando éste en la primera auditoría (programada en fecha pretérita a la presentación de este documento y cuyo resultado se anexa a esta memoria en el “Anexo 4 – Informe de auditoría”.

La sucesivas fases son iteraciones del ciclo de Deming cuyo final está marcado por la realización de una auditoría interna.

Resumen de propuestas

Granja de Máquinas virtuales

Despliegue y puesta en marcha de una infraestructura de máquinas virtuales. Esta infraestructura ofrece tolerancia a fallos, facilita la administración y simplifica enormemente la recuperación de las máquinas en una infraestructura con especificaciones similares en caso de desastre.

Externalización del sistema de backups

Actualmente las copias de seguridad se llevan a cabo localmente de manera selectiva y utilizando un dispositivo basado en cintas. Este sistema requiere una gestión administrativa sobre los juegos de cintas utilizados en las copias, sobre las cuales existe un riesgo de pérdida de información, ya sea por fallo físico de las cintas o bien por robo o extravío de éstas. Los modernos sistemas de backup en la nube eliminan estos riesgos (no existe soporte físico) y facilitan la automatización y la recuperación de las copias de seguridad.

Formación de los empleados en Seguridad de la Información

Muchos incidentes de seguridad tienen como origen el desconocimiento o a la falta de concienciación de los empleados respecto a buenas prácticas en el tratamiento de la información. Por ello, la formación en Seguridad de la información es una manera adecuada y con resultados prácticos inmediatos para reducir las incidencias relacionadas con este tema.

Instalación de sistema de respaldo de la conexión a Internet

El tipo de conexión a Internet (cable) que hay instalado actualmente en la empresa tiene implícito un riesgo de caída de la conexión por causas diversas (sección física del cable por error humano o desastre natural, avería en algún dispositivo del proveedor, etc). Es por ello que se considera el contratar una conexión alternativa con un proveedor diferente que no dependa de cables para minimizar el riesgo de quedar desconectados de Internet.

Implantación de un Software de respaldo de datos de PC's al servidor

En los ordenadores portátiles y en las estaciones de trabajo de los empleados de la compañía se almacena información cuya pérdida puede suponer un daño más o menos importante. Es por ello que se pretende facilitar la realización de copias de seguridad del contenido de las unidades y/o carpetas que puedan contener datos importantes.

Encriptación de datos en los discos duros de las estaciones de trabajo

Las estaciones de trabajo, sean ordenadores de escritorio o ordenadores portátiles, pueden contener información confidencial en sus discos duros. En caso de pérdida o robo del equipo, la confidencialidad de esta información puede quedar comprometida. Para minimizar la amenaza a la confidencialidad, se plantea la instalación de un Software de encriptación de datos que permita cifrar la información para hacerla inaccesible a terceros.

Plan de Continuidad del Negocio

Para minimizar las consecuencias de un posible desastre cuyas consecuencias lleven a la pérdida de los

sistemas de la información de la compañía, se plantea la elaboración de un Plan de Continuidad del Negocio cuyo seguimiento asegure que la actividad de la compañía pueda prevalecer en caso de que se materialice la amenaza de un desastre.

Implementación de la metodología de trabajo SCRUM

En el sub-área de desarrollo de Software es notorio que no se está siguiendo una metodología de trabajo concreta. Cada uno de los gestores de proyecto utiliza sus propios mecanismos, basados en sus propias experiencias, y sin tener una organización y una manera de planificar claras.

Este hecho conlleva un riesgo de cara al cliente de la percepción de la calidad del trabajo que se está desarrollando, por lo que se decide unificar las metodologías de trabajo en una sola (SCRUM).

Implementación de la metodología ITIL v3

En las sub-áreas de Administración de Bases de Datos y Sistemas se da el hecho de que la gran mayoría de las tareas se desempeñan siguiendo procesos de gestión de cambio. Actualmente se sigue un procedimiento propio, basado en el "workflow" definido en el software de gestión departamental (CONSERIT) y que está basado en la metodología ITIL.

La metodología ITIL va mucho más allá de la gestión de cambios, poniendo a disposición de los técnicos un conjunto de buenas prácticas en la gestión del trabajo del departamento.

Implementación de Software de Gestión Documental

De cara a mejorar la disponibilidad, la gestión de permisos de acceso, el etiquetado y la facilidad de realizar búsquedas en la información, se considera necesario poner en marcha una plataforma de software de gestión documental que implemente todas las funcionalidades necesarias para conseguir los objetivos mencionados.

El software de gestión documental, además, supondrá una mejora sustancial a la productividad.

Detalle de Propuestas

En los siguientes apartados se entra en detalle de las Propuestas enumeradas en el apartado anterior.

Granja de Máquinas virtuales

Descripción

Análisis, instalación e integración de la infraestructura necesaria para establecer una plataforma de máquinas virtuales que soporte la ejecución de los servicios requeridos por la compañía.

Esta plataforma deberá ser tolerante a fallos de Hardware, fácilmente escalable y proporcionar un rendimiento del sistema acorde con las necesidades de la compañía.

Motivación

La mejora que proporcionan las infraestructuras de máquinas virtuales respecto a la disponibilidad y la tolerancia a fallos, así como el aprovechamiento y optimización de recursos tales como el espacio físico y el consumo eléctrico.

Objetivos

- Reducir las amenazas a la disponibilidad de los sistemas a causa de fallos de Hardware.
- Optimizar los costes de mantenimiento de infraestructura de sistemas.
- Optimizar los costes tanto económicos como de tiempo y recursos a la hora de incorporar nuevos servidores a la infraestructura.
- Facilitar la administración de los sistemas.

Beneficiarios

Todos los usuarios de la compañía se beneficiarán directa o indirectamente de las ventajas de los entornos virtuales.

Por su parte, los administradores de sistemas aumentarán su productividad gracias a la administración simplificada de los entornos virtuales.

En general, todos los usuarios de la compañía se beneficiarán de las ventajas que ofrecerá la infraestructura con tolerancia a fallos en cuanto a la disponibilidad de los sistemas.

Controles/Riesgos contemplados

La implantación de la Granja de máquinas virtuales se lleva a cabo en el ámbito de la ejecución de las medidas de control especificadas en el Análisis de Riesgos, concretamente en los riesgos identificados con los números que van desde el 23 al 33.

Ámbito

La infraestructura de sistemas de información es una herramienta esencial de la actividad de la compañía, por lo que este proyecto afecta a todas las áreas del negocio.

Actividades y Tareas

- **Determinar necesidades de recursos e infraestructura:** Realizar un estudio funcional de qué recursos materiales y humanos se necesitan para implementar la infraestructura deseada en base al pliego de condiciones establecido (disponibilidad, flexibilidad, etc).
- **Estudiar ofertas de proveedores. Escoger la más adecuada:** Contactar con proveedores de Hardware y software. Transmitir las necesidades de la compañía para llevar a cabo el proyecto y solicitarles ofertas. Sopesar cuál es la oferta que cubre las necesidades planteadas en las condiciones más ventajosas.
- **Aprobación y dotación de recursos por parte de la dirección:** Dirección evalúa la rentabilidad del proyecto, la viabilidad económica, y las vías de financiación. Si todo ello es viable, se realiza el pedido al proveedor.
- **Recepción de máquinas e Instalación de la nueva infraestructura:** Se reciben las máquinas. Los administradores colaboran con los técnicos del proveedor/es en el despliegue de la infraestructura. Las máquinas deben residir en diferentes armarios, así como la cabina de discos. De la misma manera, los switches deben ubicarse en diferentes armarios también.
- **Migración de sistemas actuales a la nueva infraestructura:** Se establece un calendario de actuaciones para la migración de los servicios contenidos en los servidores actualmente en funcionamiento a la nueva infraestructura.
- **Pruebas de recuperación ante fallos:** Se elabora un plan de acciones a llevar a cabo en caso de caída de una de las máquinas de la infraestructura. Se llevan cabo pruebas de movimiento de servicios entre máquinas. Se documenta todo el procedimiento.
- **Elaboración de informe de implementación:** Una vez finalizada la implementación, los administradores elaborarán un informe detallando cómo se ha montado la infraestructura, los criterios que se han seguido en la toma de decisiones técnicas, contactos de soporte, problemas encontrados, mejoras identificadas, etc...

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. Dirección acepta la consecución del proyecto dentro del plazo de finalización establecido
2. Los costes del proyecto en el momento de la consecución no superan los presupuestos establecidos inicialmente.
3. Se aportan evidencias de la realización de pruebas de los sistemas de alta disponibilidad
4. Los administradores de sistemas emiten un informe favorable de la implementación de la infraestructura.

Calendario

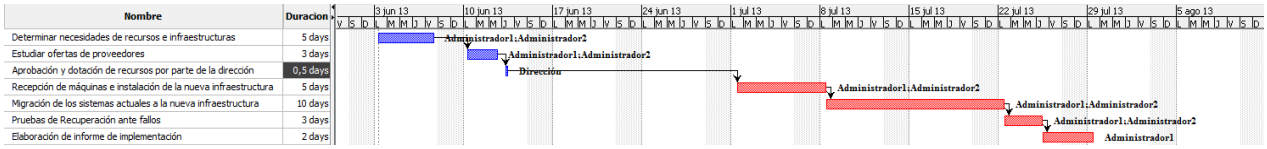


Ilustración 15: Calendario Proyecto "Granja de Máquinas virtuales"

Recursos

Materiales

La siguiente es una relación del material que se necesita adquirir para llevar a cabo el proyecto:

Material	Descripción de Requisitos	Coste estimado
1 Cabina de Discos	• Controladora del sistema MD3200 con una bandeja con capacidad para, al menos 12 discos, permitiendo agrupaciones de éstos en RAID5. La controladora debe permitir la ampliación de la capacidad de almacenamiento añadiendo más bandejas de discos. • Sistema de almacenamiento SAN que permita la conexión iSCSI. • Doble fuente de alimentación (redundante) • Al menos 6TB en Discos SAS • Al menos 8TB en Discos SATA (Nearly SAS) • Al menos 2 años de Soporte 24x7 y tiempo de respuesta de 4 horas • Puesta en marcha y arranque	18.000 €
2 Servidores	• 2 Procesadores XEON de, al menos, 6 núcleos cada uno. • 64 Gb de Memoria RAM • 2 Discos Internos SATA de 2.5” de, al menos, 146Gb cada uno configurados en RAID1 (mirror). • Doble fuente de alimentación (redundante) • 4 conexiones de Ethernet a 10Gb (para iSCSI) • VMWARE ESXi 5.1 preinstalado • Al menos 2 años de Soporte 24x7 y tiempo de respuesta de 4 horas • Puesta en marcha y arranque	12.000 € (ambas máquinas)
2 Switches ethernet de 24 puertos	• Conexiones a 10 Gb • Capacidad para crear y gestionar VLAN's	5.000 € (ambos equipos)
Licencia para 4 procesadores de VMWARE ESX5i Standard	• VMWARE Esx5i • VSphere • Vcenter • Herramientas asociadas • Soporte 24x7	6000 € + 1500 € anuales de contrato de soporte
Cableado y equipamiento diverso	• Cables de Red • Cables de Alimentación • Guías de montaje en los armarios	100€

Tabla 12: Recursos Materiales Proyecto "Granja de Máquinas virtuales"

Personal

Para el desarrollo del proyecto se estima que será necesaria la participación de las siguientes personas:

- 1 Administrador de Sistemas (224 horas, a un coste de 20€/h)
- 1 Administrador de Sistemas adjunto (208 horas a un coste de 20€/h)
- 1 Director ejecutivo (4 horas a un coste de 50€/h, para evaluar la viabilidad del proyecto y dotarlo de recursos).

Financieros

Los costes estimados asociados al proyecto son los siguientes:

42.600 € en equipamiento y materiales

8.840 € en costes de personal

El coste total del proyecto es de **51.440 €**

Externalización del sistema de backups

Descripción

Implementación de un sistema de copias de seguridad cuyo funcionamiento esté basado en que los datos respaldados se encuentran en servidores contratados a un proveedor externo y ubicados en Internet.

Motivación

Optimizar los costes de operación en la gestión de las copias de seguridad.

Eliminación de puntos de fallo en el procedimiento de copia (rotura y/o extravío de soportes, averías del Hardware que lleva a cabo el respaldo...).

Objetivos

- Reducir las amenazas a la disponibilidad de los sistemas de copias a causa de fallos de hardware o de los soportes.
- Optimizar los costes de mantenimiento de infraestructura del sistema de copias.

Beneficiarios

La simplificación de las tareas de gestión de las copias de seguridad supondrá un beneficio claro para los administradores de sistema.

Los usuarios de la compañía en su conjunto se beneficiarán de la mejora en la disponibilidad de las copias de seguridad en caso de necesitar recuperar datos desde ésta.

Controles/Riesgos contemplados

La implantación de las copias de seguridad en la Nube se lleva a cabo en el ámbito de la ejecución de las medidas de control especificadas en el Análisis de Riesgos, concretamente en los riesgos identificados con los números que van desde el 36 al 38,40 al 41,43 al 45 y 57.

De la misma manera, la implantación de este sistema obedece a los controles especificados en el apartado 10.5 (Copias de Seguridad) de la ISO-27002.

Ámbito

La seguridad en los datos constituye un servicio esencial de la actividad de la compañía, por lo que este proyecto afecta a todas las áreas del negocio.

Actividades y Tareas

- **Determinar necesidades de recursos e infraestructura:** Realizar un estudio funcional de qué recursos materiales y humanos se necesitan para implementar el sistema de copias que más se ajuste al pliego de condiciones establecido.
- **Estudiar ofertas de proveedores. Escoger la más adecuada:** Contactar con proveedores de servicios de copias de seguridad en la nube. Transmitir las necesidades de la compañía para llevar a cabo el proyecto y solicitarles ofertas al respecto. Sopesar cuál es la oferta que cubre las necesidades planteadas en las condiciones más ventajosas.
- **Aprobación y dotación de recursos por parte de la dirección:** Dirección evalúa la rentabilidad del proyecto, la viabilidad económica, y las vías de financiación. Si todo ello es viable, se realiza el pedido al proveedor.
- **Implantación del sistema de copias en la infraestructura:** Se establecen las políticas de copia adecuadas, los certificados de encriptación (si procede) , se instalan los programas en los servidores, etc.
- **Pruebas de recuperación:** Se llevan a cabo pruebas de recuperación de ficheros de copias anteriores para verificar que la solución implementada se ajusta de manera efectiva a las necesidades planteadas.

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. Dirección acepta la consecución del proyecto dentro del plazo de finalización establecido.
2. Los costes del proyecto en el momento de la consecución no superan los presupuestos establecidos inicialmente.
3. Se aportan evidencias de la realización de pruebas de recuperación de datos.
4. Los administradores de sistemas emiten un informe favorable de la implementación del sistema.

Calendario

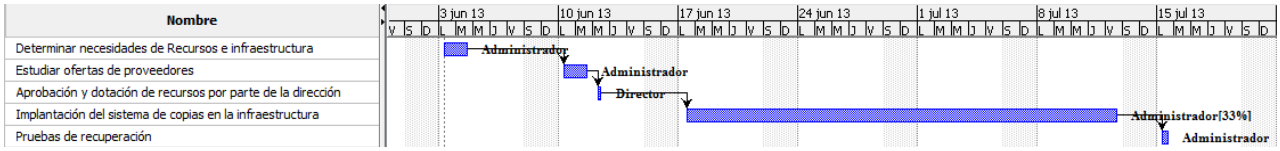


Ilustración 16: Calendario Proyecto "Externalización del sistema de backups"

Recursos

Materiales

Para la realización del proyecto se requieren los siguientes recursos materiales:

Material	Descripción de Requisitos	Coste estimado
12 Licencias del proveedor de servicio de Backup en la nube (una por servidor)	• Cada licencia otorga derecho a utilizar el espacio en los servidores del proveedor, así como a utilizar los servicios de backup.	1500 € al año (con el volumen actual de servidores)

Tabla 13: Recursos Materiales Proyecto "Externalización del sistema de backups"

Personal

Para el desarrollo del proyecto se estima que será necesaria la participación de las siguientes personas:

- 1 Administrador de Sistemas (91,48 horas, a un coste de 20€/h)
- 1 Director ejecutivo (4 horas a un coste de 50€/h, para evaluar la viabilidad del proyecto y dotarlo de recursos).

Financieros

Los costes estimados asociados al proyecto son los siguientes:

1.500 € anuales en equipamiento y materiales

2.029,60 € en costes de personal

El coste total estimado de implantación del proyecto es de **3.529,60 €**

Formación de los empleados en Seguridad de la Información

Descripción

Realización de sesiones informativas dirigidas al personal de la empresa para difundir y concienciar el uso de buenas prácticas en la Seguridad de la información.

Motivación

Mitigar riesgos asociados a la falta de formación en seguridad de la información.

Objetivos

- Reducción de la posibilidad en la materialización de riesgos sobre el ámbito de la seguridad de la información en la empresa.
- Implementación de buenas prácticas en la gestión y tratamiento de la información.

Beneficiarios

Los usuarios de la compañía en su conjunto se beneficiarán de los conocimientos adquiridos en la gestión de la seguridad de la información.

Controles/Riesgos contemplados

La formación de los empleados en Seguridad de la Información se lleva a cabo en el ámbito de la ejecución de las medidas de control especificadas en el Análisis de Riesgos, concretamente en los riesgos identificados con los números 18 y 20.

También abarca los siguientes controles especificados en la ISO-27002:

- 8.2.2 - Concienciación, formación y capacitación en seguridad de la información.
- 11.3.1 – Uso de contraseñas
- 11.3.2 – Equipo de usuario desatendido
- 11.3.3 – Política de puesto despejado y pantalla limpia
- 13.1.1 – Notificación de eventos de seguridad de la información
- 13.1.2 – Notificación de puntos débiles de la seguridad
- 13.2.3 – Recopilación de evidencias
- 15.1.5 – Prevención del uso indebido de los recursos de tratamiento de la información
- 15.2.1 – Cumplimiento de las políticas y normas de seguridad

Ámbito

La seguridad de la información constituye un servicio esencial de la actividad de la compañía, por lo que este proyecto afecta a todas las áreas del negocio.

Actividades y Tareas

- **Elaboración de un plan de formación:** Se conforman los calendarios y los grupos de personas que asistirán a la formación. Se elabora un memorando con los costes asociados al personal de la formación.
- **Estudiar ofertas de proveedores de Formación:** Buscar ofertas de proveedores de formación en Seguridad de la información. Escoger la que más adecuada a las necesidades formativas y organizativas de la empresa.
- **Aprobación de recursos y planes de formación (dirección):** La dirección revisa los planes y los memorandos y los aprueba, dotando de presupuesto y de voluntad ejecutiva al proyecto.
- **Ejecución de las acciones de formación:** Llevar a cabo las sesiones de formación y concienciación a los empleados.
- **Evaluación de la formación recibida por parte de los empleados:** Tratar de validar que los empleados han recibido una formación adecuada mediante algún tipo de prueba o test.

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. El 90% o más de los empleados de cada Área asisten a la formación.
2. Se aportan evidencias del aprovechamiento del curso por parte de los empleados.
3. Los empleados emiten valoraciones favorables sobre la formación impartida.

Calendario

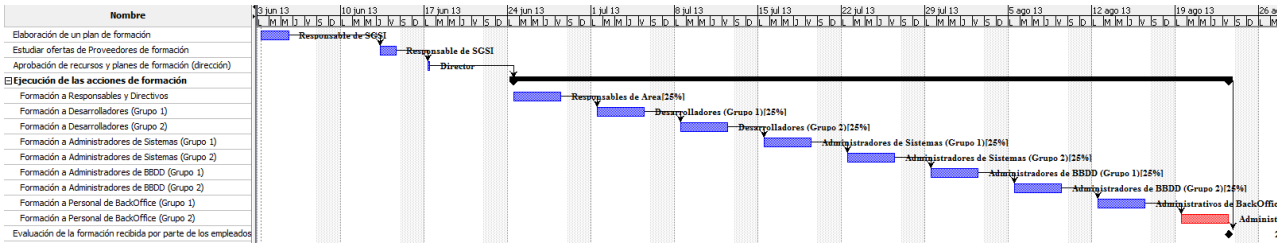


Ilustración 17: Calendario Proyecto "Formación de los empleados en Seguridad de la Información"

Recursos

Materiales

La formación se impartirá en la sala de Juntas de la empresa, que está equipada con todo el material necesario (proyector, pizarra, sillas, etc).

Dirección dotará 100€ en concepto de materiales (Libretas, bolígrafos, agua, etc).

Personal

Para la formación es necesario que asista todo el personal de la compañía. Para hacer posible esto afectando lo menos posible la actividad de la organización, se formarán diferentes grupos que asistirán a las sesiones a tiempo parcial.

Financieros

Se ha estimado el coste para la empresa, en concepto de personal, que supone la asistencia al curso (Tiempo “no-productivo”) para una formación de 8 horas de duración total:

- Administradores de BBDD (10 pax): 2.240€
- Administradores de Sistemas (10 pax): 1.600 €
- Desarrolladores (10 pax): 1.840 €
- Administrativos de BackOffice (8 pax): 960 €
- Directivos y Responsables de Area (4 pax): 1.280€

Los costes de Personal para las tareas de gestión del proyecto son:

- Directivos: 200€
- Responsable de SGSI: 1.200 €

El presupuesto para la contratación de la acción formativa a la empresa externa es de 4.000 €

Sumando todos los costes, el total es de: **13.340 €**

Instalación de sistema de respaldo de la conexión a Internet

Descripción

Instalación y puesta en marcha de un sistema alternativo de acceso a Internet para, en caso de fallo de la línea principal, garantizar la continuidad del funcionamiento de la conexión.

El sistema debe ser capaz de activarse automáticamente al detectar la pérdida de conexión del sistema primario.

Se tiene en consideración, por sugerencia de la dirección, la idea de que la conexión de respaldo sea a través de un módem 3G.

Motivación

Asegurar la disponibilidad del acceso a Internet en caso de incidencia en la conexión principal.

Objetivos

- Reducir las amenazas a la disponibilidad de la conexión a Internet a causa de fallos en la conexión principal.

Beneficiarios

Todos los usuarios de la compañía necesitan del acceso a Internet, como mínimo, para enviar y recibir correo electrónico a buzones externos a la organización. Sin embargo, los siguientes grupos de usuarios necesitan una conexión ininterrumpida para desempeñar sus tareas remotas sobre los sistemas de los clientes :

- Administradores de Sistemas
- Administradores de Bases de Datos
- Desarrolladores de Software

Controles/Riesgos contemplados

La instalación del sistema de respaldo de la conexión a Internet se lleva a cabo en el ámbito de la ejecución de las medidas de control especificadas en el Análisis de Riesgos, concretamente en el identificado con el número 14.

Ámbito

El acceso a Internet constituye un servicio esencial de la actividad de la compañía, por lo que este proyecto afecta a todas las áreas del negocio, especialmente a las áreas productivas (Administradores de Sistemas y Bases de Datos, así como a los Desarrolladores de Software).

Actividades y Tareas

- **Determinar necesidades de recursos e infraestructura:** Realización de un estudio de los trabajos técnicos y el material necesario para llevar a cabo la implementación.
- **Estudio y evaluación de proveedores de conexión 3G:** Evaluar cuál es el tipo de conexión 3G más adecuado y económicamente más ventajoso.
- **Aprobación y dotación de recursos por parte de la dirección:** Dirección aprueba la inversión a realizar.
- **Implementación de la solución escogida:** Instalación y adecuación de la infraestructura.
- **Pruebas de funcionamiento:** Realizar y documentar pruebas de funcionamiento del sistema implementado.

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. Se aportan evidencias del correcto funcionamiento del sistema.
2. La implementación del proyecto se hace dentro de los plazos estipulados y en los costes establecidos.

Calendario

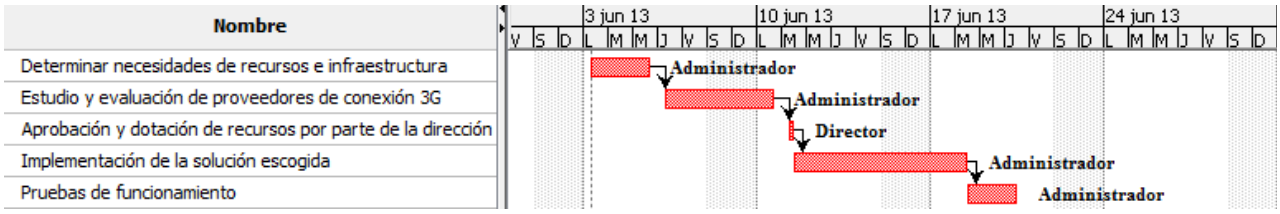


Ilustración 18: Calendario Proyecto "Instalación de sistema de respaldo de la conexión a Internet"

Recursos

Materiales

- 2 x Modem 3G (el modem que se instala y otro de reserva) = 120 €
- Tarifa de datos Mensual 3G a 7,2Mbps = 40 €

Personal

Para el desarrollo del proyecto se estima que será necesaria la participación de las siguientes personas:

- 1 Administrador de Sistemas (104 horas, a un coste de 20€/h)
- 1 Director ejecutivo (4 horas a un coste de 50€/h, para evaluar la viabilidad del proyecto y dotarlo de recursos).

Financieros

Los costes estimados asociados al proyecto son los siguientes:

- 40 € de la conexión (primer mes).
- 120€ en materiales
- 2.280 € en costes de personal

El coste total estimado de implantación del proyecto es de **2.440 €**

Implantación de un Software de respaldo de datos de PC's al servidor

Descripción

Instalación y puesta en marcha en los PC's de la compañía y en las maquetas de Sistema Operativo de un programa que automatiza las copias de la partición de datos de las estaciones de trabajo de los empleados al servidor.

Para ello, se incluirá un icono en el escritorio de los usuarios mediante el cual se ejecuta el proceso que realiza la copia de seguridad.

Motivación

Existe un riesgo de pérdida de información que viene dado por posibles fallos de hardware, errores humanos y otros factores externos que podría suceder en las estaciones de trabajo de los empleados. La realización de este proyecto pretende poner los medios necesarios para minimizar las pérdidas en caso de que la amenaza se materialice.

Objetivos

- Reducir las amenazas a la disponibilidad y la integridad de los datos en las estaciones de trabajo de los usuarios.

Beneficiarios

La totalidad de los usuarios de la compañía se beneficiarán de la implantación de esta solución, ya que todos ellos utilizan ordenadores en mayor o menor medida para desempeñar sus tareas.

Controles/Riesgos contemplados

La instalación del software de respaldo de datos de PC's al servidor se lleva a cabo en el ámbito de la ejecución de las medidas de control especificadas en el Análisis de Riesgos, concretamente en el identificado con el número 16.

Ámbito

Todos los empleados de la compañía usan en mayor o menor medida el ordenador (como mínimo para consultar el correo electrónico y visualizar o editar documentación), por lo que el ámbito de este proyecto es Global en el conjunto de la organización.

Actividades y Tareas

- **Estudio y evaluación de programas de copias de seguridad en estaciones de trabajo:** Se lleva a cabo una búsqueda de programas "freeware" que cubran las necesidades descritas. Se seleccionan los que cumplen los requisitos.
- **Elaboración de propuesta:** Se confecciona un informe destinado a la dirección donde se detallan las prestaciones de los programas, y los costes de instalación y de mantenimiento.
- **Aprobación y dotación de recursos por parte de la dirección:** Dirección escoge la propuesta más adecuada en base a lo aconsejado en el informe de propuestas y la disponibilidad de recursos.
- **Implementación de la solución escogida:** Los administradores de sistemas implementan la solución escogida.
- **Pruebas y documentación de procedimientos:** Se llevan a cabo, y se documentan, pruebas del funcionamiento del producto y de los diferentes procedimientos de operaciones asociados a éste (recuperación de copias, informes de fallos de copias, problemas encontrados, etc.).

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. Se aportan evidencias de pruebas exitosas de restauración de copias de seguridad.
2. La implementación del proyecto se hace dentro de los plazos estipulados y en los costes establecidos.
3. Se aportan evidencias de que los usuarios están utilizando la herramienta.

Calendario

Nombre	Duracion
Estudio y evaluación de programas de copias de seguric	3 days
Elaboración de propuesta	2 days
Aprobación y dotación de recursos por parte de la direc	0,5 days
Implementación de la solución escogida	10 days
Pruebas y documentación de procedimientos	2 days

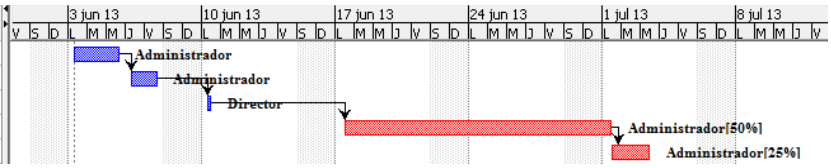


Ilustración 19: Calendario Proyecto "Implantación de un Software de respaldo de datos de PC's al servidor"

Recursos

Materiales

Programa de Backup a implementar. Se considera implementar una solución Freeware, por lo que el coste de éste sería cero.

Personal

Para el desarrollo del proyecto se estima que será necesaria la participación de las siguientes personas:

- 1 Administrador de Sistemas (84 horas, a un coste de 20€/h)
- 1 Director ejecutivo (4 horas a un coste de 50€/h, para evaluar la viabilidad del proyecto y dotarlo de recursos).

Financieros

Los costes estimados asociados al proyecto son los siguientes:

- 1.880 € en costes de personal
- 0 € en licencias de software (Freeware).

El coste total estimado de implantación del proyecto es de **1.880 €**

Encriptación de datos en los discos duros de las estaciones de trabajo

Descripción

Instalación y puesta en marcha en los PC's de la compañía y en las maquetas de Sistema Operativo de un programa que genera una unidad virtual en la que los usuarios pueden almacenar sus ficheros de manera segura.

El proceso de encriptación deberá realizarse de manera transparente al usuario, simplemente, guardando los ficheros de datos en la unidad simulada.

Se sugiere el uso del programa TrueCrypt (http://http://www.truecrypt.org/), ya que éste es conocido extensamente por los administradores de Sistemas y, además, es “open-source” lo cual implica que no tiene coste de uso.

Motivación

Existe un riesgo de revelación de información confidencial contenida en las unidades de disco duro de los equipos en caso de pérdida (en el caso de los portátiles) o de robo de éstos (en todos los casos).

Para ello, el programa deberá ser capaz de almacenar los ficheros encriptados en el disco duro asegurando que solamente será posible acceder a ellos si se conoce la clave de encriptación.

Objetivos

- Reducir las amenazas a la confidencialidad de los datos en las estaciones de trabajo de los usuarios.

Beneficiarios

La totalidad de los usuarios de la compañía se beneficiarán de la implantación de esta solución, ya que todos ellos utilizan ordenadores en mayor o menor medida para desempeñar sus tareas.

Controles/Riesgos contemplados

La instalación del software de encriptación de datos se lleva a cabo en el ámbito de la ejecución de las medidas de control especificadas en el Análisis de Riesgos, concretamente en el identificado con el número 17.

Ámbito

Todos los empleados de la compañía usan en mayor o menor medida el ordenador (como mínimo para consultar el correo electrónico y visualizar o editar documentación), por lo que el ámbito de este proyecto es Global en el conjunto de la organización.

Actividades y Tareas

- **Elaboración de Informe de viabilidad y costes:** Se elabora un informe que contemplará la idoneidad y la viabilidad de la instalación de la solución propuesta.
- **Aprobación y dotación de recursos por parte de la dirección:** Dirección considerará el informe emitido y dará orden ejecutiva para la implementación del proyecto.
- **Implementación de la solución escogida:** Los administradores de sistemas implementan la solución escogida.
- **Pruebas y documentación de procedimientos:** Se llevan a cabo, y se documentan, pruebas del funcionamiento del producto y de los diferentes procedimientos de operaciones asociados a éste.

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. Se aportan evidencias de pruebas exitosas de la confidencialidad y la integridad de los datos
2. La implementación del proyecto se hace dentro de los plazos estipulados y en los costes establecidos.
3. Se aportan evidencias de que los usuarios utilizan la herramienta de manera correcta y efectiva.

Calendario

Nombre	Duracion
Elaboración de informe de viabilidad y costes	2 days
Aprobación y dotación de recursos por parte de la dirección	0,5 days
Implementación de la solución escogida	10 days
Pruebas y documentación de procedimientos	2 days

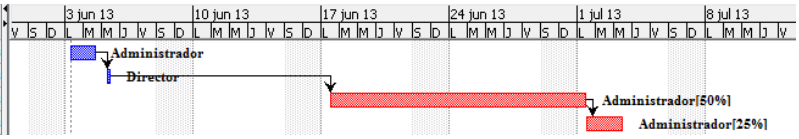


Ilustración 20: Calendario Proyecto "Encriptación de datos en los discos duros de las estaciones de trabajo"

Recursos

Materiales

Programa de encriptación a implementar. Truecrypt es “open-source” por lo que el coste de adquisición es cero.

Personal

Para el desarrollo del proyecto se estima que será necesaria la participación de las siguientes personas:

- 1 Administrador de Sistemas (60 horas, a un coste de 20€/h)
- 1 Director ejecutivo (4 horas a un coste de 50€/h, para evaluar la viabilidad del proyecto y dotarlo de recursos).

Financieros

Los costes estimados asociados al proyecto son los siguientes:

- 1.400 € en costes de personal
- 0 € en licencias de software (“open-source”).

El coste total estimado de implantación del proyecto es de **1.400 €**

Plan de Continuidad del Negocio

Descripción

Elaboración y pruebas del plan de continuidad del negocio.

Se trata de establecer el conjunto de acciones, procesos y procedimientos necesarios para que la continuidad del negocio sea posible en caso de que se produzca un evento de consecuencias mayores que de manera efectiva imposibilite el uso de la infraestructura de tecnología de la información ubicada en la sede de la compañía.

En lo que respecta a los sistemas de información, se seguirá un modelo de tipo “warm-site”, estableciendo un acuerdo de colaboración con otra compañía, con lo que se reducen los costes ostensiblemente. El acuerdo de colaboración consiste en que, en caso de desastre, la compañía no afectada cede una parte de su infraestructura para albergar los sistemas de la afectada por el desastre. Esto es técnicamente posible gracias a la tecnología de virtualización de servidores.

En el proyecto de implementación de la granja virtual se han tenido en cuenta estas necesidades y se han dimensionado los servidores para ello.

La infraestructura técnica de ambas compañías debe ser similar (Almacenamiento en cabina de discos, servidores virtuales...) y para evitar incompatibilidades estructurales, ambas compañías deberán establecer mediante acuerdos una estrategia de gestión de sistemas que implique, entre otras:

- Definición de Virtual LAN's (qué tramos de red utilizan cada una de las empresas, para que no existan solapamientos).
- Reserva de recursos en las infraestructuras correspondientes (discos, cpu, ram), para que en caso de desastre, la infraestructura definida pueda ser puesta en marcha en el “warm-site” correspondiente.
- Permisos de acceso a los centros de datos.
- Permisos de administración de las infraestructuras de máquinas virtuales
- Disponibilidad de las copias de seguridad
- Conectividad con los sistemas respaldados. Existencia de una línea de datos para asegurar la conectividad desde el exterior en caso de caída de los sistemas.

Motivación

Existe un riesgo de pérdida total de la infraestructura de sistemas de información de la compañía en caso un desastre mayor (incendio en las oficinas, explosión, terremoto, terrorismo, etc).

El plan de continuidad del negocio pretende dar respuesta a este tipo de eventualidades

Objetivos

- Elaborar y mantener un conjunto de acciones a seguir para asegurar que, en caso de desastre, se va poder continuar con la actividad de la compañía.

Beneficiarios

Todo el personal de la compañía, ya que en caso de un desastre mayor, la actividad de todos ellos quedaría afectada.

Controles/Riesgos contemplados

La confección y pruebas del plan de continuidad del negocio se lleva a cabo en el ámbito de ejecución de

las medidas de control especificadas en el apartado 14 (Gestión de la Continuidad del Negocio) de los controles de la ISO-27002.

Ámbito

El ámbito de afectación de estas medidas es de toda la compañía en su conjunto.

También se entiende que las medidas afectan a la organización colaboradora.

Actividades y Tareas

- **Determinar necesidades de recursos e infraestructura:** Realizar una revisión técnica de la infraestructura necesaria para determinar qué recursos se necesitarán en el CPD de reserva.
- **Elaboración de Informe de viabilidad y costes:** Se realiza una estimación de los costes de implementación del plan de continuidad del negocio, así como de la viabilidad técnica del proyecto.
- **Aprobación y dotación de recursos por parte de la dirección:** Dirección estudia la viabilidad económica del estudio presentado. Una vez se estima que es viable, lo dota de recursos y da la orden ejecutiva de llevarlo a cabo.
- **Confección de cláusulas y establecimiento de acuerdos:** Acuerdos con la organización colaboradora para permitir el uso de su infraestructura a modo de “warm-site”. Acuerdos sobre restricciones técnicas y políticas de trabajo para asegurar la coexistencia de los sistemas de cada una de las organizaciones.
- **Elaboración de procesos y procedimientos necesarios para mantener el plan de continuidad del negocio:** Se elaboran o modifican las instrucciones de procedimientos necesarias para el correcto mantenimiento de la consistencia de los sistemas para que éstos sean recuperables en caso de desastre. Estos procesos y procedimientos estarán basados, en parte, en los acuerdos establecidos con la empresa colaboradora.
- **Elaboración del plan de acciones a ejecutar en caso de contingencia:** Se elabora un detalle de las acciones que se han de llevar a cabo en caso de desastre.
- **Pruebas de funcionamiento del plan de continuidad del negocio:** Se contempla en el proyecto una primera prueba, aunque esta prueba se deberá llevar a cabo al menos una vez al año. En ella se simulará una situación de desastre y en la que se recuperará una copia de seguridad de los sistemas de información en el “warm-site”. De esta prueba deberán recogerse evidencias para las auditorías de Seguridad de la Información que lo requieran.

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. Se aportan evidencias de pruebas de que el plan de continuidad del negocio se ha ejecutado de manera exitosa
2. La implementación del proyecto se hace dentro de los plazos estipulados y en los costes establecidos.

Calendario

Para poder llevar a cabo este proyecto, la infraestructura técnica definida en el proyecto de *Implementación de la Granja Virtual* debe estar completamente implementada, así como la *externalización del sistema de copias de seguridad*.

Es por ello, que la fecha de inicio del proyecto será, al menos, en Agosto-2013

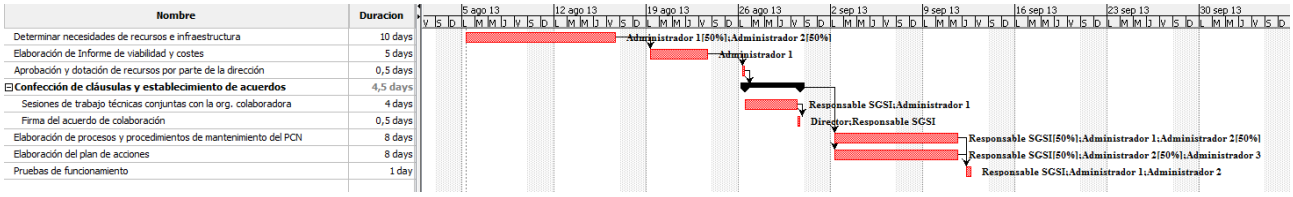


Ilustración 21: Calendario Proyecto "Plan de Continuidad del Negocio"

Recursos

Materiales

Los recursos materiales necesarios para llevar a cabo el proyecto son:

Reserva de recursos para el “warm-site” de la organización colaboradora. Esto es, reservar suficiente CPU, Memoria y Disco en los sistemas para que, en caso de desastre en la organización colaboradora, poder levantar sus sistemas en nuestra infraestructura. En el el proyecto de implementación de la granja virtual ya se ha realizado un dimensionamiento acorde a estas necesidades, por lo que no se incurre, en principio, en costes adicionales por este aspecto.

Gastos de notaría, en la firma del acuerdo de colaboración (se estiman 1.000 €)

Personal

Para el desarrollo del proyecto se estima que será necesaria la participación de las siguientes personas:

- 3 Administradores de Sistemas (328 horas en total, a un coste de 20€/h)
- Responsable del SGSI (72 horas, a un coste de 32 €/h)
- 1 Director ejecutivo (4 horas a un coste de 50€/h, para evaluar la viabilidad del proyecto y dotarlo de recursos).

Financieros

Los costes estimados asociados al proyecto son los siguientes:

- 9.064 € en costes de personal
- 1.000 € en costes de Material

El coste total estimado de implantación del proyecto es de **10.064 €**

Implementación de la metodología de trabajo SCRUM

Descripción

Establecimiento de la metodología de trabajo “SCRUM” en el sub-área de Desarrollo de Software, que es una metodología de trabajo de las denominadas “ágiles”.

Motivación

Actualmente, en el sub-área de Desarrollo de software no existe una metodología clara y documentada para gestionar los proyectos.

Esto ocasiona a veces problemas de comunicación entre los gestores de proyectos y una percepción negativa de los clientes de cómo se están desempeñando las tareas.

En el peor de los casos, los proyectos acaban fracasando porque no existe un control claro, estructurado y documentado de cómo se están desarrollando.

Objetivos

- Implementación de la metodología de trabajo SCRUM en el sub-área de Desarrollo de Software.

Beneficiarios

El Personal del sub-área de Desarrollo de Software (el Responsable del Área, los jefes de proyecto y los desarrolladores). La implementación de esta metodología les permitirá optimizar su rendimiento y evaluar mejor los resultados de su trabajo

El responsable del Área de Tecnología. La metodología de trabajo permitirá que los jefes de proyecto sean capaces de reportar de manera precisa información sobre el estado de los proyectos en curso.

Controles/Riesgos contemplados

La implantación de la metodología SCRUM se lleva a cabo en el ámbito de la ejecución de las medidas de control especificadas en el Análisis de Riesgos, concretamente en el identificado con el número 78.

Ámbito

El ámbito de afectación de estas medidas es el Sub-área de Desarrollo de Software..

Actividades y Tareas

- **Elaboración de propuesta de implementación de la metodología:** Se confecciona un informe para la dirección donde se hace un detalle de tares, una estimación de costes y un calendario de la implementación de la metodología. Se solicitan presupuestos a diferentes entidades que ofrezcan formación en la metodología. Se considera la más adecuada en la propuesta.
- **Aprobación y dotación de recursos por parte de la dirección:** Dirección aprueba la propuesta detallada en el informe y la dota de recursos.
- **Formación de las personas encargadas de dirigir la implementación:** Las personas con capacidad de gestión de proyectos asisten a una formación contratada a una empresa externa sobre la metodología.
- **Elaboración de herramientas, procesos y procedimientos necesarios para gestionar la implementación de la metodología:** Las personas que han asistido a la formación anterior elaborarán la documentación y se dotarán de las herramientas necesarias para poder trabajar bajo la metodología aprendida.
- **Formación de los empleados del Sub-área:** Los gestores de proyectos aleccionan a sus equipos en el funcionamiento de la metodología.

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. La implementación del proyecto se hace dentro de los plazos estipulados y en los costes establecidos.
2. Se aportan evidencias de que los proyectos se están desarrollando siguiendo la metodología indicada.

Calendario

Nombre	Duracion
Elaboración de propuesta de implementación de la metodología	3 days
Aprobación y dotación de recursos por parte de la dirección	0,5 days
Formación de las personas encargadas de dirigir la implementación	2 days
Elaboración de herramientas, procesos y procedimientos necesarios para gestio	3 days
Formación de los empleados del Sub-área	1 day
Formación Grupo 1	1 day
Formación Grupo 2	1 day
Formación Grupo 3	1 day

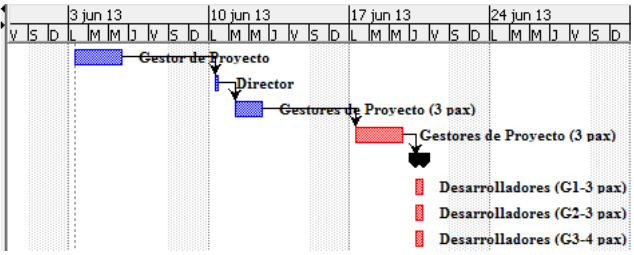


Ilustración 22: Calendario Proyecto "Implementación de la metodología de trabajo SCRUM"

Recursos

Materiales

La formación de los gestores de proyectos se impartirá en la sala de Juntas de la empresa, que está equipada con todo el material necesario (proyector, pizarra, sillas, etc).

La formación a los desarrolladores se impartirá en la propia sala de trabajo de los desarrolladores.

Dirección dotará 60€ en concepto de materiales (Libretas, bolígrafos, agua, etc).

Personal

Para las sesiones de formación es necesario que asistan todos los integrantes del sub-área de Desarrollo de Software. Para hacer posible esto afectando lo menos posible la actividad de la organización, se formarán diferentes grupos que asistirán a las sesiones.

Financieros

Se ha estimado el coste para la empresa, en concepto de personal, que supone la asistencia al curso (Tiempo “no-productivo”) para una formación de 8 horas de duración total:

- Gestores de Proyectos (3 pax): 2.760 €
- Desarrolladores (7 pax): 1.840 €

Los costes de Personal para las tareas de gestión del proyecto son:

- Directivos: 200€
- Desarrollador (Gestor de Proyectos): 552 €

El presupuesto estimado para la contratación de la acción formativa a la empresa externa es de 2.400 €

Sumando todos los costes, el total es de: **7.812 €**

Implementación de la metodología ITIL v3

Descripción

Establecimiento de la metodología de trabajo según “ITIL v3” en las sub-áreas de Administración de bases de Datos y Sistemas.

ITIL v3 son un conjunto de buenas prácticas en la gestión de departamentos de IT. Entre ellas, se engloban apartados que son directamente aplicables a las sub-áreas mencionadas, como son la gestión de incidencias, la gestión de problemas, la gestión de cambios y la gestión de configuración.

Motivación

De manera similar a lo que sucede en el sub-área de Desarrollo de software con los proyectos, actualmente no existe una metodología clara y documentada para gestionar el servicio en las sub-áreas de Administración de Sistemas y de Bases de Datos.

Esto ocasiona, con cierta frecuencia, problemas de coordinación y comunicación, así como que no existe una manera clara y definida de realizar un informe del rendimiento global de los equipos.

Objetivos

- Implementación de las recomendaciones de ITIL en las sub-áreas de Administración de Bases de Datos y Sistemas.

Beneficiarios

El Personal de las sub-áreas de Administración de Bases de Datos y Sistemas (los Responsables de sub-área y los técnicos). La implementación de esta metodología permitirá unificar criterios de gestión en las tareas comunes y, de esta manera, mejorar la comunicación y la interoperabilidad de los técnicos.

El responsable del Área de Tecnología. La unificación de criterios y de metodologías de gestión permitirá mejorar la comunicación con el personal de las sub-áreas y facilitar la gestión y la toma de decisiones operativas.

Controles/Riesgos contemplados

La implantación de ITIL v3 se lleva a cabo en el ámbito de la ejecución de las medidas de control especificadas en el Análisis de Riesgos, concretamente en el identificado con el número 78.

De la misma manera, la implementación también contempla los controles siguientes especificados en la ISO-27002:

- 12.5.1 - Procedimientos de control de cambios
- 12.6.1 - Control de las vulnerabilidades técnicas
- 10.1.2 - Gestión de Cambios
- 10.1.3 - Segregación de Tareas
- 10.10.4 - Registros de administración y operación
- 10.10.5 - Registro de fallos

Ámbito

El ámbito de afectación de estas medidas es las sub-áreas de Administración de Bases de Datos y Sistemas.

Actividades y Tareas

- **Elaboración de propuesta de implementación de la metodología:** Se confecciona un informe para la dirección donde se hace un detalle de tares, una estimación de costes y un calendario de la implementación de la metodología de trabajo. Se solicitan presupuestos a diferentes entidades que ofrezcan formación en ITIL v3. Se considera la más adecuada en la propuesta.
- **Aprobación y dotación de recursos por parte de la dirección:** Dirección aprueba la propuesta detallada en el informe y la dota de recursos.
- **Ejecución de la acción formativa:** El personal de las sub-áreas de Administración de Bases de Datos y Sistemas asiste a las sesiones de formación.
- **Elaboración de herramientas, procesos y procedimientos necesarios para gestionar la implementación de la metodología:** Una selección de las personas que han asistido a la formación anterior elaborarán la documentación y se dotarán de las herramientas necesarias para poder trabajar bajo la metodología aprendida.

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. La implementación del proyecto se hace dentro de los plazos estipulados y en los costes establecidos.
2. Se aportan evidencias de que las tareas diarias se están llevando a cabo siguiendo la metodología indicada.

Calendario

La fecha de inicio del proyecto está condicionada por las prioridades de ejecución de otros proyectos, tales como el *plan de continuidad del negocio:*

Nombre	Duracion
Elaboración de propuesta de implementación de la metodología	3 days
Aprobación y dotación de recursos por parte de la dirección	0,5 days
Formación de los empleados del Sub-área	8 days
Formación Grupo 1	2 days
Formación Grupo 2	2 days
Formación Grupo 3	2 days
Formación Grupo 4	2 days
Elaboración de herramientas, procesos y procedimientos necesarios para gestio	2 days

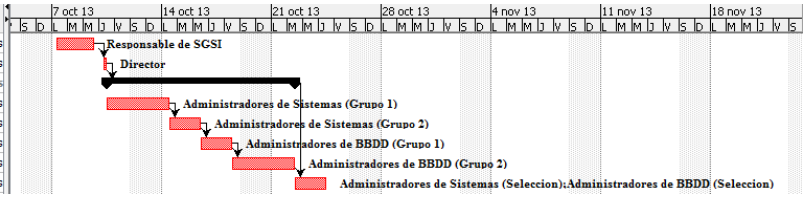


Ilustración 23: Calendario Proyecto "Implementación de la metodología ITIL v3"

Recursos

Materiales

La formación de los Administradores de BBDD y Sistemas se impartirá en la sala de Juntas de la empresa, que está equipada con todo el material necesario (proyector, pizarra, sillas, etc).

Dirección dotará 120€ en concepto de materiales (Libretas, bolígrafos, agua, etc).

Personal

Para las sesiones de formación es necesario que asistan todos los integrantes de las sub-áreas de Administración de BBDD y Sistemas. Para hacer posible esto afectando lo menos posible la actividad de la organización, se formarán diferentes grupos.

Financieros

Se ha estimado el coste para la empresa, en concepto de personal, que supone la asistencia al curso (Tiempo “no-productivo”) para una formación de 8 horas de duración total:

- Administradores de Sistemas (10 pax): 3.200 €
- Administradores de BBDD (10 pax): 4.480 €

Los costes de Personal para las tareas de gestión del proyecto son:

- Directivos: 200€
- Responsable del SGSI: 720 €

El presupuesto estimado para la contratación de la acción formativa a la empresa externa es de 3.000 €

Sumando todos los costes, el total es de: **11.720 €**

Implementación de Software de Gestión Documental

Descripción

Implementación de una plataforma de gestión documental en la infraestructura de la empresa.

La plataforma debe ser capaz de asimilar e indexar toda la documentación existente.

Debe permitir el establecimiento de perfiles y roles de acceso a la información para posibilitar niveles de acceso a ésta en base al etiquetado que se le asigne.

Debe permitir también el etiquetado de cada documento en base a los siguientes niveles:

- *Documento Público o desclasificado*
- *Documento Propietario*
- *Documento Confidencial de cliente*
- *Documento Confidencial de la organización.*

También debe ofrecer un control de las versiones de los documentos.

Motivación

En el momento actual la documentación de la compañía está ubicada en jerarquías de carpetas dentro de un servidor de ficheros.

La información está almacenada en diferentes formatos (.doc, .docx, .odf, .pdf, .xls, .odt...) y con el sistema actual no es posible realizar una búsqueda ágil por el contenido de los documentos.

De la misma manera, el control de versiones se “emula” creando copias del documento dentro de la carpeta que contiene éste, lo cual dificulta aún más el control de éstos, dando lugar a borrados accidentales, versiones duplicadas, etc.

Por otra parte, la gestión de los permisos de acceso a los documentos se hace asignando permisos de acceso a las diferentes carpetas en función de grupos a los que pertenece cada usuario por separado. Esta gestión la lleva actualmente el administrador del dominio (que es el que asigna los permisos a los recursos). Sería más lógico que la asignación de accesos a la documentación la llevaran a cabo personas con un rol en la empresa no necesariamente técnico, sino funcional.

Todos los inconvenientes anteriores dificultan la gestión del conocimiento en la empresa, ya que se invierte un esfuerzo superfluo significativo en superarlos. Éstos quedarían solventados con la implementación de una herramienta de gestión documental.

Objetivos

- Implementación de una herramienta que permita realizar una gestión del conocimiento adecuada a las necesidades de la compañía.

Beneficiarios

Todo el personal de la compañía, en mayor o menor medida, gestionan o acceden a documentación de algún tipo por lo que la cualquier mejora al respecto supone un beneficio para todos ellos.

Controles/Riesgos contemplados

La implantación de un Software de Gestión Documental se lleva a cabo en el ámbito de la ejecución de las medidas de control especificadas en el Análisis de Riesgos, concretamente en los identificados con los números 80, 81 y 82.

También facilita la adecuación a los controles de la ISO-27002 definidos en los puntos:

- 7.2.1 - Directrices de Clasificación
- 7.2.2 - Etiquetado y manipulado de la información
- 11.6.1 - Restricción del acceso a la información

Ámbito

El ámbito de afectación de estas medidas es a todos los departamentos de la compañía.

Actividades y Tareas

- **Estudio y evaluación de programas de Gestión Documental**: Se lleva a cabo un proceso de evaluación de herramientas, en el que se seleccionarán las más idóneas para ser incluidas como opciones a considerar en el informe de viabilidad y costes
- **Elaboración de Informe de viabilidad y costes**: Se lleva a cabo un estudio del coste de implementación y operación de las herramientas evaluadas anteriormente.
- **Aprobación y dotación de recursos por parte de la dirección**: Se escoge la herramienta más idónea. Dirección dota de recursos para su integración en los sistemas.
- **Implementación de la solución escogida en la infraestructura de Sistemas:** Se llevan a cabo las acciones necesarias para integrar la herramienta en los sistemas.
- **Pruebas de funcionamiento:** Se lleva a cabo una batería de pruebas para asegurar el correcto funcionamiento de la herramienta. Se documentan las pruebas realizadas como evidencia de éstas.
- **Formación a los usuarios en el funcionamiento de la herramienta:** Se realizan sesiones de formación a los usuarios en el uso y manejo de la herramienta.

Evaluación de Resultados

Los indicadores de éxito del proyecto son los siguientes:

1. La implementación del proyecto se hace dentro de los plazos estipulados y en los costes establecidos.
2. Se aportan evidencias de que los usuarios tienen conocimiento del uso de la herramienta.

Calendario

El inicio del proyecto está condicionado a la finalización de otros proyectos de formación (ITIL y SCRUMM) debido a la ocupación de los recursos destinados a la formación (personas, salas, proyector, etc).

Nombre	Duracion
Estudio y evaluación de programas de Gestión Documental	3 days
Elaboración de Informe de viabilidad y costes	2 days
Aprobación y dotación de recursos por parte de la dirección	0,5 days
Implementación de la solución	2 days
Pruebas de funcionamiento	1 day
Formación a los usuarios en el funcionamiento de la herrami	9 days
Formación a Responsables y Directivos	1 day
Formación a Desarrolladores (Grupo 1)	1 day
Formación a Desarrolladores (Grupo 2)	1 day
Formación a Administradores de Sistemas (Grupo 1)	1 day
Formación a Administradores de Sistemas (Grupo 2)	1 day
Formación a Administradores de BBDD (Grupo 1)	1 day
Formación a Administradores de BBDD (Grupo 2)	1 day
Formación a Personal de BackOffice (Grupo 1)	1 day
Formación a Personal de BackOffice (Grupo 2)	1 day

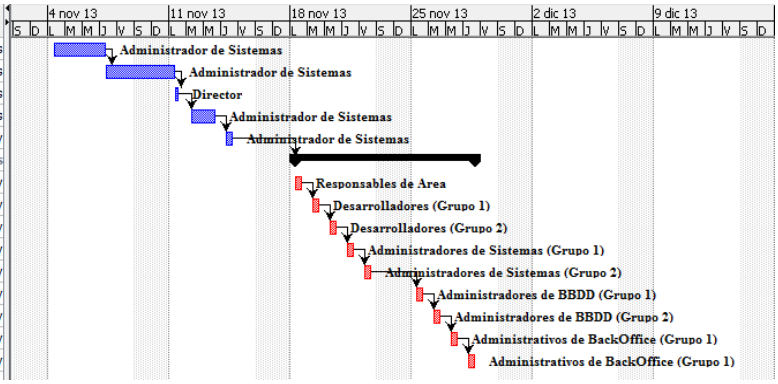


Ilustración 24: Calendario Proyecto "Implementación de Software de Gestión Documental"

Recursos

Materiales

Licencia del Software de gestión documental que se va a implementar. Coste estimado: 7.500 €, incluyendo la formación al personal y el soporte el primer año.

La formación a los usuarios se impartirá en la sala de Juntas de la empresa, que está equipada con todo el material necesario (proyector, pizarra, sillas, etc).

Dirección dotará 150€ en concepto de materiales (Libretas, bolígrafos, agua, etc).

Personal

Para la formación es necesario que asista todo el personal de la compañía. Para hacer posible esto afectando lo menos posible la actividad de la organización, se formarán diferentes grupos que asistirán a las sesiones a tiempo parcial.

Financieros

Se ha estimado el coste para la empresa, en concepto de personal, que supone la asistencia al curso (Tiempo “no-productivo”) para una formación de 4 horas de duración total:

- Administradores de BBDD (10 pax): 2.240 €
- Administradores de Sistemas (10 pax): 1.600 €
- Desarrolladores (10 pax): 1.840 €
- Administrativos de BackOffice (8 pax): 960 €
- Directivos y Responsables de Area (4 pax): 1.280 €

Los costes de Personal para las tareas de gestión e implantación del proyecto son:

- Directivos: 200€
- Administrador de Sistemas: 1.280 €

Sumando todos los costes, el total es de: **17.050 €**

Quick-Wins

En este apartado se identifican los tres proyectos que aportan un mayor beneficio inmediato con una relación coste-beneficio más favorable.

Los proyectos se enumeran por orden de importancia siendo el primero el más importante.

Plan de continuidad del Negocio

Se considera este proyecto como el más prioritario debido a que actualmente la organización no cuenta con ningún tipo de plan de continuidad del negocio, lo cual supone una no-conformidad mayor y un riesgo serio de pérdidas catastróficas en caso de producirse un desastre.

El coste total estimado de implantación del proyecto es de 10.064 €, lo cual, considerando las consecuencias de un posible desastre en la organización, supone un coste-beneficio muy favorable.

Formación de los empleados en Seguridad de la Información

Se tiene en consideración este proyecto como "quick-win" debido a que la formación de los empleados en Seguridad de la Información es clave para la implantación del SGSI, por lo que si se prioriza esta formación la implantación de todo el SGSI se beneficiará de que el personal está alineado con los objetivos y las metas que éste persigue.

Además, la formación viene a cubrir numerosos controles del análisis de Riesgos y de la ISO-27002:

Del Análisis de Riesgos, los identificados con los números 18 y 20.

De la ISO-27002:

- 8.2.2 - Concienciación, formación y capacitación en seguridad de la información.
- 11.3.1 – Uso de contraseñas
- 11.3.2 – Equipo de usuario desatendido
- 11.3.3 – Política de puesto despejado y pantalla limpia
- 13.1.1 – Notificación de eventos de seguridad de la información
- 13.1.2 – Notificación de puntos débiles de la seguridad
- 13.2.3 – Recopilación de evidencias
- 15.1.5 – Prevención del uso indebido de los recursos de tratamiento de la información
- 15.2.1 – Cumplimiento de las políticas y normas de seguridad

Por otra parte, los costes estimados de la formación son de 13.340 € por lo que, comparativamente, estaría en un punto medio dentro del resto de los proyectos.

Externalización del sistema de backups

Se destaca este proyecto como "quick-win" debido a que la relación coste-beneficio es muy favorable y a que supone la implantación de numerosos controles contemplados en el análisis de Riesgos (concretamente en los riesgos identificados con los números que van desde el 36 al 38,40 al 41,43 al 45 y 57) así como los controles especificados en el apartado 10.5 (Copias de Seguridad) de la ISO-27002.

El coste estimado de implantación es de 3.529,60 €, por lo que se situaría dentro de la escala inferior de costes en relación al resto de los proyectos considerados.

Auditoría de cumplimiento

Introducción

En el presente documento se expone un resumen de la madurez en la implementación de los controles definidos en la ISO 27002

La revisión de los controles se ha llevado a cabo siguiendo el modelo de madurez de la capacidad (CMM), cuya escala se define en el siguiente cuadro:

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

Tabla 14: Valoraciones del modelo CMM

Las valoraciones de los resultados de cada uno de los dominios se llevan a cabo realizando un promedio de los controles de éstos.

Estas valoraciones se acompañan con gráficos para facilitar su comprensión.

Madurez de los controles definidos en ISO-27002

A continuación se expone el resumen de los resultados de la evaluación de madurez de los controles definidos en la ISO-27002.

El siguiente cuadro muestra el porcentaje de madurez (% Efectividad) dividido por dominios:

Dominio	% de Efectividad	# NC Mayores	# NC Menores
5.- Política De Seguridad	100%	0	0
6.- Aspectos Organizativos de la SI	91%	1	1
7.- Gestión de activos	76%	1	0
8.- Seguridad ligada A RRHH	97%	0	3
9.- Seguridad física Y del entorno	72%	3	0
10.- Comunic. y Operaciones	90%	3	3
11.- Control De acceso	98%	1	0
12.- Adquisición, Desarrollo y Mantenimiento De los SI	90%	0	3
13.- Gestión de Incidentes deSI	85%	1	0
14.- Continuidad Del negocio	10%	5	0
15.- Cumplimiento	99%	0	0

Tabla 15: Madurez de los controles definidos en ISO-27002

Para cada uno de los dominios se muestran, además, el número de No-Conformidades mayores y No-Conformidades menores detectadas.

Del cuadro anterior podemos extrapolar el siguiente diagrama de Radar donde se muestra gráficamente el grado de madurez presente en cada uno de los Dominios:

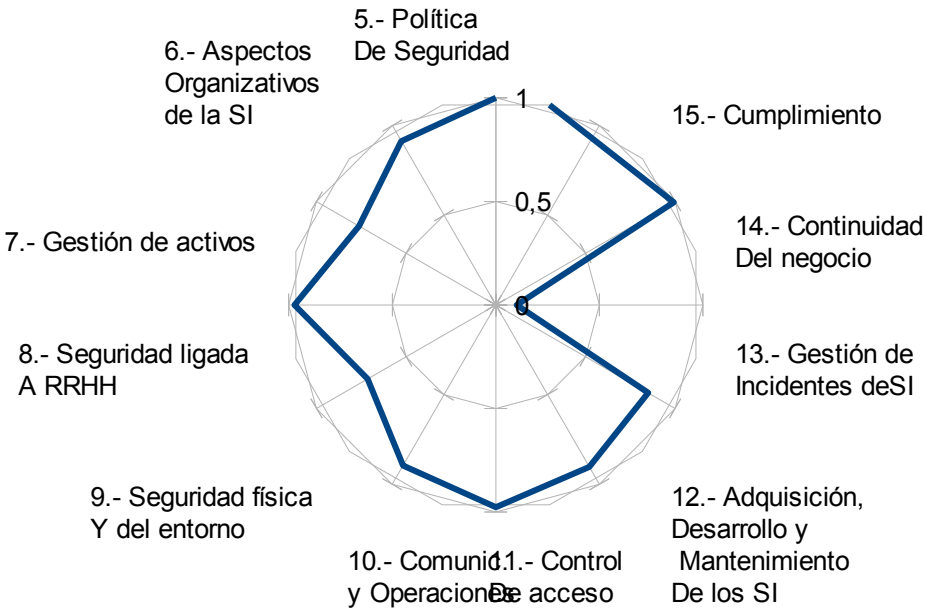


Ilustración 25: Red - Madurez de controles ISO-27002

Se observa claramente que el dominio "[14] – Continuidad del negocio" es el dominio con el grado de cumplimiento menos avanzado.

Los motivos de este hecho se exponen en el informe de auditoría anexo ("Anexo 4 – Informe de Auditoría") y en el detalle del Estado de los controles de la ISO-27002 ("Anexo 5 – Detalle Auditoría controles iso27002").

El siguiente gráfico nos muestra, para cada dominio, una escala comparativa de la madurez de los controles que forman cada uno de estos:

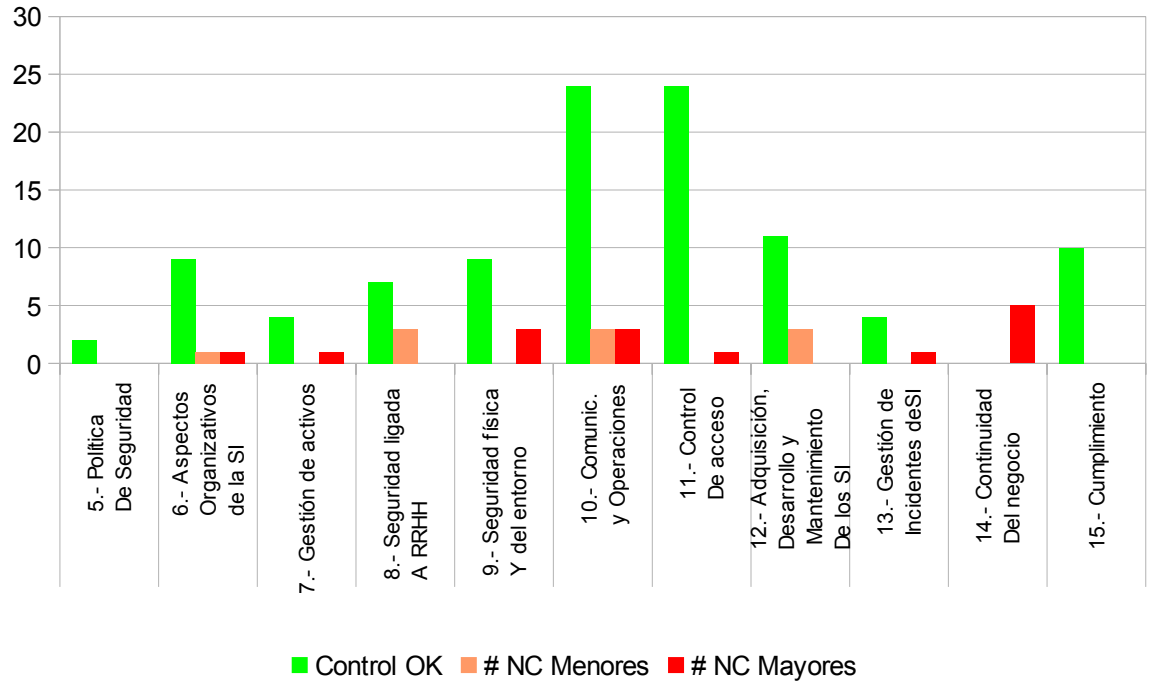


Ilustración 26: Madurez Controles iso-27002 por Dominios

Por último, se muestran las proporciones entre controles que tienen un nivel de madurez por encima del 50% (Aprobado) y por debajo (No Aprobados).

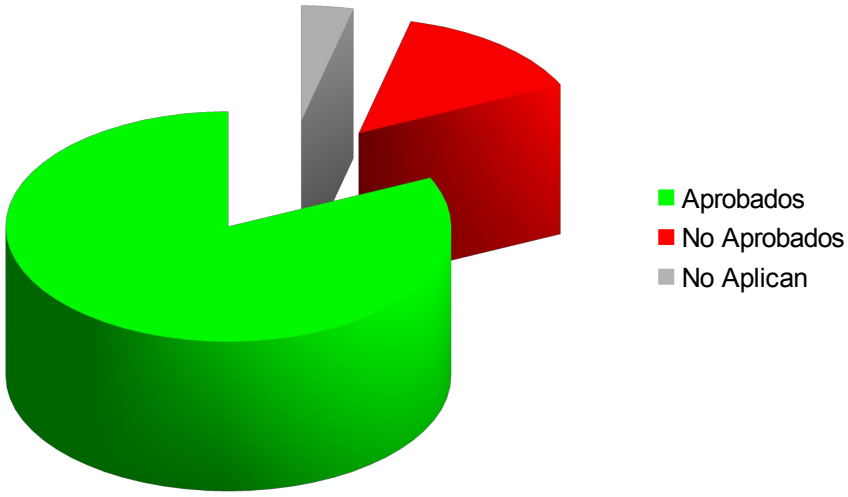


Ilustración 27: Madurez ISO-27002 Totales

Conclusiones

Objetivos Conseguidos

- **Compromiso de la dirección con la Seguridad de la Información**: Con el planteamiento de este proyecto, la dirección de la organización ha tomado conciencia de la importancia real de gestionar la Seguridad de la Información y de las implicaciones y los beneficios de establecer un SGSI.
- **Elaboración e Implantación del esquema documental**: Con la alineación de la dirección respecto a los objetivos del SGSI, se ha conseguido dar el valor necesario a la correcta documentación y seguimiento de los procedimientos. Esto conlleva de manera implícita una mejora en la calidad de los procesos independientemente del tipo que sean estos.
- **Concienciación de la organización respecto a los riesgos**: La realización del análisis de riesgos y la presentación y estudio de los resultados de éste por parte de la dirección ha otorgado una dimensión relevante de éstos dentro de la organización que previamente no existía. Esta relevancia es sumamente positiva, puesto que permite que la dirección tenga en consideración los riesgos a la hora de establecer prioridades y recursos.
- **Establecimiento de un proceso de Gestión de la Seguridad de la Información**: La seguridad de la información como proceso integrado en la compañía beneficia a ésta en su conjunto, por las garantías que ofrece respecto a la disponibilidad, confidencialidad e integridad de la información que se gestiona.

Ampliaciones del trabajo

Las posibles ampliaciones del trabajo que considero que se podrían llevar a cabo son:

- Se podría llevar a cabo un análisis más pormenorizado en el apartado de análisis de riesgos. Por ejemplo, analizar el número de vulnerabilidades que gestiona un mismo propietario para dar una idea de si, por ejemplo, un sólo propietario está gestionando demasiados activos.
- En las propuestas de proyectos, se podría haber detallado gráficamente la mejora que la implantación de cada uno de ellos tiene sobre el cumplimiento (en este momento se detalla qué controles especificados en el análisis de riesgos implementan, así como los controles de la normativa si en tal caso aplicase).

Bibliografía

Sistema de Gestión de Seguridad de la Información en una Organización

http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/

Fases de Implantación de un SGSI

http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Fases_SGSI/

Portal de ISO 27001 en Español:

http://www.iso27000.es/

Normativas:

ISO/IEC 17799:2005

ISO/IEC 27001:2005 http://es.wikipedia.org/wiki/ISO/IEC_27001

ISO/IEC 27002:2009 http://es.wikipedia.org/wiki/ISO/IEC_27002

Blog dedicado al estudio de la Seguridad de la Información - Privacidad - Seguridad Informatica - Auditoria informática:

http://seguridad-informacion.blogspot.com.es

Anexos

Anexo	Fichero	Descripción
1	*jconsuegra_TFM_062013_Anexo1_Analisis_Diferencial_27001.xls*	Hoja de Cálculo donde se detalla el análisis diferencial en la situación Inicial del cumplimiento de los controles de la ISO-27001
2	*jconsuegra_TFM_062013_Anexo2_Analisis_Diferencial_27002.xls*	Hoja de Cálculo donde se detalla el análisis diferencial en la situación Inicial del cumplimiento de los controles de la ISO-27002
3	*jconsuegra_TFM_062013_Anexo3_Analisis de Riesgos.xls*	Hoja de Cálculo donde se detalla la identificación de Activos y el Análisis de Riesgos sobre éstos.
4	*jconsuegra_TFM_062013_Anexo4_Informe de Auditoria.pdf*	Informe de la Auditoría interna realizada la organización en la que se hace un estudio del cumplimiento de las normativas ISO-27001 y 27002
5	*jconsuegra_TFM_062013_Anexo5_Estado controles 27002.xls*	Hoja de Cálculo donde se detalla el análisis diferencial en la situación Final del cumplimiento de los controles de la ISO-27002
6	*jconsuegra_TFM_062013_Anexo6_Estado controles 27001.xls*	Hoja de Cálculo donde se detalla el análisis diferencial en la situación Final del cumplimiento de los controles de la ISO-27001