Plan de Implementación de la ISO/IEC 27001:2005 en la empresa SEGNET

Autor:
Fernando París Fernández

Tutor:
Antonio José Segovia Henares

Tabla de Contenido

1. Fase 1. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

1.1 Contextualización

La empresa SEGNET (Nombre ficticio), dedicada al desarrollo de sistemas y aplicaciones a medida relacionados con medios de pago, tiene entre sus clientes a bancos y cajas, fabricantes de terminales de pago, proveedores de pago (tarjetas de crédito o pago por Internet) y consorcios de transportes.

SEGNET tiene 20 trabajadores distribuidos en 3 áreas distintas (Dirección 1 persona, IT 3 personas y I+D+I 16 personas). El personal de dirección e IT trabaja desde las oficinas centrales y el personal de I+D+I tiene libertad para teletrabajar o trabajar en las oficinas centrales. Existen teletrabajadores en sitios tan dispares como Málaga, Coruña o incluso Berlín.

Como se desprende de lo expuesto anteriormente SEGNET es una empresa distribuida y altamente dependiente de las comunicaciones de todo tipo. Las comunicaciones telefónicas entre los empleados y con el exterior se realizan mediante telefonía IP, y otro tipo de comunicaciones se realiza mediante mensajería instantánea tipo Yahoo o correo electrónico. Los sistemas de correo electrónico y telefonía IP se encuentran en una sala de las oficinas centrales con acceso restringido.

La seguridad operativa tanto de las instalaciones como de los sistemas consta de controles físicos de acceso a las zonas sensibles y controles lógicos (firewalls e VPNs), pero la respuesta ante imprevistos, incidentes o accidentes no está contemplada de forma apropiada.

Los servicios que deja la empresa disponibles para los clientes son únicamente su pagina Web, un sistema de tickets para gestionar incidencias y ocasionalmente algún sistema de prueba con un objetivo puramente demostrativo y sin implicaciones contractuales de disponibilidad pero si con cierto valor de imagen.

Existe cierta experiencia con políticas de seguridad y procedimientos dado que hace años, por necesidades de negocio, se implantó la norma PCI DSS en un área hoy extinta por el alto coste que suponía. Quedan como restos los elementos que eran globales, es decir, una política de seguridad, unas normas de uso aceptable, guías de configuración y una gestión de claves criptográficas que se sigue manteniendo.

El alcance que tendrá el plan de implementación de la ISO/IEC 27001:2005 serán los sistemas de información que dan soporte a las áreas de I+D+I e IT en el desempeño de su actividad para el negocio de SEGNET.

1.2 Objetivos del Plan Director

Los objetivos del plan director para la organización mencionada serán:

- Identificar los riesgos a los que está expuesta la organización.
- Mejorar la seguridad de la organización.
- Reducir las perdidas accidentales de información

1.3 Análisis Diferencial

A continuación se detalla el estado actual de SEGNET con respecto a la norma ISO 27001 e ISO 27002, en donde se refleja los controles que se han aplicado o no y una descripción de lo observado.

En relación a los requisitos que establece la ISO 27001 para el Sistema de Gestión anotamos lo siguiente

PUNTO	REVISIÓN
4. SGSI	
4.1 Requisitos Generales	No se cumplen
4.2 Establecimiento y Gestión del SGSI	Lo único de lo que dispone la empresa es de una política básica que define alcance y compromiso por parte de la dirección pero carece del resto de requisitos.
4.2.x	En cuanto a implantación, operación seguimiento, revisión, mantenimiento y mejora, no existe nada.
4.3 Requisitos de documentación	Únicamente existe un documento de política de seguridad y un documento de Normas y uso aceptable que ha sido firmado por todos los empleados.
5. Responsabilidad de la dirección	La dirección ha creado la política de seguridad y ha comunicado a la

PUNTO	REVISIÓN
	organización la importancia de los objetivos de seguridad mediante el documento de “uso aceptable”, pero no ha ido mas allá con recursos, análisis de riesgos, auditorias ni revisiones del SGSI
5.2 Gestión de Recursos	
5.2.1 Provisión	La dirección ha asignado únicamente el rol de director de seguridad. No hay mas responsabilidades ni asignación de recursos para la creación del comité de seguridad
5.2.2 Formación	Además del documento de uso aceptable, el director de seguridad periódicamente envía información para la toma de concienciación a todo el personal. La lectura por parte de los empleados de esta información no está acreditada.
6. Auditorias Internas	No se hacen
7. Revisión del SGSI por la dirección	No se hace
8. Mejora del SGSI	No se hace

Y en relación a los controles de la ISO 27002, anotamos lo siguiente:

CONTROL	EXISTE	REVISIÓN
5. Política de Seguridad		
5.1 Política de Seguridad de la información		
5.1.1 Documento de política de seguridad de la información	Si	La empresa dispone de un documento de política de seguridad aprobado por la dirección y conocido por todos los empleados.

CONTROL	EXISTE	REVISIÓN
5.1.2 Revisión y Evaluación	Si	El citado documento se revisa anualmente.
6. Aspectos organizativos para la seguridad		
6.1 Organización Interna		
6.1.1 Comité de gestión de seguridad de la información	Si	Existe en la empresa un grupo que se ocupa de revisar y aprobar acciones y documentos relacionados con la seguridad de la información.
6.1.2 Coordinación de la seguridad de la información	Si	El grupo que gestiona la seguridad está relacionado con todas las áreas de la empresa.
6.1.3 Asignación de responsabilidades sobre seguridad de la información	No	No existe ninguna matriz de roles y recursos asignados.
6.1.4 Proceso de autorización de recursos para el tratamiento de la información	No	No existe ningún procedimiento de asignación o autorización de recursos.
6.1.5 Acuerdos de confidencialidad	Si	Existen evidencias de acuerdos de confidencialidad firmados con los empleados y puntualmente con algunos clientes.
6.1.6 Contacto con autoridades	No	No existe una guía de actuación en caso de ataque tecnológico, o incendio etc.
6.1.7 Contacto con grupos de interés especial	Si	El director de seguridad está suscrito a varias listas de seguridad, foros y listas de detección de vulnerabilidades.
6.1.8 Revisión independiente de la seguridad de la información		
6.2 Seguridad de los accesos de terceras personas		
6.2.1 Identificación de riesgos por el acceso de terceros	No	No se realiza.

CONTROL	EXISTE	REVISIÓN
6.2.2 Requisitos de seguridad cuando se trata con clientes	No	No se distinguen normas especiales de seguridad para los clientes y tampoco se les comunican las normas de seguridad de los empleados.
6.2.3 Requisitos de seguridad en contratos de outsourcing	No	No se distinguen normas especiales de seguridad para los clientes y tampoco se les comunican las normas de seguridad de los empleados.
7. Clasificación y control de activos		
7.1 Responsabilidad sobre los activos		
7.1.1 Inventario de activos	Si	Existe un inventario de todos los activos de la empresa correctamente identificados y etiquetados.
7.1.2 Propiedad de los activos	No	Muchos activos tienen un propietario asignado, pero existen otros muchos como servidores comunes o dispositivos de almacenamiento externo que no tiene propietario asignado.
7.1.3 Uso adecuado de los activos	Si	Existe una norma interna de uso aceptable comunicada a todos los empleados y firmada como leída y entendida por los mismos.
7.2 Clasificación de la información		
7.2.1 Guías de clasificación	Si	Existe una guía para clasificar la información y es conocida.
7.2.2 Marcado y tratamiento de la información	No	Si bien es cierto que los documentos incluyen información acerca de la clasificación, los medios en los que se almacenan no la muestran.
8. Seguridad en recursos humanos		
8.1 Seguridad antes del empleo		
8.1.1 Inclusión de la seguridad en	No	Los procesos de selección no

CONTROL	EXISTE	REVISIÓN
las responsabilidades y funciones laborales		incluyen comunicación a los candidatos de funciones ni responsabilidades de seguridad.
8.1.2 Selección y política de personal	No	No se realizan.
8.1.3 Acuerdos de confidencialidad	Si	Existen evidencias de acuerdos de confidencialidad firmados con los empleados y puntualmente con algunos clientes.
8.2 Durante el empleo		
8.2.1 Responsabilidades de la gerencia	No	No se realizan estas comprobaciones
8.2.2 Conocimiento, educación y entrenamiento de la seguridad de la información	Si	Existen evidencias de cursos y listas de distribución que el director de seguridad hace llegar a los empleados con información y nociones de seguridad.
8.2.3 Proceso disciplinario	Si	En el documento de uso aceptable se informa de las medidas disciplinarias que se pueden tomar por parte de la dirección ante faltas en las actuaciones de los empleados.
8.3 Finalización o cambio de empleo		
8.3.1 Responsabilidades de finalización	Si	La dirección es responsable de las finalizaciones de empleo
8.3.2 Retorno de activos	No	No se realiza.
8.3.3 Retiro de los derechos de acceso	No	No existe un procedimiento claro para la retirada de derechos de acceso.
9. Seguridad Física y del Entorno		
9.1 Áreas seguras		

CONTROL	EXISTE	REVISIÓN
9.1.1 Perímetro de seguridad	No	El perímetro está bien delimitado con muros sólidos y rejas en las ventanas. El acceso a las oficinas se puede realizar mediante un código de acceso o por mediación de un empleado. No existe recepción. Los sistemas de almacenamiento se encuentran en una sala separada con un control de acceso independiente. Todo el recinto tiene alarma, pero las aperturas de puertas como consecuencia de emergencias no generan alarmas.
9.1.2 Controles físicos de entradas	No	No se registran los accesos a la sala de servidores. Ni empleados ni visitas llevan identificación aunque dado el tamaño de la empresa tampoco se considera necesario. El acceso a la sala segura si se ha de hacer acompañado de un empleado
9.1.3 Seguridad de oficinas, despachos y recursos	Si	El acceso a las oficinas se realiza mediante llave o código.
9.1.4 Protección contra amenazas externas y ambientales	Si	Los equipos contra incendios están de acuerdo a la normativa y no se almacena nada que no sean equipos de trabajo en la sala.
9.1.5 El trabajo en las áreas seguras	No	Ocasionalmente se trabaja en el área segura. No se revisa la sala cuando está vacía ni existe prohibición expresa de grabar en el área segura.
9.1.6 Acceso publico, áreas de carga y descarga	n/a	No aplica. No se dispone de área de carga y descarga
9.2 Seguridad de Equipos		
9.2.1 Instalación y protección de equipos	Si	Los equipos que manejan información sensible se encuentran en la sala segura que dispone de control de temperatura y humedad, y restricciones para la entrada de líquidos y comida.

CONTROL	EXISTE	REVISIÓN
9.2.2 Suministro eléctrico	No	Los equipos no disponen de SAIs.
9.2.3 Seguridad del cableado	Si	Los cableados tanto de electricidad como de red local se encuentran protegidos contra manipulación y los paneles de parcheo cerrados con llave. Existe documentación de los citados paneles y esquemas de todo el cableado.
9.2.4 Mantenimiento de equipos	No	No se llevan a cabo revisiones preventivas. Únicamente correctivas.
9.2.5 Seguridad de equipos fuera de los locales de la organización	No	La gerencia no ejerce control alguno sobre los equipos de los teletrabajadores ni sobre su entorno de trabajo en el hogar.
9.2.6 Seguridad en el rehúso o eliminación de equipos	No	No se lleva control de los equipos descatalogados.
9.2.7 Retiro de la propiedad	No	No existe procedimiento de retirada de activos.
10. Gestión de comunicaciones y operaciones		
10.1 Procedimientos y responsabilidades de operación		
10.1.1 Documentación de procedimientos operativos	No	La documentación de procedimientos operativos es incompleta. Existen ciertas guías de instalación y configuración pero no hay procedimientos de backup o recuperación
10.1.2 Gestión de Cambios	No	No existe registro de cambios ni procedimiento de gestión del cambio
10.1.3 Segregación de tareas	Si	Dado el pequeño tamaño de la empresa la asignación de tareas se realiza mediante un sistema de tickets.
10.1.4 Separación de los recursos para desarrollo y para producción	No	No existen procedimientos normalizados para el paso de desarrollo a producción, aunque los entornos físicos si que están

CONTROL	EXISTE	REVISIÓN
		separados correctamente.
10.2 Gestión de servicios externos		
10.2.1 Servicio de entrega	No	No existen procedimientos de entrega de información con elementos externos a la empresa.
10.2.2 Monitoreo y revisión de los servicios externos	No	No se realiza
10.2.3 Gestionando cambios para los servicios externos		No existen procedimientos de gestión de cambios
10.3 Planificación y aceptación del sistema		
10.3.1 Planificación de la capacidad	No	Para nuevos sistemas si que se hace una estimación de capacidad, pero no se monitoriza el uso de los recursos.
10.3.2 Aceptación del sistema	Si	Existen guías de configuración y puesta en marcha para equipos.
10.4 Protección contra software malicioso		
10.4.1 Medidas y controles contra software malicioso	No	Existen políticas que prohíben el uso de software sin licencia así como una lista de software autorizado. Existe un sistema antivirus que analiza los correos y los equipos Windows disponen de antivirus correctamente actualizado y no desactivable, pero los procedimientos de recuperación son incompletos.
10.4.2 Medidas y controles contra código móvil	Si	Solo se permite código móvil para herramientas de monitorización de equipos.
10.5 Gestión de respaldo y recuperación		
10.5.1 Recuperación de la información	No	No se realizan copias de seguridad. Existe alguna copia, pero ni son periódicas ni están documentadas.

CONTROL	EXISTE	REVISIÓN
10.6 Gestión de seguridad en redes		
10.6.1 Controles de red	Si	Existen normas y procedimientos para el acceso remoto a equipos y los equipos están monitorizados con un sistema basado en Nagios
10.6.2 Seguridad en los servicios de redes	Si	El sistema de monitorización vigila la calidad de los servicios contratados (básicamente disponibilidad), Firewalls con IDS e IPS que separan las distintas redes y un firewall de aplicaciones basado en modsecurity
10.7 Utilización de los medios de información		
10.7.1 Gestión de medios removibles	No	No existen procedimientos de uso de medios removibles
10.7.2 Eliminación de medios	No	No existen procedimientos de eliminación de medios
10.7.3 Procedimientos de manipulación de la información	No	No existen
10.7.4 Seguridad de la documentación de sistemas	No	No se protege de especial manera la documentación de sistemas.
10.8 Intercambio de información		
10.8.1 Políticas y procedimientos para el intercambio de información y software	No	En las normas de uso aceptable se incluye información acerca del uso de las comunicaciones electrónicas, la protección ante virus o adjuntos maliciosos, pero no existen procedimientos que regulen el intercambio de información.
10.8.2 Acuerdos de intercambio	No	En ciertos casos se acuerda con algún cliente alguna forma de envío cifrado de documentación o software, pero sin rigor y sin constancia por escrito
10.8.3 Medios físicos en transito	No	No existen procedimientos ni normas al respecto.

CONTROL	EXISTE	REVISIÓN
10.8.4 Seguridad en la mensajería electrónica	No	La empresa utiliza sistemas de mensajería instantánea públicos sin ninguna consideración especial de seguridad. Por otra parte los sistemas de correo si que disponen de restricción de uso mediante contraseña
10.8.5 Sistemas de información de negocios	No	Los sistemas de información de negocio disponen de restricciones de acceso para los empleados, pero una vez se accede toda la información es accesible por todos.
10.9 Servicios de comercio electrónico		
10.9.1 Comercio electrónico	n/a	La empresa no tiene comercio electrónico
10.9.2 Transacciones en línea	n/a	La empresa no tiene transacciones en línea
10.9.3 Información publica disponible	n/a	La empresa no tiene información publica
10.10 Monitoreo		
10.10.1 Registro de la auditoria	Si	La guía de configuración de sistemas incluye configuraciones de registro de logon logoff, la instalación de un Host IDS que registra cambios en ficheros etc.
10.10.2 Monitoreando el uso del sistema	No	Si bien la información de auditoria se registra, esta no se revisa periódicamente, sino mas bien cuando es necesario por un problema
10.10.3 Protección de la información de registro	Si	Los registros están duplicados tanto en el servidor como en un servidor de bitácora centralizado, de forma que la alteración es o complicada o detectable.
10.10.4 Registro de administradores y operadores	Si	Todas las operaciones privilegiadas se registran.
10.10.5 Registro de la avería	Si	Los problemas se reportan a IT

CONTROL	EXISTE	REVISIÓN
		mediante un sistema de tickets con lo que todo el proceso queda registrado.
10.10.6 Sincronización del reloj	Si	La Internet dispone de un servidor de hora y todos los equipos toman su hora de este equipo.
11. Control de Accesos		
11.1 Requisitos de negocio para el control de accesos		
11.1.1 Política de control de accesos	No	No existe una política clara de acceso a los sistemas. La concesión de acceso se realiza sin formalismos ni constancia escrita.
11.2 Gestión de acceso de usuarios		
11.2.1 Registro de usuarios	No	No existe un procedimiento formal para el registro de usuarios
11.2.2 Gestión de privilegios	No	La concesión de privilegios se realiza sin formalismos ni constancia escrita, aunque si existe una valoración de la necesidad de los privilegios por parte del administrador.
11.2.3 Gestión de contraseñas de usuario	Si	El documento de uso aceptable informa a los empleados de cómo gestionar sus contraseñas además las guías de configuración de sistemas establecen que los sistemas fuercen políticas de contraseñas seguras y renovadas periódicamente.
11.2.4 Revisión de los derechos de acceso de los usuarios	No	No existen tales procedimientos de revisión
11.3 Responsabilidades de los usuarios		
11.3.1 Uso de contraseñas	Si	El documento de uso aceptable informa a los empleados de las directrices a seguir en cuanto a contraseñas

CONTROL	EXISTE	REVISIÓN
11.3.2 Equipo informático de usuario desatendido	Si	El documento de uso aceptable informa a los empleados de las directrices a seguir cuando se deja el equipo desatendido
11.3.3 Política de pantalla y escritorio limpio	Si	El documento de uso aceptable informa a los empleados de las directrices a seguir en su área de trabajo.
11.4 Control de acceso a la red		
11.4.1 Política de uso de los servicios de la red	No	A pesar de la segmentación de la red no existen distinciones de acceso según el usuario. Los servicios si que tienen un control basado en usuario/contraseña
11.4.2 Autentificación de usuario para conexiones externas	Si	Las conexiones externas a la red se realizan o bien a servicios dotados de autentificación o bien vía red privada virtual con usuarios y contraseñas
11.4.3 Identificación de equipos en las redes	n/a	Los servicios internos de la empresa no requieren identificación del equipo
11.4.4 Diagnostico remoto y configuración de protección de puertos	Si	Los sistemas de diagnostico remoto se encuentran protegidos en los equipos que disponen de ellos por contraseña
11.4.5 Segregación de redes	Si	Las redes de usuarios y servicios están separadas por firewalls perimetrales.
11.4.6 Control de conexión a las redes	No	El acceso a redes externas es libre y no está sujeto a ninguna política.
11.4.7 Control de enrutamiento en la red	Si	Existen normas para la configuración de firewalls que especifican que solo se deben abrir los puertos de entrada necesarios. Además estas configuraciones se revisan con frecuencia.
11.5 Control de acceso al sistema operativo		

CONTROL	EXISTE	REVISIÓN
11.5.1 Procedimientos de conexión de terminales	Si	Las conexiones de terminales son vía ssh y la configuración del servidor limita el número de intentos bloqueando la cuenta 30 minutos después de 3 fallos. Todos los equipos tienen el MOTD configurado para mostrar un mensaje de seguridad.
11.5.2 Identificación y autentificación del usuario	Si	Todos los empleados tienen un identificador único para todos los sistemas y no existen cuentas de uso compartido.
11.5.3 Sistema de gestión de contraseñas	Si	Los sistemas que lo permiten fuerzan el uso de contraseñas seguras con histórico de las ultimas 10 y para los sistemas que no disponen de esa funcionalidad se instruye a los empleados en la necesidad de renovar las contraseñas
11.5.4 Utilización de las facilidades del sistema	Si	Las actuaciones privilegiadas en los sistemas están registradas
11.5.5 Desconexión automática de sesiones	Si	La guía de configuración de sistemas fuerza al cierre de sesión después de 30 minutos de inactividad
11.5.6 Limitación del tiempo de conexión	n/a	No se puede restringir los tiempos de conexión
11.6 Control de acceso a las aplicaciones y la información		
11.6.1 Restricción de acceso a la información	No	Si bien es cierto que no se da acceso a todos los empleados a todo, la concesión de acceso no es formal.
11.6.2 Aislamiento de sistemas sensibles	No	No existen sistemas calificados como sensibles y por tanto las políticas no tienen un tratamiento especial
11.7 Informática móvil y teletrabajo		

CONTROL	EXISTE	REVISIÓN
11.7.1 Informática móvil y comunicaciones	No	Las conexiones remotas desde dispositivos móviles se realizan mediante conexiones seguras. Pero el respaldo de los sistemas no está exigido por la política de la empresa y se deja a la voluntad del empleado
11.7.2 Teletrabajo	No	El Teletrabajo es generalizado en la empresa y autorizado por la gerencia. La conexión a la red de la oficina está debidamente securizada pero no existen procedimientos, normas o recomendaciones que regulen la forma en la que el empleado ha de comportarse en este entorno exceptuando el documento de uso aceptable que no incluye ningún punto específico para el teletrabajo.
12. Adquisición, desarrollo y mantenimiento de sistemas		
12.1 Requisitos de seguridad de los sistemas		
12.1.1 Análisis y especificación de los requisitos de seguridad	Si	Los requisitos de seguridad forman parte del análisis de sistemas y de la selección de productos.
12.2 Seguridad de las aplicaciones		
12.2.1 Validación de los datos de entrada	Si	La validación de los datos de entrada se encuentra en las guías de desarrollo e implementado en todos los sistemas internos.
12.2.2 Control del proceso interno	Si	Los servicios disponen de firewall de aplicaciones.
12.2.3 Integridad de mensajes	Si	Donde se requiere los mensajes disponen de firma o resumen
12.2.4 Validación de los datos de salida	Si	Los datos de salida pasan por los filtros de validación igual que los de entrada, además de por el firewall de aplicaciones.
12.3 Controles criptográficos		

CONTROL	EXISTE	REVISIÓN
12.3.1 Política de uso de los controles criptográficos	Si	Existe una política de gestión de claves con descripción de roles (Oficial de seguridad, custodios etc.) que se utiliza para los sistemas de firma internos. Existe respaldo de las claves debidamente custodiado.
12.3.2 Gestión de claves	Si	La gestión de claves está debidamente mantenida y registrada. Cada clave tiene un acta de clave en la que está consignado su ciclo de vida y sus custodios.
12.4 Seguridad de los archivos del sistema		
12.4.1 Control del software en producción	No	Aunque el control de software en producción si se realiza prácticamente como indica la norma, no podemos considerarlo correcto dado que no existen evidencias ni documentación al respecto.
12.4.2 Protección de los datos de prueba del sistema	Si	No se utilizan datos de producción en entornos de desarrollo
12.4.3 Control de acceso a los códigos de programas fuente	Si	El acceso está restringido mediante contraseña
12.5 Seguridad en los procedimientos de desarrollo y soporte		
12.5.1 Procedimientos de control de cambios	No	No existen procedimientos formales de cambio
12.5.2 Revisión técnica de los cambios en el sistema operativo	Si	Las actualizaciones de los sistemas se realizan en desarrollo antes que en producción para detectar problemas
12.5.3 Restricciones en los cambios a los paquetes de software	Si	No se modifican los paquetes adquiridos.
12.5.4 Fuga de información	No	No se monitoriza las actividades del personal ni el uso de recursos.
12.5.5 Desarrollo externo del	n/a	La empresa no externaliza

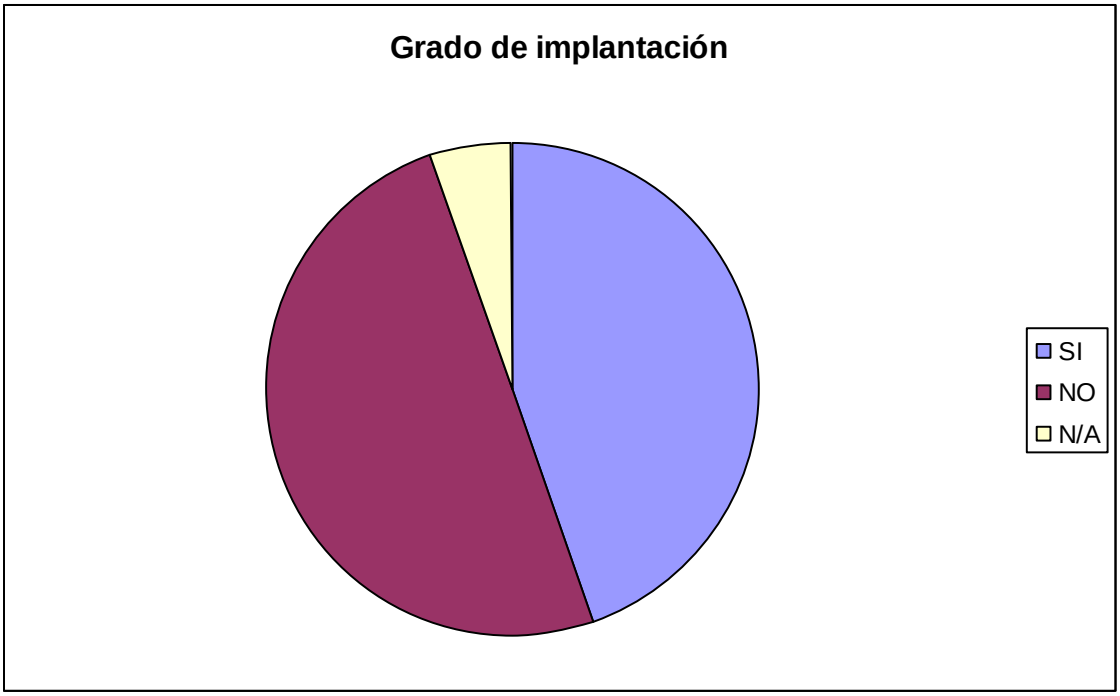
CONTROL	EXISTE	REVISIÓN
software		desarrollo
12.6 Gestión de la vulnerabilidad técnica		
12.6.1 Control de las vulnerabilidades técnicas	Si	Existe un inventario completo de los activos. Los responsables están suscritos a listas de vulnerabilidades y los parches se aplican en un plazo inferior a un mes
13. Gestión de incidentes en la seguridad de información		
13.1 Reportando eventos y debilidades de la seguridad de información		
13.1.1 Reportando los eventos en la seguridad de información	No	No existe un procedimiento formal
13.1.2 Reportando debilidades en la seguridad de información	Si	El documento de uso aceptable establece que se deben reportar faltas a su responsable directo.
13.2 Gestión de las mejoras e incidentes en la seguridad de información		
13.2.1 Responsabilidades y procedimientos	No	No existen procedimientos de mejora.
13.2.2 Aprendiendo de los incidentes en la seguridad de información	No	Los incidentes no realimentan la seguridad. Simplemente se solucionan si procede.
13.2.3 Recolección de evidencia	No	No existe un procedimiento de recolección de evidencias asociado a la gestión de incidentes.
14 Gestión de continuidad del negocio		
14.1 Aspectos de la gestión de continuidad del negocio		
14.1.1 Incluyendo la seguridad de información en el proceso de gestión de la continuidad del negocio	No	No existe un plan de continuidad del negocio

CONTROL	EXISTE	REVISIÓN
14.1.2 Continuidad del negocio y evaluación de riesgos	Si	Aunque no existe un plan de continuidad de negocio los equipos críticos si están identificados y el riesgo que supone un problema en ellos.
14.1.3 Redacción e implantación de planes de continuidad que incluyen la seguridad de información	No	No existen planes de continuidad del negocio
14.1.4 Marco de planificación para la continuidad del negocio	No	No existe un marco único para los planes de continuidad de negocio
14.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad	No	No aplican pruebas de algo que no existe.
15 Cumplimiento		
15.1 Cumplimiento de los requisitos legales		
15.1.1 Identificación de la legislación aplicable	Si	La legislación aplicable es la LOPD y ley de propiedad intelectual.
15.1.2 Derechos de propiedad intelectual	Si	El documento de uso aceptable hace referencia a restricciones en el uso de licencias y restringe el software a utilizar.
15.1.3 Salvaguarda de los registros de la organización	No	No existen salvaguardas a excepción de las que cada usuario realice a titulo personal.
15.1.4 Protección de los datos y de la privacidad de la información personal	Si	Los datos almacenados que caen bajo el ámbito de la LOPD se almacenan de acuerdo a la normativa.
15.1.5 Prevención en el mal uso de los recursos de tratamiento de la información	Si	El documento de uso aceptable informa a los empleados de que pueden y que no pueden hacer con la información
15.1.6 Regulación de los controles criptográficos	Si	Todos los sistemas criptográficos tanto hardware como software disponen de conformidad con las leyes españolas

CONTROL	EXISTE	REVISIÓN
15.2 Revisiones de la política de seguridad y de la conformidad técnica		
15.2.1 Conformidad con la política de seguridad y los estándares	No	No se realizan revisiones periódicas de cumplimiento de la política de seguridad.
15.2.2 Comprobación de la conformidad técnica	No	No se realizan comprobaciones periódicas de conformidad de los sistemas con las normas de implantación
15.3 Consideraciones sobre la auditoria de sistemas		
15.3.1 Controles de auditoria de sistemas	No	No se realizan auditorias
15.3.2 Protección de las herramientas de auditoria de sistemas	No	No se realizan auditorias

1.4 1.4 Gráfico Resumen

El siguiente gráfico muestra de una forma aproximada el grado de cumplimiento de los controles por parte de la organización en el momento actual.



2 Fase 2: Sistema de Gestión Documental

La propia ISO/IEC 27001 define cuales son los documentos necesarios para poder certificar el sistema, pero nosotros nos centraremos en los siguientes:

Política de Seguridad: incluida en el documento POLITICA DE SEGURIDAD.doc

Procedimiento de Auditorías Internas: incluida en el documento PROCEDIMIENTO DE AUDITORIAS (SEGNET).doc

Gestión de Indicadores: incluido en el documento INDICADORES.doc

Procedimiento Revisión por Dirección: incluido en el documento PROCEDIMIENTO DE REVISION.doc

Gestión de Roles y Responsabilidades: incluido en el documento POLITICA GESTION ROLES Y RESPONSABILIDADES.doc

Metodología de Análisis de Riesgos: incluido en el documento PROCEDIMIENTO DE ANALISIS DE RIESGOS.doc

Declaración de Aplicabilidad: plantilla obtenida a partir de http://www.iso27001security.com/html/iso27k_toolkit.html y nombrada en los documentos como SEGNET DDA.xls

3 Fase 3: Análisis de Riesgos

El análisis de riesgos de implantación se encuentra detallado en el documento TFM-análisis de riesgos.pdf. Extraemos la sección 8.5 de interpretación de los resultados del citado documento para que sirva de resumen de los hallazgos encontrados por el análisis:

Se puede apreciar una gran reducción en cuanto a la dimensión de la confidencialidad. Sin embargo la trazabilidad no mejora apreciablemente con las salvaguardas existentes.

También existen carencias en cuanto a los efectos que podrían tener desastres que destruyan los dispositivos. Las salvaguardas de respaldo no existen. A continuación se muestra un cuadro resumen de las amenazas que no son reducidas por salvaguardas y que hacen caer la valoración de los activos.

N.2	Daños por agua	inundaciones: posibilidad de que el agua acabe con recursos del sistema.
I.2	Daños por agua	escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
I.3	Contaminación mecánica	vibraciones, polvo, suciedad, ...
I.4	Contaminación electromagnética	interferencias de radio, campos magnéticos, luz ultravioleta, ...
I.5	Avería de origen físico o lógico	fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico pero para las consecuencias que se derivan, esta distinción no suele ser relevante.
I.6	Corte del suministro eléctrico	cese de la alimentación de potencia
I.7	Condiciones inadecuadas de temperatura y/o humedad	deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...
E.18	Destrucción de información	pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
E.24	Caída del sistema por agotamiento de recursos	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
A.7	Uso no previsto	utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
A.18	Destrucción la información	eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
A.24	Denegación de servicio	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
A.25	Robo	la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
A.26	Ataque destructivo	vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.
A.27	Ocupación enemiga	cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

El comité de seguridad deberá considerar la mejor forma de desarrollar medidas para reducir el impacto de estas amenazas.

4 Fase 4: Propuestas de Proyecto

Del análisis de riesgos realizado se desprende que la faceta principal de riesgo de los activos es la disponibilidad, aunque también existen carencias en cuanto a la integridad y la confidencialidad.

La autenticidad y la trazabilidad tienen un nivel de riesgo muy bajo y o la dirección, conociendo el dato lo considera asumible.

A continuación se detallan las amenazas que actúan sobre los activos y no son mitigadas en suficiente medida como para reducir el riesgo a unos niveles aceptables así como la determinación tomada por el comité de seguridad acerca de cómo actuar ante ellas:

ID	Descripción Breve Amenaza	Actuación
N.2	Daños por agua	Transferirlo (Seguro)
I.2	Daños por agua	Transferirlo (Seguro)
I.3	Contaminación mecánica	Reducirlo (Procedimientos)
I.4	Contaminación electromagnética	Reducirlo (Normas)
I.5	Avería de origen físico o lógico	Reducirlo (Replicación)
I.6	Corte del suministro eléctrico	Reducirlo / Evitarlo (SAI)
I.7	Condiciones inadecuadas de temperatura y/o humedad	Evitarlo (Acondicionamiento)
E.18	Destrucción de información	Reducirlo (Respaldos)
E.24	Caída del sistema por agotamiento de recursos	Reducirlo (Replicación, IDS)
A.7	Uso no previsto	Reducirlo (Host IDS)
A.18	Destrucción la información	Reducirlo (Respaldos)
A.24	Denegación de servicio	Reducirlo (Replicación, IDS)

A.25	Robo	Transferirlo (Compañía seguridad)
A.26	Ataque destructivo	Reducirlo (Respaldo, IDS)
A.27	Ocupación enemiga	Transferirlo (Compañía seguridad)

Dentro de estas amenazas se pueden identificar 2 grupos distintos de amenazas. Por una parte tenemos amenazas que tienen que ver con las instalaciones y como están preparadas las mismas para responder ante las amenazas (Daños, Robo, Suministros…) y por otra parte tenemos amenazas que atacan la disponibilidad por agotamiento de los servicios.

Con el fin de mitigar estas amenazas se han identificado una serie de actuaciones encaminadas a crear las salvaguardas necesarias para reducir estos riesgos.

- Estudio contratación seguro (P1)
- Creación procedimiento de copias de seguridad (P1)
- Creación procedimiento de acceso a Datacenter, que contemple restricciones acerca de emisiones de dispositivos, materiales, limpieza… (P1)
- Contratación servicio de “acuda” con el proveedor de seguridad física (alarma). (P1)
- Instalación IDS en intranet. (P2)
- Instalación Aire Acondicionado. (P2)
- Instalación de SAI a equipos críticos (P2)
- Instalación Host IDS en equipos críticos. (P3)
- Replicación virtualizada de sistemas críticos. (P3)

Todas estas tareas se agruparán en 3 proyectos internos:

- (P1) Adecuación normativa. Procedimientos y Contrataciones.
- (P2) Adecuación física de Datacenter
- (P3) Adecuación lógica de la Intranet y Virtualizaciones

Los proyectos P2 y P3 serán responsabilidad de la dirección de IT (esantos) y P1 será responsabilidad de la dirección de la empresa (igarcia). Existe una dependencia lógica de los proyectos P2 y P3 de P1. Una vez finalizado P1 comenzarán los otros dos proyectos.

Según el procedimiento de auditorias de la empresa, el plazo de ejecución de los proyectos será hasta 2 meses como máximo. Teniendo en cuenta los periodos vacacionales próximos se fija una fecha límite de ejecución del día 15 de Febrero de 2014.

4.1 (P1) Adecuación normativa. Procedimientos y Contrataciones.

Responsable del proyecto: Igarcia

Objetivo del proyecto: Actualizar las políticas y procedimientos de SEGNET para reducir los riesgos de la empresa y realizar las contrataciones y/o acuerdos con terceros para transferir el riesgo sobre los activos.

Prioridad: Urgente

Recursos: igarcia (toma de decisiones), fparis (director de seguridad)

Plazo de ejecución estimado: 1 semana

Presupuesto: 2.000€ + 2 recursos al 50%

Tarea	Asignada	Amenaza
Solicitud ofertas seguro	igarcia	
Valoración ofertas seguro	Igarcia	
Contratación seguro	igarcia	N.2, I.2 (Transferida) 50%
Creación política de copias de seguridad	fparis	
Creación procedimiento de copias de seguridad	fparis	E.18, E.24, A.18, A.24 (Reducida) 80%
Solicitud de servicio de “acuda” a la compañía de seguridad	igarcia	A.25, A.27 (Transferido) 50%
Creación procedimiento de acceso a Datacenter	fparis	I.3, I.4 (Reducida) 60%

4.2 (P2) Adecuación física del Datacenter.

Responsable del proyecto: Esantos

Objetivo del proyecto: Adecuar el datacenter para incrementar sus salvaguardas a la hora de mitigar en la medida de lo posible los riesgos para los activos allí contenidos.

Prioridad: Urgente (Depende de P1)

Recursos: igarcia (compras), aegido (IT), esantos (IT)

Plazo de ejecución estimado: 8 semanas

Presupuesto: 10.000€ + 3 recursos al 50%

Tarea	Asignada	Amenaza
Solicitud ofertas AA (2 equipos)	igarcia	
Valoración ofertas AA	igarcia	
Instalación AA	Externo	I.7 (Reducida) 100%
Solicitud ofertas SAI	esantos	
Valoración ofertas SAI	esantos	
Adquisición e instalación SAI	Esantos, aegido	I.6 (Reducido) 100% (1/2 hora. El resto se asume)
Selección de equipos IDS	aegido	
Instalación sistema, instalación	aegido	

SNORT		
Pruebas locales y de aceptación	Aegido, esantos	
Puesta en producción	esantos	E.24, A.12, A.24, A.26 (Reducido) 50%

4.3 (P3) Adecuación lógica de la Intranet y Virtualizaciones.

Responsable del proyecto: Esantos

Objetivo del proyecto: Adecuar el infraestructura lógica para incrementar sus salvaguardas y su resistencia ante las amenazas identificadas.

Prioridad: Urgente (Depende de P1)

Recursos: igarcia (compras), aegido (IT), esantos (IT)

Plazo de ejecución estimado: 8 semanas

Presupuesto: 0€ + 3 recursos al 50%

Tarea	Asignada	Amenaza
Instalación y configuración shamhain (Host IDS)	aegido	E.18, E.24, A.6, A.7, A.18, A.24, A.26 (Reducida) 50%
Obtención de imágenes de los sistemas instalados	aegido	
Creación de maquinas virtuales basadas en las imágenes obtenidas	Aegido	
Configuración y puesta en marcha de la configuración de alta disponibilidad	aegido	(Reducida en todos los casos)N.2, I.2 (25%), I.3,I.4, E.18, A.18, A.26 (50%) I.5, E.24, A.24 (100%)

4.4 Efecto de las nuevas salvaguardas sobre el riesgo

Una vez aplicadas estas salvaguardas el nivel de riesgo quedaría como se muestra en la siguiente tabla:

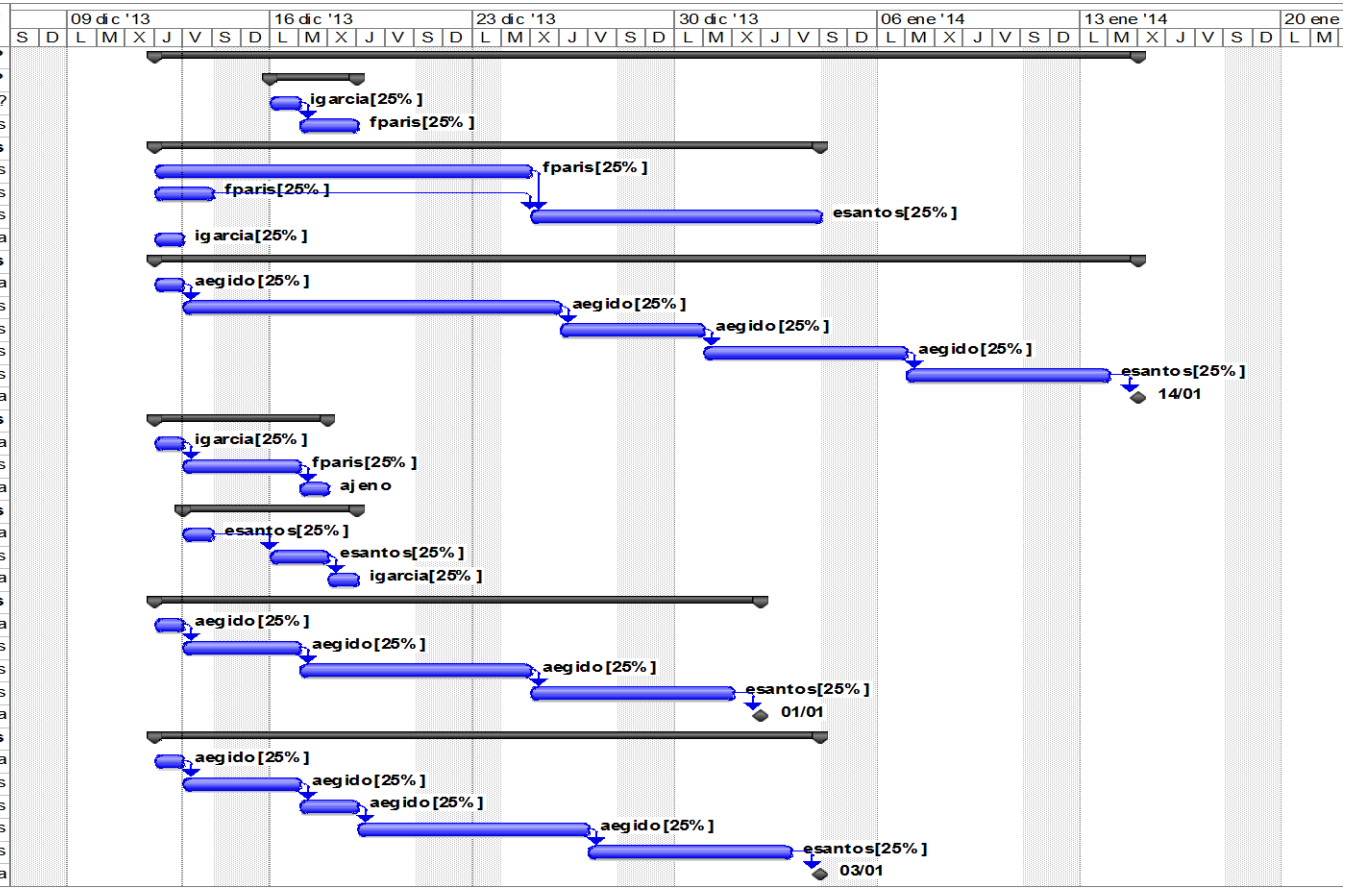
Activos		Riesgo residual						
Codigo	Nombre	D	I	C	A_S	A_D	T_S	T_D
SN_S01	S_Repo	2	0	4	4	0	0	0
SN_S02	S_Inventario	2	0	4	4	0	0	0
SN_S03	S_Monitor	2	0	4	4	0	0	0
SN_S04	S_Email	2	0	4	4	0	0	0
SN_S05	S_Telefono	2	0	4	4	0	0	0
SN_S06	S_VPN	2	0	4	4	0	0	0
SN_D01	D_Code	2	4	1	0	0	0	0
SN_D02	D_Correos	2	4	1	0	0	0	0
SN_D03	D_Inventario	2	4	1	0	0	0	0
SN_D04	D_Monitor	2	4	1	0	0	0	0
SN_D05	D_Conf_Asterisk	2	4	1	0	0	0	0
SN_D06	D_Conf_VPN	2	4	1	0	0	0	0
SN_SW01	SW_CVS	7	6	5	2	0	0	0
SN_SW02	SW_Zimbra	7	6	5	2	0	0	0
SN_SW03	SW_GLPI	7	6	5	2	0	0	0
SN_SW04	SW_Nagios	7	6	5	2	0	0	0
SN_SW05	SW_Asterisk	7	6	5	2	0	0	0
SN_HW01	HW_Server1	6	3	4	2	0	0	0
SN_HW02	HW_Server2	6	3	4	2	0	0	0
SN_HW03	HW_Server3	6	3	4	2	0	0	0
SN_HW04	HW_Server4	6	3	4	2	0	0	0
SN_HW05	HW_Server5	6	3	4	2	0	0	0
SN_HW06	HW_FwlVPN	6	3	4	2	0	0	0
SN_HW07	HW_GwRDSI	7	6	5	4	0	0	0
SN_COM01	COM_Internet	6	4	4	4	0	0	0
SN_COM02	COM_VPN_Cli	6	4	4	4	0	0	0
SN_COM03	COM_Lan	6	4	4	4	0	0	0
SN_COM04	COM_RDSI	6	4	4	4	0	0	0
SN_L01	L_Datacenter	6	1	4	0	0	0	0

Se ve que hay margen de mejora para el futuro, pero los niveles de riesgo quedan dentro de los límites aceptados por la dirección.

4.5 Diagrama GANTT

El siguiente diagrama muestra el desglose de tareas de los distintos proyectos así como su progresión planificada en el tiempo y su responsable asignado.

Id	Nombre de tarea	Duración
1	**Inicio de proyectos**	**23 días?**
2	**Contratación seguro**	**3 días?**
3	Solicitud de propuestas	1 día?
4	Estudio de propuestas	2 días
5	**Creación procedimiento de copias de seguridad**	**16 días**
6	Identificación de datos a respaldar	8 días
7	Especificación del procedimiento	2 días
8	Implantación del procedimiento	8 días
9	Contratación servicio de "acuda" con el proveedor de se	1 día
10	**Instalación IDS en intranet**	**23 días**
11	Selección de equipos	1 día
12	Instalación sistema base y hardening	8 días
13	Instalación SNORT y configuración	3 días
14	Pruebas locales	5 días
15	Pruebas de aceptacion	5 días
16	Puesta en producción	1 día
17	**Instalación Aire Acondicionado**	**4 días**
18	Solicitud de propuestas	1 día
19	Estudio de propuestas	2 días
20	Instalación	1 día
21	**Instalación de Sistema de Alimentación Ininterrum**	**4 días**
22	Solicitud de propuestas	1 día
23	Estudio de propuestas	2 días
24	Adquisición	1 día
25	**Instalación Host IDS en equipos criticos**	**14 días**
26	Selección de equipos	1 día
27	Instalación Samhain y configuración	2 días
28	Pruebas locales	5 días
29	Pruebas de aceptacion	5 días
30	Puesta en producción	1 día
31	**Replicación virtualizada de sistemas criticos**	**16 días**
32	Selección de equipo HOST	1 día
33	Obtención de imagen del sistema origen	2 días
34	Obtención de imagen virtual del sistema origen	2 días
35	Pruebas locales	5 días
36	Pruebas de aceptacion	5 días
37	Puesta en producción	1 día



5 Fase 5: Auditoria de Cumplimiento

5.1 Metodología

En esta fase comprobaremos el grado de cumplimiento del estándar ISO 27002:2005 por parte de nuestra organización.

El estándar agrupa un total de 133 controles o salvaguardas sobre buenas prácticas para la gestión de la seguridad de la información, organizado en 11 áreas y 39 objetivos de control.

A continuación enumeraremos el grado de cumplimiento de cada uno de esos controles por parte de SEGNET.

Para la valoración se ha utilizado el criterio expuesto en la siguiente tabla:

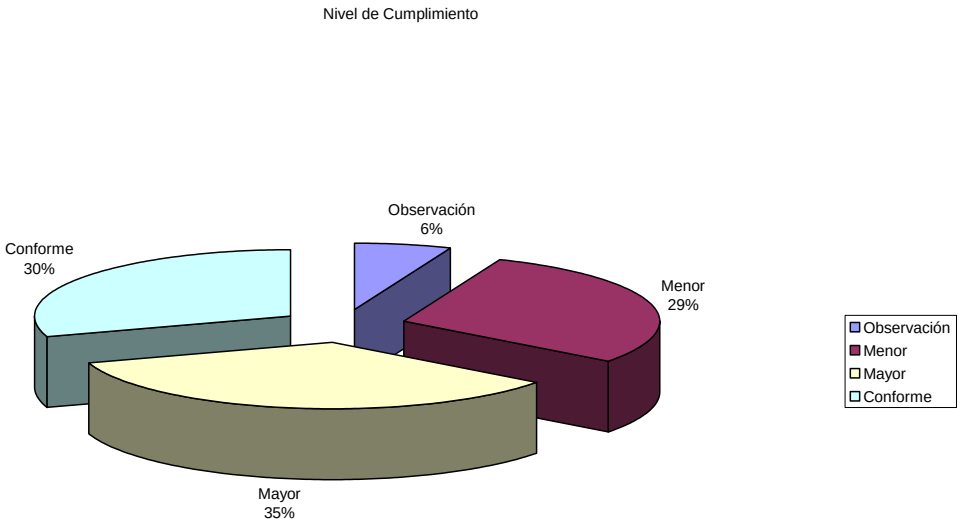
Valor	CMM	Descripción
100%	**L5**	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.
95%	**L4**	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
90%	**L3**	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
50%	**L2**	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
10%	**L1**	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
0%	**L0**	Carencia completa de cualquier proceso reconocible.
N/A	**N/A**	No aplica

5.2 Resumen de cumplimiento

La siguiente tabla muestra un resumen de los controles y de su cumplimiento.

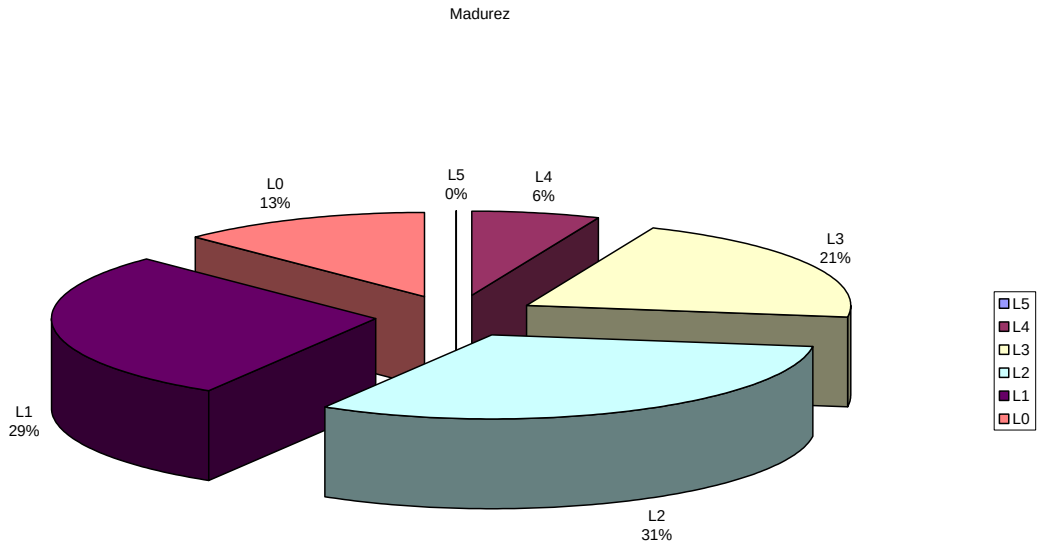
Cuenta	Etiqueta	Descripción
8	**Observación**	El control no está implementado. Se debe valorar cuando implementarlo
39	**Menor**	El control no está implementado y debe implementarse a medio plazo
46	**Mayor**	El control no está implementado y debe implementarse urgentemente
40	**Conforme**	El control está implementado
133	Total	

A continuación se muestran los resultados de una forma gráfica:



5.3 Gráfico de distribución del cumplimiento

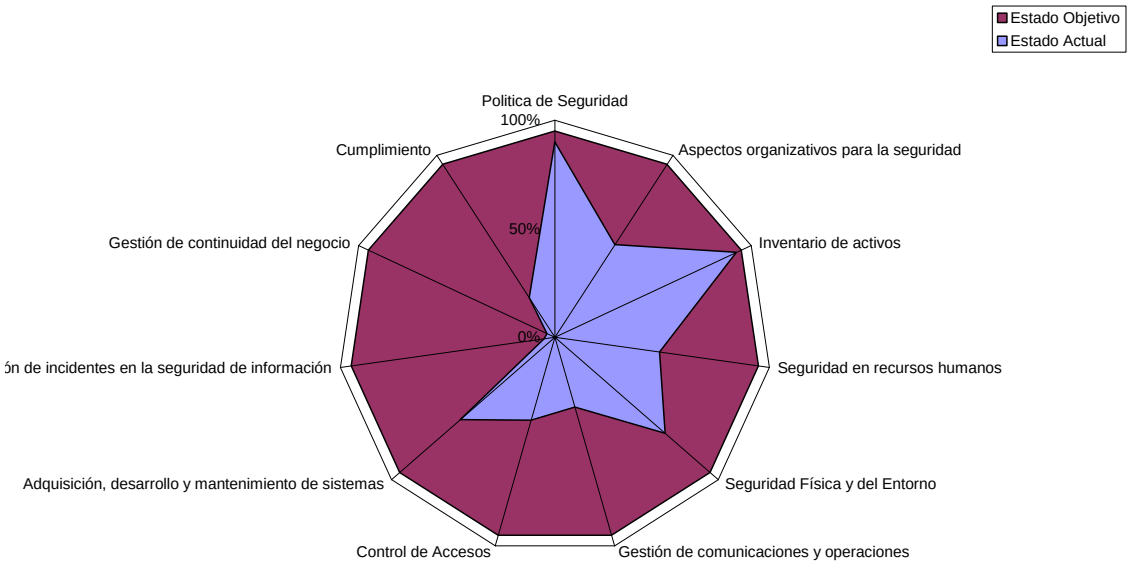
El siguiente gráfico muestra la distribución del cumplimiento.



Si consideramos L3 / L4 como el nivel objetivo y L2 como un nivel asumible aunque claramente mejorable vemos que existen grandes debilidades (un 42% de controles en L0 o L1) y una gran oportunidad de mejora (un 73% de controles mejorables en L0, L1 y L2).

5.4 Oportunidad de Mejora por Área

En el siguiente gráfico se puede observar mejor la oportunidad de mejora por área:



La zona rosa nos muestra nuestro objetivo y la zona morada nuestro estado actual. Se ven claramente las carencias en gestión de incidentes, continuidad de negocio y cumplimiento y el mejor estado aunque mejorable en seguridad física, aspectos organizativos, desarrollos y mantenimiento.

6 Fase 6: Presentación de Resultados y Entrega de Informes

En esta fase elaboramos una presentación para la dirección, mostrando el camino que hemos seguido y las actuaciones que hemos llevado a cabo. Se trata de una presentación con orador, por lo que dispone de notas en las diapositivas que no son auto explicativas. El fichero se puede encontrar junto con la documentación con el nombre Presentación Direccion.pps (para poder ver las notas hay que renombrarlo con la extensión ppt)

También elaboramos un video de presentación de todo el trabajo.

7 Anexo A. Acrónimos y Definiciones

HOST IDS. Sistema de Detección de Intrusiones para equipos. Sistema que detecta accesos o alteraciones en sistemas.

IDS. Sistema de Detección de Intrusiones. Sistema que detecta accesos no autorizados a redes.

LOPD. Ley Orgánica de Protección de Datos.

MOTD. Mensaje del Día. Cabecera que se muestra a los usuarios después de conectarse a un equipo.

NAGIOS. Sistema de monitorización de equipos, servicios y redes.

PCI DSS. Payment Card Industry Data Security Standard. Normas de seguridad de la información del Payment Card Industry Council.

SAI. Sistema de Alimentación Interrumpida.

SSH. Protocolo de acceso remoto a equipos de forma segura.

VPN. Red Privada Virtual

8 Anexo B. Referencias

Ref 1. NTC ISO/IEC 27001 – Norma Técnica Colombiana. Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la seguridad de la información. Requisitos.

Ref 2. NTP-ISO/IEC 17799 – EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información.

Ref 3. IRAM-ISO/IEC 27004 – Gestión de la seguridad de la información – Medición

Ref 4. www.iso27001security.com. Recursos para la gestión e implantación de la norma ISO 27001.