Este trabajo tiene como objetivo la elaboración de un plan de implementación de la ISO/IEC 27001:2005. Este plan incluirá desde el análisis de la situación actual hasta el informe de cumplimiento de la auditoría de la norma.

Plan de implementación de la ISO/IEC 27001:2005

MISTIC – Máster interuniversitario en la Seguridad de las TIC.

Juan Pablo Nieto Muñoz
Tutor: Arsenio Tortajada Gallego

Control de versiones.

Fecha	Versión	Autor	Revisión
11/MAR/13	0.1	JPNietoMuñoz	Inicio del documento.
15/MAR/13	1.0	JPNietoMuñoz	Fase1 completada.
20/MAR/13	2.0	JPNietoMuñoz	Fase2 inclusión.
28/MAR/13	2.1	JPNietoMuñoz	Fase2 completada.
04/ABR/13	2.2	JPNietoMuñoz	Fase1 Revisión.
08/ABR/13	3.0	JPNietoMuñoz	Fase3 inclusión.
19/ABR/13	3.1	JPNietoMuñoz	Fase3 completada
25/ABR/13	3.2	JPNietoMuñoz	Fase4 inclusión.
09/MAY/13	3.3	JPNietoMuñoz	Fase4 completada.
14/MAY/13	4.0	JPNietoMuñoz	Fase5 inclusión.
24/MAY/13	4.1	JPNietoMuñoz	Fase5 completada.
03/JUN/13	5.0	JPNietoMuñoz	Fase6 inclusión.
06/JUN/13	6.0	JPNietoMuñoz	Fase6 completada

Índice

Capítulo 1.

Situación actual: Contextualización, objetivos y análisis diferencial

1.1.- Introducción al proyecto.

La información gira en torno a nuestras vidas y al desarrollo de las organizaciones, ambos necesitamos la información para ser competitivos, lograr objetivos, obtener ventajas y para simplemente continuar con la actividad diaria. La información es imprescindible en la sociedad en la que nos encontramos, en el siglo XXI el concepto ha cambiado y actualmente podemos hablar de la sociedad de la información. Como es evidente la concepción de empresa también se ha transformado, nos encontramos en un mercado globalizado donde las telecomunicaciones son muy importantes, las transacciones y el comercio electrónico han crecido considerablemente, lo que ha supuesto que muchas empresas se conciencien incluyendo el manejo de la tecnología de la información (TI) en sus programas directivos.

"La información es un activo que, como otros activos importantes de la empresa, es esencial para las operaciones de la organización, y en consecuencia necesita ser adecuadamente protegida". *ISO 27002:2005.*

La información se presenta en una organización en distintos medios (papel, almacenada electrónicamente, trasmitida, etc.) y tiene importantes propiedades que se deben mantener: disponibilidad, integridad y confidencialidad.

Es evidente que las organizaciones se enfrentan a amenazas (internas y externas) y vulnerabilidades como por ejemplo: espionaje, sabotaje, vandalismo, incendios, etc.; por todo ello aparece la necesidad de la seguridad de la información, área que nos permitirá protegerla adecuadamente para que nuestra organización pueda mantener su competitividad, rentabilidad y en general su existencia en la sociedad. Si la seguridad de la información fallara o no se aplicara correctamente podríamos tener distintos impactos en nuestra organización, como por ejemplo: pérdidas financieras, denuncias de las autoridades, pérdidas de clientes, pérdida de cuota de mercado, interrupción de las operaciones, daño en la imagen, etc.

Una las normas internacionalmente aceptadas para llevar a cabo nuestro objetivo es ISO/IEC 27000: conjunto de normas y estándares que proporcionan un marco de gestión de la seguridad de la información aplicable a cualquier organización. Por ello consideramos importante el estudio y análisis de la norma para poder aplicarla correctamente en las

organizaciones que gestionemos, sin lugar a dudas la aplicación de la misma en la organización mejorará su competitividad, imagen y seguridad.

Las organizaciones públicas y privadas se están concienciando de la necesidad de la seguridad de la información, las normas ISO/IEC 27000 nos proporcionan una excepcional guía de procesos y controles que nos ayudarán a asegurar la información de nuestra organización.

Actualmente en España las normas ISO/IEC 27000 no son de obligada aplicación en todos los sectores pero nos proporcionan un sello diferenciador frente a otras organizaciones. La certificación de ISO/IEC 27000 demuestra al cliente y al proveedor que la organización lleva a cabo una correcta gestión de la seguridad de la información y que sin lugar a dudas la calidad está presente en la gestión de TI.

Durante la crisis económica que estamos experimentando a nivel mundial, las organizaciones buscan reducir los costes y producir un producto de mayor calidad para mantenerse en el mercado; y los clientes un producto más barato y de mayor calidad. Aunque parezca mentira las normas ISO/IEC 27000 pueden ayudar a las organizaciones a conseguir este objetivo, reduciendo sus costes, mejorando la calidad y haciendo de sus servicios y/o productos marcas diferenciadoras frente a la competencia.

En conclusión, las organizaciones públicas y privadas, grandes y pequeñas necesitan adaptarse a los tiempos reduciendo sus gastos y mejorando la calidad para sobrevivir a la competencia y para ello buscarán profesionales que les ayuden a asegurar uno de sus activos más importantes: la información. El mercado debe estar preparado para estas nuevas necesidades y requiere profesionales formados para guiarles en la nueva etapa. Mejorando la calidad y seguridad de nuestra organización nos hace más competitivos como empresa y como país en este planeta globalizado.

La buena gestión de los sistemas de información es el camino al éxito de una empresa.

1.2.- Objetivos del proyecto.

El objetivo es elaborar un plan de implementación de la ISO/IEC 27001:2005 en la organización seleccionada. El proyecto establecerá las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información) y por lo tanto deberá abordar las siguientes fases:

- Documentación normativa sobre las mejores prácticas en la seguridad de la información.
- Definición clara de la situación actual y de los objetivos del SGSI.
- Análisis de riesgos.

- Identificación y valoración de los activos corporativos como punto de partida a un análisis de riesgos.
- Identificación de amenazas, evaluación y clasificación.

- Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2005 a una organización.
- Propuestas de proyectos para conseguir una gestión de la seguridad óptima.
- Esquema documental.

Como entregables del proyecto se presentarán los siguientes productos:

- Informe del análisis diferencial.
- Esquema documental ISO/IEC 27001.
- Análisis de riesgos.
- Plan de proyectos.
- Auditoría de cumplimiento.
- Presentación de resultados.

1.3.- Enfoque y selección de la empresa.

1.3.1.- Descripción actual de la empresa.

La organización en cuestión es una mediana empresa privada, anónima, dedicada la investigación y desarrollo de recursos tecnológicos así como ofrecer servicios informáticos y telemáticos a empresas del sector turismo. Esta organización a día de hoy tiene aproximadamente 100 trabajadores y cuenta con una cartera de más de 50 clientes de envergadura, todos ellos empresas (no ofrecen servicios a personas físicas).

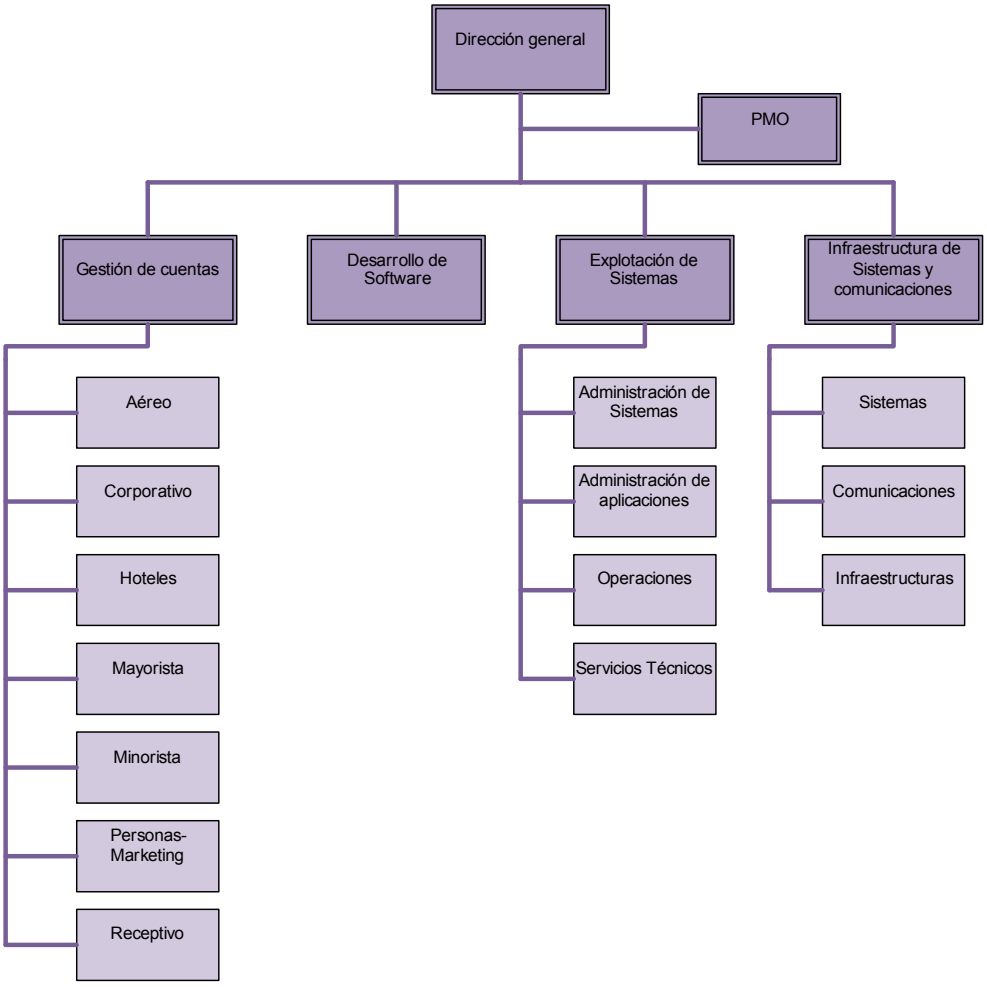
La empresa está ubicada en un polígono tecnológico de Palma de Mallorca (Illes Balears), en la misma sede podemos encontrar las oficinas y el centro de procesamiento de datos (CPD). La gran parte de los servicios (85%) que ofrece a los clientes están hosteados en el CPD de su propiedad.

La empresa tiene conocimientos sobre las buenas prácticas de la gestión de la información, controles ya implementados y la intención de mejora en su sistema de gestión de la seguridad de la información. Hasta ahora ha utilizado guías de buenas prácticas como COBIT e ITIL pero no ha llegado a implementarlas por completo.

Durante los tres últimos años ha obtenido ganancias y quieren aprovechar la situación actual para mejorar su gestión interna y optimizar los costes. Asimismo desean ampliar su cartera de clientes e incorporar nuevos servicios y productos a su catálogo (por ejemplo: desarrollos en plataformas móviles, servicios de marketing online, incentivar el I+D sector turismo, etc.)

1.3.1.- Organigrama.

En este apartado incluimos el organigrama de la empresa.



Las funciones de cada área son las siguientes:

- Dirección general: Establece la estratégica corporativa y junto con los responsables de área gestiona la organización. Preside las reuniones del consejo de administración y toma las decisiones estratégicas. Está compuesta de (1) Director General y (1) Secretaria Dirección.

- PMO: Es un área transversal a todos los departamentos que, siguiendo las directrices estratégicas del Director General establece los procesos, metodologías, procedimientos y

normas necesarias para gestionar operativamente los servicios de la empresa (gestión de proyectos, incidencias, cambios, contratación, facturación, etc.) basándose en las decisiones establecidas por los departamentos específicos. Proporciona un importante apoyo a la dirección consolidando la información directiva y estableciendo el Know-How de la organización. Está compuesto por (1) Manager y (1) Consultor. Esta área incluye las funciones de gestión de la calidad y seguridad de la empresa aunque la organización y funciones no están formalmente establecidas.

- Gestión de cuentas: Este equipo está compuesto por gestores de cuenta (Account Manager), que se encargan de gestionar la demanda y servicios de los clientes. Tienen conocimiento de la tecnología que desarrollamos en la organización y los procesos de negocio del área correspondiente. Existe un Gestor de Cuenta por área de negocio, en total (7) Account Managers y (1) Director Comercial.

- Desarrollo de Software: Es el departamento encargado de desarrollar productos de software (gestión de proyectos) y entregarlos para su puesta en producción. Está compuesto por 5 grandes áreas: Java, .NET, SAP, Business Inteligence e Integraciones, y contienen 4 perfiles, Jefe de Proyectos, Arquitectos, Analistas y Programadores. En total está compuesto por (65) empleados: (1) Director Desarrollo, (15) Jefes de Proyectos, (3) Arquitectos, (15) Analistas y (30) Programadores.

- Explotación de Sistemas: Esta área se encarga de mantener en producción los sistemas previamente desarrollados. Entre sus funciones se incluye la implementación de mejoras menores que no requieran el desarrollo de un proyecto (inferior a 1 semana de trabajo de un FTE). Está organizado en cuatro secciones (34 empleados + 1 Director):

    - Administración de Sistemas y comunicaciones: (5) Administradores de Sistemas y (1) Coordinador de equipo.

    - Administración de Aplicaciones: (10) Técnicos de Soporte AM y (1) Coordinador de equipo.

    - Operaciones: (5) Operadores de Sistemas y (1) Coordinador de equipo.

    - Servicios Técnicos: (5) Técnicos de Sistemas y (1) Coordinador de equipo.

- Infraestructura, Sistemas y Comunicaciones: Este departamento es el encargado de desarrollar e implementar los proyectos relacionados con Infraestructuras, Sistemas y Comunicaciones. El equipo está compuesto por (3) Jefes de Proyectos y (1) Responsable de equipo.

- Servicios Generales: El departamento de servicios centrales es el equipo que se encarga de los procesos “administrativos” de la organización, está compuesto por cuatro equipos:

- RRHH: (1) Responsable RRHH y (1) Técnico RRHH

- Legal: (1) Responsable Legal y (1) Técnico Legal

- Administración: (1) Responsable Administración, (1) Responsable Fiscal, (1) Administrativo y (1) Técnico Fiscal.

1.3.2.- Valores de la organización.

La empresa tiene como objeto principal proporcionar valor a organizaciones, cuya principal actividad es el turismo, a través de la tecnología de la información. El valor central: "Escuchar las necesidades del cliente y proporcionar innovación para solucionarlas. Nuestra organización conoce el negocio del turismo y nos consideramos parte de él."

Aunque la empresa se dedica a desarrollar productos tecnológicos se considera "una empresa del sector turismo". Las líneas principales de trabajo se orientan a las siguientes áreas:

- Desarrollo de software.
- Proyectos de Sistemas y Comunicaciones.
- Servicios TI (Hosting, API, Servicios Reservas, etc.)
- I+D Turismo.

1.3.3.- Activos de la organización.

La empresa tiene su sede ubicada en un polígono tecnológico de Palma de Mallorca (Illes Balears), en la misma sede podemos encontrar las oficinas y el centro de procesamiento de datos (CPD). La oficina cuenta con 2 plantas de 500 mts cuadrados dividas en dos partes iguales de Oficinas y CPD. En la [Primera Planta Oficina] encontramos las áreas de servicios generales y dirección; [Primera Planta CPD] se ubican los AACC, generadores alternativos y SAIs. En la [Segunda Planta Oficina] están situados responsables y los equipos de TI; [Segunda Planta CPD] podemos encontrar servidores y dispositivos de red del CPD.

Las oficinas cuentan con accesos restringidos mediante tarjeta y circuito cerrado de televisión. Todos los despachos tienen puerta con llave y los puestos de trabajo poseen cajoneras protegidas con cerradura.

Las oficinas no son de propiedad, se paga alquiler mensual más gastos.

Capital humano.

Grupo	Descripción	Unidades
Empleados	Directores	4
	Secretarias	1
	Responsables	6
	Coordinadores	4
	Gestores de cuenta	7
	Consultores	1
	Jefes de Proyecto	18
	Arquitectos	3
	Analistas	15
	Programadores	30
	Administradores de sistemas	5
	Técnicos de Sistemas	5
	Técnicos de Aplicaciones	10
	Operadores	5
	Técnicos SSGG	3
	Total	117

Hardware.

Grupo	Tipo	Descripción	Unidades
Hardware	Equipos Oficinas	Portátiles Dirección-Responsables	10
		Portátiles Comerciales	8
		Tabletas 10" Dirección	4
		Equipos Desarrollo	66
		Equipos Sistemas	25
		Equipos Ofimática	9
		Equipos (Repuesto)	3
		Portátiles (Repuesto)	1
	Impresoras Oficinas	Impresora Laser B/N Oficina	4
		Impresora Laser Color Oficina	2
		Impresora Multifunción Oficina	2
		Impresora Multifuncion Despachos	5
	Dispositivos Red	Switches C3 Distribución Oficinas	10
		Switches C3 Distribución CPD	10
		Switches C6 Core CPD	2
		Routers CPD	5
		Firewalls	4

	Servidores	Servidores de correo	2
		Servidores Firewall	2
		Servidores Web Presentación	10
		Servidores Web API	10
		Servidores BackOffice	5
		Servidores BBDD	5
		Servidores Backup	2
		Servidores CMS	4
		Servidores Archivos	2
		Servidores Aplicación	5
		Servidores Gestión Proyectos	2
		Servidores SAP	2
		Servidores Desarrollo Test	5
		Servidores Desarrollo Pre-Producción	5
		Servidores control ambiental	1
	Cabinas Almacenamiento	Cabinas Almacenamiento (Profesionales)	2
		Cabinas Almacenamiento (Pyme)	2

Infraestructura técnica.

Grupo	Tipo	Descripción	Unidades
Infraestructura	CPD	SAI	2
		Generadores eléctricos	2
		AACC Industriales	4
		Cámaras vigilancia	16
		Sensores ambientales	8
		Armarios comunicaciones	6
		Armarios	12

Licencias.

Grupo	Tipo	Descripción	Unidades
Software	Servidores	MS Windows 2003-2008-2012	40
		MS Exchange 2010	2
		MS TMG	2
		MS TFS	2
		HP Dataprotector Backup	2
		SAP	2
		Oracle SGBD	5

		Redhat SO	10
		Meta4	1
	Estaciones de trabajo	MS Office 2010	10
		MS Visio 2010	2
		MS Project 2012	4
		MS Visual Studio 2010	10
		Adobe Photoshop	2
		SAP	7

Código fuente.

Grupo	Tipo	Descripción	Líneas código	Observaciones
Código fuente	Aplicaciones	FrontOfficeVenta	1000000 líneas	Venta Minorista
		BackOfficeVenta	2000000 líneas	Procesos gestión Minorista
		API-Reservas	750000 líneas	API Reservas
		OTA-Reservas	500000 líneas	OTA Reservas
		CamasHotel	500000 líneas	Banco Camas Hotel
		RecepTur	500000 líneas	Gestión Receptiva
		AirjetConecta	350000 líneas	Motor Venta Aéreo
		GestHoteles	450000 líneas	Gestión Hotelera
		ReserMay	3000000 líneas	Venta Mayorista

Información / Otros.

Grupo	Tipo	Descripción
Información	TI	Contratos TIC
	Comercial	Contratos mayoristas
		Contratos empresas
		BD clientes minoristas
		BD clientes mayoristas
		BD clientes empresa
		Ofertas
	SSGG	Contratos servicios
		Contabilidad
		Finanzas
	Dirección	Plan estratégico 2015
Otros	Mercado	Capacidad de Servicios
		Imagen
		Know How
	Vehículos	Coche clase C

1.4.- Definición de los objetivos: Análisis diferencial ISO/IEC 27001-27002 y Plan Director de Seguridad.

El objetivo principal del trabajo de fin de máster consiste en el análisis de madurez de una empresa, de tamaño mediano, para la implantación de la ISO/IEC 27001:2005 y la elaboración del Plan Director de Seguridad.

Para llevar a cabo este objetivo, se realizará una auditoría superficial de los sistemas de gestión de la seguridad de la información (SGSI) de la entidad comparándolo con los controles establecidos en la norma ISO/IEC 27002:2005 y un análisis de la documentación relacionada. Estas tareas generarán como resultado un chequeo del cumplimiento de la norma y un análisis diferencial GAP.

Esta tarea evaluará el grado de cumplimiento y madurez de su sistema de gestión de la seguridad de la información (SGSI) respecto a la norma ISO/IEC 27001. Su resultado será un indicativo de las áreas a mejorar y una entrada para la elaboración del Plan Director de Seguridad y la implantación del SGSI.

Para realizar el análisis del estado de madurez de la organización respecto ISO/IEC 27001:2005 necesitaremos que la dirección sea completamente sincera respecto a las cuestiones planteadas y que el auditor, en este caso el autor del presente trabajo, tenga acceso a toda la documentación, sistemas y dispositivos de la organización que requiera para poder contrastar mediante pruebas el análisis realizado.

El análisis del estado de la organización se realizará: examinando el cumplimiento de los controles ISO/IEC 27002:2005 y mediante un análisis diferencial GAP de ISO/IEC 27002:2005, será de ayuda en el caso de un proyecto de mejora continua o implantación de ISO/IEC 27000. Finalmente se realizará verificación de un listado de la documentación presente y ausente en la entidad respecto al cumplimiento de la norma ISO/IEC 27001:2005.

Hemos seleccionado el análisis diferencial GAP como herramienta principal del análisis de madurez de una organización respecto a ISO/IEC 27001:2005 porque se realiza en poco tiempo, detecta las áreas de carencia evidentes, permite identificar las acciones de mejora sin esperar al análisis de riesgos y finalmente permite conocer el nivel de madurez de la organización respecto los controles. Para ello se analizan las áreas donde se puede valorar la madurez de la seguridad de la información y se establece una escala de puntuación, del 0 al 5, respecto la madurez del control.

Las áreas analizadas y la identificación de las escalas se pueden encontrar en el Anexo A Áreas e identificación de escalas en el Análisis diferencial.

Como resultado del análisis del estado actual se obtendrá un informe con las evidencias obtenidas, las recomendaciones realizadas, la madurez por área y el porcentaje de

implementación por control. Este informe servirá a la organización para evaluar su estado de madurez control por control y como guía de mejora, mediante las recomendaciones, para la implementación de la ISO/IEC 27001:2005.

En el Anexo B Análisis diferencial ISO 27002 podemos encontrar el resultado del análisis realizado mediante un informe en forma de tabla.

Plan Director de Seguridad.

El Plan Director de Seguridad tiene como objetivo identificar los proyectos que deben desarrollarse por la organización a corto, medio y largo plazo para garantizar una adecuada gestión de la seguridad de la información y evitar incidentes de seguridad.

El Plan Director de Seguridad debe elaborarse después del análisis de diferencial (GAP) de la norma de referencia, en nuestro caso ISO/IEC 27001:2005, y contrastándolo con el análisis de riesgos de la empresa. Este plan se basará en la estrategia del negocio y en sus necesidades específicas, los procesos y los activos de la organización son fundamentales durante la elaboración de este plan ya que marcarán las prioridades del mismo.

En el desarrollo del Plan Director de Seguridad deben considerarse los aspectos humanos, organizativos, procedimentales y técnicos asociados con los sistemas de información. Para ello, en este trabajo nos basaremos en la norma ISO/IEC 27001:2005 así como en otras normativas aplicables a nuestro negocio.

En el Plan Director de Seguridad se debe establecer un plan de proyectos a corto, medio y largo plazo así como identificar los proyectos *Quick Wins* (proyectos que requieren escasa inversión pero que suponen una mejora significativa en la seguridad de SI). Cada uno de los proyectos debe describir las medidas/tareas a realizar así como la prioridad, fechas, recursos y costes asociados; de esta manera se facilitará la implantación por parte de la empresa.

1.5.- Análisis diferencial de la empresa.

1.5.1.- Análisis diferencial detallado.

5			**POLÍTICA DE SEGURIDAD**				
5	**1**		**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**				
5	1	1	Documento de política de seguridad de la información	SEGURIDAD	Existen normativas específicas respecto al uso de los recursos de información así como procedimientos documentados sobre las arquitecturas y sistemas pero no una Política General de Seguridad (todas unidas tampoco la forman). La Dirección de la organización no es consciente de ella y por ello no la ha aprobado.	0-Inexistente	No cumple
5	1	2	Revisión de la política de seguridad de la información	SEGURIDAD	No existe Política de Seguridad, tampoco ha sido aprobada por la dirección por lo tanto no se revisa.	0-Inexistente	No cumple
6			**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**				
6	**1**		**ORGANIZACIÓN INTERNA**				
6	1	1	Compromiso de la Dirección con la seguridad de la información	SEGURIDAD	No se ha creado formalmente el Comité de Gestión de la Seguridad de la Información. Aunque la Dirección muestra su apoyo a la seguridad dentro de la organización y asigna funciones no lo hace a través de directrices claras, tampoco ha realizado una asignación explícita ni el reconocimiento de responsabilidades.	0-Inexistente	No cumple
6	1	2	Coordinación de la seguridad de la información	SEGURIDAD	Las actividades relativas a la seguridad son coordinadas y asignadas entre los diferentes roles y funciones aunque no existen procedimientos documentados.	2-Repetible	No cumple
6	1	3	Asignación de responsabilidades en seguridad de la información	SEGURIDAD	Los activos de información no están claramente definidos y aunque en algunos casos existe una asignación de responsabilidades no es formal.	1-Inicial/adHoc	No cumple
6	1	4	Proceso de autorización de recursos para la seguridad de la información	SEGURIDAD	Existe un proceso de autorización para los nuevos recursos de procesados de información aunque no es formal ni está documentado.	3-Proceso definido	No cumple
6	1	5	Acuerdos de confidencialidad	SEGURIDAD	En algunos casos se han establecidos acuerdos de confidencialidad pero no son revisados de forma periódica, tampoco cuando se incorporan nuevos activos de información.	2-Repetible	Cumple

6	1	6	Relación con las autoridades	SEGURIDAD	Existen procedimientos de prevención de riesgos y accidentes laborales (incendios, inundaciones, etc.) así como un protocolo de actuación claramente documentado. En el caso de la seguridad de la información, por ejemplo robos, ataques externos, incidentes terroristas, etc no se establece procedimiento formal.	2-Repetible	Cumple
6	1	7	Relación con grupos de interés especial	SEGURIDAD	Se establecen relaciones con grandes proveedores aunque ninguno de especial relevancia en cuestiones de seguridad de la información.	1-Inicial/adHoc	No cumple
6	1	8	Revisión independiente de la seguridad de la información	SEGURIDAD	Se realizan con frecuencia revisiones independientes de seguridad (auditorías) aunque no en todas las áreas (pe. Procedimientos, controles, etc.) No existe una política clara que defina la frecuencia y la metología.	2-Repetible	Cumple
6	**2**		**TERCERAS PARTES**				
6	2	1	Identificación de riesgos derivados del acceso de terceros	COMPRAS	Se realiza un exahustivo análisis en la selección de un proveedor (tercera parte) y siempre se confia el servicio a un importante proveedor (representa su seriedad y buenas prácticas). No se definen ni se identifican los riesgos que suponen en procesado de la información aunque se establecen controles generales de asignación de permisos y accesos.	2-Repetible	No cumple
6	2	2	Tratamiento de la seguridad en la relación con los clientes	NEGOCIO	Se revisan los requisitos de seguridad con los clientes y se establecen los controles que se solicitan.	2-Repetible	Cumple
6	2	3	Tratamiento de seguridad en los contratos con terceros	COMPRAS	Siempre que se contrata un servicio a un tercero se realiza un contrato pero no en todas las ocasionas este incluye las cláusulas de seguridad correspondientes.	3-Proceso definido	No cumple
7			**GESTIÓN DE ACTIVOS**				
7	**1**		**RESPONSABILIDAD SOBRE LOS ACTIVOS**				
7	1	1	Inventario de activos	SISTEMAS-REDES	Se realiza un inventario detallado de equipos, servidores y otros dispositivos propiedad de la organización o utilizados en sus procesos de negocios pero no existe un inventario de los activos de información.	3-Proceso definido	Cumple
7	1	2	Propietarios de los activos	SISTEMAS-REDES	En el inventario existente se asigna un propietario al activo pero no lo especifica razonablemente se hace de forma genérica.	3-Proceso definido	No cumple

7	1	3	Uso aceptable de los recursos	RRHH	Hay publicado un código de conducta y una guía general sobre el buen uso de los recursos de información de la organización.	4-Gestionado y evaluable	Cumple
7	**2**		**CLASIFICACIÓN DE LA INFORMACIÓN**				
7	2	1	Directrices de clasificación	RRHH	Se cumple con la normativa vigente de LOPD y por lo tanto se tiene clasificada la información que contiene datos personales según la legislación vigente pero no se clasifican aquellos activos de información que no contienen datos personales y tampoco se identifican según la criticidad para la organización.	3-Proceso definido	Cumple
7	2	2	Etiquetado y tratamiento de la información	SEGURIDAD FISICA	La información clasificada está etiquetada y tiene un tratamiento adecuado a las características asignadas aunque como se ha comentado anteriormente no está correctamente clasificada.	3-Proceso definido	No cumple
8			**SEGURIDAD LIGADA A LOS RRHH**				
8	**1**		**ANTES DEL EMPLEO**				
8	1	1	Funciones y responsabilidades	RRHH	Existe un documento descriptivo de todos los puesto de trabajo de la organización, donde se describe cuales son sus funciones y resposabilidades pero no en todos los casos se definen las responsabilidades de terceros. Muchas veces no se especifican las resposabilidades respecto a la seguridad.	4-Gestionado y evaluable	Cumple
8	1	2	Investigación de antecedentes	RRHH	Antes de realizar una contratación se solicitan referencias y se investigan los antecedentes del empleador o tercero. Se solicita documentación oficial sobre títulos, etc.	4-Gestionado y evaluable	Cumple
8	1	3	Términos y condiciones del empleo	RRHH	De acuerdo con la legislación se les hace firmar una cláusula legal (genérica) aunque no un código ético ni acuerdos. En contratos muy antiguos no se ha realizado nunca. Sucede con empleados y terceras partes.	3-Proceso definido	Cumple
8	**2**		**DURANTE EL EMPLEO**				
8	2	1	Responsabilidades de la Dirección	RRHH	Aunque se trasmite a los empleados una guía del buen uso de los recursos de la información no existe una política de seguridad clara.	1-Inicial/adHoc	Cumple

8	2	2	Concienciación, formación y capacitación en seguridad de la información	RRHH	No se realiza concienciación, formación o capacitación respecto a la seguridad de la información.	0-Inexistente	No cumple
8	2	3	Proceso disciplinario	RRHH	No existe un proceso disciplinario formal y claro para los empleados que hayan provocado la violación de la seguridad.	0-Inexistente	No cumple
8	**3**		**CESE DEL EMPLEO O CAMBIO DE PUESTO DE TRABAJO**				
8	3	1	Responsabilidad del cese o cambio	RRHH	Existe un procedimiento documentado respecto a la baja o cambio de puesto del personal. Se han asignado claramente las responsabilidades.	4-Gestionado y evaluable	Cumple
8	3	2	Devolución de activos	RRHH	Existe un procedimiento (aunque no documentado) sobre la devolución de los activos de la organización al finalizar su empleo, contrato o acuerdo.	4-Gestionado y evaluable	Cumple
8	3	3	Supresión de los derechos de acceso	RRHH	Existe un procedimiento documentado y revisado respecto a la supresión de derechos de acceso en el caso de cese o cambio de función. En algunos casos puntuales no son informados los cambios de función inmediatamente,	4-Gestionado y evaluable	Cumple
9			**SEGURIDAD FÍSICA Y AMBIENTAL**				
9	**1**		**ÁREAS SEGURAS**				
9	1	1	Perímetro de seguridad física	SEGURIDAD FISICA	Las instalaciones de la organización están cerradas al personal ajeno a esta mediante muros, barreras, puertas y otros elementos físicos. No es posible el acceso a las instalaciones físicas sin autorización.	5-Optimizado	Cumple
9	1	2	Control físicos de entrada	SEGURIDAD FISICA	Todas las instalaciones de la organización están controladas mediante un perímetro de seguridad al cual se accede por tarjeta con supervisión de personal de la organización, sin ella no es posible el acceso. Las zonas sensibles están protegidas con tarjeta y código.	5-Optimizado	Cumple
9	1	3	Seguridad de oficinas, despachos y salas	SEGURIDAD FISICA	Las salas sensibles (rack de switches, servidores, SAIs y otros aparatos) están protegidos mediante una puerta con llave siempre cerrada a custodia de los responsables. Los despachos están protegidos con puertas con cerradura y se cierran siempre que es necesario.	5-Optimizado	Cumple

9	1	4	Protección contra amenazas externas y de origen ambiental	SEGURIDAD FISICA	La organización tiene instaladas protecciones contra amenazas externas: sistemas de extinción de incendios en todos los espacios, protección del fuego en zonas mediante infraestructuras especiales (puertas ignífugas, etc.). Zonas sensibles en espacios altos para evitar daños en inundaciones acompañadas de desagües en zonas de riesgo. En cuanto a amenazas provocadas por el hombre cuenta con las barreras físicas habituales (puertas, muros, etc).	5-Optimizado	Cumple
9	1	5	Trabajo en áreas seguras	SEGURIDAD FISICA	La organización tiene implementada una serie de directrices para el uso de espacio comunes, asegurando las zonas de trabajo (no se puede entrar alimentos, áreas limpias de materiales, etc.)	5-Optimizado	Cumple
9	1	6	Acceso publico, zonas de carga y descarga	SEGURIDAD FISICA	En las zonas de acceso al público o zonas de carga y descarga siempre está presente un empleado de la organización supervisando el acceso o las tareas que se deben realizar. Estas zonas se mantienen libre del tratamiento de información o está protegida adecuadamente.	5-Optimizado	Cumple
9	**2**		**SEGURIDAD DE LOS EQUIPOS**				
9	2	1	Emplazamiento y protección de los equipos	SEGURIDAD FISICA	Los equipos de la organización y otros dispositivos de tratamiento o mantenimiento de la información son adecuadamente ubicados mediante la protección de los mismos; accesos no autorizados, problemas ambientales (goteras, lluvia, etc), etc.	5-Optimizado	Cumple
9	2	2	Instalaciones de suministro	SEGURIDAD FISICA	Todas las instalaciones de la organización están protegidas ante fallos de alimentación (Diferenciales, SAIs, grupos electrógenos y otros dispositivos). Las zonas especialmente sensibles están reforzadas con un sistema adicional y redundante que asegura el funcionamiento y la continuidad de la operativa en caso de fallo eléctricos o la protección ante los mismos.	5-Optimizado	Cumple
9	2	3	Seguridad del cableado	SISTEMAS-REDES	Tanto el cableado eléctrico como de comunicaciones está protegido ante interceptaciones o daños. Se ubican en sus correspondientes bandejas y los accesos del cableado especialmente protegido sólo es conocido por el personal autorizado.	5-Optimizado	Cumple

9	2	4	Mantenimiento de los equipos	SISTEMAS-REDES	Los equipos (servidores, etc) y dispositivos tienen un mantenimiento adecuado y se monitorizan constantemente ante fallos hardware, en caso de fallo son inmediatamente reparados. Los equipos y dispositivos especialmente críticos tienen asociado un contrato de reparación en caso de fallo (por importantes proveedores). Aunque no existe una evaluación de riesgos ni una política clara.	5-Optimizado	Cumple
9	2	5	Seguridad de equipos fuera de los locales propios	SEGURIDAD FISICA	Los equipos que se emplean fuera de la organización cumplen las mismas medidas que los equipos que se emplean dentro, no se aplican medidas especiales (encriptación, etc) y aunque suele existir una autorización del responsable no se lleva una buena gestión de ellas.	1-Inicial/adHoc	No cumple
9	2	6	Seguridad en la reutilización o eliminación de equipos	SISTEMAS-REDES	La organización es consciente de la importancia de las buenas prácticas de la retirada o reutilización de equipos por la importancia de los datos que contienen pero no existe ninguna política formal al respecto. Aunque los dispositivos de almancenamiento son retirados y reutilizados de forma segura el procedimiento no está controlado ni revisado. Se lleva el control de las licencias a modo general (no muy exhaustivo).	2-Repetible	No cumple
9	2	7	Retirada de materiales de propiedad de la empresa	SEGURIDAD FISICA	Existen controles sobre la retirada de materiales pero son débiles y no están documentados. Se protege la salida de los activos propiedad de la organización aunque no se está especialmente concienciado del peligro que conlleva.	1-Inicial/adHoc	No cumple
10			**GESTIÓN DE COMUNICACIONES Y OPERACIONES**				
10	**1**		**RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIONES**				
10	1	1	Documentación de los procedimientos de operaciones	SISTEMAS-REDES	La mayoría de los procedimientos de operaciones están correctamente documentados y habitualmente se revisan. Se modifican mediante autorización del responsable y se lleva un control de las versiones. Además están a disposición de todos los usuarios que los necesiten, tampoco permite asociar los activos afectados (equipos, software, información, etc).	5-Optimizado	Cumple
10	1	2	Gestión de los cambios	SISTEMAS-REDES	Se lleva un control de cambios (con un proceso claro y previa autorización) aunque no es muy exhaustivo y no identifica el área de trabajo (sistemas, comunicaciones, software, etc) ni aplica ninguna clasificación.	3-Proceso definido	Cumple

10	1	3	Segregación de tareas	SISTEMAS-REDES	Se segregan funciones y tareas en todos los departamentos de forma indirecta para evitar las modificaciones no autorizadas o usos indevidos. Como punto débil, no existe documentación o política documentada al respecto.	4-Gestionado y evaluable	Cumple
10	1	4	Separación de los entornos de desarrollo, pruebas y explotación	SISTEMAS-REDES	Las áreas de desarrollo y explotación, tanto en Sistemas como en Programación, están diferenciadas aunque no de todas las aplicaciones. Se segregan funciones en todos los departamentos para evitar las modificaciones no autorizadas o usos indevidos. Como punto débil, no existe documentación o política documentada al respecto.	3-Proceso definido	Cumple
10	**2**		**GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS**				
10	2	1	Provisión de servicios	SISTEMAS-REDES	Al contratar un servicio se comprueban las definiciones, los acuerdos de provisión y los recursos empleados por el tercero aunque no existe una política general de revisión (check list). No se revisan los acuerdos de forma periódica salvo cause pérdidas para la organización.	3-Proceso definido	Cumple
10	2	2	Supervisión y revisión de los servicicios prestados por terceros	SISTEMAS-REDES	Los niveles de servicios de terceros se monitorizan con frecuencia. No se realizan auditorías de los servicios de terceros ni existe una política específica para la gestión de servicios de terceros.	3-Proceso definido	Cumple
10	2	3	Gestión de cambios en los servicios prestados por terceros	SISTEMAS-REDES	Se gestionan los cambios realizados en servicios de terceros, se actualizan los procedimientos establecidos y se tiene presente la criticidad del servicio para la organización. Aunque su gestión no es óptima.	3-Proceso definido	Cumple
10	**3**		**PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS**				
10	3	1	Gestión de capacidades	SISTEMAS-REDES	Se gestiona, en la mayoría de servicios/sistemas, las capacidades de los mismos y se ajusta el consumo. Adicionalmente se realizan proyecciones de los requisitos futuros de capacidad. No existe una política clara y formal al respecto pero se lleva a cabo de manera continua.	5-Optimizado	Cumple
10	3	2	Aceptación de sistemas	SISTEMAS-REDES	Existen pruebas y revisiones de los sistemas antes de ser puestos en explotación por el departamento receptor (está documentado y se revisa frecuentemente), no sucede lo mismo con los productos de software.	3-Proceso definido	Cumple
10	**4**		**PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y CÓDIGO MÓVIL**				

10	4	1	Controles contra software malicioso	SISTEMAS-REDES	Todos los equipos y servidores tienen instalados antivirus locales (centralizados) además de sus correspondientes firewalls. Adicionalmente se aplican protecciones adicionales en las zonas en contacto con Internet (Firewalls). El control está documentado y se revisa frecuentemente.	5-Optimizado	Cumple
10	4	2	Controles contra código móvil	SISTEMAS-REDES	Las barreras perimetrales de acceso a Internet así como los antivirus locales (incluyen antimalware) y la propia protección del navegador protegen a los equipos y servidores del código móvil. Aunque no hay una política específica la organización es consciente de la necesidad del control.	4-Gestionado y evaluable	Cumple
10	**5**		**COPIAS DE SEGURIDAD**				
10	5	1	Copias de seguridad de la información	SISTEMAS-REDES	La organización evalua la necesidad de las copias de seguridad al poner en explotación un nuevo sistema y realiza un inventario y control de las mismas. Adicionalmente se revisan de forma periódica y se hacen pruebas puntuales de recuperación aunque no de todos los sistemas. La mayoría de procesos de copias de seguridad están documentados y existen procedimientos para llevarlos a cabo.	5-Optimizado	Cumple
10	**6**		**GESTIÓN DE LA SEGURIDAD DE LA RED**				
10	6	1	Controles de red	SISTEMAS-REDES	La organización cuenta con una red segmentada (dependiendo de la criticidad de los datos y la exposición al exterior) por Firewalls y asegurada por rutas y reglas de acceso. Adicionalmente cuenta con dispositivos avanzados que detectan comportamientos extraños en la red.	5-Optimizado	Cumple
10	6	2	Seguridad de los servicios de red	SISTEMAS-REDES	Los servicios de red están identificados y tienen asignados las características de seguridad y algunas veces los requisitos de gestión pero no en todos los servicios (sobre todo los internos) se identifican los acuerdos con la dirección.	4-Gestionado y evaluable	Cumple
10	**7**		**MANIPULACIÓN DE SOPORTES**				
10	7	1	Gestión de soportes extraíbles	SISTEMAS-REDES	Aunque se establecen controles técnicos sobre el uso de memorias extraíbles no se realizan sobre unidades de CD/DVD u otros dispositivos.Tampoco se establecen procedimientos formales (por escrito) ni recomendaciones.	1-Inicial/adHoc	No cumple
10	7	2	Retirada de soportes	SISTEMAS-REDES	Aunque no existe una política o procedimiento formal (por escrito) la mayoría de soportes se destruyen manualmente al ser retirados aunque no sucede así con las estaciones de trabajo u otros dispositivos de menor envergadura.	2-Repetible	No cumple

10	7	3	Procedimiento de manipulación de la información	SISTEMAS-REDES	La información se manipula correctamente y existen controles/procedimientos que la protegen contra los accesos no autorizados o el uso indebido pero no existe política o procedimiento por escrito sobre las prácticas o recomendaciones.	4-Gestionado y evaluable	Cumple
10	7	4	Seguridad de la documentación de los sistemas	SISTEMAS-REDES	La documentación y la información en general está protegida mediante reglas de acceso proporcionadas por los responsables de los datos. Se está mejorando la gestión en la centralización creando accesos por grupos de recursos.	3-Proceso definido	Cumple
10	**8**		**INTERCAMBIO DE INFORMACIÓN**				
10	8	1	Políticas y procedimientos de intercambio de información	SEGURIDAD	Se han establecido políticas y procedimientos para el intercambio de información sobre todo aquella que contiene datos personales aunque no ha sido comunicada a todas las partes. En algunos casos no se observan cláusulas de confidencialidad y en la comunicación de voz no se han aplicado correctamente los controles adecuados.	3-Proceso definido	Cumple
10	8	2	Acuerdos de intercambio	RRHH	En ninguno de los casos se han establecido acuerdos de intercambio de información entre la organización y terceros.	0-Inexistente	No cumple
10	8	3	Soportes físicos en transito	SEGURIDAD FISICA	La organización tiene una política clara y formal sobre los procedimientos de tránsito de soportes físicos, se lleva a cabo correctamente y se revisa con cierta frecuencia.	5-Optimizado	Cumple
10	8	4	Correo electrónico	SISTEMAS-REDES	La información contenida en el correo electrónico presenta las protecciones estándar del producto, no se han aplicado certificados ni encriptación.	3-Proceso definido	Cumple
10	8	5	Sistemas de información empresariales	SISTEMAS-REDES	La interconexión de los sistemas empresariales están debidamente controlados y se gestiona correctamente su alta, baja y modificación de accesos. Existe una documentación asociada al respecto.	4-Gestionado y evaluable	Cumple
10	**9**		**SERVICIOS DE COMERCIO ELECTRONICO**				
10	9	1	Comercio electrónico	SISTEMAS-REDES	La organización utiliza el comercio electrónico y por ello cumple con la legislación vigente asociada (LOPD, LSSI, etc) adicionalmente se protege de actividades faudulentas y disputas contractuales mediante sistemas de seguridad (Firewalls, encriptación, certificados digitales, etc). Existe una política formal al respecto.	5-Optimizado	Cumple

10	9	2	Transacciones en línea	SISTEMAS-REDES	Las transacciones en línea se realizan mediante encriptación del canal de comunicación, ya sea por certificados digitales u otros medios. Se llevan a cabo otros controles que aseguran la transacción pero no existe una política formal al respecto.	4-Gestionado y evaluable	Cumple
10	9	3	Información con acceso publico	SISTEMAS-REDES	La información puesta a disposición pública está debidamente protegida frente a modificaciones no autorizadas y se revisa frecuentemente. Los servidores están correctamente actualizados y presentan sistemas antivirus/antimalware activos.	4-Gestionado y evaluable	Cumple
10	**10**		**MONITORIZACIÓN**				
10	10	1	Registro de auditorías	SISTEMAS-REDES	Todos los sistemas de información tienen activo el registro de eventos de seguridad pero no se ha establecido ninguna política común de almacenamiento. Tampoco existe documentación respecto a la configuración o los requisitos del negocio.	3-Proceso definido	No cumple
10	10	2	Monitorización del uso de los sistemas	SISTEMAS-REDES	La organización ha establecido los procedimientos para la monitorización y supervisión de los recursos de procesamiento de información, estos se revisan periódicamente. No existe una política formal pero las medidas se toman de forma adecuada.	5-Optimizado	Cumple
10	10	3	Protección de la información de los registros	SISTEMAS-REDES	Los registros de seguridad de los sistemas se protegen de forma adecuada de los accesos no autorizadas y de manipulaciones indebidas. No se revisan de forma frecuente.	5-Optimizado	Cumple
10	10	4	Registros de administración y operación	SISTEMAS-REDES	Los registros de seguridad registran cualquier evento del sistema, incluyendo aquellos realizados por los operadores y los administradores de sistemas. No existe ningún procedimiento de revisión periódica.	3-Proceso definido	Cumple
10	10	5	Registros de fallos	SISTEMAS-REDES	Se realiza la gestión de fallos de los sistemas mediante varias herramientas de monitorización que permiten a los administradores actuar para prevenir la interrupción o solucionarla.	5-Optimizado	Cumple
10	10	6	Sincronización de relojes	SISTEMAS-REDES	Los relojes de todos los sistemas están sincronizados con una precisión de tiempo acordada. Existe un procedimiento forma que se revisa con cierta frecuencia.	5-Optimizado	Cumple
11			**CONTROL DE ACCESO**				
11	**1**		**REQUISITOS DE NEGOCIO PARA EL CONTROL ACCESO**				
11	1	1	Política de control de acceso	SEGURIDAD	Aunque la organización lleva a cabo un control de acceso siguiendo las indicaciones de la dirección o los clientes (requisitos del negocio) no existe ninguna política de control acceso formal (documentada y revisada).	3-Proceso definido	Cumple
11	**2**		**GESTIÓN DE ACCESO DE USUARIO**				

11	2	1	Registro de usuario	SISTEMAS-REDES	La organización tiene un procedimiento formal de alta, baja y modificación de usuarios mediante el cual se concenden y revocan los derechos de acceso. Este documento se actualiza y revisa con frecuencia.	5-Optimizado	Cumple
11	2	2	Gestión de privilegios	SISTEMAS-REDES	La gestión de privilegios sólo corresponde al departamento de Administración de Sistemas (en el caso de sistemas comunes) y explotación de aplicaciones (en el caso de aplicaciones). Ningún otro usuario puede realizar estas funciones. Aunque no existe un esquema formal de autorización el procedimiento se realiza correctamente.	3-Proceso definido	Cumple
11	2	3	Gestión de las contraseñas de los usuarios	SISTEMAS-REDES	Se realiza una gestión correcta de las contraseñas de los usuarios tanto a nivel de aplicación como de sistema a través de un proceso formal (se establece caducidad y bloqueo) aunque no existe ninguna política formal sobre la gestión de contraseñas (entrega, cambio, etc). Tampoco se firman cláusulas de confidencialidad de la contraseña.	4-Gestionado y evaluable	Cumple
11	2	4	Revisión de los derechos de accesos	SISTEMAS-REDES	No existe ningún procedimiento formal de revisión de los derechos de acceso, los responsables de la información confian en los derechos establecidos y sólo se revisan en caso de error, anomalía o incidencia.	0-Inexistente	No cumple
11	**3**		**RESPONSABILIDAD DE USUARIO**				
11	3	1	Uso de las contraseñas	SISTEMAS-REDES	La organización ha establecido métodos técnicos para que las contraseñas cumplan con unos requisitos de seguridad adecuados (no está aplicado en las aplicaciones) pero no existe una guía de recomendaciones en la selección de contraseñas para los usuarios.	3-Proceso definido	Cumple
11	3	2	Equipo de usuario desatendido	SISTEMAS-REDES	Se han establecido controles técnicos para el bloqueo de equipos desatendidos (tanto en estaciones de trabajo como servidores) pero no existe una guía/formación de concienciación dirigida a los usuarios.	4-Gestionado y evaluable	Cumple
11	3	3	Política de puesto de trabajo despejado y bloqueo de pantalla	SISTEMAS-REDES	No existe ninguna política formal de puesto de trabajo despejado y bloqueo de pantalla aunque la organización ha establecido métodos técnicos para el bloqueo de sesiones.	3-Proceso definido	Cumple
11	**4**		**CONTROL DE ACCESO A LA RED**				
11	4	1	Política de uso de los servicios de red	SISTEMAS-REDES	El uso de los servicios de red (un gran porcentaje) está controlado técnicamente y sólo se habilita el acceso previa autorización pero no existe una política formal sobre la solicitud de acceso. Como debilidad la organización permite el acceso a la red por DHCP si un dispositivo se conecta a una toma (sin autorización previa).	3-Proceso definido	Cumple

11	4	2	Autenticación de usuarios para conexiones externas	SISTEMAS-REDES	Se establecen la autentificación de usuarios para conexiones externas mediante rangos de IP y enrutamientos preestablecidos, estos controles se acompañan de reglas de acceso en Firewalls.	5-Optimizado	Cumple
11	4	3	Identificación de equipos en la red	SISTEMAS-REDES	Todos los equipos de la red están identificados e inventariados (de forma automática), se realiza un control sobre la incorporación de nuevos equipos (evalúa la autorización de su acceso a la red). Existe una estructura definida de la red y la asignación de IPs por zonas.	5-Optimizado	Cumple
11	4	4	Diagnóstico remoto y protección de los puertos de configuración	SISTEMAS-REDES	De forma general los puertos de configuración de equipos, servidores, switches y otros están protegidos ya sea por medidas lógicas como físicas.	5-Optimizado	Cumple
11	4	5	Segregaciones de la red	SISTEMAS-REDES	Las redes de la organización están completamente segregadas y protegidas teniendo en cuenta su criticidad, exposición al exterior y el valor de la información que protegen. Esto se complementa con dispositivos avanzados de vigilancia de la red.	5-Optimizado	Cumple
11	4	6	Control de conexión a la red	SISTEMAS-REDES	La organización establece controles de conexión a la red mediante enrutamientos, firewalls y otros elementos. Adicionalmente se monitorizan los accesos y se controla el consumo de recursos.	5-Optimizado	Cumple
11	4	7	Control de encaminamiento en la red	SISTEMAS-REDES	La organización tiene implementado un control de encaminamiento de red, todas las redes que están controladas se encaminan a sus correspondientes firewalls y en estos se establecen las reglas de acceso.	5-Optimizado	Cumple
11	**5**		**CONTROL DE ACCESO AL SISTEMA OPERATIVO**				
11	5	1	Procedimiento seguros de inicio de sesión	SISTEMAS-REDES	Se establecen mecanismos técnicos de inicio de sesión seguro: no muestra el último usuario logeado, bloqueo de contraseñas por intentos fallidos, tiempo de espera al bloqueo de cuenta, comunicación cifrada de la contraseña, etc pero estos no se recogen en una política. Tampoco se muestra un aviso general del acceso limitado a los usuarios autorizados.	5-Optimizado	Cumple
11	5	2	Identificación y autenticación de usuario	SISTEMAS-REDES	No todos los usuarios del sistema tienen identificadores personales, existen muchos usuarios genéricos donde no se puede trazar la persona (tanto en sistema como en aplicación).	3-Proceso definido	No cumple
11	5	3	Sistema de gestión de contraseñas	SISTEMAS-REDES	El sistema de gestión de contraseñas es correcto, se almacenan cifradas, se establece una complejidad a las contraseñas, un periodo de caducidad, un historial recordatorio. Además se permite al usuario la modificación de contraseña en la mayoría de casos, etc.	5-Optimizado	Cumple

11	5	4	Uso de las utilidades de los sistemas operativos	SISTEMAS-REDES	Tanto en equipos como en servidores se limita el uso y acceso a las herramientas y utilidades del sistema operativo que puedan dañar parte del mismo. Sólo el personal técnico autorizado/capacitado tiene acceso a estas. Adicionalmente todas las aplicaciones innecesarias son eliminadas del sistema pero no existe una política formal al respecto.	5-Optimizado	Cumple
11	5	5	Desconexión automática de sesión	SISTEMAS-REDES	En el acceso a sistemas remotos se establece un timeout de sesión (Citrix, Terminal Server, TMG, etc) pero no sucede lo mismo en las aplicaciones internas de la organización ni en las sesiones de usuario en las estaciones de trabajo.	4-Gestionado y evaluable	Cumple
11	5	6	Limitación de las ventanas de conexión	SISTEMAS-REDES	Dadas las necesidades del negocio no se han establecido ventanas de limitación de conexión ya que los clientes requieren el uso del sistema en cualquier hora/día del año.	4-Gestionado y evaluable	Cumple
11	**6**		**CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN**				
11	6	1	Restricción de acceso a la información	SISTEMAS-REDES	Las aplicaciones tienen asignados distintos menus dependiendo el perfil del usuario, sólo los usuarios de soporte tienen acceso a toda la información. Existe documentación al respecto.	4-Gestionado y evaluable	Cumple
11	6	2	Aislamiento de sistemas sensibles	SISTEMAS-REDES	Los sistemas sensibles están aislados y correctamente protegidos bajo los requisitos del negocio y del propietario de los datos.	5-Optimizado	Cumple
11	**7**		**ORDENADORES PORTÁTILES Y TELETRABAJO**				
11	7	1	Ordenadores portátiles y comunicaciones móviles.	SISTEMAS-REDES	Aunque la mayor parte de la información está centralizada y se utilizan protocolos seguros así como mecanismos adicionales, no existe una política formal sobre la utilización de equipos y dispositivos portátiles o móviles.	1-Inicial/adHoc	No cumple
11	7	2	Teletrabajo	RRHH	No existe una política formal de teletrabajo donde se indiquen los requisitos necesarios (antivirus, firewall, conexión, ubicación física, etc) así como acuerdos de licencia o propiedad intelectual, reglas de uso (acceso a la familia, …), etc.	1-Inicial/adHoc	No cumple
12			**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**				
12	**1**		**REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN**				
12	1	1	Análisis y especificaciones de requisitos de seguridad	DESARROLLO	En el análisis y especificaciones de los nuevos productos se suelen evaluar las características y controles de seguridad aunque no en todas las ocasiones. Cuando se asumen debilidades de seguridad no se realiza una evaluación de riesgos.	3-Proceso definido	No cumple

12	**2**		**PROCESO CORRECTO EN LAS APLICACIONES**				
12	2	1	Validación de los datos de entrada	DESARROLLO	Las aplicaciones tienen aplicada la validación de datos de entrada, detectando y evitando los errores. Estos controles protegen a las aplicaciones de ataques estándar.	4-Gestionado y evaluable	Cumple
12	2	2	Control del proceso interno	DESARROLLO	Las aplicaciones de la organización realizan un control interno de la información que manejan vigilando la integridad de los datos y evitando los ataques estándar.	4-Gestionado y evaluable	Cumple
12	2	3	Integridad de los mensajes	DESARROLLO	Las aplicaciones no incorporan la verificación de la integridad de los mensajes aunque existen controles adicionales que pueden complementar este objetivo.	2-Repetible	No cumple
12	2	4	Validación de los datos de salida	DESARROLLO	No se realiza la validación de los datos de salida en todas las aplicaciones/informes aunque en todos los casos se proporciona a los usuarios la información suficiente para que se pueda evaluar correctamente.	2-Repetible	No cumple
12	**3**		**CONTROLES CRIPTOGRÁFICOS**				
12	3	1	Política de uso de los controles criptográficos	SEGURIDAD	No existe una política formal sobre el uso de los controles criptográficos que recoja la información el enfoque, el análisis de riesgos y las medidas implementadas.	1-Inicial/adHoc	No cumple
12	3	2	Gestión de claves	SEGURIDAD	La organización tiene un implementado un sistema de gestión de claves en donde se generan y almacenan los certificados, gestión de claves, etc. Este sistema está protegido y existe una política no formal sobre su uso.	3-Proceso definido	No cumple
12	**4**		**SEGURIDAD EN LOS ARCHIVOS DE SISTEMA**				
12	4	1	Control del software en explotación	SISTEMAS-REDES	Existen controles del software en explotación mediante la gestión de cambios y se realizan las actualizaciones del sistema mediante un proceso documentado y probado. Adicionalmente existe un registro de auditoría de los cambios realizados y la posibilidad de restaurar un sistema si en el cambio se producen errores.	4-Gestionado y evaluable	Cumple
12	4	2	Protección de los datos de prueba	DESARROLLO	No se establece protección adicional a los datos de pruebas, se utilizan los mismos mecanismos y controles que con los datos reales.	1-Inicial/adHoc	No cumple
12	4	3	Control de acceso al código fuente	DESARROLLO	La gestión del acceso al código fuente se realiza de forma correcta; sólo los usuarios autorizados tienen acceso al código fuente y este está protegido contra modificaciones. Adicionalmente se realiza un registro de los cambios.	4-Gestionado y evaluable	Cumple

12	**5**		**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**				
12	5	1	Procedimiento de control de cambios	SISTEMAS-REDES	La organización lleva a cabo un procedimiento de gestión de cambios donde se establece el nivel de autorización, los sistemas afectados, los cambios realizados, etc. Esta gestión de cambios realiza un registro de los pasos realizados y permite trazar una auditoría del proceso. Aunque es necesario mejorarlo ya que no se puede asociar el activo	2-Repetible	Cumple
12	5	2	Revisión técnica de las aplicaciones después de cambios en los sistemas operativos	SEGURIDAD	Siempre que se realiza un cambio a nivel de sistema o a nivel de software se realiza una revisión técnica sobre el cambio realizado u otros aspectos relacionados. Aunque es necesario mejorar el área de Quality y Testing.	4-Gestionado y evaluable	Cumple
12	5	3	Restricción en los cambios a los paquetes de software	SISTEMAS-REDES	La organización sólo realiza cambios en paquetes de software cuando el cliente tiene una necesidad, el software presenta un problema o con intención de mejorar su rendimiento/funcionamiento. Todos los cambios son evaluados y probados, no se realizan sin previa autorización y el software original se conserva.	5-Optimizado	Cumple
12	5	4	Fuga de información	DESARROLLO	La organización no tiene a disposición de los empleados escáneres u otros dispositivos similares, además limita el tamaño de salida de los correos, no permite el uso de sticks de memoria, y otros controles similares que impiden la fuga de información.	4-Gestionado y evaluable	Cumple
12	5	5	Desarrollo externalizado de software	DESARROLLO	Se realiza el desarrollo externalizado de software pero no en todos los casos se han establecido: los contratos de licencia, propiedad del código, requisitos de calidad y seguridad del software, etc.	4-Gestionado y evaluable	Cumple
12	**6**		**GESTIÓN DE VULNERABILIDADES TÉCNICAS**				
12	6	1	Control de vulnerabilidades técnicas	SEGURIDAD	Normalmente la organización lleva a cabo la gestión de las vulnerabilidades técnicas en cuanto a sistemas operativos Microsoft pero no en el resto de software (Acrobat, Java, etc. - incluido aplicaciones Microsoft) y dispositivos (Cisco, etc).	3-Proceso definido	Cumple
13			**GESTIÓN DE INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN**				
13	**1**		**REPORTE DE INCIDENCIAS Y DEBILIDADES**				

13	1	1	Notificación de los eventos de seguridad de la información	HELP DESK	La organización posee un help desk de soporte 24x365 (punto único: web, teléfono y correo electrónico) donde usuarios y proveedores pueden notificar las incidencias aunque no se hace distinción entre problemas habituales o incidencias de seguridad. No existe documentación del sistema de gestión de incidencias.	3-Proceso definido	No cumple
13	1	2	Notificación de los puntos débiles de la seguridad	HELP DESK	Los empleados, contratistas y terceros notifican las incidencias pero no están obligados (por política, por cláusula, o similar) a notificar los puntos débiles de seguridad.	1-Inicial/adHoc	No cumple
13	**2**		**GESTIÓN DE INCIDENCIAS DE SEGURIDAD Y MEJORAS**				
13	2	1	Responsabilidades y procedimientos	HELP DESK	La organización no cuenta con un esquema formal de responsabilidades y procedimientos para el tratamiento de las incidencias de seguridad (específico).	1-Inicial/adHoc	No cumple
13	2	2	Aprendizaje de los incidentes de seguridad de la información	HELP DESK	La organización no cuenta con ningún mecanismo que permita el aprendizaje sobre los incidentes de seguridad.	1-Inicial/adHoc	No cumple
13	2	3	Recopilación de evidencias	HELP DESK	En caso de incidentes de seguridad la organización realiza la recopilación de evidencias pero no sigue ningún procedimiento específico y muchas veces por desconocimiento no las realiza rigurosamente.	2-Repetible	No cumple
14			**GESTIÓN DE LA CONTINUIDAD DE NEGOCIO**				
14	**1**		**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO**				
14	1	1	Incluir la seguridad de la información en el proceso de gestión de la continuidad de negocio	SEGURIDAD	La organización cuenta una gestión de la continuidad del negocio a baja escala, sin analizar grandes catástrofes/daños y sin incluir la seguridad de la información.	2-Repetible	No cumple
14	1	2	Continuidad de negocio y análisis de riesgos	SEGURIDAD	La organización no ha realizado un plan de continuidad a partir del análisis de un análisis de riesgos.	1-Inicial/adHoc	No cumple
14	1	3	Desarrollo e implantación de planes de continuidad incluyendo la seguridad de la información	SEGURIDAD	Ídem	1-Inicial/adHoc	No cumple

14	1	4	Marco de planificación de la continuidad de negocio	SEGURIDAD	Ídem	1-Inicial/adHoc	No cumple
14	1	5	Prueba, mantenimiento y revisión de los planes de continuidad de negocio	SEGURIDAD	Ídem	1-Inicial/adHoc	No cumple
15			**CUMPLIMIENTO**				
15	**1**		**CUMPLIMIENTO DE LOS REQUISITOS LEGALES**				
15	1	1	Identificación de la legislación aplicable	ASESORIA JURIDICA	La organización cumple con la LOPD, LSSI y otra legislación vigente y así lo demuestra los informes de auditoría presentados.	5-Optimizado	Cumple
15	1	2	Derechos de propiedad intelectual	ASESORIA JURIDICA	La organización cumple con la propiedad intelectual; compra las licencias a fuentes de confianza, mantiene un inventario de los productos, realiza un revisión anual de los mismos, etc. Aunque no tiene publicada una política sobre el cumplimiento de la DPI.	5-Optimizado	Cumple
15	1	3	Protección de los documentos de la organización	ASESORIA JURIDICA	La organización almacena y protege adecuadamente la documentación oficial requerida además de establecer adecuadamente los periodos de retención de la información. En su contra no se establece ningún documento formal que indique el calendario de conservación o las directrices de conservación.	5-Optimizado	Cumple
15	1	4	Protección de datos de carácter personal y privacidad	ASESORIA JURIDICA	La organización cumple con la LOPD, LSSI y otra legislación vigente y así lo demuestra los informes de auditoría presentados.	5-Optimizado	Cumple
15	1	5	Prevención del mal uso de los recursos informáticos	RRHH	La organización realiza la prevención del mal uso de los recursos informáticos mediante medidas y controles técnicas e informa a los empleados sobre el uso indebido de estos.	5-Optimizado	Cumple
15	1	6	Regulación de controles criptográficos	SEGURIDAD	La organización cumple con la regulación de los controles criptográficos e implanta su uso cuando es necesario aunque no existe una documentación específica al respecto.	3-Proceso definido	Cumple
15	**2**		**CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD**				
15	2	1	Cumplimiento de las políticas y normas de seguridad.	AUDIT	No se detectan informes formales sobre las revisiones del cumplimiento por parte de los directores aunque parece que informalmente se realiza este seguimiento.	2-Repetible	No cumple

15	2	2	Comprobación del cumplimiento técnico	AUDIT	En los últimos años se han realizado auditorías técnicas y procedimentales, la organización posee los informes resultados. Ha analizado los informes y está implementando las mejoras.	5-Optimizado	Cumple
15	**3**		**CONSIDERACIONES SOBRE LAS AUDITORIAS DE LOS SISTEMAS DE INFORMACIÓN**				
15	3	1	Controles de auditoría de los sistemas de información	AUDIT	En la realización de las auditorías se ha seleccionado el ámbito y los controles necesarios para minimizar el riesgo de las interrupciones. No existe documento general pero se prepara un contrato con cada auditoría.	5-Optimizado	Cumple
15	3	2	Protección de las herramientas de auditoría de sistemas de información	AUDIT	Todas las herramientas de auditoría están especialmente protegidas y sólo son accesibles para los administradores/auditores.	4-Gestionado y evaluable	Cumple

1.5.2.- Resumen análisis diferencial.

Dominio	Cumple	No cumple
5.- Política de seguridad.	0 %	100 %
6.- Organización de la seguridad y la información.	36 %	64 %
7.- Gestión de activos.	60 %	40 %
8.- Seguridad ligada a los RRHH.	78 %	22 %
9.- Seguridad física y ambiental.	77 %	23 %
10.- Gestión de las comunicaciones y operaciones.	87 %	13 %
11.- Control de acceso.	84 %	16 %
12.- Adquisición, desarrollo y mantenimiento de sistemas de información.	60 %	40 %
13.- Gestión de incidencias de la seguridad de la información.	0 %	100 %
14.- Gestión de la continuidad del negocio.	0 %	100 %
15.- Cumplimiento.	90 %	10 %

1.6.- Planificación del proyecto.

Inicio	**10 días**	**lun 04/03/13**	**vie 15/03/13**	
Fase1 - Situación actual	**10 días**	**lun 04/03/13**	**vie 15/03/13**	
Documentación y redacción de: Objetivos del TFM	1 día	lun 04/03/13	lun 04/03/13	
Documentación y redacción de: Marco de trabajo.	1 día	mar 05/03/13	mar 05/03/13	3
Elaboración introducción	1 día	mié 06/03/13	mié 06/03/13	4
Conocimiento de la ISO/IEC 27002	**2 días**	**jue 07/03/13**	**vie 08/03/13**	
Búsqueda, investigación y estudio: Norma ISO/IEC 27000	1 día	jue 07/03/13	jue 07/03/13	5
Análisis y selección de información.	1 día	vie 08/03/13	vie 08/03/13	7
Contextualización	**7 días**	**jue 07/03/13**	**vie 15/03/13**	
Selección empresa	2 días	jue 07/03/13	vie 08/03/13	5
Identificación alcance	1 día	lun 11/03/13	lun 11/03/13	10
Identificacion objetivos plan director	1 día	mar 12/03/13	mar 12/03/13	11
Elaboración análisis diferencial	3 días	mié 13/03/13	vie 15/03/13	12
Resultados fase 1	1 día	vie 15/03/13	vie 15/03/13	
Planificación	**1 día**	**lun 18/03/13**	**lun 18/03/13**	
Elaboración plan fase 1	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 2	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 3	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 4	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 5	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 6	1 día	lun 18/03/13	lun 18/03/13	13
Estimación esfuerzo y costes	1 día	lun 18/03/13	lun 18/03/13	13

Planificación	**1 día**	**lun 18/03/13**	**lun 18/03/13**	
Elaboración plan fase 1	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 2	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 3	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 4	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 5	1 día	lun 18/03/13	lun 18/03/13	13
Elaboración plan fase 6	1 día	lun 18/03/13	lun 18/03/13	13
Estimación esfuerzo y costes	1 día	lun 18/03/13	lun 18/03/13	13
Ejecución	**58 días**	**mar 19/03/13**	**jue 06/06/13**	
Fase2 - Sistema gestion documental	**8 días**	**mar 19/03/13**	**jue 28/03/13**	
Elaboracion política de seguridad	1 día	mar 19/03/13	mar 19/03/13	15
Elaboración procedimiento de auditorias internas	1 día	mié 20/03/13	mié 20/03/13	25
Definición de indicadores	1 día	jue 21/03/13	jue 21/03/13	26
Definición de procedimiento de revisión dirección	1 día	vie 22/03/13	vie 22/03/13	27
Elaboración comité seguridad	1 día	lun 25/03/13	lun 25/03/13	28
Establecer metodología de análisis riesgos	1 día	mar 26/03/13	mar 26/03/13	29
Elaboración declaración de aplicabilidad	1 día	mié 27/03/13	mié 27/03/13	30
Resultados fase 2	1 día	jue 28/03/13	jue 28/03/13	31
Fase3 - Analisis de riesgos	**14 días**	**vie 29/03/13**	**mié 17/04/13**	
Elaboración inventario de activos	1 día	vie 29/03/13	vie 29/03/13	32
Valoración de los activos	2 días	lun 01/04/13	mar 02/04/13	34
Identificación criticidad activos	2 días	mié 03/04/13	jue 04/04/13	35
Análisis de las amenazas	2 días	vie 05/04/13	lun 08/04/13	36
Identificación riesgo residual y aceptable	2 días	mar 09/04/13	mié 10/04/13	37
Elaboración análisis de riesgos	4 días	jue 11/04/13	mar 16/04/13	38
Resultados fase 3	1 día	mié 17/04/13	mié 17/04/13	39

Fase4 - Propuesta de proyectos	**18 días**	**mié 17/04/13**	**vie 10/05/13**	
Elaboración de propuestas mejora	5 días	mié 17/04/13	mar 23/04/13	39
Resultados fase 4	**1 día**	**vie 10/05/13**	**vie 10/05/13**	
Fase5 - Auditoria cumplimiento ISO/IEC 27000	**23 días**	**mié 24/04/13**	**vie 24/05/13**	
Recogida de información.	2 días	mié 24/04/13	jue 25/04/13	42
Análisis de controles establecidos.	6 días	vie 26/04/13	vie 03/05/13	45
Análisis diferencial ISO/IEC 27002.	6 días	lun 06/05/13	lun 13/05/13	46
Revisión de documentación necesaria ISO/IEC 27000.	3 días	mar 14/05/13	jue 16/05/13	47
Reunión con cliente: Resumen del estado actual.	3 días	vie 17/05/13	mar 21/05/13	48
Resultados fase 5	**1 día**	**vie 24/05/13**	**vie 24/05/13**	
Preparación de la memoria TFM	**6 días**	**mié 22/05/13**	**mié 29/05/13**	
Revisión completa del documento.	2 días	mié 22/05/13	jue 23/05/13	49
Análisis de la extensión.	1 día	vie 24/05/13	vie 24/05/13	52
Corrección de errores.	1 día	lun 27/05/13	lun 27/05/13	53
Formateo del documento a entregar.	2 días	mar 28/05/13	mié 29/05/13	54
Preparación de la presentación TFM	**6 días**	**jue 30/05/13**	**jue 06/06/13**	
Resumen del TFM	2 días	jue 30/05/13	vie 31/05/13	55
Distinción de puntos importantes.	1 día	lun 03/06/13	lun 03/06/13	57
Documentación y redacción: Presentación TFM	2 días	mar 04/06/13	mié 05/06/13	58
Formateo del documento a entregar.	1 día	jue 06/06/13	jue 06/06/13	59
Cierre	**1 día**	**vie 07/06/13**	**vie 07/06/13**	
Fase6 - Presentacion resultados e informes	**1 día**	**vie 07/06/13**	**vie 07/06/13**	
Entrega TFM	1 día	vie 07/06/13	vie 07/06/13	60
Monitorización y control	**70 días?**	**lun 04/03/13**	**vie 07/06/13**	
Informes seguimiento y control	70 días?	lun 04/03/13	vie 07/06/13	
Revisión de tareas establecidas.	70 días	lun 04/03/13	vie 07/06/13	
Re-planificación de tareas.	70 días	lun 04/03/13	vie 07/06/13	

Capítulo 2.

Sistema de gestión documental

2.1.- Introducción.

Todos los sistemas de gestión tienen como base un sistema de gestión documental según indica el cumplimiento normativo, en este capítulo desarrollaremos la documentación básica para implementar un SGSI según la norma ISO/IEC 27001 y se proporcionarán las pautas para trabajar la biblioteca.

La existencia de todos estos documentos constituyen una evidencia imprescindible para certificar que el SGSI está funcionando correctamente.

2.2.- Política de seguridad.

Incluida en el Anexo A de este documento.

2.3.- Procedimiento de auditorías internas.

Incluido en el Anexo B de este documento.

2.4.- Gestión de indicadores.

En esta sección vamos a definir los indicadores necesarios para medir la eficiencia de los controles de seguridad implantados.

Para ello, uno de los indicadores de la buena aplicación de los controles de seguridad es la documentación generada por el SGSI. A continuación enumeramos un listado de la documentación que debería estar presente en nuestra biblioteca documental.

Nombre

Código ético sobre el uso de los medios informáticos

Estándares de autenticación

Estándares de cifrado

Estándares de seguridad durante el desarrollo SW

Estrategia de continuidad de suministro electrico

Guía de buen uso de las contraseñas

Guía de clasificación de la información

Guía para el uso de dispositivos portátiles en lugares públicos

Guía sobre protección de datos en entorno de pruebas

Guía sobre SW malicioso

Manual de bienvenida

Manual de seguridad

Manual de seguridad LOPD

Marco de referencia de Planes de Continuidad

Método de análisis y gestión de riesgos

Método de auditoría

Metodología de desarrollo

Norma de cableado seguro

Norma de revisión de los servicios de suministro

Norma de uso de los servicios ofimáticos

Norma para el uso de material informático fuera de las oficinas

Norma para la gestión de contraseñas

Norma para procedimiento de inicio de sesión

Norma sobra carga y descarga de material

Norma sobre cambios en paquetes de SW

Norma sobre copias de respaldo

Norma sobre intercambio de información

Norma sobre manejo de soportes extraíbles

Norma sobre perímetros de seguridad

Norma sobre protección de los fuentes

Norma sobre publicación de información

Norma sobre ubicación de equipos

Normas de seguridad en áreas seguras

Normas de seguridad en el edificio

Planes-acuerdos de recuperación

Política de control de accesos

Política de medios portátiles

Política de puesto de trabajo despejado y pantalla limpia

Política de seguridad de la información

Política de teletrabajo

Política de uso de los controles criptográficos

Política de uso de los servicios de red

Política sobre Propiedad intelectual

Procedimiento de acciones correctivas y preventivas

Procedimiento de actualización y revisión de los Planes de Continuidad del Negocio

Procedimiento de asignación de contraseñas

Procedimiento de asignación de privilegios

Procedimiento de autorización de recursos para el tratamiento de la información

Procedimiento de autorización para el uso externo de recursos informáticos

Procedimiento de borrado o reutilización seguro

Procedimiento de cese o cambio de puesto de trabajo

Procedimiento de comprobación de antecedentes de RRHH

Procedimiento de comprobación de antecedentes en contratistas

Procedimiento de comprobación y pruebas de las copias de respaldo

Procedimiento de comprobación y registro de entrada y salida de material

Procedimiento de comunicación y aceptación de responsabilidades de los empleados

Procedimiento de comunicación y aceptación de responsabilidades de los terceros contratados

Procedimiento de control de cambios en aplicativos

Procedimiento de copias de respaldo

Procedimiento de corrección de vulnerabilidades técnicas

Procedimiento de gestión de cambios en los niveles de servicio

Procedimiento de gestión de capacidades

Procedimiento de gestión de incidencias

Procedimiento de gestión de la documentación

Procedimiento de gestión de soportes

Procedimiento de gestión del mantenimiento

Procedimiento de inclusión de requerimientos de seguridad en Aplicaciones

Procedimiento de marcado/etiquetado

Procedimiento de monitorización y revisión de los servicios

Procedimiento de obtención y presentación de evidencias

Procedimiento de paso a producción de HW-SW

Procedimiento de publicación de información

Procedimiento de registro de usuarios

Procedimiento de reparación contra SW malicioso

Procedimiento de reporte de incidencias

Procedimiento de revisión de accesos a áreas seguras

Procedimiento de revisión de derechos de acceso

Procedimiento de revisión de la monitorización

Procedimiento de revisión de la política de seguridad

Procedimiento de revisión de las incidencias

Procedimiento de revisión de logs

Procedimiento de revisión del inventario de activos

Procedimiento de revisiones de las obligaciones y de los acuerdos

Procedimiento de uso de datos reales en pruebas

Procedimiento disciplinario

Procedimientos de operaciones de T.I documentados

Procedimientos organizativos de adecuación a la Ley

A parte de la documentación se asignan los siguientes indicadores adicionales:

Control	Indicador
5.1.2	Número de revisiones de la política de seguridad por parte de la Dirección.
6.1.8 15.3.1	Número de auditorías realizadas (internas y externas). Número de “No conformidades” identificadas en las auditorías.
8.2.2	Número de cursos y asistentes por curso.
9.1.4	Número de chequeos de mantenimiento de los sistemas anti-incendio (Anuales)
9.1.2	% de accesos fallidos/irregulares a las instalaciones físicas. *Cálculo:* [(Accesos Fallidos-Irregulares / Accesos Totales) * 100] Valor Tolerable: 20%
9.2.1	% de dispositivos extraviados respecto del total.

11.3.2 11.7.1 15.2.1	*Cálculo:* [(Número de dispositivos extraviados / Número de dispositivos inventariados) * 100] Valor Tolerable: 10%
9.2.6	Número de equipos / dispositivos reutilizados. *Cálculo:* [Número de equipos-dispositivos reutilizados / Número de equipos-dispositivos retirados+reutilizados] Valor Tolerable: 75%
10.1.1 10.8.1	% de documentación de seguridad elaborada respecto a la esperada. *Cálculo:* [(Número documentos seguridad / Número ideal de documentos seguridad) * 100] Valor Tolerable: 75%
10.1.2 12.4.1 12.5.1	Número de cambios fallidos. *Cálculo:* [(Número de cambios fallidos / Número total de cambios) *100] Valor Tolerable: 10% Número de rollbacks aplicados correctamente. *Cálculo:* [(Número de cambios fallidos / Número total de cambios) *100] Valor Tolerable: 90%
10.3.1	% de espacio libre en unidades de disco. *Cálculo:* [(MB libres discos / MB total discos) *100] Valor Tolerable:20% % de memoria disponible en servidores. *Cálculo:* [(MB libres memoria / MB total memoria) *100] Valor Tolerable:20% % de uso de procesador en servidores.
10.4.1 10.4.2	% de equipos sin antivirus instalado. *Cálculo:* [(Número equipos sin antivirus / Número total equipos) *100] Valor Tolerable:10%

	Número de virus detectados en servidores / estaciones de trabajo (mensuales)
10.5.1	Número de copias de seguridad y volumen de datos copiados. % de copias de seguridad fallidas (por semanas) *Cálculo:* [(Número copias fallidas / Número total copias) *100] Valor Tolerable:10%
10.7.2	Número de soportes retirados.
10.8.2	Número de acuerdos de intercambio de datos.
10.9.1 10.9.2	Número de transacciones económicas. % de transacciones económicas fallidas. *Cálculo:* [(Número transacciones fallidas / Número total transacciones) *100] Valor Tolerable:5%
10.10.2	% de sistemas monitorizados respecto del total. *Cálculo:* [(Número sistemas monitorizados / Número total sistemas) *100] Valor Tolerable: 10%
11.2.1 11.6.1	% de accesos fallidos/irregulares a las aplicaciones. *Cálculo:* [(Número accesos fallidos / Número total accesos) *100] Valor Tolerable: 20%
11.2.1 11.2.2 11.2.4	Número de usuarios de baja en un año. Número de personas con permisos de Administrador/root.
11.4.2 11.4.3 11.4.6	Número de empleados con acceso VPN habilitado.
11.4.3 11.4.6	% de equipos sin asociación a un dominio. *Cálculo:* [(Número equipos sin asociación dominio / Número total equipos) *100]

	Valor Tolerable: 10%
11.4.5	Número de equipos / dispositivos por sub-red.
11.4.6	% de accesos no autorizados a la red de la organización. *Cálculo:* [(Número accesos no autorizados a la red / Número total de accesos) *100] Valor Tolerable: 20%
11.4.7	Número de rutas por router.
11.5.1 11.5.3	% de servidores sin política de seguridad en contraseñas. *Cálculo:* [(Número servidores sin política seguridad / Número total servidores) *100] Valor Tolerable: 10%
13.1.1 13.2.2	Número de incidentes de seguridad. Tiempo de recuperación medio por indisponibilidad. % de disponibilidad de los sistemas de información. % de disponibilidad de los sistemas de información.
13.2.2	% de problemas (incidencias repetitivas) identificados. *Cálculo:* [(Número de problemas / Número de incidencias) *100] Valor Tolerable: 5%
15.1.1 15.1.2	% de aplicaciones instaladas por licencia. *Cálculo:* [(Número de aplicaciones instaladas / Número de licencias) *100] Valor Tolerable: 90%
15.1.3 15.1.4	Número de cláusulas de confidencialidad para contratos, correos y otros documentos (plantillas).
Todos	% de reducción de amenazas anual.

2.5.- Procedimiento de revisión de la dirección.

La implementación de una política de seguridad sin el apoyo de la Dirección está destinada al fracaso, por ello es imprescindible que la Dirección proporcione medios y apoyo para llevar a cabo cualquier cambio en la cultura de la seguridad.

La Dirección de la organización deberá participar en la toma de decisiones relacionada con la seguridad de la información y hacer un "seguimiento" de los procedimientos, controles, u otros mecanismos implementados para garantizar el buen funcionamiento del SGSI.

Este apartado tiene como objetivo describir cual será el procedimiento de revisión de la dirección como acción indispensable en el SGSI.

- La Dirección realizará, con un periodo inferior a un año, controles para verificar el cumplimiento de todos los estándares, normas y procedimientos establecidos en el SGSI. El Responsable de Seguridad será el encargado de realizar esta revisión.

- El análisis de la situación se realizará al menos sobre las siguientes áreas / controles:

o Comprobación del conocimiento de las normas de seguridad por parte de las personas que acceden a los sistemas de información de la organización.

o Control, revisión y evaluación de registros de: usuarios, incidencias de seguridad, inventario de activos, etc.

o Control de autorizaciones de delegación de funciones relacionadas con la seguridad.

- El Responsable de Seguridad realizará un breve informe sobre la revisión realizada anualmente. En este se incluirán las incidencias y deficiencias detectadas y una relación de soluciones y propuestas de mejora.

- La organización, además de mantener actualizado los documentos del SGSI, y realizará una revisión, teniendo presente los últimos informes de auditoría, las incidencias y las revisiones internas.

- La Dirección se encargará de revisar el resultado de las auditorías internas anuales y hacer un seguimiento de las acciones correctivas (al menos semestralmente). Se actuará de la misma manera con las auditorías externas con una frecuencia de 3 años, haciendo un seguimiento de las acciones al menos de forma anual.

- De forma puntual se solicitará (al menos una vez al año) un resumen de los indicadores de seguridad y se analizarán en el comité de seguridad.

2.6.- Gestión de roles y responsabilidades.

El organigrama de la organización, la asignación de puestos de trabajo y las funciones desarrolladas por cada uno de estos se hallan descritas en la descripción de la empresa, en este apartado desarrollaremos las funciones y obligaciones del personal clave que interactúa con el SGSI.

Como norma general se entenderá que las normas y obligaciones afectan por igual a todos (internos y externos) salvo se indique expresamente lo contrario (bien desarrollado o mediante una excepción).

Cumpliendo con la obligación de dar a conocer las normas de seguridad y las funciones de cada puesto de trabajo, el responsable de seguridad comunicará a las partes afectadas el contenido de la Política de Seguridad y establecerá los medios y recursos necesarios para su entendimiento.

2.6.1.- Comité de seguridad.

El comité de seguridad multi-disciplina compuesto de los diferentes responsables de la organización, sus funciones serán las siguientes:

- Implantar las directrices del comité de dirección.
- Asignar roles y funciones en materia de seguridad.
- Presentar la aprobación de políticas, normas y responsabilidades en materia de seguridad.
- Validar el mapa de riesgos y sus acciones.
- Validar el plan director de seguridad.
- Supervisar el plan de continuidad del negocio.
- Velar por el cumplimiento de la legislación vigente en materia de seguridad.
- Promover la formación y cultura de seguridad.
- Aprobar y revisar periódicamente el SGSI.

En nuestra organización estará compuesto por las siguientes personas:

- Representante de la dirección.
- Responsable de Seguridad de la Organización.
- Responsable de Explotación de Sistemas.
- Responsable de Desarrollo y proyectos.
- Responsable de Infraestructuras, Sistemas y Comunicaciones.
- Responsable de Jurídico.
- Responsable de Administración y Personal.
- Equipo de asesores especializados en seguridad.

2.6.2.- Funciones y obligaciones del personal.

Las funciones que los empleados de la organización desarrollen, en relación a los sistemas de información, serán aquellas para las que hayan sido expresamente autorizados, independientemente de las limitaciones (organizativas, técnicas, automáticas, etc.) que se establecen para controlar sus accesos.

Los empleados y las entidades relacionadas con los sistemas de información estarán obligados a respetar las normas, tanto con carácter general como específico. A efectos de garantizar el cumplimiento de estas obligaciones, se ha definido una política general, contenida en el presente documento.

Independientemente de las funciones y responsabilidades específicas asignadas a los usuarios y/o entidades sobre los respectivos sistemas de información, a cualquier empleado de la organización o entidad colaboradora se les exige con carácter general:

- Confidencialidad, respecto a la información y documentación que reciben y/o usan perteneciente a la organización o de su responsabilidad.

- No incorporar a la organización información o datos sin autorización de la entidad.

- No ceder datos de carácter personal ni usarlos con una finalidad distinta por la que han sido recogidos (fichero).

- Comunicar al responsable de seguridad cualquier incidencia respecto a la seguridad de la información.

2.6.2.1- Personal con acceso privilegiado y personal técnico.

El personal técnico que administra el sistema de acceso a los sistemas de información no tiene por qué estar presente en todos los casos, siendo en algunas ocasiones subcontratado o asumido por otros roles. En cualquiera de los casos, se podría clasificar en las siguientes categorías según sus funciones:

Administradores (red, sistemas operativos, aplicaciones y bases de datos): serán los responsables de los máximos privilegios, y por tanto con alto riesgo de que una actuación errónea o incorrecta pueda afectar a los sistemas. Tendrá acceso a todos los sistemas necesarios para desarrollar su función y resolver los problemas que surjan.

Operadores (red, sistemas operativos, aplicaciones y bases de datos): sus actuaciones están limitadas dentro de los sistemas de información y generalmente supervisadas por los administradores, utilizarán las herramientas de gestión disponibles y autorizadas. En principio no deben tener acceso a los ficheros que contengan datos personales salvo la tarea lo requiera.

Mantenimiento de los sistemas y aplicaciones: personal responsable de la resolución de incidencias en sistemas hardware y software. En principio no deben tener acceso a los datos de los sistemas de información salvo la tarea lo requiera.

Como cualquier otro empleado de la organización el personal con acceso privilegiado y personal técnico debe cumplir con las obligaciones establecidas en el documento, extremando aún más las precauciones al realizar acciones en el sistema de información. Para estas categorías laborales serán de aplicación las normas y obligaciones establecidas para todo el personal con perfil de usuario.

A continuación identificaremos algunas de las funciones y responsabilidades exclusivas del personal de técnico y con acceso privilegiado:

- Procurar que la integridad, autentificación, control de acceso auditoría y registro se contemplen e incorporen en el diseño, implantación y operación de los sistemas de información y telecomunicaciones.

- Procurar la confidencialidad y disponibilidad de la información almacenada en los sistemas de información (ya sea de forma electrónica o no) así como su salvaguarda mediante copias de seguridad de una forma periódica.

- Conceder a los usuarios acceso únicamente a los datos y recursos a los que estén autorizados y precisen para el desarrollo de su trabajo.

- No acceder a los datos aprovechando sus privilegios sin autorización del Responsable de Seguridad.

- Custodiar con especial cuidado los identificadores y contraseñas que dan acceso a los sistemas con privilegios de administrador.

- Notificar las incidencias oportunas ante cualquier violación de las normas de seguridad o vulnerabilidades detectadas en los sistemas.

- No revelar a terceros ninguna posible debilidad en materia de seguridad de los sistemas sin previa autorización del Responsable de Seguridad y con el propósito de su corrección.

2.6.2.2- Personal con perfil de usuario.

Los usuarios con acceso a los sistemas de información y con acceso a los sistemas de información sólo podrán acceder a aquellos que estén autorizados y sean necesarios para el desempeño de su función.

Por tanto, todos los usuarios involucrados en el uso de sistemas de información deberán cumplir con las siguientes obligaciones, dependiendo de la función que realicen:

- Guardar el secreto de la información a la que tuviere acceso, incluso aún después de haber finalizado la relación con la organización.

- Conocer y cumplir la normativa interna en cuestión de seguridad de la información y especialmente la referida a la protección de datos de carácter personal.

- Conocer y atenerse a las responsabilidades y consecuencias en caso de incurrir en el incumplimiento de la normativa interna.

- Respetar los procedimientos, mecanismos y dispositivos de seguridad, evitando cualquier intento de acceso no autorizado o recursos no permitidos.

- Usar de forma adecuada los procedimientos, mecanismos y controles de identificación y autentificación ante los sistemas de información. En el caso particular de usuarios y contraseñas, se deberá cumplir lo específicamente previsto en la normativa adjunta (sintaxis, distribución, custodia, etc.).

- Utilizar las contraseñas según las instrucciones recibidas al respecto, tampoco informarlas ni cederlas a terceros ya que son de carácter personal y con uso exclusivo por parte del titular.

- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) ha sido comprometido o está siendo utilizado por otra persona, debe proceder al cambio de contraseña y comunicar la correspondiente incidencia de seguridad.

- Proteger especialmente los datos personales de la organización que con carácter excepcional tuvieran que almacenarse, usarse o trasportarse fuera de trabajo (oficinas de clientes, instalaciones temporales, propio domicilio, etc.).

- Salir o bloquear el acceso de los ordenadores u otros dispositivos similares, cuando se encuentre ausente de su puesto de trabajo.

- Los usuarios deben notificar al Responsable de Seguridad de la organización cualquier incidencia que detecten que afecte o pueda afectar a los datos de los sistemas de información (pérdida de información, acceso no autorizado por otras personas, recuperación de datos, etc.).

- Entregar cuando sea requerido por la organización, y especialmente cuando cause baja en la empresa, las llaves, claves, tarjetas de identificación, material, documentación, equipos dispositivos y cuantos activos sean de propiedad de la empresa.

2.6.3.- Funciones y obligaciones del responsable de seguridad.

El Responsable de Seguridad es la persona la persona que coordina y controla las medidas de seguridad aplicables en la organización.

A continuación enumeraremos las principales funciones asociadas a los Responsables de Seguridad:

- Asesorar en la definición de requisitos sobre las medidas de seguridad que se deben adoptar.

- Validar la implantación de los requisitos de seguridad necesarios.

- Revisar periódicamente los sistemas de información y elaborar un informe de las revisiones realizadas y los problemas detectados.

- Verificar la ejecución de los controles establecidos según lo dispuesto en el documento de seguridad.

- Mantener actualizadas las normas y procedimientos en materia de seguridad de afecten a la organización.

- Definir y comprobar la aplicación del procedimiento de copias de respaldo y recuperación de datos.

- Definir y comprobar la aplicación del procedimiento de notificación y gestión de incidencias.

- Controlar que la auditoría de seguridad se realice con la frecuencia necesaria.

- Analizar los informes de auditoría y si lo considera necesario modificar las medidas correctoras para prevenir incidentes.

- Trasladar los informes de auditoría a la dirección.

- Establecer los controles y medidas técnicas y organizativas para asegurar los sistemas de información.

- Gestionar y analizar las incidencias de seguridad acaecidas en la organización y su registro según el procedimiento indicado en el Documento de Seguridad.

- Coordinar la puesta en marcha de las medidas de seguridad y colaborar en el cumplimiento y difusión del Documento de Seguridad.

2.7.- Metodología de análisis de riesgos.

El análisis de riesgos es la primera y principal tarea de una organización antes de realizar cualquier planteamiento en aspectos de seguridad; evidentemente cualquier análisis de riesgos debe realizarse atendiendo una metodología, ya sea una de mercado o creada específicamente por la organización, en este apartado describiremos como desarrollaremos nuestro método de análisis de riesgos.

En nuestro caso particular nuestra metodología de análisis de riesgos se basará en MAGERIT aunque se personalizarán alguno de los aspectos atendiendo las características de nuestra organización.

Fase 1 - Toma de datos y proceso de información: En esta fase se definirá el alcance y se analizarán los procesos de la organización. Durante este proceso se debe tener en cuenta la granularidad del análisis ya que impactará directamente en el coste del análisis de riesgos.

Fase 2 – Establecimiento de parámetros: Durante esta actividad se identificarán los parámetros que se utilizarán durante el análisis de riesgos; serán los siguientes:

- Valor de los activos: Se asignará un valor económico al objeto analizado. A la hora de asignar el valor económico se tendrá en cuenta el valor de reposición, configuración, uso y pérdida de oportunidad.

Valoración	Rango	Valor
Muy Alta	Valor > 200.000 €	300.000 €
Alta	100.000 € < Valor > 200.000 €	150.000 €
Media	50.000 € < Valor > 100.000 €	75.000 €
Baja	10.000 € < Valor > 50.000 €	30.000 €
Muy baja	Valor < 10.000 €	10.000 €

- Vulnerabilidad: La vulnerabilidad se entiende como frecuencia de la ocurrencia de una amenaza. Esta valoración numérica se realizará mediante estimaciones anuales, para ello se aplicará la siguientes fórmula [Vulnerabilidad = Frecuencia estimada / días año]

Vulnerabilidad	Rango	Valor
Frecuencia extrema	1 vez al día	1
Frecuencia Alta	1 vez cada 2 semanas	26/365
Frecuencia Media	1 vez cada 2 meses	6/365
Frecuencia Baja	1 vez cada 6 meses	2/365
Frecuencia Muy baja	1 vez cada año	1/365

- Criticidad: Impacto en la organización si se produce un problema sobre el activo.

Criticidad	Rango	Valor
Crítico	[100-90%]Parada total de todos los servicios o un servicio esencial de la organización. Parada total de la actividad empresarial. Afecta a la imagen de la organización. Causa un daño económico muy elevado.	95 %
Alto	[89-75%]Parada de un servicio no esencial de la organización. Parada parcial de la actividad empresarial. Causa daños económicos elevados.	75 %
Medio	[74-25%]Parada de un departamento o equipo de trabajo. Causa daños económicos medios.	50 %
Bajo	[25-0%]Parada de un puesto de trabajo. No causa daños económicos apreciables.	25 %

- Impacto: Se entiende como impacto el tanto por ciento del activo que se pierde en caso de que un impacto suceda sobre él.

Impacto	Rango
Muy Alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

- Efectividad del control de seguridad: Este parámetro indicará la efectividad de las medidas de protección de los riesgos, pueden reducir la vulnerabilidad o el impacto dependiendo del control.

Variación Impacto/Vulnerabilidad	Valor
Muy Alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

Fase 3 – Análisis de activos: Durante esta fase se identificaran los activos de la empresa que se requieren para llevar a cabo la actividad. Se debe tener presente que en la organización puede poseer distintos tipos de activos (físicos, lógicos o de personal, infraestructura, intangibles, etc.) y se valorarán teniendo en cuenta los parámetros de valoración de activos.

Fase 4 – Análisis de amenazas: Las amenazas son aquellas situaciones que pueden provocar un problema de seguridad. Las amenazas dependen del tipo de organización así como de su "configuración" y características. Según MAGERIT las amenazas se pueden clasificar en cuatro grandes grupos:

- Accidentes: Situaciones no provocadas voluntariamente y que la mayor parte de las veces no puede evitarse. Por ejemplo: incendio, inundación, etc.
- Errores: Situaciones provocadas involuntariamente provocadas por el desarrollo de las actividades cotidianas ya sea por desconocimiento y/o descuido. Por ejemplo: Errores de desarrollo, errores de actualización, etc.
- Amenazas intencionales presenciales: Son provocadas por el propio personal de la organización de forma voluntaria y conociendo el daño que puede ocasionar. Por ejemplo: Accesos no autorizados, filtración de datos, etc.
- Amenazas intencionales remotas: Son provocadas por terceras personas ajenas a la organización con el objetivo de dañarla. Ejemplos: Suplantación de origen, gusanos, DoS, etc.

Fase 5 – Establecimiento de las vulnerabilidades: Las vulnerabilidades son aquellos agujeros que permiten explotar una amenaza dañando un activo. En la metodología MAGERIT no es necesario listar las vulnerabilidades pero sí tenerlas identificadas para poder estimar la frecuencia de la ocurrencia de una determinada amenaza sobre un activo.

Fase 6 – Valoración de impactos: Las amenazas pueden dañar los activos de la organización, es necesario cuantificar el impacto de una amenaza sobre el activo. Por ejemplo: daño económico, pérdidas cualitativas, etc.

Fase 7 – Análisis de riesgos intrínseco: Llegados a este punto y habiendo identificado los valores anteriores podemos realizar el estudio de riesgos actuales de la organización y para ello utilizaremos la siguiente fórmula:

Riesgo = Valor del activo x Vulnerabilidad x Impacto

Debemos recordar que los riesgos intrínsecos son aquellos a los que la organización está expuesta sin tener en consideración las medidas de seguridad que podamos implantar.

Nivel aceptable de riesgos.

Durante esta fase se establecerá el nivel aceptable de riesgos que se basará en la siguiente tabla:

Nivel aceptable de riesgo	**Valor**
Alto	75%
Medio	50%
Bajo	25%

Se asignarán los niveles aceptables de riesgos de forma manual y siempre estarán alineados con la criticidad del activo en la organización.

Fase 8 – Influencia de las salvaguardas: Tras identificar los riesgos se iniciará la fase de gestión del riesgo donde debemos analizar cada uno de los riesgos y aplicar la mejor solución técnica que permita reducirlos al máximo.

Utilizaremos dos tipos de salvaguardas:

- Preventivas (reducen las vulnerabilidades): Nueva vulnerabilidad = Vulnerabilidad x % disminución vulnerabilidad.
- Correctivas (reducen el impacto): Nuevo impacto = Impacto x % disminución impacto.

Fase 9 – Análisis de riesgos efectivos: Una vez finalizada la aplicación de salvaguardas se deberá calcular el riesgo efectivo incluyendo la reducción resultante después de la aplicación de las salvaguardas.

Para el cálculo del riesgo efectivo se utilizará la siguiente fórmula:

Valor efectivo × Nueva vulnerabilidad × Nuevo Impacto = Valor activo × (Vulnerabilidad × Porcentaje de disminución de vulnerabilidad) × (Impacto × Porcentaje de disminución de impacto) = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución de impacto

Fase 10 – Gestión de riesgos: La última fase del análisis de riesgos comienza con la gestión del riesgo, es decir la toma de decisiones de la organización ante las medidas de seguridad a aplicar. Ante la selección de las medidas de seguridad se debe tener presente el umbral del riesgo aceptable y el coste de la aplicación de las medidas de seguridad. A la hora de gestionar los riesgos existen distintas estrategias que a continuación enumeraremos:

- Reducirlos
- Transferirlos
- Aceptarlos

A la hora de gestionar los riesgos será necesario establecer un plan de acción que contenga al menos la siguiente información:

- Establecimiento de prioridades
- Análisis coste / beneficio
- Selección de controles
- Asignación de responsabilidades
- Implantación de controles

2.8.-Declaración de aplicabilidad.

Nº	Objeto de control	Control	Aplica
5.1	**Política de seguridad de la información**	**Objetivo: La Dirección proporcionará indicaciones y dará apoyo la seguridad de la información de acuerdo con los requisitos del negocio y con la legislación y las normativas aplicables.**	
5.1.1	Documento de política de seguridad de la información	La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados y terceros afectados.	SI
5.1.2	Revisión de la política de seguridad e la información	La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	SI
6.1	**Organización interna**	**Objetivo: Gestionar la seguridad de la información dentro de la organización**	
6.1.1	Compromiso de la Dirección con la seguridad de la información.	La Dirección debe prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información.	SI
6.1.2	Coordinación de la seguridad de la información	Las actividades relativas a la seguridad de la información deben ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones de trabajo.	SI
6.1.3	Asignación de responsabilidades relativas a la seguridad de la información	Deben definirse claramente todas las responsabilidades relativas a la seguridad de la información.	SI
6.1.4	Proceso de autorización de recursos para el tratamiento de la información	Para cada nuevo recurso de tratamiento de la información, debe definirse e implantarse un proceso de autorización por parte de la Dirección.	SI
6.1.5	Acuerdos de confidencialidad	Debe determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información	SI
6.1.6	Contacto con las autoridades	Deben mantenerse los contactos adecuados con las autoridades competentes	SI
6.1.7	Contacto con grupos de especial interés	Deben mantenerse los contactos adecuados con grupos de interés especial u otros foros, y asociaciones profesionales especializados en seguridad.	SI
6.1.8	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	SI

6.2	**Terceros**	**Objetivo: Mantener la seguridad de la información de la organización y de los dispositivos de tratamiento de la información que son objeto de acceso, procesado, comunicación o gestión por terceros.**	
6.2.1	Identificación de los riesgos derivados del acceso de terceros	Deben identificarse los riesgos para la información y para los dispositivos de tratamiento de la información de la organización derivados de los procesos de negocio que requieran de terceros, e implantar los controles apropiados antes de otorgar el acceso.	SI
6.2.2	Tratamiento de la seguridad en la relación con los clientes	Deben tratarse todos los requisitos de seguridad identificados antes de otorgar acceso a los clientes a los activos o a la información de la organización.	SI
6.2.3	Tratamiento de la seguridad en contratos con terceros	Los acuerdos con terceros que conlleven acceso, procesado, comunicación o gestión, bien de la información de la organización, o de los recursos de tratamiento de la información, o bien la incorporación de productos o servicios a los recursos de tratamiento de la información, deben cubrir todos los requisitos de seguridad pertinentes.	SI
7.1	**Responsabilidad sobre los activos**	**Objetivo: Conseguir y mantener una protección adecuada de los activos de la organización.**	
7.1.1	Inventario de activos	Todos los activos deben estar claramente identificados y debe elaborarse y mantenerse un inventario de todos los activos importantes.	SI
7.1.2	Propiedad de los activos	Toda la información y activos asociados con los recursos para el tratamiento de la información deben tener un propietario que forme parte de la organización y haya sido designado como propietario.	SI
7.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implantar las reglas para el uso aceptable de la información y los activos asociados con los recursos para el tratamiento de la información.	SI
7.2	**Clasificación de la información**	**Objetivo: Asegurar que la información recibe un nivel adecuado de protección.**	
7.2.1	Directrices de clasificación	La información debe ser clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización.	SI
7.2.2	Etiquetado y manipulado de la información	Se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	SI
8.1	**Antes del empleo**	**Objetivo: Asegurar que los empleados, los contratistas y los terceros conocen y comprenden sus responsabilidades, y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos.**	
8.1.1	Funciones y responsabilidades	Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros se deben definir y documentar de acuerdo con la política de seguridad de la información de la organización.	SI

8.1.2	Investigación de antecedentes	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo, de los contratistas o de los terceros, se debe llevar a cabo de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos considerados.	SI
8.1.3	Términos y condiciones de contratación	Como parte de sus obligaciones contractuales, los empleados, los contratistas y los terceros deben aceptar y firmar los términos y condiciones de su contrato de trabajo, que debe establecer sus responsabilidades y las de la organización en lo relativo a seguridad de la información.	SI
8.2	**Durante el empleo**	**Objetivo: Asegurar que todos los empleados, contratistas y terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización, en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano.**	
8.2.1	Responsabilidades de la Dirección	La Dirección debe exigir a los empleados, contratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización.	SI
8.2.2	Concienciación, formación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deben recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.	SI
8.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad.	SI
8.3	**Cese del empleo o cambio de puesto de trabajo**	**Objetivo: Asegurar que los empleados, contratistas y terceros abandonan la organización o cambian de puesto de trabajo de una manera ordenada.**	
8.3.1	Responsabilidad del cese o cambio	Las responsabilidades para proceder al cese en el empleo o al cambio de puesto de trabajo deben estar claramente definidas y asignadas.	SI
8.3.2	Devolución de activos	Todos los empleados, contratistas y terceros deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	SI
8.3.3	Retirada de los derechos de acceso	Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados, contratistas y terceros deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o bien deben ser adaptados a los cambios producidos.	SI
9.1	**Áreas seguras**	**Objetivo: Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización.**	
9.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad (barreras, muros, puertas de entrada con control de acceso a través de tarjeta, o puestos de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.	SI
9.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	SI
9.1.3	Seguridad de oficinas, despachos e instalaciones.	Se deben diseñar y aplicar las medidas de seguridad física para las oficinas, despachos e instalaciones.	SI

9.1.4	Protección contra las amenazas externas y de origen ambiental.	Se debe diseñar y aplicar una protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.	SI
9.1.5	Trabajo en áreas seguras	Se deben diseñar e implantar una protección física y una serie de directrices para trabajar en las áreas seguras.	SI
9.1.6	Áreas de acceso público y de carga y descarga	Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, a través de los que personal no autorizado puede acceder a las instalaciones, y si es posible, dichos puntos se deben aislar de las instalaciones de tratamiento de la información para evitar los accesos no autorizados.	SI
9.2	**Seguridad de los equipos**	**Objetivo: Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización.**	
9.2.1	Emplazamiento y protección de equipos	Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental así como las ocasiones de que se produzcan accesos no autorizados.	SI
9.2.2	Instalaciones de suministro	Los equipos deben estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro.	SI
9.2.3	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debe estar protegido frente a interceptaciones o daños.	SI
9.2.4	Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.	SI
9.2.5	Seguridad de los equipos fuera de las instalaciones	Teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización, deben aplicarse medidas de seguridad a los equipos situados fuera dichas instalaciones.	SI
9.2.6	Reutilización o retirada segura de equipos	Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han borrado o sobreescrito de manera segura, antes de su retirada.	SI
9.2.7	Retirada de materiales propiedad de la empresa	Los equipos, la información o el software no deben sacarse de las instalaciones, sin una autorización previa.	SI
10.1	**Responsabilidades y procedimientos de operación**	**Objetivo: Asegurar el funcionamiento correcto y seguro de los recursos de tratamiento de la información.**	
10.1.1	Documentación de los procedimientos de operación.	Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.	SI
10.1.2	Gestión de cambios	Deben controlarse los cambios en los recursos y en los sistemas de tratamiento de la información.	SI
10.1.3	Segregación de tareas	Las tareas y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	SI
10.1.4	Separación de los recursos de desarrollo, prueba y operación.	Deben separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado o los cambios en el sistema en producción.	SI

10.2	**Gestión de la provisión de servicios por terceros**	**Objetivo: Implantar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros.**	
10.2.1	Provisión de servicios	Se debe comprobar que los controles de seguridad, las definiciones de los servicios y los niveles de provisión, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero.	SI
10.2.2	Supervisión y revisión de los servicios prestados por terceros	Los servicios, informes y registros proporcionados por un tercero deben ser objeto de supervisión y revisión periódicas, y también deben llevarse a cabo auditorias periódicas.	SI
10.2.3	Gestión del cambio en los servicios prestados por terceros	Se deben gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos.	SI
10.3	**Planificación y aceptación del sistema**	**Objetivo: Minimizar el riesgo de fallos de los sistemas.**	
10.3.1	Gestión de capacidades	La utilización de los recursos se debe supervisar y ajustar así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	SI
10.3.2	Aceptación del sistema	Se deben establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y se deben llevar a cabo pruebas adecuadas de los sistemas durante el desarrollo y previamente a la aceptación.	SI
10.4	**Protección contra código malicioso y descargable**	**Objetivo: Proteger la integridad del software y de la información.**	
10.4.1	Controles contra el código malicioso	Se deben implantar controles de detección, prevención y recuperación que sirvan como protección contra código malicioso y se deben implantar procedimientos adecuados de concienciación del usuario.	SI
10.4.2	Controles contra el código descargado en el cliente	Cuando se autorice el uso de código descargado en el cliente, la configuración debe garantizar que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida, y se debe evitar que se ejecute el código no autorizado.	SI
10.5	**Copias de seguridad**	**Objetivo: Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información.**	
10.5.1	Copias de seguridad de la información	Se deben realizar copias de seguridad de la información y del software, y se deben probar periódicamente conforme a la política de copias de seguridad acordada.	SI
10.6	**Gestión de la seguridad de las redes**	**Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.**	
10.6.1	Controles de red	Las redes deben estar adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo la información en tránsito.	SI
10.6.2	Seguridad de los servicios de red	Se deben identificar las características de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en todos los acuerdos relativos a servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	SI
10.7	**Manipulación de los soportes**	**Objetivo: Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización.**	
10.7.1	Gestión de soportes	Se deben establecer procedimientos para la gestión de los	SI

	extraíbles	soportes extraíbles.	
10.7.2	Retirada de soportes	Los soportes deben ser retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos.	SI
10.7.3	Procedimientos de manipulación de la información	Deben establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.	SI
10.7.4	Seguridad de la documentación del sistema	La documentación del sistema debe estar protegida contra accesos no autorizados.	SI
10.8	**Intercambio de información**	**Objetivo: Mantener la seguridad de la información y del software intercambiados dentro de una organización y con un tercero.**	
10.8.1	Políticas y procedimientos de intercambio de información	Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	SI
10.8.2	Acuerdos de intercambio	Deben establecerse acuerdos para el intercambio de información y de software entre la organización y los terceros.	SI
10.8.3	Soportes físicos en tránsito	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	SI
10.8.4	Mensajería electrónica	La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	SI
10.8.5	Sistemas de información empresariales	Deben formularse e implantarse políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información empresariales.	SI
10.9	**Servicios de comercio electrónico**	**Objetivo: Garantizar la seguridad de los servicios de comercio electrónico, y el uso seguro de los mismos**	
10.9.1	Comercio electrónico	La información incluida en el comercio electrónico que se transmita a través de redes públicas debe protegerse contra las actividades fraudulentas, las disputas contractuales, y la revelación o modificación no autorizada de dicha información.	SI
10.9.2	Transacciones en línea	La información contenida en las transacciones en línea debe estar protegida para evitar transmisiones incompletas, errores de direccionamiento, alteraciones no autorizadas de los mensajes, la revelación, la duplicación o la reproducción no autorizadas del mensaje.	SI
10.9.3	Información públicamente disponible	La integridad de la información puesta a disposición pública se debe proteger para evitar modificaciones no autorizadas.	SI
10.1	**Supervisión**	**Objetivo: Detectar las actividades de tratamiento de la información no autorizadas.**	
10.10.1	Registro de auditorias	Se deben generar registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deberían mantener estos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.	SI
10.10.2	Supervisión del uso del sistema	Se deben establecer procedimientos para supervisar el uso de los recursos de tratamiento de la información y se deben revisar periódicamente los resultados de las actividades de supervisión.	SI
10.10.3	Protección de la información de los registros	Los dispositivos de registro y la información de los registros deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	SI

10.10.4	Registros de administración y operación	Se deben registrar las actividades del administrador del sistema y de la operación del sistema.	SI
10.10.5	Registro de fallos	Los fallos deben ser registrados y analizados y se deben tomar las correspondientes acciones.	SI
10.10.6	Sincronización del reloj	Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.	SI
11.1	**Requisitos de negocio para el control de acceso**	**Objetivo: Controlar el acceso a la información**	
11.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso.	SI
11.2	**Gestión de acceso de usuario**	**Objetivo: Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información**	
11.2.1	Registro de usuario	Debe establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.	SI
11.2.2	Gestión de privilegios	La asignación y el uso de privilegios deben estar restringidos y controlados.	SI
11.2.3	Gestión de contraseñas de usuario	La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal.	SI
11.2.4	Revisión de los derechos de acceso de usuario	La Dirección debe revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.	SI
11.3	**Responsabilidades de usuario**	**Objetivo: Prevenir el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de información o de recursos de tratamiento de la información.**	
11.3.1	Uso de contraseñas	Se debe requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de las contraseñas.	SI
11.3.2	Equipo de usuario desatendido	Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.	SI
11.3.3	Política de puesto de trabajo despejado y pantalla limpia	Debe adoptarse una política de puesto de trabajo despejado de papeles y de soportes de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de tratamiento de la información.	SI
11.4	**Control de acceso a la red**	**Objetivo: Prevenir el acceso no autorizado a los servicios en red.**	
11.4.1	Política de uso de los servicios en red	Se debe proporcionar a los usuarios únicamente el acceso a los servicios para que los que hayan sido específicamente autorizados.	SI
11.4.2	Autenticación de usuario para conexiones externas	Se deben utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos.	SI
11.4.3	Identificación de los equipos en las redes	La identificación automática de los equipos se debe considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos.	SI
11.4.4	Diagnóstico remoto y protección de los puertos de configuración	Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración.	SI
11.4.5	Segregación de las redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en redes.	SI

11.4.6	Control de la conexión a la red	En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debe restringirse la capacidad de los usuarios para conectarse a la red, esto debe hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones empresariales (véase 11.1).	SI
11.4.7	Control de encaminamiento (routing) de red	Control Se deben implantar controles de encaminamiento (routing) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales.	SI
11.5	**Control de acceso al sistema operativo**	**Objetivo: Prevenir el acceso no autorizado a los sistemas operativos**	
11.5.1	Procedimientos seguros de inicio de sesión	El acceso a los sistemas operativos se debe controlar por medio de un procedimiento seguro de inicio de sesión.	SI
11.5.2	Identificación y autenticación de usuario	Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal y exclusivo, y se debe elegir una técnica adecuada de autenticación para confirmar la identidad solicitada del usuario.	SI
11.5.3	Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas de calidad.	SI
11.5.4	Uso de los recursos del sistema	Se debe restringir y controlar de una manera rigurosa el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	SI
11.5.5	Desconexión automática de sesión.	Las sesiones inactivas deben cerrarse después de un periodo de inactividad definido.	SI
11.5.6	Limitación del tiempo de conexión	Para proporcionar seguridad adicional a las aplicaciones de alto riesgo, se deben utilizar restricciones en los tiempos de conexión.	SI
11.6	**Control de acceso a las aplicaciones y a la información**	**Objetivo: Prevenir el acceso no autorizado a la información que contienen las aplicaciones.**	
11.6.1	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida.	SI
11.6.2	Aislamiento de sistemas sensibles	Los sistemas sensibles deben tener un entorno dedicado (aislado) de ordenadores.	SI
11.7	**Ordenadores portátiles y teletrabajo**	**Objetivo: Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y servicios de teletrabajo.**	
11.7.1	Ordenadores portátiles y comunicaciones móviles	Se debe implantar una política formal y se deben adoptar las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles.	SI
11.7.2	Teletrabajo	Se debe redactar e implantar, una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondientes.	SI
12.1	**Requisitos de seguridad de los sistemas de información**	**Objetivo: Garantizar que la seguridad está integrada en los sistemas de información.**	

12.1.1	Análisis y especificación de los requisitos de seguridad	En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deben especificar los requisitos de los controles de seguridad.	SI
12.2	**Tratamiento correcto de las aplicaciones**	**Objetivo: Evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones.**	
12.2.1	Validación de los datos de entrada	La introducción de datos en las aplicaciones debe validarse para garantizar que dichos datos son correctos y adecuados.	SI
12.2.2	Control del procesamiento interno	Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deben incorporar comprobaciones de validación en las aplicaciones.	SI
12.2.3	Integridad de los mensajes	Se deben identificar los requisitos para garantizar la autenticidad y para proteger la integridad de los mensajes en las aplicaciones y se deben identificar e implantar los controles adecuados.	SI
12.2.4	Validación de los datos de salida	Los datos de salida de una aplicación se deben validar para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias.	SI
12.3	**Controles criptográficos**	**Objetivo: Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos.**	
12.3.1	Política de uso de los controles criptográficos	Se debe formular e implantar una política para el uso de los controles criptográficos para proteger la información.	SI
12.3.2	Gestión de claves	Debe implantarse un sistema de gestión de claves para dar soporte al uso de técnicas criptográficas por parte de la organización.	SI
12.4	**Seguridad de los archivos de sistema**	**Objetivo: Garantizar la seguridad de los archivos de sistema.**	
12.4.1	Control del software en explotación	Deben estar implantados procedimientos para controlar la instalación de software en los sistemas en producción o en explotación.	SI
12.4.2	Protección de los datos de prueba del sistema	Los datos de prueba se deben seleccionar cuidadosamente y deben estar protegidos y controlados.	SI
12.4.3	Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas.	SI
12.5	**Seguridad en los procesos de desarrollo y soporte**	**Objetivo: Mantener la seguridad del software y de la información de las aplicaciones.**	
12.5.1	Procedimientos de control de cambios	La implantación de cambios debe controlarse mediante el uso de procedimientos formales de control de cambios.	SI
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Cuando se modifiquen los sistemas operativos, las aplicaciones empresariales críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o en la seguridad de la organización.	SI
12.5.3	Restricciones a los cambios en los paquetes de software	Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	SI
12.5.4	Fugas de información	Deben evitarse las situaciones que permitan que se produzcan fugas de información.	SI
12.5.5	Externalización del desarrollo de software	La externalización del desarrollo de software debe ser supervisada y controlada por la organización.	SI

12.6	**Gestión de la vulnerabilidad técnica**	**Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.**	
12.6.1	Control de las vulnerabilidades técnicas	Se debe obtener la información adecuada acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	SI
13.1	**Notificación de eventos y puntos débiles de la seguridad de la información**	**Objetivo: Asegurarse de que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, se comunican de manera que sea posible emprender las acciones correctivas oportunas.**	
13.1.1	Notificación de eventos de seguridad de la información	Los eventos de seguridad de la información se deben notificar a través de los canales adecuados de gestión lo antes posible.	SI
13.1.2	Notificación de los puntos débiles de seguridad	Todos los empleados, contratistas, y terceros que sean usuarios de los sistemas y servicios de información deben estar obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios.	SI
13.2	**Gestión de incidentes de seguridad de la información y mejoras**	**Objetivo: Garantizar que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información.**	
13.2.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	SI
13.2.2	Aprendizaje de los incidentes de seguridad de la información	Deben existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información.	SI
13.2.3	Recopilación de evidencias	Cuando se emprenda una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), deben recopilarse las evidencias, y conservarse y presentarse conforme a las normas establecidas en la jurisdicción correspondiente.	SI
14.1	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**	**Objetivo: Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación.**	
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Debe desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio.	SI
14.1.2	Continuidad del negocio y evaluación de riesgos	Deben identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información.	SI
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	Deben desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requeridos, después de una interrupción o un fallo de los procesos críticos de negocio.	SI

14.1.4	Marco de referencia para la planificación de la continuidad del negocio	Debe mantenerse un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes sean coherentes, para cumplir los requisitos de seguridad de la información de manera consistente y para identificar las prioridades de realización de pruebas y del mantenimiento.	SI
14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Los planes de continuidad del negocio deben probarse y actualizarse periódicamente para asegurar que están al día y que son efectivos.	SI
15.1	**Cumplimiento de los requisitos legales**	**Objetivo: Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad.**	
15.1.1	Identificación de la legislación aplicable	Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplir dichos requisitos, deben estar definidos, documentados y mantenerse actualizados de forma explícita para cada sistema de información de la organización.	SI
15.1.2	Derechos de propiedad intelectual (IPR) [Intellectual Property Rights]	Deben implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software propietario.	SI
15.1.3	Protección de los documentos de la organización	Los documentos importantes deben estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, regulatorios, contractuales y empresariales.	SI
15.1.4	Protección de datos y privacidad de la información de carácter personal	Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y la reglamentación aplicables y, en su caso, en las cláusulas contractuales pertinentes.	SI
15.1.5	Prevención del uso indebido de los recursos de tratamiento de la información	Se debe disuadir a los usuarios de utilizar los recursos de tratamiento de la información para fines no autorizados.	SI
15.1.6	Regulación de los controles criptográficos	Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	SI
15.2	**Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico**	**Objetivo: Asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización.**	
15.2.1	Cumplimiento de las políticas y normas de seguridad	Los directores deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad.	SI
15.2.2	Comprobación del cumplimiento técnico	Debe comprobarse periódicamente que los sistemas de información cumplen las normas de aplicación para la implantantación de la seguridad.	SI
15.3	**Consideraciones sobre la auditoría de los sistemas de información**	**Objetivo: Lograr que el proceso de auditoría de los sistemas de información alcance la máxima eficacia con las mínimas interferencias.**	
15.3.1	Controles de auditoría de los sistemas de información	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas en producción deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos del negocio.	SI
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	El acceso a las herramientas de auditoría de los sistemas de información debe estar protegido para evitar cualquier posible peligro o uso indebido.	SI

Capítulo 3.

Análisis de riesgos.

3.1.- Introducción.

El análisis de riesgos es la fase más importante del proceso de Seguridad de la Información, esta tarea nos ayudará a descubrir que necesidades tiene la organización y cuáles son nuestras "vulnerabilidades" y amenazas.

En la segunda fase del análisis de riesgos se inicia la gestión de riesgos, en donde se seleccionarán las mejores soluciones de seguridad para afrontar los riesgos.

Este capítulo contiene el desarrollo del análisis de riesgos y su gestión, desde el inventario de riesgos hasta la evaluación del impacto potencial.

3.2.- Inventario de activos, valoración y criticidad.

El inventario de activos se encuentra detallado en el apartado 1.3.1 donde se describe la organización. En este punto agruparemos los activos con el objetivo de simplificar el análisis de riesgos.

Capital humano.

Grupo	Descripción	Unidades	Valor	Valor €	Criticidad
Empleados	Mandos	22	Muy Alta	300.000 €	Crítico
	Especialistas	72	Muy Alta	300.000 €	Crítico
	Operarios	20	Muy Alta	300.000 €	Crítico
	Administración	2	Muy Alta	300.000 €	Crítico

Hardware.

Tipo	Descripción	Unidades	Valor	Valor €	Criticidad
Equipos Oficinas	Portátiles	19	Baja	30.000 €	Bajo
	Tabletas	4	Muy Baja	10.000 €	Bajo
	Equipos	103	Media	75.000 €	Medio
Impresoras Oficinas	Impresoras	13	Baja	30.000 €	Bajo

Dispositivos Red	Switches Oficinas	10	Media	75.000 €	Medio
	Switches CPD	12	Media	75.000 €	Crítico
	Routers CPD	5	Baja	30.000 €	Crítico
	Firewalls	4	Media	75.000 €	Crítico
Servidores	Servidores de correo	2	Baja	30.000 €	Crítico
	Servidores Firewall	2	Baja	30.000 €	Medio
	Servidores Web	20	Muy Alta	300.000 €	Crítico
	Servidores Aplicación	19	Muy Alta	300.000 €	Crítico
	Servidores BBDD	5	Media	75.000 €	Crítico
	Servidores Backup	2	Baja	30.000 €	Bajo
	Servidores SAP	2	Baja	30.000 €	Medio
	Servidores Desarrollo	10	Alta	150.000 €	Medio
Cabinas Almacenamiento	Cabinas Almacenamiento	4	Alta	150.000 €	Crítico

Infraestructura técnica.

Tipo	Descripción	Unidades	Valor	Valor €	Criticidad
CPD	SAI	2	Media	75.000 €	Medio
	Generadores eléctricos	2	Media	75.000 €	Bajo
	AACC Industriales	4	Media	75.000 €	Crítico
	Cámaras vigilancia + sensores	24	Baja	30.000 €	Bajo
	Armarios	18	Baja	30.000 €	Bajo

Licencias.

Tipo	Descripción	Unidades	Valor	Valor €	Criticidad
Servidores	Licencias SO	50	Media	75.000 €	Bajo
	Licencias Aplicación	11	Media	75.000 €	Bajo
	Licencias SGBD	5	Media	75.000 €	Bajo
Estaciones de trabajo	Licencias Ofimática	14	Muy Baja	10.000 €	Bajo
	Licencias Proyectos	16	Baja	30.000 €	Bajo
	Licencias SAP	7	Baja	30.000 €	Bajo

Código fuente.

Descripción	Líneas código	Observaciones	Valor	Valor €	Criticidad
FrontOfficeVenta	1000000 líneas	Venta Minorista	Muy Alta	300.000 €	Crítico
BackOfficeVenta	2000000 líneas	Procesos gestión Minorista	Alta	150.000 €	Alto
API-Reservas	750000 líneas	API Reservas	Alta	150.000 €	Crítico
OTA-Reservas	500000 líneas	OTA Reservas	Alta	150.000 €	Crítico
CamasHotel	500000 líneas	Banco Camas Hotel	Alta	150.000 €	Crítico
RecepTur	500000 líneas	Gestión Receptiva	Alta	150.000 €	Crítico
AirjetConecta	350000 líneas	Motor Venta Aéreo	Alta	150.000 €	Crítico
GestHoteles	450000 líneas	Gestión Hotelera	Alta	150.000 €	Alto
ReserMay	3000000 líneas	Venta Mayorista	Muy Alta	300.000 €	Crítico

Información / Otros.

Grupo	Tipo	Descripción	Valor	Valor €	Criticidad
Información	TI	Contratos TIC	Baja	30.000 €	Bajo
	Comercial	Contratos Comerciales	Media	75.000 €	Bajo
		BD Clientes	Alta	150.000 €	Crítico
		Ofertas	Baja	30.000 €	Bajo
	SSGG	Contratos servicios	Baja	30.000 €	Bajo
		Contabilidad-Finanzas	Muy Baja	10.000 €	Medio
	Dirección	Plan estratégico 2015	Alta	150.000 €	Crítico
Otros	Mercado	Capacidad de Servicios	Muy Baja	10.000 €	Medio
		Imagen	Media	75.000 €	Crítico
		Know How	Media	75.000 €	Medio
	Vehículos	Coche clase C	Baja	30.000 €	Bajo

3.3.- Análisis de amenazas.

Definimos amenazas como aquellas situaciones que podrían materializarse en una empresa y que pueden llegar a dañar a activos, provocando que no funcionen correctamente impidiendo la actividad del negocio.

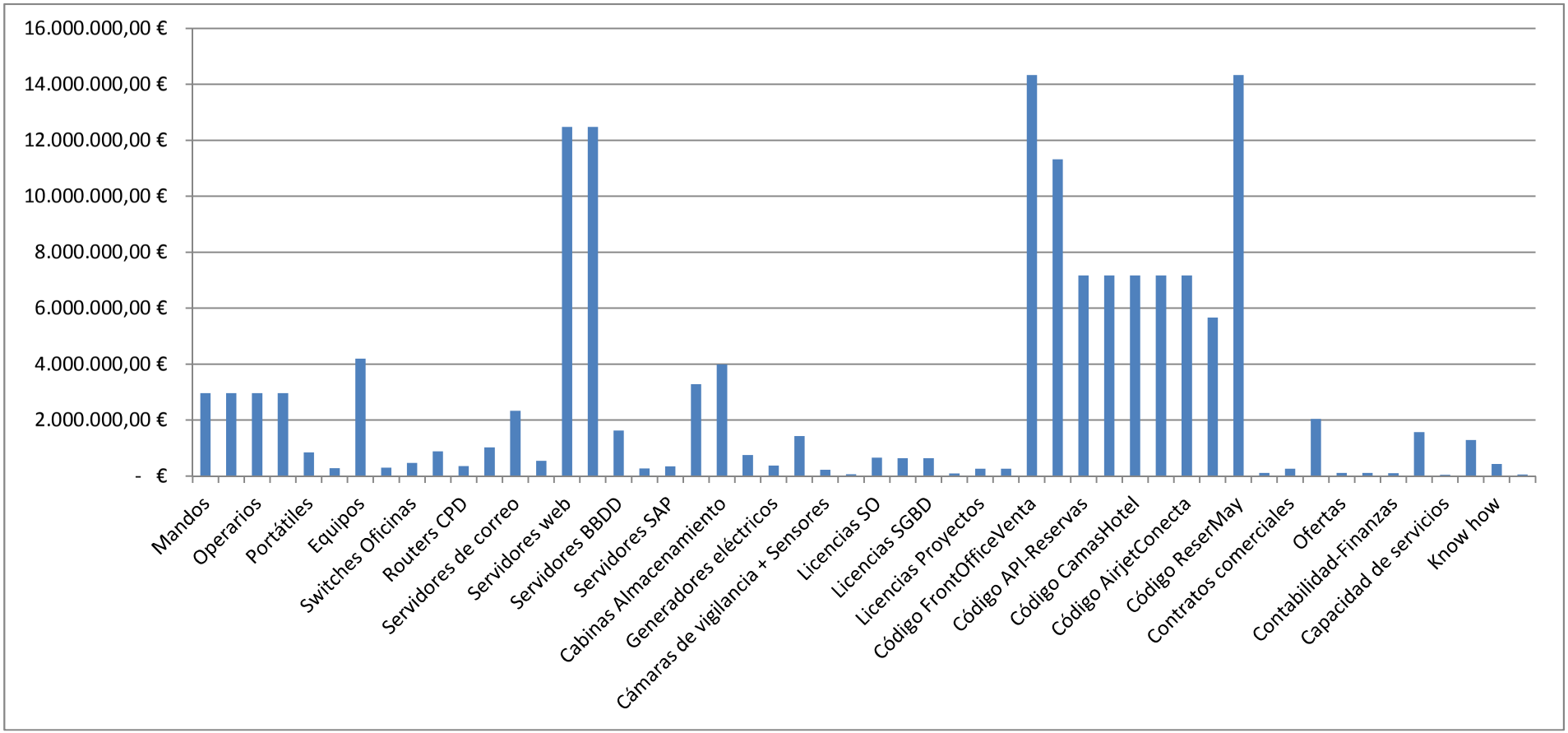
En este apartado expondremos las amenazas a las que está expuesta nuestra organización; su origen, motivación y acción. A continuación se procederá a evaluar el impacto y frecuencia de cada amenaza sobre el activo.

		Fuente					
ID	**Amenaza**	**Natural**	**Humana**	**Entorno**	**Origen**	**Motivación**	**Acción**
1	Infección de virus y/o malware		X		Indeterminado	Obtención de beneficio económico	Intrusión de código malicioso
2	Robo de información confidencial		X		Empleados descontentos o desleales	Obtención de beneficio económico	Extracción de información confidencial
3	Recepción de correo basura		X		Indeterminado	Obtención de beneficio económico	Envío de correos SPAM
4	Ataque DoS		X		Indeterminado	Ocasionar daños a empresa	Ataque al sistema
5	Intrusión hacker		X		Indeterminado	Obtención de información industrial	Ataque al sistema
6	Obtención de información industrial		X		Empresas competidoras	Obtención de ventaja competitiva	Robo de información
7	Sabotaje de los equipos hardware		X		Empresas competidoras y personal descontentos/desleales	Ocasionar daños a empresa	Inserción de fallas hardware
8	Fallo hardware			X	Indeterminado	Indeterminada	Error de diseño hardware o mala fabricación
9	Inserción de datos corruptos de forma malintencionada		X		Empleados descontentos o desleales	Ocasionar daños a empresa	Introducción de datos erróneos por empleados

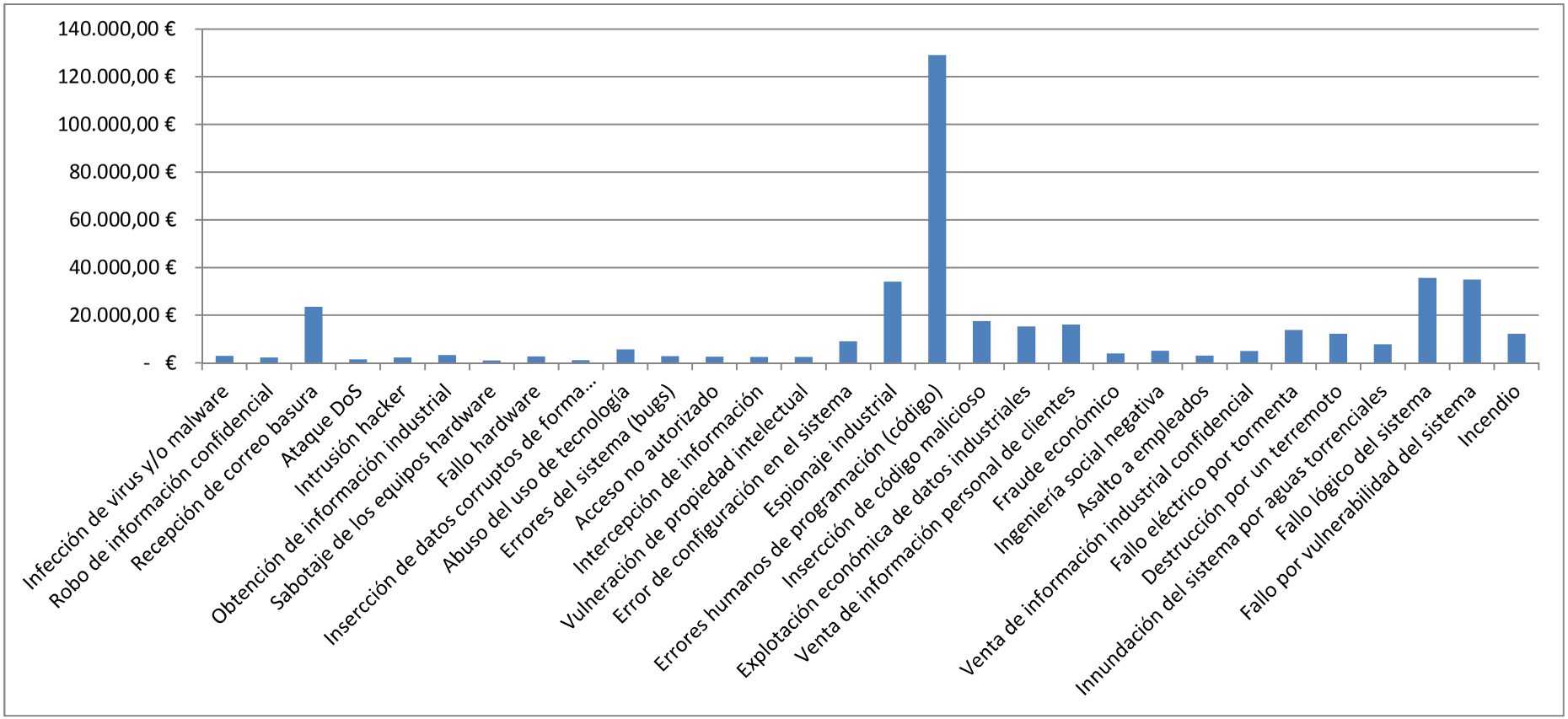
10	Abuso del uso de tecnología		X		Empleados descontentos o desleales	Beneficio propio	Uso indebido de la tecnología
11	Errores del sistema (bugs)			X	Indeterminado	Indeterminada	Errores de diseño o mala implementación
12	Acceso no autorizado		X		Indeterminado	Obtención de información industrial	Ataque al sistema
13	Intercepción de información		X		Indeterminado	Obtención de información confidencial	Errores en controles de seguridad
14	Vulneración de propiedad intelectual		X		Empresas competidoras y personal descontentos/desleales	Ocasionar daños a empresa	Uso indebido de la tecnología
15	Error de configuración en el sistema		X		Empleados	Indeterminada	Errores humanos de empleados
16	Espionaje industrial		X		Empresas competidoras y personal descontentos/desleales	Obtención de ventaja competitiva	Errores en controles de seguridad
17	Errores humanos de programación (código)		X		Empleados	Indeterminada	Errores humanos de empleados
18	Inserción de código malicioso		X		Empresas competidoras y personal descontentos/desleales	Ocasionar daños a empresa	Descontento con la empresa
19	Explotación económica de datos industriales		X		Empresas competidoras y personal descontentos/desleales	Obtención de beneficio económico	Descontento con la empresa o necesidad económica
20	Venta de información personal de clientes		X		Empleados descontentos o desleales	Obtención de beneficio económico	Descontento con la empresa o necesidad económica
21	Fraude económico		X		Empleados descontentos o desleales	Ocasionar daños a empresa	Necesidad económica
22	Ingeniería social negativa		X		Empresas competidoras y personal descontentos/desleales	Ocasionar daños a empresa	Descontento con la empresa
23	Asalto a empleados		X		Indeterminado	Obtención de beneficio económico	Delincuencia
24	Venta de información industrial confidencial		X		Empleados descontentos o desleales	Obtención de beneficio económico	Descontento con la empresa o necesidad económica
25	Fallo eléctrico por tormenta	X			Desastre natural	Indeterminada	Tormenta
26	Destrucción por un terremoto	X			Desastre natural	Indeterminada	Terremoto

27	Inundación del sistema por aguas torrenciales	X			Desastre natural	Indeterminada	Inundación por lluvias
28	Fallo lógico del sistema			X	Indeterminado	Indeterminada	Errores de diseño o mala implementación
29	Fallo por vulnerabilidad del sistema			X	Indeterminado	Indeterminada	Errores de diseño o mala implementación
30	Incendio	X			Indeterminado	Indeterminada	Incendio por fuego u otras causas

3.4.- Resumen Riesgo Intrínseco Activos.



3.5.- Resumen Riesgo Intrínseco Amenazas.



3.6.- Nivel aceptable del riesgo.

El nivel aceptable del riesgo se ha establecido manualmente y analizando concienzudamente cada activo. Se establecen tres niveles de riesgo (Bajo=75%, Medio=50%, Alto=25%) que se aplicarán sobre el riesgo intrínseco anual del activo, a partir de este resultado se establecerán las medidas necesarias para gestionar el riesgo.

Evidentemente estos niveles aceptables del riesgo están comunicados y autorizados por la dirección de la organización.

Capital humano.

Grupo	Descripción	Nivel riesgo aceptable
Empleados	Mandos	Medio
	Especialistas	Medio
	Operarios	Medio
	Administración	Medio

Hardware.

Tipo	Descripción	Nivel riesgo aceptable
Equipos Oficinas	Portátiles	Medio
	Tabletas	Medio
	Equipos	Alto
Impresoras Oficinas	Impresoras	Alto
Dispositivos Red	Switches Oficinas	Medio
	Switches CPD	Bajo
	Routers CPD	Medio
	Firewalls	Medio
Servidores	Servidores de correo	Bajo
	Servidores Firewall	Medio
	Servidores Web	Bajo
	Servidores Aplicación	Bajo
	Servidores BBDD	Bajo

	Servidores Backup	Alto
	Servidores SAP	Medio
	Servidores Desarrollo	Medio
Cabinas Almacenamiento	Cabinas Almacenamiento	Bajo

Infraestructura técnica.

Tipo	Descripción	Nivel riesgo aceptable
CPD	SAI	Medio
	Generadores eléctricos	Medio
	AACC Industriales	Bajo
	Cámaras vigilancia + sensores	Alto
	Armarios	Alto

Licencias.

Tipo	Descripción	Nivel riesgo aceptable
Servidores	Licencias SO	Alto
	Licencias Aplicación	Alto
	Licencias SGBD	Medio
Estaciones de trabajo	Licencias Ofimática	Alto
	Licencias Proyectos	Alto
	Licencias SAP	Alto

Código fuente.

Descripción	Líneas código	Observaciones	Nivel riesgo aceptable
FrontOfficeVenta	1000000 líneas	Venta Minorista	Bajo
BackOfficeVenta	2000000 líneas	Procesos gestión Minorista	Bajo
API-Reservas	750000 líneas	API Reservas	Bajo
OTA-Reservas	500000 líneas	OTA Reservas	Bajo
CamasHotel	500000 líneas	Banco Camas Hotel	Bajo
RecepTur	500000 líneas	Gestión Receptiva	Bajo
AirjetConecta	350000 líneas	Motor Venta Aéreo	Bajo
GestHoteles	450000 líneas	Gestión Hotelera	Bajo
ReserMay	3000000 líneas	Venta Mayorista	Bajo

Información / Otros.

Grupo	Tipo	Descripción	Nivel riesgo aceptable
Información	TI	Contratos TIC	Medio
	Comercial	Contratos Comerciales	Medio
		BD Clientes	Bajo
		Ofertas	Alto
	SSGG	Contratos servicios	Alto
		Contabilidad-Finanzas	Medio
	Dirección	Plan estratégico 2015	Medio
Otros	Mercado	Capacidad de Servicios	Medio
		Imagen	Bajo
		Know How	Medio
	Vehículos	Coche clase C	Alto

3.7.- Conclusiones.

La aplicación de la metodología del análisis de riesgos en nuestra organización nos proporciona importantes conclusiones que serán el punto de partida para el establecimiento de los proyectos de seguridad de la empresa.

Mediante el análisis de amenazas podemos observar que la fuente más representativa (73%) entre las amenazas identificadas corresponde al origen humano, este hecho refleja la importancia de prestar especial atención a la aplicación de medidas y controles relacionadas con las *personas* (empleados, proveedores, clientes, etc.).

Respecto al riesgo intrínseco de activos observamos que entre los niveles más altos de riesgos se encuentran los activos relacionados con el *Core* de nuestra organización, es decir la aplicaciones que soportan los servicios que proporcionamos a nuestros clientes (pe. FrontOfficeVenta, ReserMay, etc.) y la infraestructura que mantiene estas aplicaciones es decir servidores Web y Bases de Datos.

En cuanto a las amenazas que más impacto tienen en nuestros activos podemos encontrar *Errores humanos de programación*. Esta amenaza impacta directamente en nuestras *Aplicaciones Core* y otros activos que TIC (Servidores, Dispositivos de red, etc.) que requieren de un software para funcionar.

El trabajo para reducir las amenazas y riesgos de seguridad deberán orientarse a proyectos que fortalezcan las aplicaciones de la organización y la infraestructura en donde se ubican así como en procedimientos, controles y herramientas destinadas a evitar errores humanos en la programación.

Capítulo 4.

Propuesta de proyectos.

4.1.- Introducción.

En esta fase tenemos a nuestra disposición nuestro estado de cumplimiento de la ISO/IEC 27001:2005 y un análisis de riesgos, es momento de proponer soluciones para mejorar nuestro estado. Para ello, en este capítulo se realizará la propuesta de un programa de proyectos y se definirán cuales son las expectativas de mejora previstas si se llevan a cabo. La propuesta de los proyectos tiene como objeto minimizar el riesgo y evolucionar el cumplimiento de la ISO.

4.2.- Propuestas.

A continuación se presentan las propuestas de proyectos mediante una ficha técnica muy ejecutiva donde se identifican los siguientes datos:

- ID y Nombre.
- Objetivos.
- Requisitos.
- Especificaciones.
- Esfuerzo (Plan de trabajo, coste y dificultad).
- Implicaciones en la organización.
- Impacto en la empresa (económico y estratégico).

<table>
<tr><td>Proyecto 1: Organización de la seguridad y su política de aplicación.</td><td colspan="4">Objetivos: Desarrollar la organización de la seguridad y su política de aplicación. Establecer la base del SGSI basado en ISO/IEC 27001. Implicar a la Dirección y obtener su soporte.</td></tr>
<tr><td>Requisitos</td><td>Especificaciones</td><td colspan="3">Esfuerzo</td></tr>
<tr><td rowspan="8">Elaboración, aceptación y comunicación política seguridad.

Definición de organigrama y responsabilidades de seguridad.

Definición de procesos y elaboración de metodologías básicas de seguridad.

Establecimiento de medidas para el aseguramiento de la seguridad de terceras partes.</td><td rowspan="8">Política de seguridad basada en el estándar ISO 27001 y alineada con el alcance proporcionado.</td><td>Plan de trabajo

1 mes.</td><td>Coste

5.000 € - Consultoría externa especializada.

2 FTE internos / mes</td><td>Dificultad implantación

Baja. La máxima dificultad se concentra en la implicación de la Dirección</td></tr>
<tr><td colspan="3">Implicaciones en la organización</td></tr>
<tr><td colspan="3">Necesidad del establecimiento de la organización y política de seguridad.</td></tr>
<tr><td colspan="3">Impacto</td></tr>
<tr><td colspan="2">Económico

Indirecto. Reducirá los riesgos de seguridad e impactos de las amenazas.

Potencial:

-5% impacto amenazas = 20.000 € aprox

-1% riesgo intrínseco = 1.500.000 € aprox</td><td>Estratégico

Concienciación de la empresa en la seguridad. Mejora y optimización de los procesos de seguridad.</td></tr>
</table>

<table>
<tr><td>Proyecto 2: Formación y concienciación de seguridad.</td><td colspan="4">Objetivos: Establecer e implantar un plan de formación, capacitación y concienciación destinado a todos los empleados de la organización y a terceros (colaboradores, proveedores, etc.)</td></tr>
<tr><td>Requisitos</td><td>Especificaciones</td><td colspan="3">Esfuerzo</td></tr>
<tr><td rowspan="6">Plan tri-anual

Incluirá las áreas de formación, capacitación y concienciación.

Destinado a empleados y terceros (clientes, proveedores, etc)</td><td rowspan="6">No aplica.</td><td>Plan de trabajo

1 mes (desarrollo)</td><td>Coste

15.000 € destinado a formación /año

1 FTE interno / año</td><td>Dificultad implantación

Baja. La máxima dificultad se concentra en la implicación de los trabajadores.</td></tr>
<tr><td colspan="3">Implicaciones en la organización</td></tr>
<tr><td colspan="3">Necesidad de desarrollo e implementación de planes de formación (actualmente no existen).</td></tr>
<tr><td colspan="3">Impacto</td></tr>
<tr><td colspan="2">Económico

Incremento de la productividad de los empleados.

Incremento productividad +3% = 400.000 € anuales</td><td>Estratégico

Incremento en la calidad y seguridad de los servicios ofrecidos.</td></tr>
<tr><td colspan="3"></td></tr>
</table>

<table>
<tr><td>Proyecto 3: Asegurando el ciclo de vida del software.</td><td colspan="4">Objetivos: Mejorar y optimizar el ciclo de vida del software (core de nuestros servicios). Proporcionar las metodologías, herramientas e infraestructura necesaria para asegurar las fases del ciclo de vida de las aplicaciones.</td></tr>
<tr><td>Requisitos</td><td>Especificaciones</td><td colspan="3">Esfuerzo</td></tr>
<tr><td rowspan="8">Establecimiento de estándares de requisitos de seguridad.

Diferenciación de entornos Desarrollo, Test y Producción.

Definición de las actividades del ciclo de vida de software.

Política de controles criptográficos.</td><td rowspan="8">Infraestructura de Sistemas (Virtualizada)</td><td>Plan de trabajo

3 meses</td><td>Coste

20.000 € Consultoría externa

40.000 € Infraestructura

1’5 FTE internos / 3 meses</td><td>Dificultad implantación

Media.

La re-definición de procesos y metodologías requiere la implicación del equipo de personas.</td></tr>
<tr><td colspan="3">Implicaciones en la organización</td></tr>
<tr><td colspan="3">Necesidad de entornos independientes de producción, test y desarrollo.</td></tr>
<tr><td colspan="3">Impacto</td></tr>
<tr><td colspan="2">Económico

Reducción de los errores en producción y su correspondiente dedicación a resolución.

Incremento productividad +5% = 700.000 €

Descenso dedicación resolución errores -10% = 500.000 €</td><td>Estratégico

Mejora en la calidad y seguridad del software.</td></tr>
</table>

<table>
<tr><td>Proyecto 4: Mejora de la gestión de incidencias y problemas.</td><td colspan="4">Objetivos: Optimizar la gestión de incidencias y problemas. Definir y formalizar los procesos. Identificar indicadores de productividad. Incorporar mejoras o nuevas herramientas.</td></tr>
<tr><td>Requisitos</td><td>Especificaciones</td><td colspan="3">Esfuerzo</td></tr>
<tr><td rowspan="8">Optimización del proceso de gestión de incidencias y problemas.

Definición del proceso y flujo de actividades.

Adaptación de la herramienta de ticketing.

Formación y training.

Establecimiento del proceso de mejora continua.</td><td rowspan="8">Modelo estándar de referencia: ITIL®</td><td>Plan de trabajo

3 meses</td><td>Coste

10.000 € consultoría externa

1 FTE interno / mes</td><td>Dificultad implantación

Media.

Requiere la implicación y formación de los usuarios finales.</td></tr>
<tr><td colspan="3">Implicaciones en la organización</td></tr>
<tr><td colspan="3">Mejorar la eficacia y eficiencia de la gestión de incidencias / problemas.</td></tr>
<tr><td colspan="3">Impacto</td></tr>
<tr><td colspan="2">Económico

Reducción de incidencias.

Mejora de productividad.

Incremento productividad 1% = 140.000 €

Descenso dedicación resolución incidencias -10% = 100.000 €</td><td>Estratégico

Aumento de la satisfacción de los clientes.</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
</table>

<table>
<tr><td>Proyecto 5: Continuidad y recuperación del negocio.</td><td colspan="4">Objetivos: Establecer un plan de continuidad y recuperación del negocio ante desastres.</td></tr>
<tr><td>Requisitos</td><td>Especificaciones</td><td colspan="3">Esfuerzo</td></tr>
<tr><td rowspan="6">Análisis de riesgos (amenazas)

Plan de continuidad y recuperación

Pruebas y simulación.

Proceso de mejora continua.</td><td rowspan="6">Debe incluir un estudio de la zona (ubicación) y la identificación de los desastres naturales más probables.</td><td>Plan de trabajo

5 meses</td><td>Coste

40.000 € Consultoría externa

100.000 € Infraestructura

1,5 FTE Internos / Mes</td><td>Dificultad implantación

Alta.

Requiere una importante implicación de la dirección y mandos intermedios</td></tr>
<tr><td colspan="3">Implicaciones en la organización</td></tr>
<tr><td colspan="3">Proteger la continuidad de la empresa en el mercado en caso de desastre.</td></tr>
<tr><td colspan="3">Impacto</td></tr>
<tr><td colspan="2">Económico

Refuerzo del valor de la marca ante desastres. Reducción de las pérdidas económicas en caso de problemas.

Reducción 35% pérdidas económicas en caso de desastre = 1.750.000 €</td><td>Estratégico

Resistencia del negocio ante desastres. No desaparición de la empresa.</td></tr>
<tr><td colspan="3"></td></tr>
</table>

<table>
<tr><td>Proyecto 6: Oficina de Calidad, Testing y Arquitectura.</td><td colspan="4">Objetivos: Creación de un área / departamento destinado a la calidad, testing y arquitectura de software.</td></tr>
<tr><td>Requisitos</td><td>Especificaciones</td><td colspan="3">Esfuerzo</td></tr>
<tr><td rowspan="6">Estructura organizativa.

Definición de roles y funciones.

Diseño de arquitectura de aplicaciones y BBDD.

Establecimiento de procesos, procedimientos y metodologías de desarrollo.

Auditoría y control de la normativa.

Formación y capacitación del equipo.</td><td rowspan="6">Separación de capas (negocio, aplicación, presentación y BBDD).

Estándares de programación de fabricantes.</td><td>Plan de trabajo

6 meses.</td><td>Coste

25.000 € consultoría externa

3 FTE internos / año</td><td>Dificultad implantación

Media.

Requiere la implicación de todo el equipo de desarrollo y modificación en los procesos de trabajo.

Deberá elaborarse un plan alternativo de adaptación de código antiguo.</td></tr>
<tr><td colspan="3">Implicaciones en la organización</td></tr>
<tr><td colspan="3">Mejorar la organización implicada en el desarrollo de aplicaciones, optimización de procesos, etc.</td></tr>
<tr><td colspan="3">Impacto</td></tr>
<tr><td colspan="2">Económico

Reducción de los errores en el código.

Reducción de tiempo de resolución de problemas.

Reducción de riesgos de</td><td>Estratégico

Mejora de la imagen y calidad de los productos desarrollados.</td></tr>
</table>

		seguridad. Aumento del rendimiento de aplicaciones. Aumento 15% rendimiento aplicaciones = 100.000 € Reducción -5% resolución problemas = 50.000 €	

<table>
<tr><td>Proyecto 7: Evolución de plataformas de desarrollo.</td><td colspan="4">Objetivos: Sustituir las plataformas y tecnologías de desarrollo por las nuevas versiones, activar funcionalidades y establecer reglas de calidad y control.</td></tr>
<tr><td>Requisitos</td><td>Especificaciones</td><td colspan="3">Esfuerzo</td></tr>
<tr><td rowspan="6">Aplicaciones de control y repositorios de código (integradas).

Establecimiento de normas y procedimientos de uso.

Almacenamiento del código antiguo en nueva aplicación.

Formación y capacitación del equipo.</td><td rowspan="6">Herramientas integradas con los fabricantes de lenguajes de programación o estándares de facto.</td><td>Plan de trabajo

2 meses</td><td>Coste

15.000 € consultoría externa

3.000 € licencias

1 FTE /mes</td><td>Dificultad implantación

Baja.

La dificultad se concentra en la migración del código y formación al personal.</td></tr>
<tr><td colspan="3">Implicaciones en la organización</td></tr>
<tr><td colspan="3">Evolucionar las herramientas de trabajo de los empleados.</td></tr>
<tr><td colspan="3">Impacto</td></tr>
<tr><td colspan="2">Económico

Aumento de la productividad de los empleados.

Aumento +5% productividad = 700.000 €</td><td>Estratégico

Evolución de la plataforma de trabajo (desarrollo).</td></tr>
<tr><td colspan="3"></td></tr>
</table>

<table>
<tr><td>Proyecto 8: Aseguramiento de infraestructuras críticas.</td><td colspan="4">Objetivos: Asegurar la continuidad de las infraestructuras críticas ante desastres naturales o incidentes.</td></tr>
<tr><td>Requisitos</td><td>Especificaciones</td><td colspan="3">Esfuerzo</td></tr>
<tr><td rowspan="6">Segmentación y redundancia de sistemas críticos.

Actualización y modernización de sistemas.

Simulación de amenazas y traning al equipo.</td><td rowspan="6">Virtualización de servidores.

Redundancia de sistemas.</td><td>Plan de trabajo

7 meses</td><td>Coste

150.000 €
Infraestructura

3 FTE Internos /mes</td><td>Dificultad implantación

Media.

Requiere modificaciones en la infraestructura y migración de sistemas.</td></tr>
<tr><td colspan="3">Implicaciones en la organización</td></tr>
<tr><td colspan="3">Resistencia ante incidentes de seguridad.</td></tr>
<tr><td colspan="3">Impacto</td></tr>
<tr><td>Económico

Reducción de daños económicos en caso de incidente.

Reducción de -20% daños ante desastre = 1.000.000 €</td><td colspan="2">Estratégico

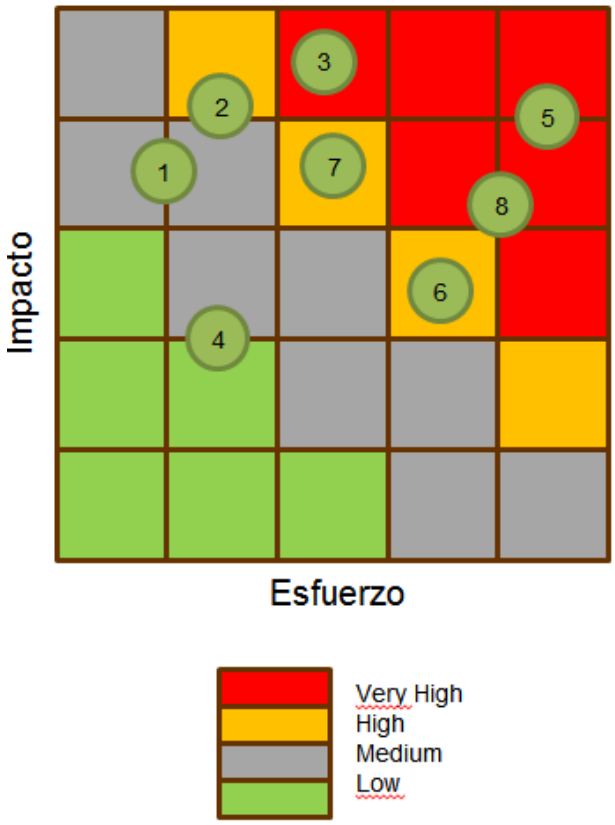
Continuidad del negocio frente a desastres e incidentes.</td></tr>
<tr><td colspan="3"></td></tr>
</table>

3.3.- Resumen ejecutivo.

En este apartado se incluye una representación gráfica de los proyectos basándonos en dos de sus atributos: Impacto y Dificultad.

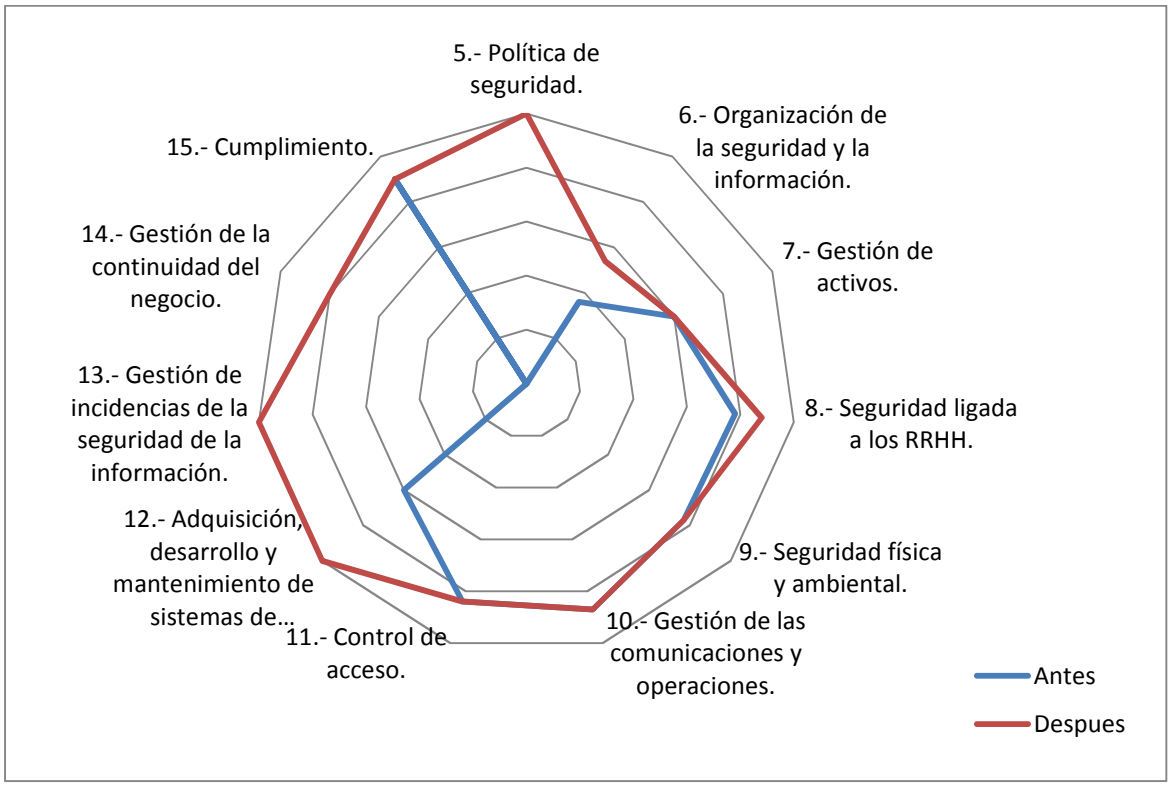
El gráfico nos muestra de una forma clara y sencilla como están posicionados los proyectos respecto a estos dos atributos. Su objetivo permite identificar fácilmente cuales son los prioritarios, es decir, requieren menos esfuerzo y tendrán mayor impacto positivo en la organización.

#	Proyecto
1	Organización de la seguridad y su política de aplicación
2	Formación y concienciación de seguridad
3	Asegurando el ciclo de vida del software
4	Mejora de la gestión de incidencias y problemas
5	Continuidad y recuperación del negocio
6	Oficina de Calidad, Testing y Arquitectura
7	Evolución de plataformas de desarrollo
8	Aseguramiento de infraestructuras críticas



A continuación se presenta una estimación del cumplimiento de los dominios ISO/IEC 27001:2005 después de implementar los proyectos. Primero con datos y después mediante un gráfico de tipo radar.

Dominio	Antes	Después
5.- Política de seguridad.	0%	100%
6.- Organización de la seguridad y la información.	36%	54%
7.- Gestión de activos.	60%	60%
8.- Seguridad ligada a los RRHH.	78%	88%
9.- Seguridad física y ambiental.	77%	77%
10.- Gestión de las comunicaciones y operaciones.	87%	87%
11.- Control de acceso.	84%	84%
12.- Adquisición, desarrollo y mantenimiento de sistemas de información.	60%	100%
13.- Gestión de incidencias de la seguridad de la información.	0%	100%
14.- Gestión de la continuidad del negocio.	0%	80%
15.- Cumplimiento.	90%	90%



4.3.- Conclusiones.

Después de analizar la propuesta de proyectos (esfuerzo e impacto) se ha elaborado un RoapMap de ejecución de los proyectos teniendo en cuenta su duración e impacto en la organización.

Podemos identificar que el proyecto que mayor impacto positivo tendrá en la organización bajo mínimo esfuerzo es *Asegurando el ciclo de vida del software,* por lo tanto lo hemos posicionados en la primera fase del año con el objeto de obtener los beneficios cuanto antes. Aunque siendo coherentes previo a este proyecto se lanzan los dos proyectos básicos e imprescindibles de cualquier plan de SGSI, *Organización de la seguridad y Formación / concienciación de la seguridad,* sin lugar a duda son clave para el éxito del resto.

A continuación el proyecto con mejor impacto, aunque con un importante grado de complejidad es *Continuidad y recuperación del negocio,* por ello se considera adecuado lanzarlo cuanto antes asegurando la disponibilidad recursos internos.

Otro de los proyectos rentables del programa es *Evolución de plataformas de desarrollo*, este proyecto se planifica inmediatamente después de *Asegurando el ciclo de vida del software* ya que es requisito imprescindible para aumentar la calidad de los resultados (primero metodologías/procesos, luego herramientas).

En junio se inician dos proyectos al mismo tiempo pero ambos muy diferentes, *Mejora de la gestión de incidencias* y *Aseguramiento de infraestructuras críticas*. Este último muy complejo y con importantes requisitos económicos aunque de vital importancia para soportar incidentes de seguridad.

Y finalmente *Oficina de calidad, testing y arquitectura,* posicionado en la base de los ejes de impacto y esfuerzo comparándolo con el resto pero de vital importancia para el mantenimiento y la mejora continua del desarrollo de aplicaciones, core de nuestro negocio.

RoapMap de proyectos

#	Proyecto	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	Organización de la seguridad												
2	Formación y concienciación de seguridad												
3	Asegurando el ciclo de vida del software												
4	Mejora de la gestión de incidencias y problemas												
5	Continuidad y recuperación del negocio												
6	Oficina de Calidad, Testing y Arquitectura												
7	Evolución de plataformas de desarrollo												
8	Aseguramiento de infraestructuras críticas												

Capítulo 5.

Auditoría de cumplimiento.

5.1.- Introducción.

Este capítulo llega el momento de evaluar el cumplimiento de la empresa en materia de seguridad. La ISO/IEC 27002:2005 nos proporcionará un marco de control del estado de la seguridad.

Durante el desarrollo de este trabajo se han llevado a cabo acciones de mejora y por lo tanto el estado de madurez de la empresa ha mejorado respecto su situación inicial pero es necesario realizar una auditoría de su estado actual para identificar las deficiencias y las oportunidades de mejora.

Para llevar a cabo este trabajo se llevará a cabo la evaluación de la madurez de cada uno de los dominios de control y los controles de la ISO/IEC 27002:2005 y se elaborará un informe de conclusiones de su análisis.

5.2.- Metodología.

En este apartado describiremos brevemente la metodología de auditoría empleada para llevar a cabo el análisis de madurez y cumplimiento de la ISO/IEC 27002:2005 de la organización.

El resumen de las actividades a realizar será el siguiente:

1. **Plan de auditoría**. Definición de objetivos de la auditoría, estimación de recursos y esfuerzos y tiempo necesario para realizar la auditoría.

2. **Análisis de la organización, procesos de negocio y sistemas.** Identificación y entendimiento de los procesos de negocio y sistemas de información.

3. **Definición del programa y alcance de la auditoría.** Selección de los objetivos de control aplicables y elaboración del programa de auditoría.

4. **Evaluación del sistema de control interno.** Identificación de los controles existentes y su eficiencia. Evaluación del diseño y grado de protección.

5. **Definición y diseño de las pruebas de auditoría.**

6. **Ejecución de las pruebas de auditoría.**

7. **Evaluación de los resultados obtenidos en las pruebas de auditoría.**

8. **Elaboración del informe de resultados de auditoría.** Elaboración del resumen de observaciones. Desarrollo y aprobación del informe preliminar. Elaboración y emisión del informe final de auditoría.

Durante la evaluación de los dominios de control de la ISO/IEC 27002:2005 se utilizará un orden basado en el objetivo y función de cada control. Es decir, primero se analizarán los dominios estratégicos, después los tácticos y finalmente los operativos. A continuación clasificamos los dominios con los criterios seleccionados.

Estratégicos:

- 5.1. Política de seguridad.

- 6. Organización de la seguridad.

Tácticos

- 7. Gestión de activos.

- 11. Control de accesos.

- 15. Cumplimiento.

- 13. Gestión de incidencias de la seguridad de la información.

- 8. Seguridad ligada a los RRHH.

- 9. Seguridad física y ambiental.

Operativos:

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

- 10. Gestión de las comunicaciones y operaciones.

- 14. Gestión de la continuidad del negocio.

Para llevar a cabo cada una de las tareas se llevarán a cabo las siguientes acciones:

- Observación de instalaciones, metodologías y procesos de negocio.

- Análisis de la documentación.

- Pruebas de auditoría.

5.3.- Evaluación de cumplimiento.

Este apartado incluye la evaluación del cumplimiento de cada uno de los 133 controles que contiene la norma ISO/IEC 27002:2005 y la identificación del estado de madurez basándonos en el Modelo de Madurez de la Capacidad (CMM). Esta información mostrará las evidencias del cumplimiento de la norma.

5			**POLÍTICA DE SEGURIDAD**				
5	**1**		**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**				2
5	1	1	Documento de política de seguridad de la información	SEGURIDAD	Existen normativas específicas respecto al uso de los recursos de información así como procedimientos documentados sobre las arquitecturas y sistemas. Se ha establecido una Política General de Seguridad que ha sido revisada y aprobada por la Dirección.	4-Gestionado y evaluable	Cumple
5	1	2	Revisión de la política de seguridad de la información	SEGURIDAD	La dirección revisa y aprueba la política de seguridad y existe un procedimiento que establece como debe revisarse.	4-Gestionado y evaluable	Cumple
6			**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**				
6	**1**		**ORGANIZACIÓN INTERNA**				
6	1	1	Compromiso de la Dirección con la seguridad de la información	SEGURIDAD	Existe un Comité de Gestión de la Seguridad de la Información y la Dirección muestra su apoyo a la seguridad dentro de la organización y asigna funciones y responsabilidades a través de directrices claras (documentado).	4-Gestionado y evaluable	Cumple
6	1	2	Coordinación de la seguridad de la información	SEGURIDAD	Las actividades relativas a la seguridad son coordinadas y asignadas entre los diferentes roles y funciones; existen procedimientos documentados.	3-Proceso definido	Cumple
6	1	3	Asignación de responsabilidades en seguridad de la información	SEGURIDAD	Se han definido y comunicado las funciones y obligaciones del personal, en especial aquellos que intervienen directamente en la gestión de la seguridad.	4-Gestionado y evaluable	Cumple
6	1	4	Proceso de autorización de recursos para la seguridad de la información	SEGURIDAD	Existe un proceso de autorización para los nuevos recursos de procesados de información aunque no es formal ni está documentado.	2-Repetible	No cumple
6	1	5	Acuerdos de confidencialidad	SEGURIDAD	En algunos casos se han establecidos acuerdos de confidencialidad pero no son revisados de forma periódica, tampoco cuando se incorporan nuevos activos de información.	2-Repetible	Cumple

6	1	6	Relación con las autoridades	SEGURIDAD	Existen procedimientos de prevención de riesgos y accidentes laborales (incendios, inundaciones, etc.) así como un protocolo de actuación claramente documentado. En el caso de la seguridad de la información, por ejemplo robos, ataques externos, incidentes terroristas, etc no se establece procedimiento formal.	2-Repetible	Cumple
6	1	7	Relación con grupos de interés especial	SEGURIDAD	Se establecen relaciones con grandes proveedores aunque ninguno de especial relevancia en cuestiones de seguridad de la información.	1-Inicial/adHoc	No cumple
6	1	8	Revisión independiente de la seguridad de la información	SEGURIDAD	Se realizan con frecuencia revisiones independientes de seguridad (auditorías) aunque no en todas las áreas (pe. Procedimientos, controles, etc.) Existe una política clara que define la frecuencia y la metodología	4-Gestionado y evaluable	Cumple
6	**2**		**TERCERAS PARTES**				
6	2	1	Identificación de riesgos derivados del acceso de terceros	COMPRAS	Se realiza un exhaustivo análisis en la selección de un proveedor (tercera parte) y siempre se confía el servicio a un importante proveedor (representa su seriedad y buenas prácticas). Existe una metodología de la gestión del riesgo y se ha realizado un análisis exhaustivo de los riesgos a los que está sometida la organización.	4-Gestionado y evaluable	Cumple
6	2	2	Tratamiento de la seguridad en la relación con los clientes	NEGOCIO	Se revisan los requisitos de seguridad con los clientes y se establecen los controles que se solicitan.	2-Repetible	Cumple
6	2	3	Tratamiento de seguridad en los contratos con terceros	COMPRAS	Siempre que se contrata un servicio a un tercero se realiza un contrato pero no en todas las ocasionas este incluye las cláusulas de seguridad correspondientes.	3-Proceso definido	No cumple
7			**GESTIÓN DE ACTIVOS**				
7	**1**		**RESPONSABILIDAD SOBRE LOS ACTIVOS**				
7	1	1	Inventario de activos	SISTEMAS-REDES	Se realiza un inventario detallado de equipos, servidores y otros dispositivos propiedad de la organización o utilizados en sus procesos de negocios pero no existe un inventario de los activos de información.	3-Proceso definido	Cumple
7	1	2	Propietarios de los activos	SISTEMAS-REDES	En el inventario existente se asigna un propietario al activo pero no lo especifica razonablemente se hace de forma genérica.	3-Proceso definido	No cumple

7	1	3	Uso aceptable de los recursos	RRHH	Hay publicado un código de conducta y una guía general sobre el buen uso de los recursos de información de la organización.	4-Gestionado y evaluable	Cumple
7	**2**		**CLASIFICACIÓN DE LA INFORMACIÓN**				
7	2	1	Directrices de clasificación	RRHH	Se cumple con la normativa vigente de LOPD y por lo tanto se tiene clasificada la información que contiene datos personales según la legislación vigente pero no se clasifican aquellos activos de información que no contienen datos personales y tampoco se identifican según la criticidad para la organización.	3-Proceso definido	Cumple
7	2	2	Etiquetado y tratamiento de la información	SEGURIDAD FISICA	La información clasificada está etiquetada y tiene un tratamiento adecuado a las características asignadas aunque como se ha comentado anteriormente no está correctamente clasificada.	3-Proceso definido	No cumple
8			**SEGURIDAD LIGADA A LOS RRHH**				
8	**1**		**ANTES DEL EMPLEO**				
8	1	1	Funciones y responsabilidades	RRHH	Existe un documento descriptivo de todos los puesto de trabajo de la organización, donde se describe cuáles son sus funciones y responsabilidades pero no en todos los casos se definen las responsabilidades de terceros. Muchas veces no se especifican las responsabilidades respecto a la seguridad.	4-Gestionado y evaluable	Cumple
8	1	2	Investigación de antecedentes	RRHH	Antes de realizar una contratación se solicitan referencias y se investigan los antecedentes del empleador o tercero. Se solicita documentación oficial sobre títulos, etc.	4-Gestionado y evaluable	Cumple
8	1	3	Términos y condiciones del empleo	RRHH	De acuerdo con la legislación se les hace firmar una cláusula legal (genérica) aunque no un código ético ni acuerdos. En contratos muy antiguos no se ha realizado nunca. Sucede con empleados y terceras partes.	3-Proceso definido	Cumple
8	**2**		**DURANTE EL EMPLEO**				
8	2	1	Responsabilidades de la Dirección	RRHH	Aunque se trasmite a los empleados una guía del buen uso de los recursos de la información. Existe una política clara de las responsabilidades	3-Proceso definido	Cumple

8	2	2	Concienciación, formación y capacitación en seguridad de la información	RRHH	No se realiza concienciación, formación o capacitación respecto a la seguridad de la información.	0-Inexistente	No cumple
8	2	3	Proceso disciplinario	RRHH	No existe un proceso disciplinario formal y claro para los empleados que hayan provocado la violación de la seguridad.	0-Inexistente	No cumple
8	**3**		**CESE DEL EMPLEO O CAMBIO DE PUESTO DE TRABAJO**				
8	3	1	Responsabilidad del cese o cambio	RRHH	Existe un procedimiento documentado respecto a la baja o cambio de puesto del personal. Se han asignado claramente las responsabilidades.	4-Gestionado y evaluable	Cumple
8	3	2	Devolución de activos	RRHH	Existe un procedimiento (aunque no documentado) sobre la devolución de los activos de la organización al finalizar su empleo, contrato o acuerdo.	4-Gestionado y evaluable	Cumple
8	3	3	Supresión de los derechos de acceso	RRHH	Existe un procedimiento documentado y revisado respecto a la supresión de derechos de acceso en el caso de cese o cambio de función. En algunos casos puntuales no son informados los cambios de función inmediatamente,	4-Gestionado y evaluable	Cumple
9			**SEGURIDAD FÍSICA Y AMBIENTAL**				
9	**1**		**ÁREAS SEGURAS**				
9	1	1	Perímetro de seguridad física	SEGURIDAD FISICA	Las instalaciones de la organización están cerradas al personal ajeno a esta mediante muros, barreras, puertas y otros elementos físicos. No es posible el acceso a las instalaciones físicas sin autorización.	5-Optimizado	Cumple
9	1	2	Control físicos de entrada	SEGURIDAD FISICA	Todas las instalaciones de la organización están controladas mediante un perímetro de seguridad al cual se accede por tarjeta con supervisión de personal de la organización, sin ella no es posible el acceso. Las zonas sensibles están protegidas con tarjeta y código.	5-Optimizado	Cumple
9	1	3	Seguridad de oficinas, despachos y salas	SEGURIDAD FISICA	Las salas sensibles (rack de switches, servidores, SAIs y otros aparatos) están protegidos mediante una puerta con llave siempre cerrada a custodia de los responsables. Los despachos están protegidos con puertas con cerradura y se cierran siempre que es necesario.	5-Optimizado	Cumple

9	1	4	Protección contra amenazas externas y de origen ambiental	SEGURIDAD FISICA	La organización tiene instaladas protecciones contra amenazas externas: sistemas de extinción de incendios en todos los espacios, protección del fuego en zonas mediante infraestructuras especiales (puertas ignífugas, etc.). Zonas sensibles en espacios altos para evitar daños en inundaciones acompañadas de desagües en zonas de riesgo. En cuanto a amenazas provocadas por el hombre cuenta con las barreras físicas habituales (puertas, muros, etc).	5-Optimizado	Cumple
9	1	5	Trabajo en áreas seguras	SEGURIDAD FISICA	La organización tiene implementada una serie de directrices para el uso de espacio comunes, asegurando las zonas de trabajo (no se puede entrar alimentos, áreas limpias de materiales, etc.)	5-Optimizado	Cumple
9	1	6	Acceso publico, zonas de carga y descarga	SEGURIDAD FISICA	En las zonas de acceso al público o zonas de carga y descarga siempre está presente un empleado de la organización supervisando el acceso o las tareas que se deben realizar. Estas zonas se mantienen libre del tratamiento de información o está protegida adecuadamente.	5-Optimizado	Cumple
9	**2**		**SEGURIDAD DE LOS EQUIPOS**				
9	2	1	Emplazamiento y protección de los equipos	SEGURIDAD FISICA	Los equipos de la organización y otros dispositivos de tratamiento o mantenimiento de la información son adecuadamente ubicados mediante la protección de los mismos; accesos no autorizados, problemas ambientales (goteras, lluvia, etc), etc.	5-Optimizado	Cumple
9	2	2	Instalaciones de suministro	SEGURIDAD FISICA	Todas las instalaciones de la organización están protegidas ante fallos de alimentación (Diferenciales, SAIs, grupos electrógenos y otros dispositivos). Las zonas especialmente sensibles están reforzadas con un sistema adicional y redundante que asegura el funcionamiento y la continuidad de la operativa en caso de fallo eléctricos o la protección ante los mismos.	5-Optimizado	Cumple
9	2	3	Seguridad del cableado	SISTEMAS-REDES	Tanto el cableado eléctrico como de comunicaciones está protegido ante interceptaciones o daños. Se ubican en sus correspondientes bandejas y los accesos del cableado especialmente protegido sólo es conocido por el personal autorizado.	5-Optimizado	Cumple

9	2	4	Mantenimiento de los equipos	SISTEMAS-REDES	Los equipos (servidores, etc) y dispositivos tienen un mantenimiento adecuado y se monitorizan constantemente ante fallos hardware, en caso de fallo son inmediatamente reparados. Los equipos y dispositivos especialmente críticos tienen asociado un contrato de reparación en caso de fallo (por importantes proveedores). Aunque no existe una evaluación de riesgos ni una política clara.	5-Optimizado	Cumple
9	2	5	Seguridad de equipos fuera de los locales propios	SEGURIDAD FISICA	Los equipos que se emplean fuera de la organización cumplen las mismas medidas que los equipos que se emplean dentro, no se aplican medidas especiales (encriptación, etc) y aunque suele existir una autorización del responsable no se lleva una buena gestión de ellas.	1-Inicial/adHoc	No cumple
9	2	6	Seguridad en la reutilización o eliminación de equipos	SISTEMAS-REDES	La organización es consciente de la importancia de las buenas prácticas de la retirada o reutilización de equipos por la importancia de los datos que contienen pero no existe ninguna política formal al respecto. Aunque los dispositivos de almancenamiento son retirados y reutilizados de forma segura el procedimiento no está controlado ni revisado. Se lleva el control de las licencias a modo general (no muy exhaustivo).	2-Repetible	No cumple
9	2	7	Retirada de materiales de propiedad de la empresa	SEGURIDAD FISICA	Existen controles sobre la retirada de materiales pero son débiles y no están documentados. Se protege la salida de los activos propiedad de la organización aunque no se está especialmente concienciado del peligro que conlleva.	1-Inicial/adHoc	No cumple
10			**GESTIÓN DE COMUNICACIONES Y OPERACIONES**				
10	**1**		**RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIONES**				
10	1	1	Documentación de los procedimientos de operaciones	SISTEMAS-REDES	La mayoría de los procedimientos de operaciones están correctamente documentados y habitualmente se revisan. Se modifican mediante autorización del responsable y se lleva un control de las versiones. Además están a disposición de todos los usuarios que los necesiten, tampoco permite asociar los activos afectados (equipos, software, información, etc).	5-Optimizado	Cumple
10	1	2	Gestión de los cambios	SISTEMAS-REDES	Se lleva un control de cambios (con un proceso claro y previa autorización) aunque no es muy exhaustivo y no identifica el área de trabajo (sistemas, comunicaciones, software, etc) ni aplica ninguna clasificación.	3-Proceso definido	Cumple

10	1	3	Segregación de tareas	SISTEMAS-REDES	Se segregan funciones y tareas en todos los departamentos de forma indirecta para evitar las modificaciones no autorizadas o usos indevidos. Como punto débil, no existe documentación o política documentada al respecto.	4-Gestionado y evaluable	Cumple
10	1	4	Separación de los entornos de desarrollo, pruebas y explotación	SISTEMAS-REDES	Las áreas de desarrollo y explotación, tanto en Sistemas como en Programación, están diferenciadas aunque no de todas las aplicaciones. Se segregan funciones en todos los departamentos para evitar las modificaciones no autorizadas o usos indevidos. Como punto débil, no existe documentación o política documentada al respecto.	3-Proceso definido	Cumple
10	**2**		**GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS**				
10	2	1	Provisión de servicios	SISTEMAS-REDES	Al contratar un servicio se comprueban las definiciones, los acuerdos de provisión y los recursos empleados por el tercero aunque no existe una política general de revisión (check list). No se revisan los acuerdos de forma periódica salvo cause pérdidas para la organización.	3-Proceso definido	Cumple
10	2	2	Supervisión y revisión de los servicicios prestados por terceros	SISTEMAS-REDES	Los niveles de servicios de terceros se monitorizan con frecuencia. No se realizan auditorías de los servicios de terceros ni existe una política específica para la gestión de servicios de terceros.	3-Proceso definido	Cumple
10	2	3	Gestión de cambios en los servicios prestados por terceros	SISTEMAS-REDES	Se gestionan los cambios realizados en servicios de terceros, se actualizan los procedimientos establecidos y se tiene presente la criticidad del servicio para la organización. Aunque su gestión no es óptima.	3-Proceso definido	Cumple
10	**3**		**PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS**				
10	3	1	Gestión de capacidades	SISTEMAS-REDES	Se gestiona, en la mayoría de servicios/sistemas, las capacidades de los mismos y se ajusta el consumo. Adicionalmente se realizan proyecciones de los requisitos futuros de capacidad. No existe una política clara y formal al respecto pero se lleva a cabo de manera continua.	5-Optimizado	Cumple
10	3	2	Aceptación de sistemas	SISTEMAS-REDES	Existen pruebas y revisiones de los sistemas antes de ser puestos en explotación por el departamento receptor (está documentado y se revisa frecuentemente), no sucede lo mismo con los productos de software.	3-Proceso definido	Cumple
10	**4**		**PROTECCIÓN CONTRA CÓDIGO MALICIOSO Y CÓDIGO MÓVIL**				

10	4	1	Controles contra software malicioso	SISTEMAS-REDES	Todos los equipos y servidores tienen instalados antivirus locales (centralizados) además de sus correspondientes firewalls. Adicionalmente se aplican protecciones adicionales en las zonas en contacto con Internet (Firewalls). El control está documentado y se revisa frecuentemente.	5-Optimizado	Cumple
10	4	2	Controles contra código móvil	SISTEMAS-REDES	Las barreras perimetrales de acceso a Internet así como los antivirus locales (incluyen antimalware) y la propia protección del navegador protegen a los equipos y servidores del código móvil. Aunque no hay una política específica la organización es consciente de la necesidad del control.	4-Gestionado y evaluable	Cumple
10	**5**		**COPIAS DE SEGURIDAD**				
10	5	1	Copias de seguridad de la información	SISTEMAS-REDES	La organización evalúa la necesidad de las copias de seguridad al poner en explotación un nuevo sistema y realiza un inventario y control de las mismas. Adicionalmente se revisan de forma periódica y se hacen pruebas puntuales de recuperación aunque no de todos los sistemas. La mayoría de procesos de copias de seguridad están documentados y existen procedimientos para llevarlos a cabo.	5-Optimizado	Cumple
10	**6**		**GESTIÓN DE LA SEGURIDAD DE LA RED**				
10	6	1	Controles de red	SISTEMAS-REDES	La organización cuenta con una red segmentada (dependiendo de la criticidad de los datos y la exposición al exterior) por Firewalls y asegurada por rutas y reglas de acceso. Adicionalmente cuenta con dispositivos avanzados que detectan comportamientos extraños en la red.	5-Optimizado	Cumple
10	6	2	Seguridad de los servicios de red	SISTEMAS-REDES	Los servicios de red están identificados y tienen asignados las características de seguridad y algunas veces los requisitos de gestión pero no en todos los servicios (sobre todo los internos) se identifican los acuerdos con la dirección.	4-Gestionado y evaluable	Cumple
10	**7**		**MANIPULACIÓN DE SOPORTES**				
10	7	1	Gestión de soportes extraíbles	SISTEMAS-REDES	Aunque se establecen controles técnicos sobre el uso de memorias extraíbles no se realizan sobre unidades de CD/DVD u otros dispositivos. Tampoco se establecen procedimientos formales (por escrito) ni recomendaciones.	1-Inicial/adHoc	No cumple
10	7	2	Retirada de soportes	SISTEMAS-REDES	Aunque no existe una política o procedimiento formal (por escrito) la mayoría de soportes se destruyen manualmente al ser retirados aunque no sucede así con las estaciones de trabajo u otros dispositivos de menor envergadura.	2-Repetible	No cumple

10	7	3	Procedimiento de manipulación de la información	SISTEMAS-REDES	La información se manipula correctamente y existen controles/procedimientos que la protegen contra los accesos no autorizados o el uso indebido pero no existe política o procedimiento por escrito sobre las prácticas o recomendaciones.	4-Gestionado y evaluable	Cumple
10	7	4	Seguridad de la documentación de los sistemas	SISTEMAS-REDES	La documentación y la información en general está protegida mediante reglas de acceso proporcionadas por los responsables de los datos. Se está mejorando la gestión en la centralización creando accesos por grupos de recursos.	3-Proceso definido	Cumple
10	**8**		**INTERCAMBIO DE INFORMACIÓN**				
10	8	1	Políticas y procedimientos de intercambio de información	SEGURIDAD	Se han establecido políticas y procedimientos para el intercambio de información sobre todo aquella que contiene datos personales aunque no ha sido comunicada a todas las partes. En algunos casos no se observan cláusulas de confidencialidad y en la comunicación de voz no se han aplicado correctamente los controles adecuados.	3-Proceso definido	Cumple
10	8	2	Acuerdos de intercambio	RRHH	En ninguno de los casos se han establecido acuerdos de intercambio de información entre la organización y terceros.	0-Inexistente	No cumple
10	8	3	Soportes físicos en transito	SEGURIDAD FISICA	La organización tiene una política clara y formal sobre los procedimientos de tránsito de soportes físicos, se lleva a cabo correctamente y se revisa con cierta frecuencia.	5-Optimizado	Cumple
10	8	4	Correo electrónico	SISTEMAS-REDES	La información contenida en el correo electrónico presenta las protecciones estándar del producto, no se han aplicado certificados ni encriptación.	3-Proceso definido	Cumple
10	8	5	Sistemas de información empresariales	SISTEMAS-REDES	La interconexión de los sistemas empresariales están debidamente controlados y se gestiona correctamente su alta, baja y modificación de accesos. Existe una documentación asociada al respecto.	4-Gestionado y evaluable	Cumple
10	**9**		**SERVICIOS DE COMERCIO ELECTRONICO**				
10	9	1	Comercio electrónico	SISTEMAS-REDES	La organización utiliza el comercio electrónico y por ello cumple con la legislación vigente asociada (LOPD, LSSI, etc.) adicionalmente se protege de actividades fraudulentas y disputas contractuales mediante sistemas de seguridad (Firewalls, encriptación, certificados digitales, etc.). Existe una política formal al respecto.	5-Optimizado	Cumple

10	9	2	Transacciones en línea	SISTEMAS-REDES	Las transacciones en línea se realizan mediante encriptación del canal de comunicación, ya sea por certificados digitales u otros medios. Se llevan a cabo otros controles que aseguran la transacción pero no existe una política formal al respecto.	4-Gestionado y evaluable	Cumple
10	9	3	Información con acceso publico	SISTEMAS-REDES	La información puesta a disposición pública está debidamente protegida frente a modificaciones no autorizadas y se revisa frecuentemente. Los servidores están correctamente actualizados y presentan sistemas antivirus/antimalware activos.	4-Gestionado y evaluable	Cumple
10	**10**		**MONITORIZACIÓN**				
10	10	1	Registro de auditorías	SISTEMAS-REDES	Todos los sistemas de información tienen activo el registro de eventos de seguridad pero no se ha establecido ninguna política común de almacenamiento. Tampoco existe documentación respecto a la configuración o los requisitos del negocio.	3-Proceso definido	No cumple
10	10	2	Monitorización del uso de los sistemas	SISTEMAS-REDES	La organización ha establecido los procedimientos para la monitorización y supervisión de los recursos de procesamiento de información, estos se revisan periódicamente. No existe una política formal pero las medidas se toman de forma adecuada.	5-Optimizado	Cumple
10	10	3	Protección de la información de los registros	SISTEMAS-REDES	Los registros de seguridad de los sistemas se protegen de forma adecuada de los accesos no autorizadas y de manipulaciones indebidas. No se revisan de forma frecuente.	5-Optimizado	Cumple
10	10	4	Registros de administración y operación	SISTEMAS-REDES	Los registros de seguridad registran cualquier evento del sistema, incluyendo aquellos realizados por los operadores y los administradores de sistemas. No existe ningún procedimiento de revisión periódica.	3-Proceso definido	Cumple
10	10	5	Registros de fallos	SISTEMAS-REDES	Se realiza la gestión de fallos de los sistemas mediante varias herramientas de monitorización que permiten a los administradores actuar para prevenir la interrupción o solucionarla.	5-Optimizado	Cumple
10	10	6	Sincronización de relojes	SISTEMAS-REDES	Los relojes de todos los sistemas están sincronizados con una precisión de tiempo acordada. Existe un procedimiento forma que se revisa con cierta frecuencia.	5-Optimizado	Cumple
11			**CONTROL DE ACCESO**				
11	**1**		**REQUISITOS DE NEGOCIO PARA EL CONTROL ACCESO**				
11	1	1	Política de control de acceso	SEGURIDAD	Aunque la organización lleva a cabo un control de acceso siguiendo las indicaciones de la dirección o los clientes (requisitos del negocio) no existe ninguna política de control acceso formal (documentada y revisada).	3-Proceso definido	Cumple
11	**2**		**GESTIÓN DE ACCESO DE USUARIO**				

11	2	1	Registro de usuario	SISTEMAS-REDES	La organización tiene un procedimiento formal de alta, baja y modificación de usuarios mediante el cual se conceden y revocan los derechos de acceso. Este documento se actualiza y revisa con frecuencia.	5-Optimizado	Cumple
11	2	2	Gestión de privilegios	SISTEMAS-REDES	La gestión de privilegios sólo corresponde al departamento de Administración de Sistemas (en el caso de sistemas comunes) y explotación de aplicaciones (en el caso de aplicaciones). Ningún otro usuario puede realizar estas funciones. Aunque no existe un esquema formal de autorización el procedimiento se realiza correctamente.	3-Proceso definido	Cumple
11	2	3	Gestión de las contraseñas de los usuarios	SISTEMAS-REDES	Se realiza una gestión correcta de las contraseñas de los usuarios tanto a nivel de aplicación como de sistema a través de un proceso formal (se establece caducidad y bloqueo) aunque no existe ninguna política formal sobre la gestión de contraseñas (entrega, cambio, etc.). Tampoco se firman cláusulas de confidencialidad de la contraseña.	4-Gestionado y evaluable	Cumple
11	2	4	Revisión de los derechos de accesos	SISTEMAS-REDES	No existe ningún procedimiento formal de revisión de los derechos de acceso, los responsables de la información confían en los derechos establecidos y sólo se revisan en caso de error, anomalía o incidencia.	0-Inexistente	No cumple
11	**3**		**RESPONSABILIDAD DE USUARIO**				
11	3	1	Uso de las contraseñas	SISTEMAS-REDES	La organización ha establecido métodos técnicos para que las contraseñas cumplan con unos requisitos de seguridad adecuados (no está aplicado en las aplicaciones) pero no existe una guía de recomendaciones en la selección de contraseñas para los usuarios.	3-Proceso definido	Cumple
11	3	2	Equipo de usuario desatendido	SISTEMAS-REDES	Se han establecido controles técnicos para el bloqueo de equipos desatendidos (tanto en estaciones de trabajo como servidores) pero no existe una guía/formación de concienciación dirigida a los usuarios.	4-Gestionado y evaluable	Cumple
11	3	3	Política de puesto de trabajo despejado y bloqueo de pantalla	SISTEMAS-REDES	No existe ninguna política formal de puesto de trabajo despejado y bloqueo de pantalla aunque la organización ha establecido métodos técnicos para el bloqueo de sesiones.	3-Proceso definido	Cumple
11	**4**		**CONTROL DE ACCESO A LA RED**				
11	4	1	Política de uso de los servicios de red	SISTEMAS-REDES	El uso de los servicios de red (un gran porcentaje) está controlado técnicamente y sólo se habilita el acceso previa autorización pero no existe una política formal sobre la solicitud de acceso. Como debilidad la organización permite el acceso a la red por DHCP si un dispositivo se conecta a una toma (sin autorización previa).	3-Proceso definido	Cumple

11	4	2	Autenticación de usuarios para conexiones externas	SISTEMAS-REDES	Se establecen la autentificación de usuarios para conexiones externas mediante rangos de IP y enrutamientos preestablecidos, estos controles se acompañan de reglas de acceso en Firewalls.	5-Optimizado	Cumple
11	4	3	Identificación de equipos en la red	SISTEMAS-REDES	Todos los equipos de la red están identificados e inventariados (de forma automática), se realiza un control sobre la incorporación de nuevos equipos (evalúa la autorización de su acceso a la red). Existe una estructura definida de la red y la asignación de IPs por zonas.	5-Optimizado	Cumple
11	4	4	Diagnóstico remoto y protección de los puertos de configuración	SISTEMAS-REDES	De forma general los puertos de configuración de equipos, servidores, switches y otros están protegidos ya sea por medidas lógicas como físicas.	5-Optimizado	Cumple
11	4	5	Segregaciones de la red	SISTEMAS-REDES	Las redes de la organización están completamente segregadas y protegidas teniendo en cuenta su criticidad, exposición al exterior y el valor de la información que protegen. Esto se complementa con dispositivos avanzados de vigilancia de la red.	5-Optimizado	Cumple
11	4	6	Control de conexión a la red	SISTEMAS-REDES	La organización establece controles de conexión a la red mediante enrutamientos, firewalls y otros elementos. Adicionalmente se monitorizan los accesos y se controla el consumo de recursos.	5-Optimizado	Cumple
11	4	7	Control de encaminamiento en la red	SISTEMAS-REDES	La organización tiene implementado un control de encaminamiento de red, todas las redes que están controladas se encaminan a sus correspondientes firewalls y en estos se establecen las reglas de acceso.	5-Optimizado	Cumple
11	**5**		**CONTROL DE ACCESO AL SISTEMA OPERATIVO**				
11	5	1	Procedimiento seguros de inicio de sesión	SISTEMAS-REDES	Se establecen mecanismos técnicos de inicio de sesión seguro: no muestra el último usuario logeado, bloqueo de contraseñas por intentos fallidos, tiempo de espera al bloqueo de cuenta, comunicación cifrada de la contraseña, etc pero estos no se recogen en una política. Tampoco se muestra un aviso general del acceso limitado a los usuarios autorizados.	5-Optimizado	Cumple
11	5	2	Identificación y autenticación de usuario	SISTEMAS-REDES	No todos los usuarios del sistema tienen identificadores personales, existen muchos usuarios genéricos donde no se puede trazar la persona (tanto en sistema como en aplicación).	3-Proceso definido	No cumple
11	5	3	Sistema de gestión de contraseñas	SISTEMAS-REDES	El sistema de gestión de contraseñas es correcto, se almacenan cifradas, se establece una complejidad a las contraseñas, un periodo de caducidad, un historial recordatorio. Además se permite al usuario la modificación de contraseña en la mayoría de casos, etc.	5-Optimizado	Cumple

11	5	4	Uso de las utilidades de los sistemas operativos	SISTEMAS-REDES	Tanto en equipos como en servidores se limita el uso y acceso a las herramientas y utilidades del sistema operativo que puedan dañar parte del mismo. Sólo el personal técnico autorizado/capacitado tiene acceso a estas. Adicionalmente todas las aplicaciones innecesarias son eliminadas del sistema pero no existe una política formal al respecto.	5-Optimizado	Cumple
11	5	5	Desconexión automática de sesión	SISTEMAS-REDES	En el acceso a sistemas remotos se establece un timeout de sesión (Citrix, Terminal Server, TMG, etc) pero no sucede lo mismo en las aplicaciones internas de la organización ni en las sesiones de usuario en las estaciones de trabajo.	4-Gestionado y evaluable	Cumple
11	5	6	Limitación de las ventanas de conexión	SISTEMAS-REDES	Dadas las necesidades del negocio no se han establecido ventanas de limitación de conexión ya que los clientes requieren el uso del sistema en cualquier hora/día del año.	4-Gestionado y evaluable	Cumple
11	**6**		**CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN**				
11	6	1	Restricción de acceso a la información	SISTEMAS-REDES	Las aplicaciones tienen asignados distintos menus dependiendo el perfil del usuario, sólo los usuarios de soporte tienen acceso a toda la información. Existe documentación al respecto.	4-Gestionado y evaluable	Cumple
11	6	2	Aislamiento de sistemas sensibles	SISTEMAS-REDES	Los sistemas sensibles están aislados y correctamente protegidos bajo los requisitos del negocio y del propietario de los datos.	5-Optimizado	Cumple
11	**7**		**ORDENADORES PORTÁTILES Y TELETRABAJO**				
11	7	1	Ordenadores portátiles y comunicaciones móviles.	SISTEMAS-REDES	Aunque la mayor parte de la información está centralizada y se utilizan protocolos seguros así como mecanismos adicionales, no existe una política formal sobre la utilización de equipos y dispositivos portátiles o móviles.	1-Inicial/adHoc	No cumple
11	7	2	Teletrabajo	RRHH	No existe una política formal de teletrabajo donde se indiquen los requisitos necesarios (antivirus, firewall, conexión, ubicación física, etc.) así como acuerdos de licencia o propiedad intelectual, reglas de uso (acceso a la familia, …), etc.	1-Inicial/adHoc	No cumple
12			**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**				
12	**1**		**REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN**				
12	1	1	Análisis y especificaciones de requisitos de seguridad	DESARROLLO	En el análisis y especificaciones de los nuevos productos se suelen evaluar las características y controles de seguridad. Existe una metodología de gestión del riesgo aplicable a toda la organización.	3-Proceso definido	Cumple
12	**2**		**PROCESO CORRECTO EN LAS APLICACIONES**				

12	2	1	Validación de los datos de entrada	DESARROLLO	Las aplicaciones tienen aplicada la validación de datos de entrada, detectando y evitando los errores. Estos controles protegen a las aplicaciones de ataques estándar.	4-Gestionado y evaluable	Cumple
12	2	2	Control del proceso interno	DESARROLLO	Las aplicaciones de la organización realizan un control interno de la información que manejan vigilando la integridad de los datos y evitando los ataques estándar.	4-Gestionado y evaluable	Cumple
12	2	3	Integridad de los mensajes	DESARROLLO	Las aplicaciones no incorporan la verificación de la integridad de los mensajes aunque existen controles adicionales que pueden complementar este objetivo.	2-Repetible	No cumple
12	2	4	Validación de los datos de salida	DESARROLLO	No se realiza la validación de los datos de salida en todas las aplicaciones/informes aunque en todos los casos se proporciona a los usuarios la información suficiente para que se pueda evaluar correctamente.	2-Repetible	No cumple
12	**3**		**CONTROLES CRIPTOGRÁFICOS**				
12	3	1	Política de uso de los controles criptográficos	SEGURIDAD	No existe una política formal sobre el uso de los controles criptográficos que recoja la información el enfoque, el análisis de riesgos y las medidas implementadas.	1-Inicial/adHoc	No cumple
12	3	2	Gestión de claves	SEGURIDAD	La organización tiene un implementado un sistema de gestión de claves en donde se generan y almacenan los certificados, gestión de claves, etc. Este sistema está protegido y existe una política no formal sobre su uso.	3-Proceso definido	No cumple
12	**4**		**SEGURIDAD EN LOS ARCHIVOS DE SISTEMA**				
12	4	1	Control del software en explotación	SISTEMAS-REDES	Existen controles del software en explotación mediante la gestión de cambios y se realizan las actualizaciones del sistema mediante un proceso documentado y probado. Adicionalmente existe un registro de auditoría de los cambios realizados y la posibilidad de restaurar un sistema si en el cambio se producen errores.	4-Gestionado y evaluable	Cumple
12	4	2	Protección de los datos de prueba	DESARROLLO	No se establece protección adicional a los datos de pruebas, se utilizan los mismos mecanismos y controles que con los datos reales.	1-Inicial/adHoc	No cumple
12	4	3	Control de acceso al código fuente	DESARROLLO	La gestión del acceso al código fuente se realiza de forma correcta; sólo los usuarios autorizados tienen acceso al código fuente y este está protegido contra modificaciones. Adicionalmente se realiza un registro de los cambios.	4-Gestionado y evaluable	Cumple
12	**5**		**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**				

12	5	1	Procedimiento de control de cambios	SISTEMAS-REDES	La organización lleva a cabo un procedimiento de gestión de cambios donde se establece el nivel de autorización, los sistemas afectados, los cambios realizados, etc. Esta gestión de cambios realiza un registro de los pasos realizados y permite trazar una auditoría del proceso. Aunque es necesario mejorarlo ya que no se puede asociar el activo	2-Repetible	Cumple
12	5	2	Revisión técnica de las aplicaciones después de cambios en los sistemas operativos	SEGURIDAD	Siempre que se realiza un cambio a nivel de sistema o a nivel de software se realiza una revisión técnica sobre el cambio realizado u otros aspectos relacionados. Aunque es necesario mejorar el área de Quality y Testing.	4-Gestionado y evaluable	Cumple
12	5	3	Restricción en los cambios a los paquetes de software	SISTEMAS-REDES	La organización sólo realiza cambios en paquetes de software cuando el cliente tiene una necesidad, el software presenta un problema o con intención de mejorar su rendimiento/funcionamiento. Todos los cambios son evaluados y probados, no se realizan sin previa autorización y el software original se conserva.	5-Optimizado	Cumple
12	5	4	Fuga de información	DESARROLLO	La organización no tiene a disposición de los empleados escáneres u otros dispositivos similares, además limita el tamaño de salida de los correos, no permite el uso de sticks de memoria, y otros controles similares que impiden la fuga de información.	4-Gestionado y evaluable	Cumple
12	5	5	Desarrollo externalizado de software	DESARROLLO	Se realiza el desarrollo externalizado de software pero no en todos los casos se han establecido: los contratos de licencia, propiedad del código, requisitos de calidad y seguridad del software, etc.	4-Gestionado y evaluable	Cumple
12	**6**		**GESTIÓN DE VULNERABILIDADES TÉCNICAS**				
12	6	1	Control de vulnerabilidades técnicas	SEGURIDAD	Normalmente la organización lleva a cabo la gestión de las vulnerabilidades técnicas en cuanto a sistemas operativos Microsoft pero no en el resto de software (Acrobat, Java, etc. - incluido aplicaciones Microsoft) y dispositivos (Cisco, etc.).	3-Proceso definido	Cumple
13			**GESTIÓN DE INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN**				
13	**1**		**REPORTE DE INCIDENCIAS Y DEBILIDADES**				

13	1	1	Notificación de los eventos de seguridad de la información	HELP DESK	La organización posee un help desk de soporte 24x365 (punto único: web, teléfono y correo electrónico) donde usuarios y proveedores pueden notificar las incidencias aunque no se hace distinción entre problemas habituales o incidencias de seguridad. No existe documentación del sistema de gestión de incidencias.	3-Proceso definido	No cumple
13	1	2	Notificación de los puntos débiles de la seguridad	HELP DESK	Los empleados, contratistas y terceros notifican las incidencias y en la política se indica que su notificación es de obligado cumplimiento.	3-Proceso definido	Cumple
13	**2**		**GESTIÓN DE INCIDENCIAS DE SEGURIDAD Y MEJORAS**				
13	2	1	Responsabilidades y procedimientos	HELP DESK	La organización cuenta con un esquema formal de responsabilidades y procedimientos para el tratamiento de las incidencias de seguridad (se incluye en el apartado de roles y responsabilidades.	3-Proceso definido	Cumple
13	2	2	Aprendizaje de los incidentes de seguridad de la información	HELP DESK	La organización no cuenta con ningún mecanismo que permita el aprendizaje sobre los incidentes de seguridad.	1-Inicial/adHoc	No cumple
13	2	3	Recopilación de evidencias	HELP DESK	En caso de incidentes de seguridad la organización realiza la recopilación de evidencias pero no sigue ningún procedimiento específico y muchas veces por desconocimiento no las realiza rigurosamente.	2-Repetible	No cumple
14			**GESTIÓN DE LA CONTINUIDAD DE NEGOCIO**				
14	**1**		**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO**				
14	1	1	Incluir la seguridad de la información en el proceso de gestión de la continuidad de negocio	SEGURIDAD	La organización cuenta una gestión de la continuidad del negocio a baja escala, sin analizar grandes catástrofes/daños y sin incluir la seguridad de la información.	2-Repetible	No cumple
14	1	2	Continuidad de negocio y análisis de riesgos	SEGURIDAD	La organización no ha realizado un plan de continuidad a partir del análisis de un análisis de riesgos.	1-Inicial/adHoc	No cumple
14	1	3	Desarrollo e implantación de planes de continuidad incluyendo la seguridad de la información	SEGURIDAD	Ídem	1-Inicial/adHoc	No cumple
14	1	4	Marco de planificación de la continuidad de negocio	SEGURIDAD	Ídem	1-Inicial/adHoc	No cumple

14	1	5	Prueba, mantenimiento y revisión de los planes de continuidad de negocio	SEGURIDAD	Ídem	1-Inicial/adHoc	No cumple
15			**CUMPLIMIENTO**				
15	**1**		**CUMPLIMIENTO DE LOS REQUISITOS LEGALES**				
15	1	1	Identificación de la legislación aplicable	ASESORIA JURIDICA	La organización cumple con la LOPD, LSSI y otra legislación vigente y así lo demuestra los informes de auditoría presentados.	5-Optimizado	Cumple
15	1	2	Derechos de propiedad intelectual	ASESORIA JURIDICA	La organización cumple con la propiedad intelectual; compra las licencias a fuentes de confianza, mantiene un inventario de los productos, realiza un revisión anual de los mismos, etc. Aunque no tiene publicada una política sobre el cumplimiento de la DPI.	5-Optimizado	Cumple
15	1	3	Protección de los documentos de la organización	ASESORIA JURIDICA	La organización almacena y protege adecuadamente la documentación oficial requerida además de establecer adecuadamente los periodos de retención de la información. En su contra no se establece ningún documento formal que indique el calendario de conservación o las directrices de conservación.	5-Optimizado	Cumple
15	1	4	Protección de datos de carácter personal y privacidad	ASESORIA JURIDICA	La organización cumple con la LOPD, LSSI y otra legislación vigente y así lo demuestra los informes de auditoría presentados.	5-Optimizado	Cumple
15	1	5	Prevención del mal uso de los recursos informáticos	RRHH	La organización realiza la prevención del mal uso de los recursos informáticos mediante medidas y controles técnicas e informa a los empleados sobre el uso indebido de estos.	5-Optimizado	Cumple
15	1	6	Regulación de controles criptográficos	SEGURIDAD	La organización cumple con la regulación de los controles criptográficos e implanta su uso cuando es necesario aunque no existe una documentación específica al respecto.	3-Proceso definido	Cumple
15	**2**		**CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD**				
15	2	1	Cumplimiento de las políticas y normas de seguridad.	AUDIT	No se detectan informes formales sobre las revisiones del cumplimiento por parte de los directores aunque parece que informalmente se realiza este seguimiento.	2-Repetible	No cumple
15	2	2	Comprobación del cumplimiento técnico	AUDIT	En los últimos años se han realizado auditorías técnicas y procedimentales, la organización posee los informes resultados. Ha analizado los informes y está implementando las mejoras.	5-Optimizado	Cumple

15	3		CONSIDERACIONES SOBRE LAS AUDITORIAS DE LOS SISTEMAS DE INFORMACIÓN				
15	3	1	Controles de auditoría de los sistemas de información	AUDIT	En la realización de las auditorías se ha seleccionado el ámbito y los controles necesarios para minimizar el riesgo de las interrupciones. No existe documento general pero se prepara un contrato con cada auditoría.	5-Optimizado	Cumple
15	3	2	Protección de las herramientas de auditoría de sistemas de información	AUDIT	Todas las herramientas de auditoría están especialmente protegidas y sólo son accesibles para los administradores/auditores.	4-Gestionado y evaluable	Cumple

5.4.- Fichas de NO conformidades y observaciones.

Ficha No conformidades: Política de seguridad.

No se identifican NO Conformidades de este dominio.

Ficha No conformidades: Organización de la seguridad y la información.

Organización de la seguridad y la información	
NC Mayor: 1	NC Menor: 2
Descripción de la no-conformidades: 6.1.4: Se identifican recursos de tratamiento de información que no tienen definidos formalmente el proceso de autorización por parte de la Dirección. 6.1.7: No se evidencian contactos con grupos de interés especial, foros o asociaciones especializadas con la seguridad. 6.2.3: Se evidencian contratos con terceros que conllevan tratamiento de información que no contienen cláusulas NDA	
Párrafos de la norma: 6.1.4, 6.1.7 y 6.2.3	Documentos SGSI: N/A
Acción correctora propuesta: Analizar los recursos de tratamiento de información y establecer el proceso de autorización por parte de la Dirección para aquellos para los cuales no estén definidos. Establecer contactos con grupos de especial interés, foros o boletines de noticias especializados con la seguridad, algunas recomendaciones: HISPASEC, INTECO, etc.	

Revisar todos los contratos que impliquen tratamiento de información y comprobar que cumplen los requisitos de seguridad. En caso necesario incluir los anexos necesarios firmados por ambas partes.

Ficha No conformidades: Gestión de activos.

Gestión de activos	
NC Mayor: 0	NC Menor: 2
Descripción de la no-conformidades: 7.1.2: Aunque todos los activos tienen identificado un propietario en algunos casos no se puede asignar la responsabilidad a una persona o entidad. Se evidencian identificaciones de propietarios difusas. 7.2.2: No se identifica una política formal y clara del etiquetado y manipulado de la información, aunque se evidencian cláusulas de privacidad y confidencialidad en la mayoría de documentación	
Párrafos de la norma: 7.1.2 y 7.2.2	Documentos SGSI: Listado de activos
Acción correctora propuesta: Siempre que sea posible asignar una persona física como propietario de los activos, en caso de no ser posible identificar claramente la entidad que tiene esta responsabilidad. Elaborar una política de clasificación de la información, revisar el etiquetado aplicado y realizar las modificaciones del etiquetado adecuándola a la política de clasificación.	

Ficha No conformidades: Seguridad ligada a los RRHH.

NC Mayor: 2	NC Menor: 0
Descripción de la no-conformidades: 8.2.2: No se identifican evidencias de la formación y concienciación de los empleados y/o terceros respecto la seguridad de la información. 8.2.3: No se evidencia proceso disciplinario formal para los empleados que hayan provocado	

alguna violación de seguridad.	
Párrafos de la norma: 8.2.2 y 8.2.3	Documentos SGSI: N/A
Acción correctora propuesta: Elaborar un plan de formación respecto la seguridad de la información y recopilar evidencias de la implementación del mismo. Elaborar y formalizar los procesos disciplinarios en caso de incumplimiento de las normas de seguridad. Comunicar a empleados y terceras partes (recopilar evidencias).	

Ficha No conformidades: Seguridad física y ambiental.

Seguridad física y ambiental	
NC Mayor: 2	NC Menor: 1
Descripción de la no-conformidades: 9.2.5: Los equipos y dispositivos que se utilizan fuera de las instalaciones no tienen asignadas medidas de seguridad adicionales a los que se utilizan en las instalaciones. 9.2.6: No se evidencia ningún procedimiento formal para la reutilización o retirada segura de equipos. Los equipos se retiran y se guardan en un almacén sin tomar medidas adicionales. 9.2.7: La organización no tiene ningún control sobre los equipos y/o dispositivos que se sacan fuera de la organización. El ejemplo más claro son los portátiles y dispositivos móviles.	
Párrafos de la norma: 9.2.5, 9.2.6 y 9.2.7	Documentos SGSI: N/A
Acción correctora propuesta: Elaborar una política de seguridad más estricta para los equipos que se utilizan fuera de las instalaciones y se debería acompañar de una guía de uso y buenas prácticas para los usuarios que los utilizan. Establecer un procedimiento formal de reutilización y retirada de equipos y recopilar evidencias de su uso. Identificar a los empleados y terceras partes que trabajan fuera de la oficina, inventariar sus activos y controlar su entrada/salida. Establecer controles tecnológicos para evitar un uso indebido.	

Ficha No conformidades: Gestión de las comunicaciones y operaciones.

Gestión de las comunicaciones y operaciones	
NC Mayor: 2	NC Menor: 2
Descripción de la no-conformidades: 10.7.1: Se evidencia la aplicación de ninguna medida de control sobre los soportes ópticos (CDROM, DVDROM, etc.). Se localizan discos ópticos no almacenados bajo control adicionalmente no existe ningún inventario de este tipo de soportes. 10.7.2: No existe una política de reutilización y/o retirada de soportes. Asimismo se constata que las estaciones de trabajo retiradas no tienen los discos duros borrados. 10.8.2: Se evidencia la carencia de una política clara de intercambio de información, no todos los contratos que conllevan el intercambio de información incluyen cláusulas para su protección. 10.10.1: Existen registros de auditoria pero los periodos de retención e información contenida en algunos casos no corresponde con la necesaria. No existe una política clara de gestión de registros de auditoria.	
Párrafos de la norma: 10.7.1, 10.7.2, 10.8.2 y 10.10.1	Documentos SGSI: N/A
Acción correctora propuesta: Se deberían aplicar las mismas medidas de gestión aplicadas a los soportes magnéticos que a los soportes ópticos. Establecer una política de retirada de soportes y recoger evidencias de su aplicación. Identificar los intercambios de información e asegurar que se establecen acuerdos para su tratamiento, ya sea por medio de contratos, procedimientos, normas, etc. Identificar los requisitos necesarios para la gestión de registros de auditoría y establecer una política de uso, retención y supervisión.	

Ficha No conformidades: Control de acceso.

Control de acceso	
NC Mayor: 3	NC Menor: 1
Descripción de la no-conformidades: 11.2.4: No hay evidencias de ningún proceso formal de revisión de derechos usuarios por parte de la Dirección. 11.5.2: Se evidencia el uso de usuarios genéricos utilizados por varias personas al mismo tiempo. 11.7.1: No existe una política formal específica para la protección de los ordenadores portátiles y comunicaciones móviles. 11.7.2: Se evidencia la existencia de empleados que realizan teletrabajo pero no existe una política de actividades específica para el teletrabajo.	
Párrafos de la norma: 11.2.4, 11.5.2, 11.7.1 y 11.7.2	Documentos SGSI: N/A
Acción correctora propuesta: Establecer un proceso formal, al menos trimestral, de revisión de derechos de accesos de usuarios por parte de la Dirección. Eliminar / bloquear los usuarios genéricos. Se debería asignar a todo el personal usuarios personales y asegurar una entrega correcta de la contraseña. Analizar los riesgos que conllevan los ordenadores portátiles y comunicaciones móviles y establecer una política específica para la protección de estos dispositivos. Identificar las actividades autorizadas para el teletrabajo y establecer una política formal para llevarla a cabo.	

Ficha No conformidades: Adquisición, desarrollo y mantenimiento de SI.

Adquisición, desarrollo y mantenimiento de SI.	
NC Mayor: 2	NC Menor: 3
Descripción de la no-conformidades:	

12.2.3: No existen evidencias de la identificación de requisitos para garantizar la autenticidad e integridad de los mensajes. 12.2.4: No existen evidencias de la aplicación de métodos de validación de los datos de salida. 12.3.1: No existe ninguna política del uso de controles criptográficos aunque si se evidencia el uso de este tipo de tecnología en algunos productos puntuales. 12.3.2: Dado que no existe ninguna política de uso de técnicas criptográficas tampoco existe una gestión clara de las claves. 12.4.2: Los datos de pruebas de tratan de igual manera que los datos reales.	
Párrafos de la norma: 12.2.3, 12.2.4, 12.3.1, 12.3.2 y 12.4.2	Documentos SGSI: N/A
Acción correctora propuesta: Identificar y seleccionar una tecnología criptográfica y establecer una política formal sobre su uso y gestión de claves. Los datos de pruebas están accesibles a personas o terceras partes no controladas, se deberían tomar medidas especiales para proteger los datos de pruebas: autorizaciones independientes, borrado tras uso, pruebas de auditoría, etc.	

Ficha No conformidades: Gestión de incidencias de la seguridad de la información.

Gestión de incidencias de la seguridad de la información	
NC Mayor: 1	NC Menor: 2
Descripción de la no-conformidades: 13.1.1: Se evidencia un proceso para la notificación de incidencias de seguridad pero no existe documentación sobre el sistema de notificación de incidencias. Tampoco está notificado a los usuarios el objeto del mismo. 13.2.2: Se evidencia la notificación y gestión de los eventos de seguridad pero no se realizan análisis post-morten de los incidentes. Tampoco se reflexiona sobre el coste del incidente y como evitarlo en un futuro. 13.2.3: No existe ningún procedimiento de recopilación de evidencias en caso de incidentes	

de seguridad que implique acciones legales.	
Párrafos de la norma: 13.1.1, 13.2.2 y 13.2.3	Documentos SGSI: N/A
Acción correctora propuesta: Comunicar a los usuarios el objetivo y función de la notificación de incidencias de seguridad; documentar la herramienta, su uso y finalidad. Establecer un procedimiento de gestión de incidentes post-morten (evaluación de costes y mejora continua). Establecer un procedimiento de recopilación de evidencias, es recomendable que este servicio se realice por personal altamente cualificado y con experiencia.	

Ficha No conformidades: Gestión de la continuidad del negocio.

Gestión de la continuidad del negocio	
NC Mayor: 4	NC Menor: 1
Descripción de la no-conformidades: No se está gestionando la continuidad del negocio con ningún tipo de plan o procedimiento.	
Párrafos de la norma: N/A	Documentos SGSI: N/A
Acción correctora propuesta: Elaborar un proyecto de implantación de la gestión de la continuidad del negocio.	

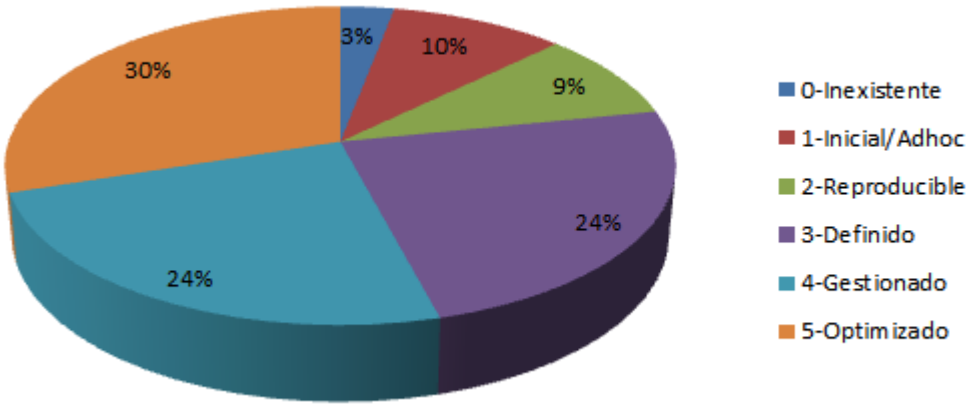
Ficha No conformidades: Cumplimiento.

NC Mayor: 1	NC Menor: 0
Descripción de la no-conformidades: 15.2.1: No existen evidencias de la revisión periódica por parte de la Dirección de los procedimientos de seguridad dentro de su área de responsabilidad.	

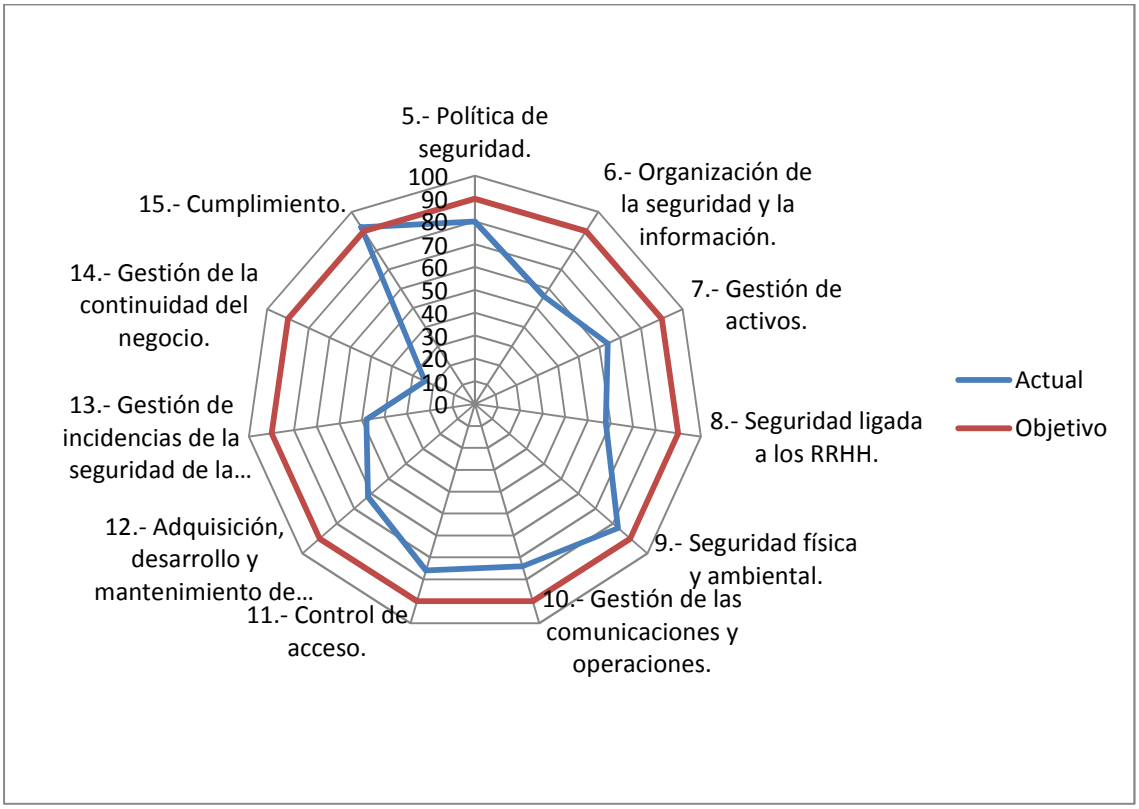
Párrafos de la norma: 15.2.1	Documentos SGSI: N/A
Acción correctora propuesta: Elaborar un checklist de procedimientos de seguridad por área de trabajo y asignar un responsable de revisión. Recopilar evidencias de su verificación.	

5.5.- Presentación de resultados.

5.5.1.- Estado de madurez de los controles.



5.5.2.- Gráfico radar nivel madurez.

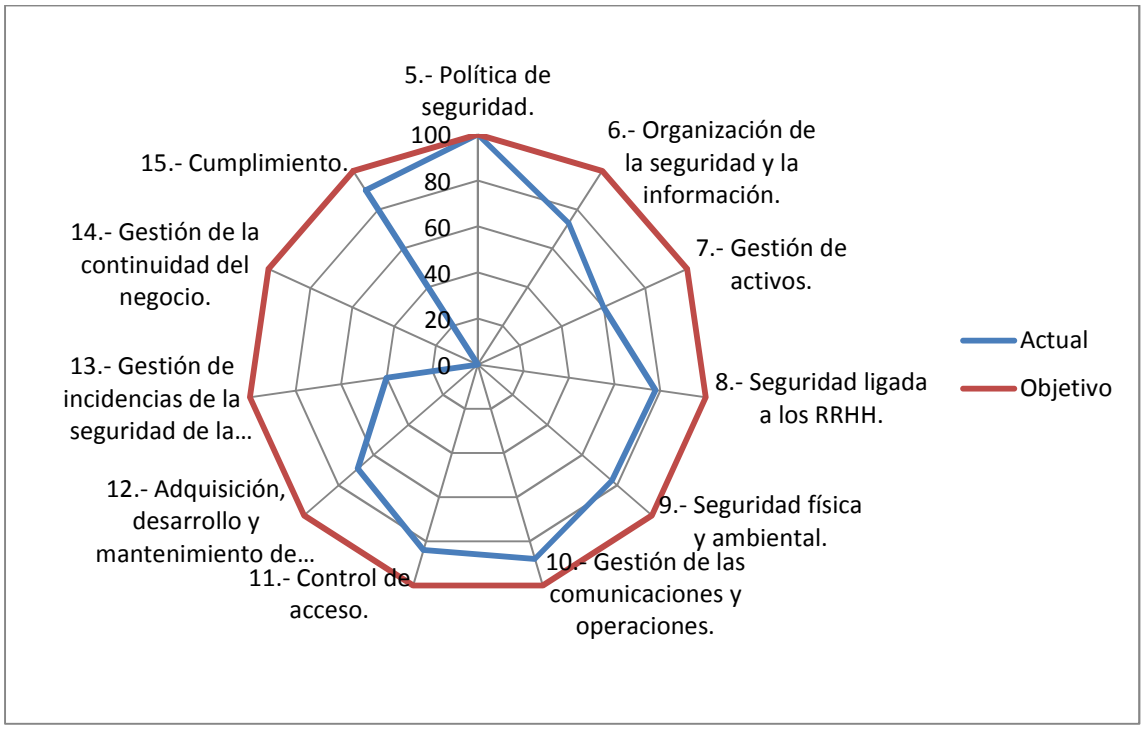


5.5.3.- Resumen de NO-Conformidades dominios.

	No conformidades	
Dominio	**Mayores**	**Menores**
5.- Política de seguridad.	0	0
6.- Organización de la seguridad y la información.	1	2
7.- Gestión de activos.	0	2
8.- Seguridad ligada a los RRHH.	2	0
9.- Seguridad física y ambiental.	2	1
10.- Gestión de las comunicaciones y operaciones.	2	2
11.- Control de acceso.	3	1
12.- Adquisición, desarrollo y mantenimiento de SI.	2	3
13.- Gestión de incidencias de la seguridad de la información.	1	2
14.- Gestión de la continuidad del negocio.	4	1
15.- Cumplimiento.	0	1
Total	17	15

Se entienden como disconformidades mayores (CMM = L0-L1) y disconformidades menores (CMM= L2-L3).

5.5.4.- Gráfico radar cumplimiento dominios.



5.6.- Conclusiones.

Tras finalizar la auditoría de cumplimiento ISO/IEC 27002:2005 observamos que la organización ha experimentado una importante mejoría en la seguridad de la información respecto su posición inicial aunque todavía se identifican dominios con niveles de madurez muy bajos a los que deberían dedicarse esfuerzos para obtener un mejor resultado general.

Un 54% de los controles se mantienen en niveles de madurez L5 y L4, un 33% en niveles de L3-L2 y un 13% en niveles de L1-L0, esto datos demuestran que la organización está a medio camino de obtener un estado maduro de la seguridad de la información y que existen un número elevado controles (13%) que no están definidos o que se encuentran en un estado inicial.

Respecto a la situación de los controles por dominios, evidenciamos un elevado nivel de madurez en los dominios de Política de seguridad, Seguridad Física y Ambiental, Gestión de las operaciones y comunicaciones y control de acceso; todos ellos por encima del 75% de madurez. Pero por el contrario dominios con un bajo control de madurez o simplemente deficientes como por ejemplo: Gestión de incidencias de seguridad y Gestión de la continuidad del negocio, este último de vital importancia para obtener la continuidad del negocio en caso de incidente. Se recomienda tomar medidas inmediatas para mejorar estos dos dominios,

pilares básicos del SGSI, ya que sin ellos no se podrá evidenciar el buen funcionamiento del SGSI. El resto de dominios se encuentran en un nivel de madurez intermedio y requieren potenciar su eficiencia para mejorar su posicionamiento.

Durante la auditoría se han identificado 17 No-conformidades-Mayores y 15 No-conformidades-menores, limitando las conformidades a una por control lo que evidencia que 32 controles (32/133 = 24%) de nuestro SGSI no estaría apto de superar una “auditoría real”. Entre los dominios más afectados, la Gestión de la continuidad del negocio y el Control de acceso; y entre los mejores posicionados la Política de la seguridad de la información y el dominio de Cumplimiento.

Se recomienda a la organización fortalecer el proceso de mejora continua para mejorar el funcionamiento de los controles más débiles y tomar acciones rápidas y contundentes sobre el dominio de la Gestión de la continuidad sin lugar a dudas vital para la supervivencia de la empresa en caso de desastre.

Capítulo 6.

Resumen ejecutivo

La información gira en torno a nuestras vidas y al desarrollo de las organizaciones, ambos necesitamos la información para ser competitivos, lograr objetivos, obtener ventajas y para simplemente continuar con la actividad diaria. La información es imprescindible en la sociedad en la que nos encontramos, en el siglo XXI el concepto ha cambiado y actualmente podemos hablar de la sociedad de la información. Como es evidente la concepción de empresa también se ha transformado, nos encontramos en un mercado globalizado donde las telecomunicaciones son muy importantes, las transacciones y el comercio electrónico han crecido considerablemente, lo que ha supuesto que muchas empresas se conciencien incluyendo el manejo de la tecnología de la información (TI) en sus programas directivos.

"La información es un activo que, como otros activos importantes de la empresa, es esencial para las operaciones de la organización, y en consecuencia necesita ser adecuadamente protegida". *ISO 27002:2005.*

La información se presenta en una organización en distintos medios (papel, almacenada electrónicamente, trasmitida, etc.) y tiene importantes propiedades que se deben mantener: disponibilidad, integridad y confidencialidad.

Es evidente que las organizaciones se enfrentan a amenazas (internas y externas) y vulnerabilidades como por ejemplo: espionaje, sabotaje, vandalismo, incendios, etc.; por todo ello aparece la necesidad de la seguridad de la información, área que nos permitirá protegerla adecuadamente para que nuestra organización pueda mantener su competitividad, rentabilidad y en general su existencia en la sociedad. Si la seguridad de la información fallara o no se aplicara correctamente podríamos tener distintos impactos en nuestra organización, como por ejemplo: pérdidas financieras, denuncias de las autoridades, pérdidas de clientes, pérdida de cuota de mercado, interrupción de las operaciones, daño en la imagen, etc.

Una las normas internacionalmente aceptadas para llevar a cabo nuestro objetivo es ISO/IEC 27000: conjunto de normas y estándares que proporcionan un marco de gestión de la seguridad de la información aplicable a cualquier organización. Por ello consideramos importante el estudio y análisis de la norma para poder aplicarla correctamente en las organizaciones que gestionemos, sin lugar a dudas la aplicación de la misma en la organización mejorará su competitividad, imagen y seguridad.

La buena gestión de los sistemas de información es el camino al éxito de una empresa.

Este trabajo tiene objetivo principal la implementación de la ISO/IEC 27001:2005 en una organización de tamaño mediano dedicada al sector TIC para el turismo. En las primeras fases se ha descrito y contextualizado la organización sobre la que se ha trabajado y a continuación se ha elaborado un análisis diferencial. En este se ha observado que la organización cuenta amplios conocimientos de las tecnologías de la información y con intención de mejorar su sistema de gestión de la seguridad pero no está preparada para superar una certificación oficial de la norma ISO/IEC 27001:2005 y donde sus grandes debilidades: son el apoyo y concienciación de la dirección, el establecimiento de normas, políticas y procedimientos de seguridad bajo una criterio común y la falta de personal cualificado.

En la siguiente fase se ha desarrollado el sistema de gestión documental elaborando documentos tan importantes como la Política de seguridad, Gestión de indicadores, metodología de análisis de riesgos, etc. La empresa no contaba con ninguno de los documentos elaborados en este capítulo, evidencia que demostraba su fuerte debilidad a la formalización de políticas, metodologías y procesos de seguridad. Este apartado ha sido vital para proporcionar una fuerte base para la implementación de la ISO/IEC 27001:2005.

A continuación se ha elaborado el análisis de riesgos de la organización, punto de partida imprescindible para desarrollar un SGSI. Los resultados demuestran importantes amenazas provenientes del factor humano por errores y/o desconocimiento e identifica los activos críticos de la organización (aplicaciones core). Este output es el más importante input para el plan estratégico de seguridad.

Una vez identificadas las amenazas, los activos críticos y realizado el cálculo de riesgos ha sido necesario elaborar el plan estratégico de seguridad, vital para mejorar y evolucionar la seguridad de la organización. La mayoría de estos proyectos orientados a solucionar los problemas más graves de seguridad y a reducir los riesgos evidenciados. Entre estos proyectos el más destacable: Continuidad y recuperación del negocio. Para finalizar este apartado se ha realizado una simulación de mejoras para identificar los beneficios que obtendría la organización en caso de llevarlos a cabo.

Y finalmente hemos concluido el trabajo con una auditoría de la organización tomando como referente la norma ISO/IEC 27002:2005 y de esta manera evidenciar las mejoras obtenidas y detectar las no conformidades no superadas. Con su resultado se evidencia la necesidad de llevar a cabo los proyectos planteados y continuar trabajando en el SGSI.

Bibliografía.

Normas UNE ISO/IEC 27001:2005, AENOR.

Normas UNE ISO/IEC 27002:2005, AENOR.

Análisis GAP ISO/IEC 27002:2005. Adhoc Security. Tristan Ramaget.

Chequeo de cumplimiento ISO/IEC 27001:2005 por Vinod Kumar.

(Material didáctico curso Aenor S0-B) Especialista implantador de sistemas de gestión de la seguridad de la información. AENOR Formación.

Normas ISO de la seguridad de la información. Carlos Ormella Meyer.

ISO/IEC 27000: Implantación y certificación. TFC – JP Nieto Muñoz.

Implantación de la LOPD en la PYMEM. TFC – JP Nieto Muñoz.

Sistema de gestión de la seguridad de la información. UOC. Daniel Cruz / Silvia Garre.

Enfoque metodológico de auditoría a las tecnologías de información y comunicaciones. OLACEFS. Carlos Yañes de la Melena / Sigfrid Enrique Ibsen Muñoz

Anexos.

Anexo A. Política de seguridad.

Control de versiones.

Fecha	Versión	Autor	Revisión
19/MAR/13	0.1	JPNietoMuñoz	Creación política de seguridad.

A.1.- Introducción.

La pérdida o uso indebido de información confidencial y/o sensible así como el deterioro o indisponibilidad de los Sistemas de Información pueden causar la interrupción total o parcial de los procesos de negocio de nuestra organización, produciendo efectos negativos sobre la productividad, beneficios, calidad del servicio e imagen de la entidad.

Garantizar la confidencialidad, integridad y disponibilidad de la información, así como minimizar la probabilidad de que los riesgos a los que está expuesta nuestra organización se manifiesten es el propósito que persigue la definición de las Directrices generales de Seguridad.

El ámbito de aplicación de las Directrices Generales de Seguridad alcanza a todos los Sistemas de Información, instalaciones informáticas y redes de comunicaciones que se encuentren bajo la gestión y responsabilidad de la organización.

El Responsable de Seguridad se compromete a implantar y actualizar esta normativa de obligado cumplimiento. Todas las personas que tengan acceso a los sistemas de información se encuentran obligadas a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Las medidas de seguridad presentadas en esta política de seguridad afectan a toda la organización y deben ser comprendidas, cumplidas y observadas por todo el personal. Esto incluye a las terceras partes (clientes, proveedores, colaboradores, etc.) que pudieran emplear los sistemas de información de la organización.

Recordemos que estas directrices como el resto de normas, procedimientos, estándares o cualquier documento relacionado con la seguridad de la información y los datos que tratan tienen un carácter confidencial y sólo está permitida su uso y difusión con carácter interno y por personal autorizado.

A.2.- Funciones y obligaciones del personal.

En este apartado se recogen las funciones y obligaciones para el personal con acceso a los Sistemas de Información de esta organización. La definición de las funciones y obligaciones del personal tienen como objeto:

- Proteger los Sistemas de información y las redes de comunicación propiedad de la organización o bajo su responsabilidad, contra el acceso o uso no autorizado, alteración indebida, destrucción, mal uso o robo.

- Proteger la información perteneciente o proporcionada a la organización, contra revelaciones no autorizadas o accidentales, alteración, destrucción o mal uso.

A efectos de garantizar el cumplimiento de estas obligaciones, independientemente de su función y responsabilidad, la entidad exige con carácter general a cualquier empleado el cumplimiento de los siguientes aspectos:

- Confidencialidad de la información.
- Propiedad intelectual.
- Control de acceso físico.
- Salidas de información.
- Incidencias.
- Uso apropiado de los recursos.
- Software.
- Hardware.
- Conectividad a Internet.
- Correo electrónico.

A.2.1.- Confidencialidad de la información.

- Se debe proteger la información, propia o confiada a la organización, evitando un uso indebido o su envío no autorizado al exterior a través de cualquier medio de comunicación.

- Se deberá guardar máxima reserva, por tiempo indefinido, la información, documentos, metodologías, claves, análisis, programas y el resto de información a la que se tenga acceso.

- En caso de tratar con información confidencial, en cualquier tipo de soporte, se deberá entender que la posesión de esta es temporal, con obligación de secreto y sin que ello le concediera derecho alguno de posesión, titularidad o copia sobre esta. Inmediatamente después de la finalización de las tareas que hubieran originado el uso, debería devolverse a la entidad.

A.2.2.- Propiedad Intelectual.

Queda totalmente prohibido en los Sistemas de Información de la organización:

- El uso de aplicaciones informáticas sin la correspondiente licencia. Los programas informáticos propiedad de la organización están protegidos por la propiedad intelectual y por lo tanto está prohibida su reproducción, modificación, cesión o comunicación sin autorización.

- El uso, reproducción, modificación, cesión o comunicación de cualquier otro tipo de obra protegida por la propiedad intelectual sin debida autorización.

A.2.3.- Control de acceso físico.

Las normas en cuanto al acceso físico a las instalaciones de la organización que albergan los Sistemas de Información y los locales de tratamiento son las siguientes:

- El acceso a las instalaciones donde se encuentran los Sistemas de Información y los locales de tratamiento, se realizará previo paso por un sistema de control de acceso físico o con autorización del responsable de las instalaciones.

A.2.4.- Salidas de información.

Toda salida de información de datos de carácter personal (en soportes informáticos o sistemas de información) deberá ser realizada por el personal autorizado y será necesario autorización formal del Responsable del Fichero del que provienen los datos.

En la salida de información de nivel alto / confidencial se deberán cifrar los mismos o utilizar cualquier otro mecanismo que no permita el acceso o su manipulación durante el transporte.

A.2.5.- Incidencias.

El personal de la organización y terceras partes (clientes, proveedores, etc.) tienen como obligación comunicar cualquier incidencia que se produzca y esté relacionada con los sistemas de información o cualquier otro recurso informático de la entidad.

La comunicación, gestión y resolución de las incidencias de seguridad se realizarán mediante el sistema de gestión de incidencias habilitado por la organización. Toda esta información está recogida en el capítulo Notificación y gestión de incidencias.

A.2.6.- Uso apropiado de los recursos.

Los recursos informáticos ofrecidos por la organización (datos, software, comunicaciones, etc.) están disponibles exclusivamente para cumplir con las obligaciones laborales y con una

finalidad corporativa. Por lo tanto, queda terminantemente prohibido cualquier uso distinto al indicado, algunos ejemplos:

- El uso de los recursos de la organización o aquellos que estén bajo su supervisión para actividades no relacionadas con la finalidad de la entidad.

- El uso de equipos, dispositivos o aplicaciones que no estén especificados como parte de software y/o hardware contenidos en la organización.

- Introducir en los sistemas de información o red corporativa contenidos ilegales, inmorales u ofensivos y en general, sin utilidad para los procesos de negocio de la organización.

- Introducir voluntariamente programas, virus, spyware o cualquier otro software malicioso que sean susceptibles de causar alteraciones en los recursos informáticos de la organización o de terceros.

- Desactivar o inutilizar los programas antivirus y de protección del equipo (pe. Firewall) y sus actualizaciones.

- Intentar eliminar, modificar, inutilizar los datos, programas o cualquier otra información propios de la organización o confiados a ella.

- Conectarse a la red corporativa a través de otros medios que no sean los definidos y administrados por la empresa.

- Intentar falsear los registros de software (logs) de los sistemas de información.

- Intentar descubrir o descifrar las claves de acceso o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la organización.

A.2.7.- Software.

- Los usuarios deben utilizar únicamente las versiones de software facilitadas por la organización y seguir sus normas de utilización.

- El servicio de informática (o en su defecto el encargado de su función) es el responsable de definir los programas de uso estandarizado en la organización y de realizar las instalaciones en los PCs.

- Los usuarios no deben instalar ni borrar ningún tipo de programa informático en su PC.

A.2.8.- Hardware.

- Los usuarios, en su actividad laboral, deben hacer uso únicamente del hardware instalado en los equipos propiedad de la organización y cuya función lo requiera para el trabajo que desempeña.

- El usuario en ningún caso accederá físicamente al interior del equipo que tiene asignado para su trabajo o que pertenezca a la propiedad de la organización. En caso necesario se comunicará la incidencia, según protocolo habilitado, para que el departamento indicado (o en su defecto el encargado de su función) realice las tareas de reparación, instalación o mantenimiento.

- Los usuarios no manipularán los mecanismos de seguridad que la organización implemente en los dispositivos (equipos, portátiles, móviles, smartphones, etc.) de su parque informático.

- No sacar equipos, dispositivos o soportes de las instalaciones sin la autorización necesaria, y en todo caso, con los controles y medidas que se hayan establecido para cada supuesto.

A.2.9.- Conexión a Internet.

La autorización de acceso a Internet se podría conceder o bloquear de manera acorde con la labor que los usuarios desempeñan en la organización. Los accesos a Internet podrían estar regulados y controlados por el servicio de informática de la entidad (o en su defecto el encargado de su función).

- El acceso a Internet se realiza exclusivamente a través de la red establecida para ello y por los medios facilitados por la organización.

- El uso de Internet es un servicio que la organización pone a disposición de los usuarios para un uso estrictamente profesional en las tareas asignadas en la organización.

- La transferencia de datos a/desde Internet se realizará exclusivamente cuando las actividades propias del trabajo lo exijan. En el caso de tratarse de datos de carácter personal de nivel alto sólo se podrán transferir en forma cifrada.

A.2.10.- Correo electrónico.

Las normas referentes al correo electrónico son:

- El servicio de correo electrónico (o cuentas de correo) que la organización pone a disposición de los usuarios tiene un uso estrictamente profesional y destinado a cubrir las necesidades de su puesto.

- Queda terminantemente prohibido intentar leer, borrar, copiar o modificar mensajes de correo electrónico de otros usuarios.

- Los usuarios no deben enviar mensajes de correo electrónico de forma masiva o de tipo piramidal con fines publicitarios o comerciales. En el caso que sea necesario, dada la función del usuario, este tipo de mensajes se gestionarán con la dirección de la organización y con el responsable de seguridad.

- El servicio de informática (o en su defecto el encargado de su función) velará por el uso correcto del correo electrónico con el fin de prevenir actividades que puedan afectar a la seguridad de los sistemas de información y de los datos.

A.3.- Monitorización.

Con el fin de velar por el uso correcto de los distintos sistemas de información de la organización, así como garantizar la integridad, confidencialidad y disponibilidad de los datos de la organización, la organización a través de los mecanismos formales y técnicos que considere oportuno, podría comprobar, ya sea de forma periódica o cuando la situación técnica lo requiera, la correcta utilización de los recursos de la organización por todo el personal.

En el caso de apreciar un uso incorrecto de los recursos asignados al usuario (aplicaciones, correo electrónico, conexión a Internet, etc.) se le comunicará la circunstancia y se le facilitará la formación necesaria para el uso correcto de los recursos.

En el caso de apreciarse mala fe en la utilización de los recursos informáticos, la organización podría ejercer las acciones legales que le amparen para la protección de sus derechos.

A.4.- Actualizaciones de las directrices de seguridad.

Dada la evolución de la tecnología, de las amenazas de seguridad y las nuevas aportaciones legales en la materia, la organización se reserva el derecho a modificar cualquiera de los aspectos incluidos en este capítulo “Directrices de seguridad” cuando sea necesario. Los cambios realizados en esta serán divulgados a todas las personas de la organización y en especial a aquellas que tengan acceso a los sistemas de información.

Es responsabilidad final de cada persona la lectura y conocimiento de las directrices aquí expuestas.

A.5.- Política de usuarios y contraseñas.

- Todos los usuarios con acceso al sistema de información dispondrán de una autorización de acceso compuesta de usuario y contraseña.

- Se usarán usuarios personales y se evitarán el uso de usuarios genéricos (su uso sólo estará justificado cuando se pueda asociar su acceso con una única persona).

- El nombre de usuario y contraseña asignados a una persona se comunicarán de forma verbal junto con una copia de las obligaciones del personal en materia de seguridad de la información. La primera vez que la persona inicie sesión en el sistema deberá modificar la contraseña proporcionada para que esta sólo sea conocida por él.

- El almacenamiento de usuarios y contraseñas se realizará utilizando los mecanismos propios de los Sistemas Operativos y aplicaciones, de manera que estos no sean inteligibles y preferentemente utilizando cifrado.

- La longitud será igual o superior a 6 caracteres alfabéticos, numéricos y especiales. Se obligará el uso de la longitud mínima.

- La vigencia máxima de las contraseñas (caducidad) será de 180 días.

- El sistema inhabilitará, siempre que tecnológicamente se permita, el acceso que intente conectarse de forma consecutiva mediante identificadores y/o contraseñas incorrectas. El número máximo de intentos permitidos es 5.

A.6.- Acceso físico a las instalaciones.

Este apartado tiene como objeto el control de acceso físico a las instalaciones para prevenir el acceso accidental, no autorizado de terceros a los datos, así como prevenir accidentes y daños sobre los sistemas de información de la organización.

Los entornos a proteger serán los centros de procesamiento de datos (en el caso de que existan), despachos o ubicaciones con ordenadores personales y/o servidores, armarios y otras ubicaciones similares destinadas al tratamiento y almacenamiento de datos personales.

- Sólo el personal autorizado tendrá el acceso permitido a los locales, instalaciones o despachos donde se encuentren los sistemas de información con datos de carácter personal. En el caso en donde su ubicación sea una zona común se bloqueará el acceso a este mediante las medidas oportunas.

- La seguridad de los centros de tratamiento y almacenamiento de datos de carácter personal serán responsabilidad del Responsable del Fichero y Responsable de Seguridad.

- En las ubicaciones en donde no exista control de acceso físico, las personas que trabajan en el mismo y el personal de seguridad (si existe) deberá controlar especialmente el acceso de personas.

- Los equipos, soportes y documentos que contengan datos personales no serán sacados de las dependencias sin autorización expresa del Responsable del Fichero tal y como indica la política general de la organización.

- Si los usuarios dejan su puesto desatendido deberán guardar todos los soportes que contengan datos personales (CD, DVD, documentos, expedientes, etc.) de forma que no puedan ser accedidos por personas no autorizadas.

A.7.- Responsabilidades.

En todo momento el Responsable de Seguridad velará por el cumplimiento de las normas descritas en la Política de Seguridad y la legislación vigente, y si detectan el incumplimiento de las mismas, ya sea de forma deliberada o accidental, alertará a los causantes realizando un seguimiento hasta asegurarse de que desaparece el problema.

En el caso de un incumplimiento deliberado, reincidente o de relevante gravedad se analizarán las circunstancias pudiendo incurrir en la imputación de una falta disciplinaria, leve, grave o muy grave dependiendo de los hechos acontecidos. En tal caso, se adoptarán las medidas previstas y se informará a las autoridades competentes.

A.8.- Resumen política seguridad.

El comité de dirección de la organización considera que la información y los sistemas del negocio son activos estratégicos por lo que manifiesta su determinación para mantener y garantizar su seguridad.

Este documento denominado *Política de Seguridad* tiene como objeto proporcionar las directrices básicas para garantizar los sistemas de información de la empresa en base a los criterios de confidencialidad, integridad y disponibilidad.

Alcance.

Dado su carácter de política es de obligado conocimiento y cumplimiento para toda la organización y terceras partes (clientes, proveedores, asociados, etc.) que utilicen los sistemas de información corporativos.

Especificaciones.

La Dirección de la organización concede un interés prioritario y el máximo apoyo a la protección de la información por su carácter estratégico para el negocio y su continuidad.

Esta política tiene como objetivo preservar los tres componentes básicos de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad; Y será de aplicación en todas las

fases del ciclo de vida de la información, desde la generación hasta su destrucción, así como para los sistemas que la soportan: desde el análisis hasta la explotación y mantenimiento.

La Política debe ser comunicada fehacientemente a toda la Organización y otras partes interesadas (clientes, proveedores, colaboradores, etc.).

La función de seguridad recae sobre el Comité de seguridad, que será el encargado de establecer las directrices y principios básicos de seguridad, así como velar por su cumplimiento.

Cada activo de información tendrá asignado un responsable que será el que velará por su utilización y protección, asimismo todo usuario de los sistemas de información es responsable del uso adecuado de los mismos y de cumplir con los controles y recomendaciones establecidas.

La empresa tiene la obligación de cumplir con la legislación vigente en materia de protección y seguridad de la información, por lo tanto deberán identificarse las leyes aplicables en el tratamiento y seguridad de la información así como establecer los mecanismos para cumplirlas.

Formación y concienciación.

El método más efectivo para mejorar y mantener la seguridad es mediante la formación continuada, por ello se incluirán en los planes de formación de la empresa cursos específicos de seguridad acorde con los destinatarios. Asimismo se realizarán campañas de concienciación dirigida a todo el personal, proveedores y otras terceras partes.

Vigencia.

Esta política de seguridad está en vigencia desde el día de hoy y será revisada al menos anualmente.

Anexo B. Procedimiento auditorias internas.

La certificación de una organización es la valoración de los propios esfuerzos en la implementación del SGSI así como la oportunidad de ampliación de mercado y diferenciación con respecto a la competencia. Recordemos que obtener la certificación significa adherirse a un estándar internacional de referencia ISO/IEC 27001:2005 demostrando la conformidad con el mismo por medio de evidencias objetivas además de demostrar la eficacia del SGSI. Aunque el objetivo puede parecer sencillo debemos recordar que implica una serie de tareas que requieren la asignación de recursos y el compromiso de la dirección.

Entre las tareas que se deben realizar para acceder y mantener la certificación se incluye el procedimiento de auditorías internas. Este apartado describe el procedimiento de auditorías internas, que actuará de forma similar a los procesos de auditoría externa de re-certificación.

1.- Fase 1 - Auditoría documental: Durante esta fase los auditores deben revisar la documentación del SGSI (según lo previsto en el requerimiento 4.3.1 del estándar) para comprobar si la organización cuenta con un sistema suficientemente maduro y completo como para superar la fase 2. En esta fase los auditores revisan la política y el alcance del SGSI, el análisis de riesgos, la selección de controles y los procedimientos establecidos.

Con el resultado de estas valoraciones se prepara un informe en donde se recogerán los puntos fuertes y los puntos débiles del SGSI así como las no conformidades halladas, con indicación de su gravedad. Existen tres tipos de hallazgos:

- No conformidades mayores: indican un incumplimiento de requisito de la norma o del SGSI, el auditor considera que pone en peligro la seguridad de la información de la organización. Estas no conformidades deben estar resueltas antes de comenzar la fase 2.

- No conformidades menores: son incumplimientos parciales o menores de la norma o de alguna de las reglas internas. Debe estar como mínimo en fase de resolución antes de llegar a la fase 2.

- Observaciones u oportunidades de mejora: son anotaciones que no requieren ser tratadas de momento pero que en próximas auditorías puede ser revisado su estado para determinar si la situación ha empeorado.

2.- Fase 2 - Auditoría de certificación: En esta fase los auditores deben confirmar que la organización cumple con las políticas, objetivos y procedimientos del SGSI y que estos son eficaces. Para ello se realizarán pruebas de cumplimiento, es decir, se buscarán evidencias objetivas del cumplimiento y eficacia de las normas establecidas por la organización. Algunos ejemplos:

- Revisión de los registros de incidencias, para comprobar que se gestionan.

- Informes de pruebas de recuperación, para comprobar que se realizan.

A continuación se describe la normativa a aplicar para la realización de auditorías.

- La organización establecerá una auditoría interna cada año, que verificará el cumplimiento de los requerimientos de la certificación ISO.

- Se realizarán auditorías externas cada tres años, previas a las auditorías de re-certificación (al menos con 6 meses de antelación). En estas auditorías se simulará la auditoría de todo el SGSI como si de la entidad certificadora se tratase.

- El Responsable de Seguridad trasmitirá el informe de auditoría al comité de Seguridad.

- Los informes de auditoría serán analizados por el Responsable de Seguridad, que tomará las medidas correctoras oportunas.

- Los informes de las auditorías realizadas se depositarán y archivarán en la organización junto a la documentación relativa al SGSI. Esta documentación quedará a disposición de las entidades de certificación.