Plan de mejora de la Seguridad de la Información, a través de la implantación de un SGSI

Memoria del Proyecto

Nombre Estudiante: Carlos Vila Martínez
Programa: Proyecto Final de Posgrado Gestión y Auditoría de la Seguridad
Nombre Consultor: Arsenio Tortajada Gallego
Centro: Universitat Oberta de Catalunya
Fecha Entrega: 7 de Junio de 2017

Índice

1. Introducción..... 1
1.1 Contexto y justificación del Proyecto..... 1
1.2 Objetivos del Proyecto..... 1
1.3 Enfoque y método seguido..... 1
1.4 Planificación del Proyecto..... 2
2. La empresa FCA..... 4
2.1 Misión, descripción y estado actual..... 4
2.2 Caso de estudio..... 4
3. Descripción..... 5
3.1 Organigrama..... 5
3.2 Cultura de la empresa FCA..... 6
3.3 Medios..... 8
3.3 Tareas..... 16
4. Situación actual..... 17
5. Plan de Acción..... 19
6. Política de Seguridad..... 20
7. Procedimiento Auditorías Internas..... 20
8. Gestión de indicadores..... 20
9. Procedimiento de revisión directiva..... 20
10. Gestión roles y responsabilidades..... 20
11. Metodología de Análisis de Riesgos..... 21
12. Proyecto de mejora de la seguridad..... 24
13. Auditoría de cumplimiento..... 24
14. Conclusiones..... 25
14. Glosario..... 26
15. Bibliografía..... 29
Anexo I. Inventario y valoración activos..... 30
Anexo II. Política de Seguridad..... 34
Anexo III. Auditorías Internas..... 39
Anexo IV. Gestión de Indicadores..... 41
Anexo V. Revisión por la Dirección..... 47
Anexo VI. Roles y Responsabilidades..... 48
Anexo VII. Análisis de las amenazas..... 49
Anexo VIII. Análisis de los riesgos..... 50
Anexo IX. Propuestas de proyectos..... 54
Anexo X. Declaración de Aplicabilidad..... 64
Anexo XI. Auditoría de cumplimiento..... 85
Anexo XII. Evaluación estado del CMM..... 90

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SenseObraDerivada 3.0 España de Creative Commons

FICHA DEL PROYECTO FINAL

Título del Proyecto:	*Plan de mejora de la Seguridad de la Información, a través de la implantación de un SGSI*
Nombre del autor:	*Carlos Vila Martínez*
Nombre del consultor:	*Arsenio Tortajada Gallego*
Fecha de presentación (mm/aaaa):	*06/2017*
Área del Proyecto Final:	*Gestión y Auditoría de la Seguridad*
Titulación:	*Posgrado en Gestión y Auditoría de la Seguridad*

Resumen del Proyecto (máximo 250 palabras):

La empresa FCA se dedica al sector de la Ferretería y Suministro Industrial. Inicia su actividad en el año 1967 y con motivo de su 50 aniversario, ha decidido llevar a cabo una reorganización de sus procesos, entre los cuales destaca un importante avance en lo que a Seguridad de la Información se refiere.

En los últimos años ha establecido relaciones comerciales con diferentes administraciones (estatales, autonómicas y locales), lo que ha llevado implícito un frecuente intercambio de información de carácter confidencial. Este ha sido el principal motivo por el que se ha considerado conveniente incrementar el nivel de seguridad en sus sistemas de información.

Por este motivo se han puesto en contacto con una Consultoría Tecnológica especializada, que va a llevar a cabo el diseño, implementación e integración de un Sistema de gestión de Seguridad de la Información (SGSI).

En un principio, no se considera necesario su certificación en la ISO/IEC 27001:2013, pero si conveniente que el SGSI quede totalmente preparado para este proceso.

Se estima que la duración aproximada del proyecto sea de 4 meses y su fecha de entrega dentro de la primera quincena del mes de junio del presente año.

Abstract (in English, 250 words oro less):

The company FCA is dedicated to the sector of the Hardware and Industrial Supply. It begins its activity in the year 1967 and on the occasion of its 50th anniversary, has decided to carry out a reorganization of its processes, among which stands out an important advance as far as Information Security is concerned.

In recent years it has established commercial relations with different administrations (state, regional and local), which has implied a frequent exchange of confidential information. This has been the main reason why it has been considered desirable to increase the level of security in their information systems.

At first, it´s not considered necessary to be certified in ISO / IEC 27001: 2013, but it is desirable that the ISMS be fully prepared for this process.

It´s estimated that the approximate duration of the project is 4 months and its delivery date within the first half of June of this year.

Palabras clave (entre 4 y 8):

SGSI, ISO, 27001, Seguridad, Auditoría, Certificación

Lista de figuras

Nombre	Página
Proyecto implantación SGSI en la empresa	3
Organigrama de la empresa FCA	5
Cultura de la empresa FCA	6
Tabla de medios relacionados con el entorno	9
Tabla de equipamiento informático - Sede 1	10
Tabla de información base de las operaciones de empresa	10
Tabla de funcionalidades o servicios	11
Tabla de otros activos importantes	11
Plano tienda – Sede 1	12
Plano almacén 1 – Sede 1	13
Plano almacén 2 – Sede 1	14
Plano nave – Sede 2	15
Tabla tareas: Dirección, compras, informática, administración, almacén, RRHH y PRL	16
Tabla propuesta de actuaciones	19
Tabla estimación de probabilidad de ocurrencia de una amenaza	21
Tabla impacto provocado por la materialización de la amenaza	21
Tabla con los criterios de aceptación del riesgo	21
Tabla cruce probabilidad-impacto-riesgo	22
Tablas con el inventario y valoración de activos	30-33
Tabla con las dimensiones de seguridad de la información	31
Tabla con la valoración del daño y criterio	31
Tabla resumen valoración criticidad de los activos según dimensiones ACIDT	32-33
Tablas gestión de indicadores	41-46
Tablas gestión de roles y responsabilidades	48
Tabla con el análisis de amenazas sobre las 5 dimensiones de seguridad (ACIDT)	49
Tabla con el cruce del análisis de amenazas y tratamiento del riesgo	50-52
Diagrama de radar con la evolución de la ISO27001:2013	63
Tablas con la declaración de aplicabilidad	64-84
Tabla con los dominios evaluados para FCA	85
Tabla de efectividad y significado del modelo CMM	85
Tablas con las no conformidades	87-89
Tablas de evaluación del estado de madurez del CMM	90-100
Diagrama circular CMM sobre los dominios ISO27002:2013	101

1. Introducción

1.1 Contexto y justificación del Proyecto

El contexto en el que nos situamos es el de FCA, una empresa familiar con 50 años de experiencia, fundada en el año 1967 y dedicada al sector de la Ferretería y Suministro Industrial.

En el año 1986 se incorpora el primer ordenador para automatizar el proceso de facturación. Posteriormente, en 1993 se procede a la implantación de un ERP (Enterprise Resource Planning) para todos los procesos de gestión y contabilidad. La evolución de su Sistema de Información ha ido pareja a los diferentes cambios tecnológicos y actualmente dispone de una red corporativa de 6 puestos fijos y 5 móviles, entre los que se encuentran 2 ordenadores portátiles, 1 tablet y 2 dispositivos tipo smartphone.

Desde hace unos años ha establecido relaciones comerciales con diferentes administraciones públicas, lo que ha llevado a plantearse la necesidad de incrementar su nivel de seguridad en los Sistemas de Información.

Por este motivo se plantea la implantación de un Sistema de Gestión de Seguridad de la Información, tomando como referencia la Norma ISO 27001. Se ha determinado que la finalidad de este SGSI sea la de incrementar notablemente la seguridad de todos los procesos en los que esté involucrada la Información e inicialmente de descarta la necesidad de certificarse en la Norma ISO 27001. Lo que si se ha determinado es que el SGSI quede preparado para este futuro escenario de certificación se haga de forma adecuada y ordenada.

1.2 Objetivos del Proyecto

El objetivo principal de este proyecto es la implantación de un SGSI, en la empresa FCA, que siente las bases para la mejora continua en materia de Seguridad de la Información, y que esté alineado con una normativa internacional de referencia, como es la ISO/IEC 27001:2013. De este modo, se dota a la organización de los procesos y herramientas adecuados para que, en todo momento, tengan conocimiento del estado de la seguridad de su información. Se pretende que la empresa esté preparada para minimizar el impacto de los potenciales riesgos que puedan afectar a la seguridad de cualquiera de sus activos.

1.3 Enfoque y método seguido

Partimos del estudio preliminar de la empresa FCA y del análisis de su situación actual en lo que a seguridad de la información se refiere, con la intención de proceder al diseño e implantación de un Sistema de Gestión

de Seguridad de la Información, que pueda ayudar a incrementar su nivel de seguridad y posteriormente, si fuese necesario, certificarse en la Norma ISO 27001.

La estrategia de trabajo está basada en la implantación de un SGSI sobre el ERP actual, modificando aquellos procesos que sean necesarios, eliminando aquellos otros que hayan quedado obsoletos e incorporando otro nuevos, en función de los requerimientos y necesidades actuales.

1.4 Planificación del Proyecto

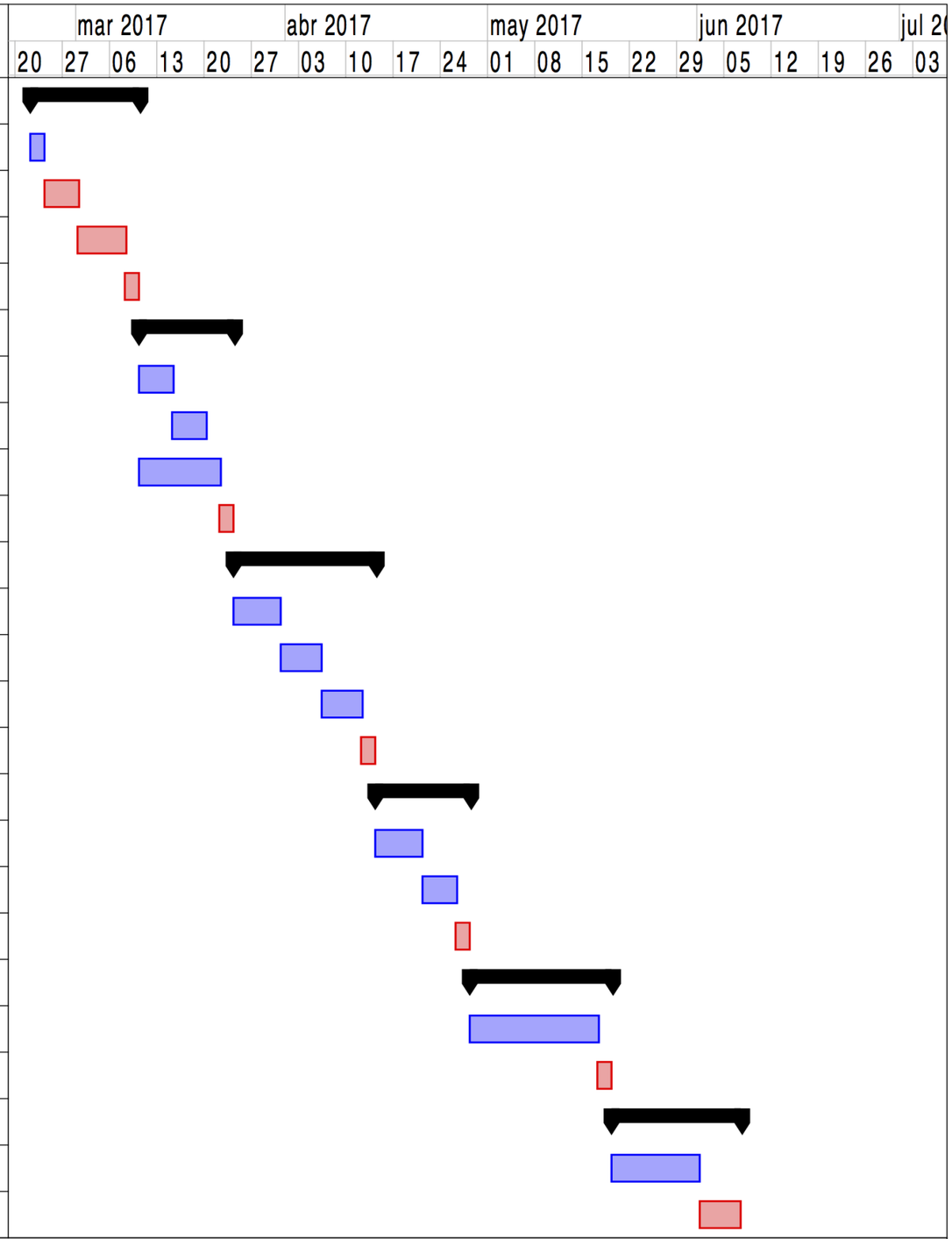
Para la realización de las diferentes fases del presente proyecto se han utilizado los siguientes recursos:

- Ordenador iMAC con procesador Intel Core i7 a 4Ghz con 16Gb de memoria RAM y almacenamiento de 1TB. Sistema Operativo anfitrión OS X El Capitán versión 10.11.6.
- Ordenador portátil Toshiba Satellite C855-21M con procesador Intel Core i3 a 2,8Ghz y 500Gb de almacenamiento interno. Sistema Operativo Ubuntu 16.10 LTS.
- Dispositivo USB 3.0 ScanDisk de 128Gb de capacidad.
- Paquete ofimático Libre Office versión 5.2.3.
- Programa de manipulación de imágenes GIMP versión 2.8.14.
- Software de virtualización Parallels Desktop versión 11.2.1.
- Máquinas virtuales: Windows 7, Ubuntu 16.10 LTS y Kali Linux.

El proyecto de implantación del SGSI tiene una duración aproximada de 4 meses. Su planificación se ha llevado a cabo en base a 6 Hitos distribuidos entre el 22 de Febrero (fecha de inicio del proyecto) y el 7 de Junio (fecha estimada de entrega).

El gráfico que se presenta a continuación corresponde al diagrama de Gantt con la temporización semanal y la relación de tareas a llevar a cabo para la consecución de cada hito.

	Nombre	Duracion	Inicio	Terminado
1	**Hito 1: Situación actual**	**13 days**	**22/02/17 8:00**	**10/03/17 17:00**
2	Enfoque y selección de la empresa	3 days	22/02/17 8:00	24/02/17 17:00
3	Definición objetivos Plan Director Seguridad	4 days	24/02/17 8:00	1/03/17 17:00
4	Análisis diferencial	6 days	1/03/17 8:00	8/03/17 17:00
5	Presentación de resultados	3 days	8/03/17 8:00	10/03/17 17:00
6	**Hito 2: Sistema de Gestión Documental**	**11 days**	**10/03/17 8:00**	**24/03/17 17:00**
7	Elaboración Política de Seguridad	4 days	10/03/17 8:00	15/03/17 17:00
8	Declaración Aplicabilidad (SOA)	4 days	15/03/17 8:00	20/03/17 17:00
9	Documentación SGSI	9 days	10/03/17 8:00	22/03/17 17:00
10	Presentación de resultados	3 days	22/03/17 8:00	24/03/17 17:00
11	**Hito 3: Análisis de Riesgos**	**16 days**	**24/03/17 8:00**	**14/04/17 17:00**
12	Identificación y valoración de Activos	6 days	24/03/17 8:00	31/03/17 17:00
13	Identificación Amenazas, Vulnerabilidades	5 days	31/03/17 7:00	6/04/17 17:00
14	Cálculo del riesgo	5 days	6/04/17 7:00	12/04/17 17:00
15	Presentación de resultados	3 days	12/04/17 7:00	14/04/17 17:00
16	**Hito 4: Propuesta de Proyectos**	**11 days**	**14/04/17 8:00**	**28/04/17 17:00**
17	Evaluación y elección de Proyecto	6 days	14/04/17 8:00	21/04/17 17:00
18	Cuantificación económica y temporal	4 days	21/04/17 8:00	26/04/17 17:00
19	Presentación de resultados	3 days	26/04/17 8:00	28/04/17 17:00
20	**Hito 5: Auditoría de cumplimiento ISO27702:2013**	**16 days**	**28/04/17 8:00**	**19/05/17 17:00**
21	Evaluación de controles, madurez y nivel cumplimiento	14 days	28/04/17 8:00	17/05/17 17:00
22	Presentación de resultados	3 days	17/05/17 8:00	19/05/17 17:00
23	**Hito 6: Entrega de Informes finales y presentación Proyecto**	**14 days**	**19/05/17 8:00**	**7/06/17 17:00**
24	Confección de informes finales	10 days	19/05/17 8:00	1/06/17 17:00
25	Presentación ejecutiva y entrega del Proyecto	5 days	1/06/17 8:00	7/06/17 17:00



Proyecto implantación SGSI en la empresa FCA

2. La empresa FCA

2.1 Misión, descripción y estado actual

FCA es una empresa familiar que se dedica actualmente a la venta de productos/prestación de servicios de ferretería y suministro industrial en territorio nacional.

- Se fundó en el año 1967 e inicio su actividad con dos personas.
- Tiene sus instalaciones en Ferrol (A Coruña).
- Actualmente cuenta con una plantilla de seis empleados.
- Sus principales clientes son profesionales y pymes del sector de la carpintería de madera/metal, así como empresas del sector naval.
- El 100% de sus clientes están asentados en territorio español.
- El indice de rotación de sus empleados es muy bajo.

Actualmente patrocina una asociación de torneros que está muy ligada a su proceso de negocio de forma:

- FCA ha construido un taller de torneado en una de sus instalaciones, que cede de forma altruista a la asociación para la realización de diferentes actividades.
- El taller está ubicado en parte de una nave destinada al almacenaje de productos.
- La finalidad de dicho taller es la realización de cursos de formación, así como servir de exposición de maquinaria.
- La empresa FCA acaba de obtener la distribución exclusiva para Galicia de una linea de productos para profesionales de la carpintería de madera.
- La empresa FCA vende maquinaria y consumibles a los miembros de esta asociación, así como a cualquier otro profesional o particular interesado.

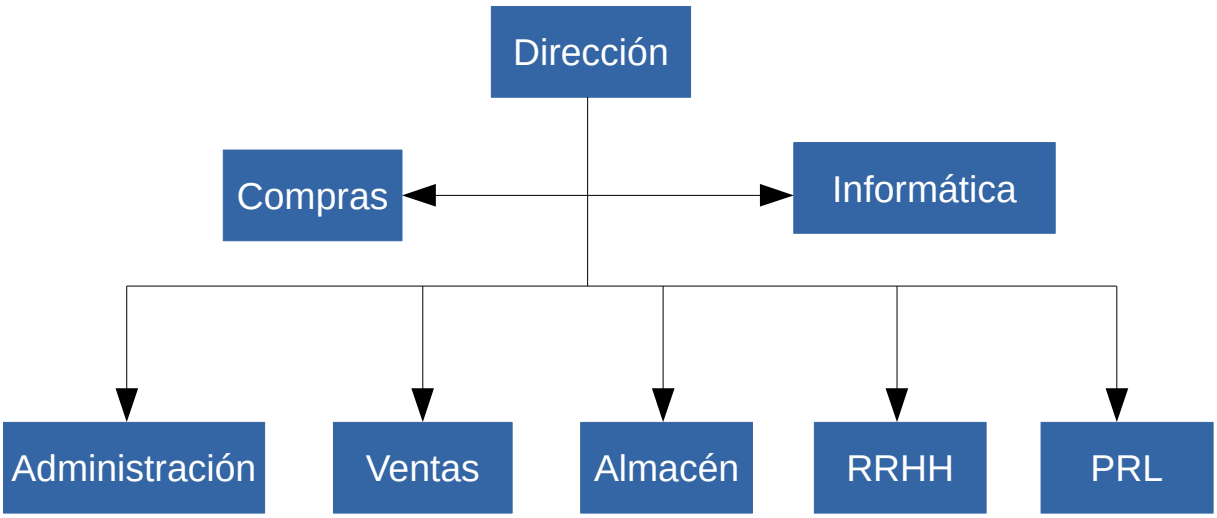
2.2 Caso de estudio

En los últimos años, la empresa FCA ha establecido relaciones comerciales con diferentes administraciones públicas. Dado el carácter confidencial de la información que se puede llegar a compartir, se hace necesaria la mejora de la seguridad, a través de la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) que además pueda certificarse en la norma ISO/IEC 27001, en caso de ser requerido.

3. Descripción

3.1 Organigrama

La empresa FCA cuenta con el siguiente organigrama:



Dirección: La empresa está constituida como sociedad limitada de tres miembros, en la que el Gerente es la cabeza visible y responsable de la misma. El resto de socios no pertenecen a la estructura organizativa de la misma.

Compras: La persona encargada de compras es el propio gerente, que además desarrolla otras labores de apoyo en la administración.

Informática: Está externalizada en dos empresas que llevan por un lado el mantenimiento del ERP y por el otro la consultoría de seguridad, comercio electrónico y social media. Ambas empresas están supervisadas directamente por el gerente.

Administración: Esta función es llevada a cabo por una persona, que se encarga de la contabilidad y gestión.

Ventas: Esta función es realizada por 4 personas, de las cuales 1 realiza también la labor comercial fuera de la empresa (dos días por semana).

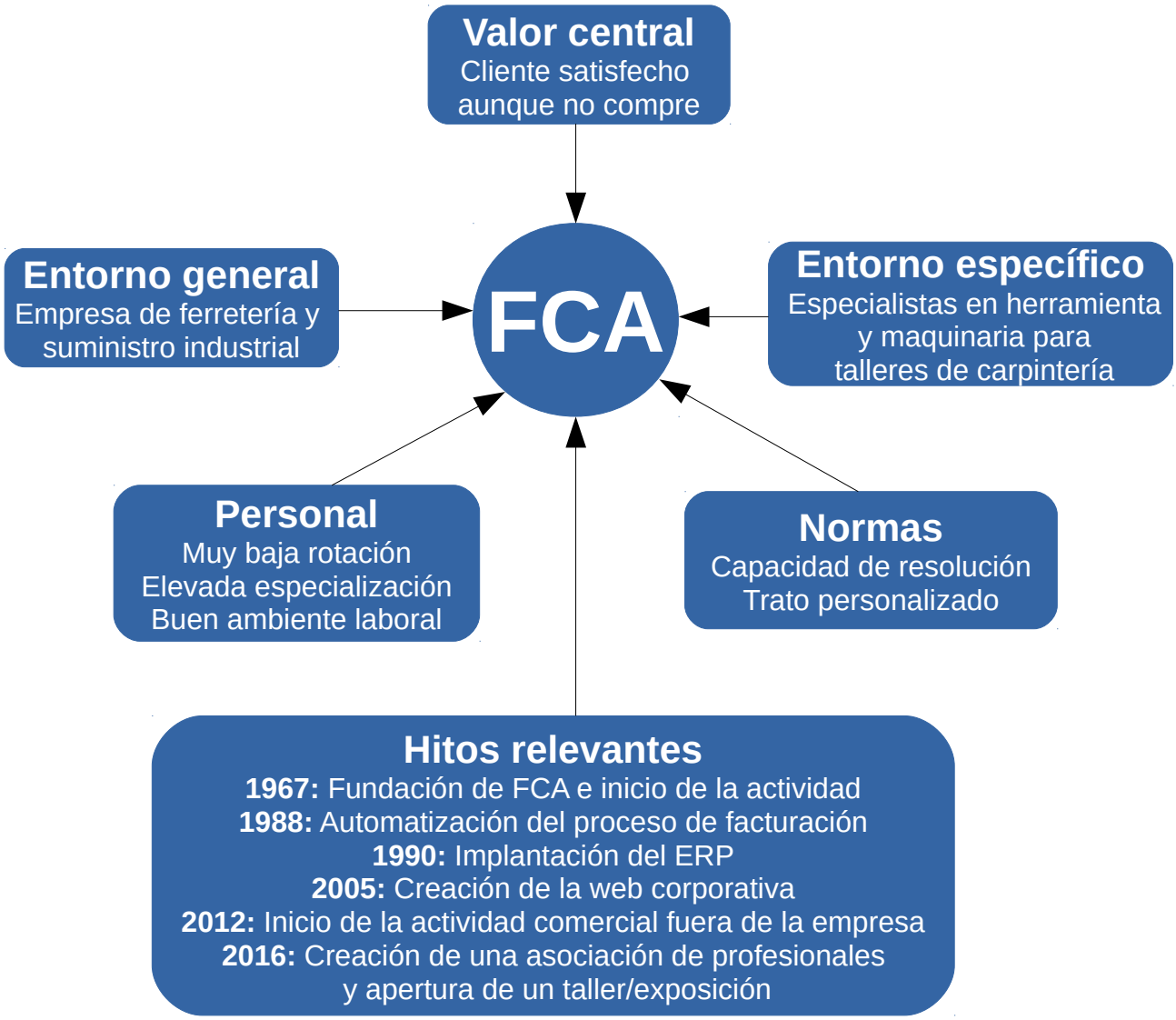
Almacén: Una persona es la encargada de esta función, que complemente sus funciones dando apoyo a ventas cuando es requerido.

RRHH: La labor de gestión de recursos humanos depende directamente del gerente, que es el que la materializa.

PRL: La prevención de riesgos laborales está externalizada y supervisada por la gerencia. La empresa no cuenta con delegado de prevención.

3.2 Cultura de la empresa FCA

En FCA, la cultura de empresa hace referencia al conjunto de normas, valores y forma de actuar y pensar de cada uno de sus miembros, así como aquellos hitos históricos que la han forjado a lo largo del tiempo. Esta cultura la identifica ante clientes, proveedores y todos aquellos que tienen conocimiento de su existencia, aún no teniendo relación comercial con ella.



El valor central de FCA, en torno al cual gira toda la filosofía de trabajo, es la satisfacción total del cliente, aportándole soluciones independientemente de que la relación comercial llegue a formalizarse. La frase que que resume este valor es: “El cliente debe salir satisfecho del trato personal que ha recibido, con una solución a su problema, aunque esta implique que compre en otra parte”.

La empresa se vuelca en un trato personalizado y especializado, con el que ha conseguido ser referente en el sector.

Entorno general

El entorno general de la empresa FCA está enmarcado en el sector de la ferretería y suministro industrial. Venta al por menor a particulares y a profesionales y empresas de diferentes sectores, tanto productivo como de servicios.

Entorno específico

La empresa FCA se dedica a la venta y prestación de servicios a los siguientes sectores:

- Particulares.
- Profesionales del sector de la carpintería de madera y metálica.
- Empresas de construcción.
- Empresas de diseño y montaje de instalaciones.
- Empresas de servicios.
- Centros educativos de formación profesional.
- Universidad.
- Servicio público de salud.
- Ayuntamientos.
- Otras administraciones públicas.

La venta de productos es directa, a través de stock propio, mientras que la prestación de alguno de los servicios que ofrece se externaliza en otras empresas.

Personal

El personal que forma parte del equipo de FCA tiene unos roles claramente definidos y un elevado grado implicación y especialización. El ambiente laboral es muy bueno. Dada la dimensión de la empresa, todos sus miembros desempeñan más de una labor.

Por este mismo motivo, existen las siguientes funciones externalizadas: soporte TIC, gestión de recursos humanos, asesoría legal/fiscal/contable y prevención de riesgos laborales.

Normas

En FCA existen una serie de normas de actuación que son revisadas periódicamente y comentadas en una reunión que se realiza con carácter semanal. Entre ellas destacan:

- La puntualidad en el acceso al centro de trabajo y apertura del mismo es prioritaria. Los horarios de trabajo permanecen invariables durante todo el año.
- Se atiende indistintamente a particulares y profesionales, sin establecer una prioridad por razón de ésta condición.

- Todo el proceso de atención al cliente está orientado para aportar soluciones personalizadas, incluso cuando estas no van a ser comercializadas por FCA.
- Se enfatiza en que la venta de un producto o servicio vaya acompañada de una explicación detallada del mismo. Este es el rasgo diferenciador que FCA aporta con respecto a su competencia.
- La formación continua está muy presente en FCA, dadas las necesidades de conocimiento de los nuevos productos que se comercializan.
- Apenas existe conflicto con los clientes, ya que como norma de FCA, se prioriza la satisfacción del cliente sobre la perdida del negocio. Como norma prioritaria está la de no entablar un conflicto directo bajo circunstancia alguna.
- Los periodos de devolución son mucho mas flexibles que en cualquier otro establecimiento de este tipo.

Hitos relevantes

La cultura de la empresa FCA es un fiel reflejo de sus 50 años de actividad como empresa familiar que ha evolucionado a lo largo del tiempo. Actualmente mantiene el control total y organización en la figura del gerente. A continuación se relaciona alguno de los hitos mas relevantes en la historia de FCA:

- **Año 1967**. Se funda e inicia la actividad la empresa FCA.
- **Año 1986**. Se incorpora el primer ordenador para automatizar el proceso de facturación.
- **Año 1993**. Se procede a la implantación del ERP para todos los procesos de gestión y contabilidad.
- **Año 2005**. Se publica la primera versión de la web corporativa y se inicia el proceso para el establecimiento de una canal de venta B2C.
- **Año 2007**. Se procede a la migración del sistema operativo de red, de SCO UNIX a Suse Linux.
- **Año 2014**. Se inicia la actividad comercial fuera de la empresa a través de una persona especializada en venta e instalación de maquinaria para talleres.
- **Año 2016**. Se pone en marcha una asociación de profesionales patrocinada por FCA, con la incorporación de un taller/exposición en una de sus instalaciones.

3.3 Medios

La empresa FCA dispone de dos centros de trabajo (tienda y nave). En el primero (tienda) desarrolla su labor el total de la plantilla, mientras que la segunda ubicación (nave) es utilizada como almacén y ocasionalmente como taller de torneado para la asociación que patrocina y exposición de maquinaria grande de taller. Ambos centros únicamente disponen de medidas básicas de seguridad en cuanto al control de accesos. Ninguno de ellos dispone de alarma

y el centro principal (tienda) cuenta con un circuito cerrado de televisión pero sin registros de grabación. La sede principal cuenta con una caja fuerte.

En cuanto a otros elementos de seguridad física, ambas sedes cuentan con sistemas de extinción de incendios manuales, siendo automáticos en aquellos puntos en los que se almacenan mercancías peligrosas. A continuación se presenta un resumen de los medios:

Grupo	**Medios relacionados con el entorno**			
Subgrupo	**Ubicación**	**Descripción**	**Otros**	**Descripción**
Espacio (Sede1)	Tienda	Venta directa	140 m^2	Planta baja
	Almacén 1	Almacén mercancía	150 m^2	Planta baja
		Oficina	6 m^2	Planta baja
		Aseos	4 m^2	Planta baja
		Altillo oficina	6 m^2	Planta superior
	Almacén 2	Almacén mercancía	150 m^2	Planta baja
		Almacén mercancía	100 m^2	Planta superior
		Aseos	5 m^2	Planta baja
		Almacén catálogos	5 m^2	Planta baja
Espacio (Sede2)	Nave	Almacén, taller	2.000 m^2 (total)	Planta baja y sup.
		Exposición	500 m^2	Planta baja
		Exposición	400 m^2	Planta superior
		Aseos	50 m^2	Planta inferior
		Oficina 1	35 m^2	Planta superior
		Oficina 2	15 m^2	Planta superior
		Almacén izquierdo	150 m^2	Planta baja
		Almacén derecho	330 m^2	Planta baja
		Taller torneado	35 m^2	Planta baja
		Sala formación	35 m^2	Planta baja
Personal (Sede 1)		Compras	1 persona	Varias funciones
		Ventas tienda	4 personas	Varias funciones
		Ventas comercial	1 personas	Varias funciones
		Admon. RRHH	1 persona	Varias funciones
		Admon. PRL	1 persona	Varias funciones
		Admon. Contabilidad	1 personas	Varias funciones
Personal (Externo)	Remota	Informática soporte	1 persona	Soporte ERP
	Remota	Informática varios	1 persona	Varias funciones
Soporte	Tienda	Climatización		No hay
	Almacenes	Climatización		No hay
	Oficina	Climatización		Calefacción
	Seguridad	Caja fuerte	1 unidad	Oficina
Comunicaciones	Sede 1	ADSL RTC	10 Mb	Rack Almacén 1
		ADSL RDSI	10 Mb	Rack Almacén 1

Grupo	Equipamiento informático (Sede 1)			
Subgrupo	**Ubicación**	**Descripción**	**Otros**	**Descripción**
Hardware	Tienda	PC,s Windows 98	2 unidades en red	Ventas tienda
		Pc,s Windows XP	2 unidades en red	Ventas tienda
	Oficina	Servidor Suse Linux	1 unidad en red	Administración
		PC Windows 7	1 unidad en red	Administración
	Oficina y tienda	Portátil Windows 7	1 unidad en red	Duplicado mandos
	Oficina y tienda	iPad iOS 10.2.1	1 unidad en red	Ventas comercial
		Portátil Windows XP	1 unidad en red	Backup anual
	Tienda	Impresora matricial	2 unidad en red	Carro 80 columnas
		Impresora matricial	1 unidad en red	Carro 30 columnas
	Oficina	Impresora matricial	1 unidad en red	Carro 123 columnas
		Multifunción láser HP	1 unidad en red	
		Disco USB 1 TB	1 unidad	Backup Windows
		Disco USB 200 Gb	3 unidades	Backup Linux
Red	Sede 1	Hub 16 tomas	1 unidad	Velocidad 100Mbps
	Router ADSL	4 salidas Ethernet	1 unidad	Wifi hasta 10Mb
	Router ADSL	4 salidas Ethernet	1 unidad	Wifi hasta 10Mb
Soporte	Fuente alimentación	S.A.I	1 unidad	Sólo en servidor
Software	Windows 98	Emulador ERP	2 licencias	Ventas tienda
	Windows XP	Emulador ERP	3 licencias	Ventas tienda
	Windows 7 Pro	PC Administración	1 licencia	Oficina
	Windows 7 Starter	PC Portátil	1 licencia	Oficina y tienda
	iOS versión 10	iPad	1 licencia	Oficina y tienda
	Microsoft Office	Versión 2010	1 licencia	PC Oficina
	Microsoft Office	Versión 2003	1 licencia	Portátil Oficina
	Adobe Photoshop	Versión 2007	1 licencia	PC oficina
	Kaspersky Antivirus	Versión 2017	1 licencia	PC oficina
	CX_Gestión	Módulo de gestión	10 puestos	ERP en red
	CX_Contabilidad	Módulo contabilidad	10 puestos	ERP en red
	iPreventa	Modulo ventas	1 licencia	Ipad

Grupo	Información base de las operaciones de empresa			
Subgrupo	**Ubicación**	**Descripción**	**Otros**	**Descripción**
Código fuente	Oficina	CX_Gestión	3.138.133 líneas de código	Módulo del ERP
		CX_Contabilidad	619.120 líneas de código	Módulo del ERP
		iPreventa	138.430 líneas de código	Módulo del ERP
		Bases de datos	Indeterminado	

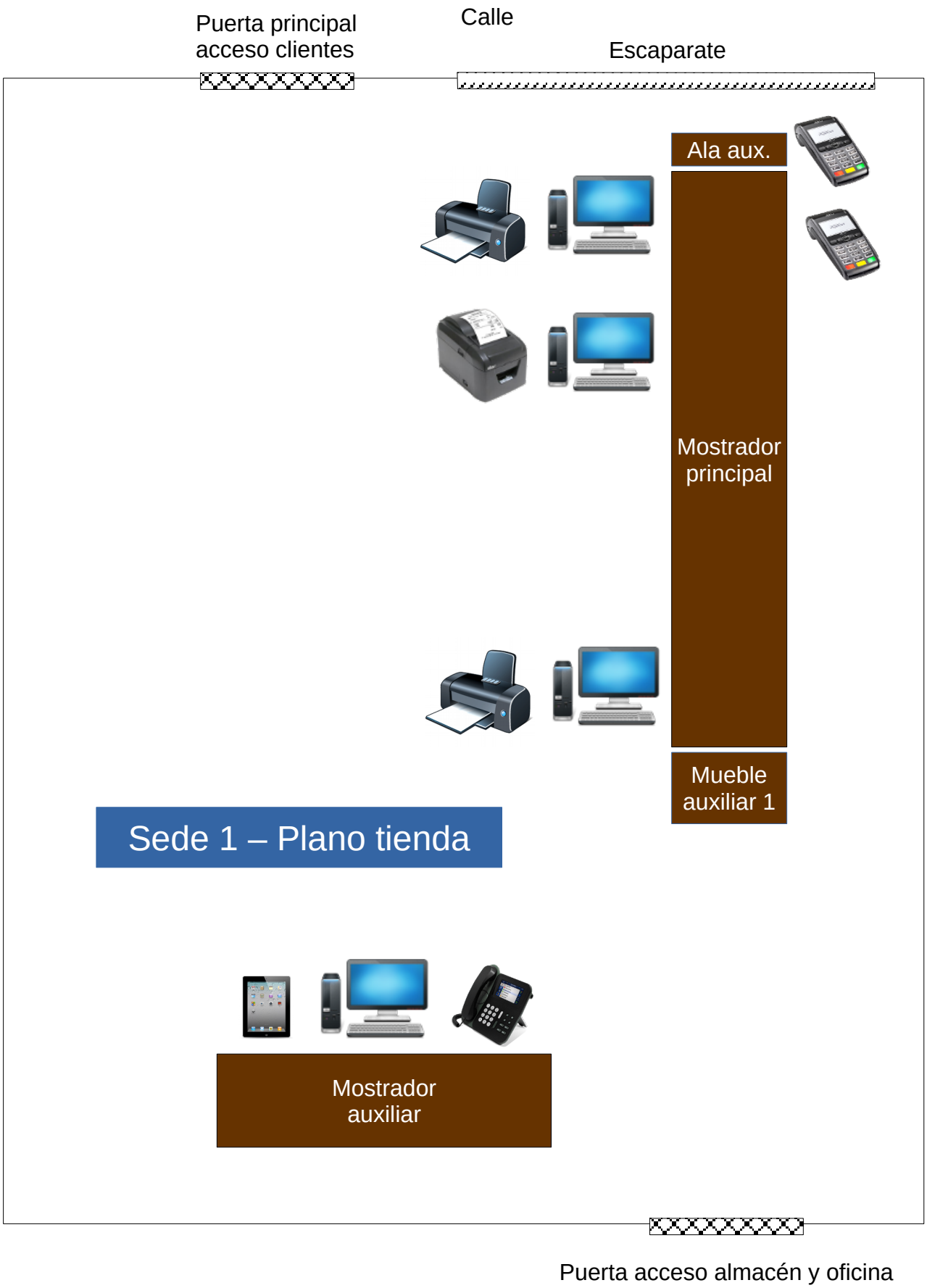
Grupo	Información base de las operaciones de empresa			
Subgrupo	**Ubicación**	**Descripción**	**Otros**	**Descripción**
Código fuente	Oficina	Comercio electrónico	En desarrollo	Previsto 06/2017
Administración	Oficina	Contratos		
		Contabilidad		
		Facturación		
		Backup Windows		300 Gb
		Backup CX_Gestion		3.30 Gb
		Backup CX_Contabilidad		653 Mb
Comercial	Oficina y comercial	Bases datos clientes		
	Oficina y comercial	Presupuestos		

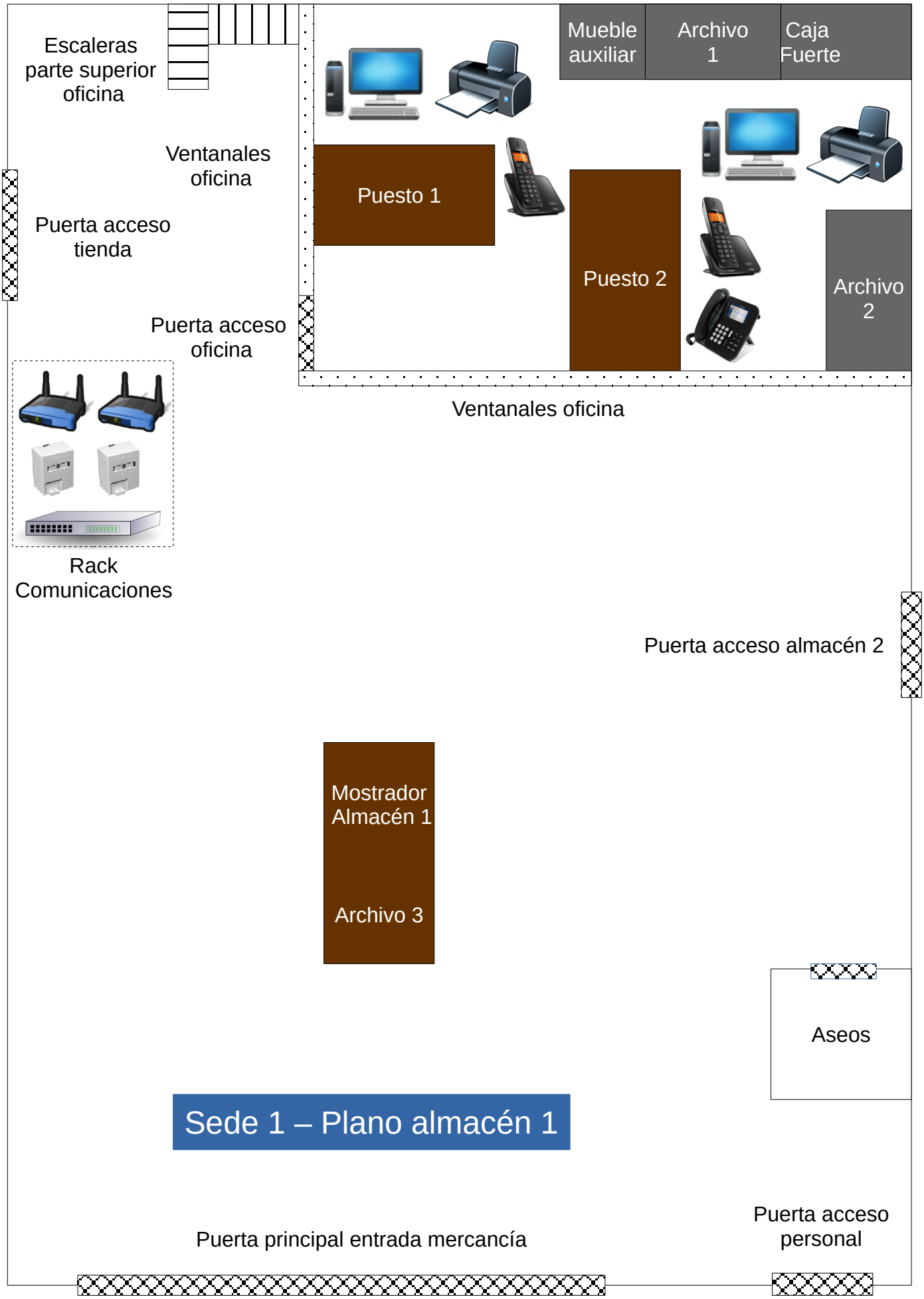
Grupo	Funcionalidades o servicios			
Subgrupo	**Ubicación**	**Descripción**	**Otros**	**Descripción**
Internas	Oficina y comercial	Correo electrónico		
	Comercial	WhatsApp corporativo		
	Oficina	Gestión backups	Modo local	Linux y Windows
Externas	Mantenimiento	Gestión backups	Modo remoto	Linux
	Web corporativa	Informativa y contacto		
	Web para B2C	Comercio electrónico		

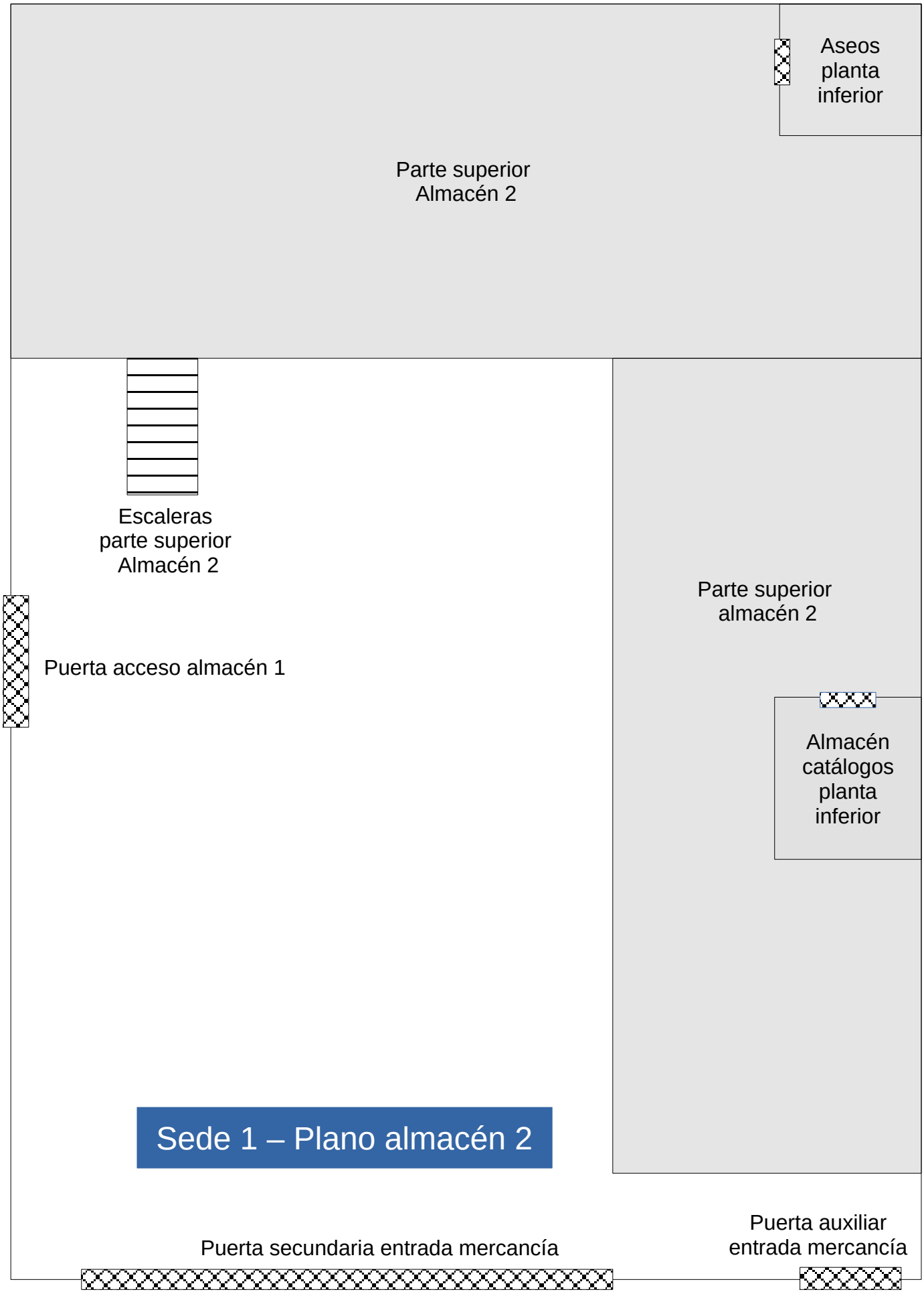
Grupo	Otros activos importantes			
Mercado	Especialización	Sector madera y metal		
	Imagen	Tradición y servicio		
	Solvencia	Garantizada		
Otros	Vehículo comercial	Comercial y distribución		
	Know how	50 años de experiencia		

A continuación se adjuntan los planos orientativos de las instalaciones según la siguiente relación:

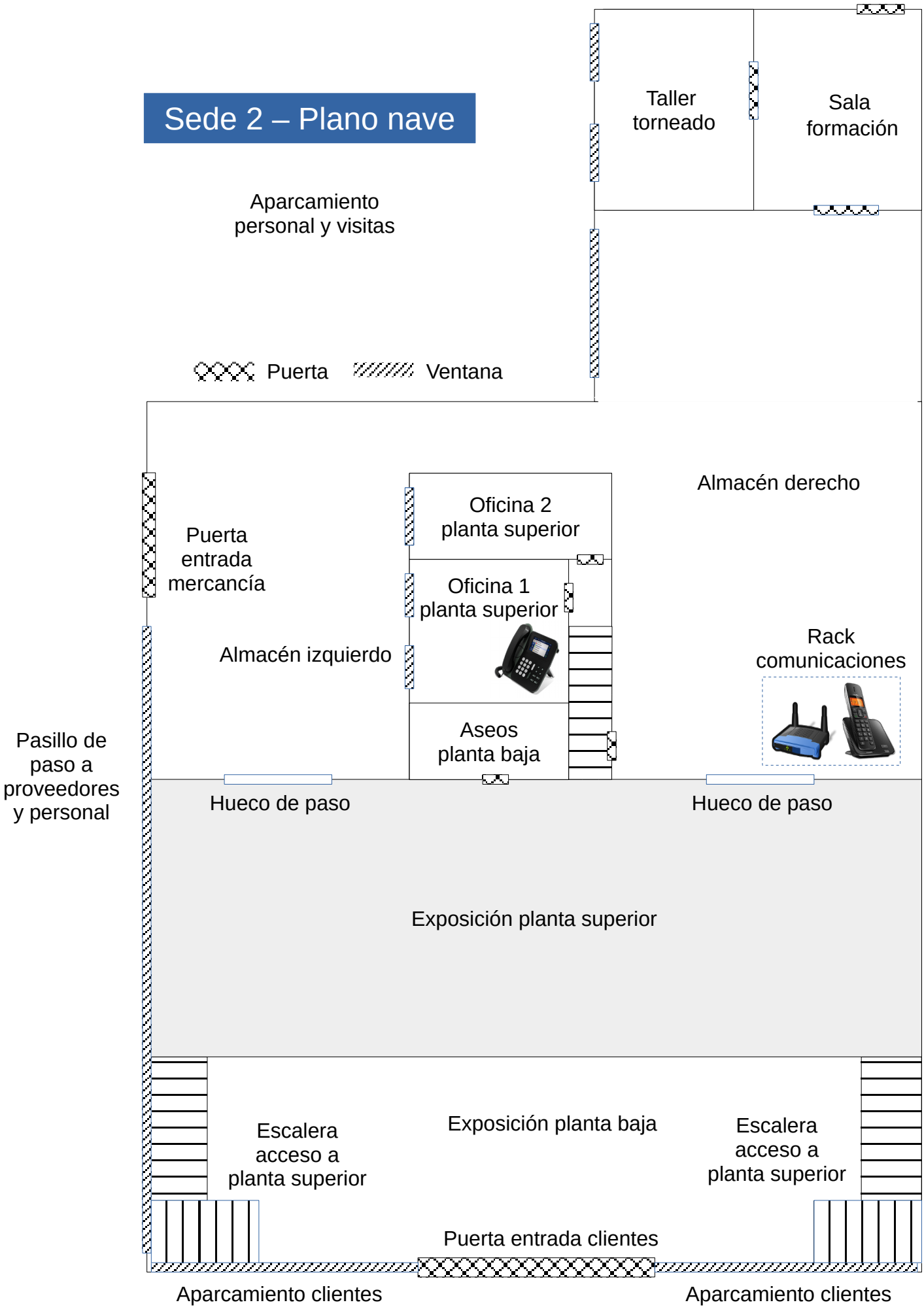
- **Sede 1 – Plano tienda**: Superficie destinada a la venta al público.
- **Sede 1 – Plano almacén 1**: Superficie conectada con la tienda y destinada a almacén, oficina (con almacén en la parte superior) y aseo.
- **Sede 1 – Plano almacén 2**: Superficie conectada con la anterior y destinada a almacén de mercancía. Su parte superior ocupa el 70% de la superficie total. Dispone de un aseo y un pequeño almacén.
- **Sede 2 – Nave**: Segundo centro de trabajo, destinado a almacén, exposición y taller de torneado. No está abierta de cara al público ni tiene personal fijo asignado. Se abre ocasionalmente para recepción de mercancía, escaparate comercial de maquinaria grande y eventos de la asociación patrocinada por FCA.


Puerta principal
acceso clientes
Calle
Escaparate
Ala aux.
Mostrador
principal
Mueble
auxiliar 1
Sede 1 – Plano tienda
Mostrador
auxiliar
Puerta acceso almacén y oficina


Escaleras parte superior oficina
Mueble auxiliar
Archivo 1
Caja Fuerte
Ventanales oficina
Puesto 1
Puerta acceso tienda
Puesto 2
Archivo 2
Puerta acceso oficina
Ventanales oficina
Rack Comunicaciones
Puerta acceso almacén 2
Mostrador Almacén 1
Archivo 3
Aseos
Sede 1 – Plano almacén 1
Puerta principal entrada mercancía
Puerta acceso personal


Aseos planta inferior
Parte superior Almacén 2
Escaleras parte superior Almacén 2
Parte superior almacén 2
Puerta acceso almacén 1
Almacén catálogos planta inferior
Sede 1 – Plano almacén 2
Puerta auxiliar entrada mercancía
Puerta secundaria entrada mercancía

Sede 2 – Plano nave



3.3 Tareas

La siguiente tabla muestra la relación de todas las tareas que se llevan a cabo.

Departamento	Dirección
Subgrupos	**Descripción**
Compras	La tarea de compras es realizada en exclusiva por la Dirección de la empresa.
Informática	Esta tarea está externalizada en dos empresas supervisadas por la Dirección.
Administración	Labor de apoyo en las tareas de contabilidad y gestión.
Ventas	La Dirección interviene habitualmente en esta tarea con ventas fuera de la tienda.
Almacén	La Dirección supervisa este trabajo y en ocasiones apoya a este personal
RRHH	La gestión de recursos humanos es llevada a cabo directamente por la Dirección.
PRL	La prevención de riesgos laborales está externalizada y supervisada por la Dirección.

Departamento	Compras
Subgrupos	**Descripción**
Dirección	La labor de este departamento recae únicamente en la Dirección de la empresa.

Departamento	Informática
Subgrupos	**Descripción**
Freelance 1	Las tareas de mantenimiento y soporte son realizadas por personal externo a FCA.
Freelance 2	Las tareas de B2C, Social Media y Seguridad de la Información están externalizadas.
Dirección	Coordina y supervisa el trabajo de las dos empresas que ofrecen el servicio.
Otros Dptos.	En ningún caso intervienen en procesos/tareas relacionadas con Informática.

Departamento	Administración
Subgrupos	**Descripción**
Dirección	Colabora activamente y supervisa con todas las tareas administrativas.

Departamento	Ventas
Subgrupos	**Descripción**
Dirección	Ocasionalmente apoya las ventas físicas en la tienda.
Almacén	La Dirección supervisa este trabajo y en ocasiones apoya a este personal

Departamento	Almacén
Subgrupos	**Descripción**
Ventas	Ocasionalmente en ausencia del responsable, se hacen cargo de esta tarea.
Dirección	Ocasionalmente, ante pedidos especiales, se hace cargo de esta tarea.

Departamento	RRHH y PRL
Subgrupos	**Descripción**
Dirección	Encargada de la selección, contratación y supervisión del personal de la empresa.
	Supervisa el servicio externo de PRL. No existe delegado de prevención.

4. Situación actual

Actualmente la empresa FCA no dispone de ninguna *política en materia de seguridad de la información* que haya sido aprobada por la dirección e integrada en los procesos habituales de negocio. Por este motivo tampoco se revisa ni actualiza.

Las responsabilidades en esta materia recaen en la dirección de la empresa, que recibe asesoramiento externo de las dos empresas que le proporcionan el soporte tecnológico. No hay por tanto un *rol* específico para el *responsable de seguridad TIC*.

En cuanto a la seguridad de los recursos humanos, se lleva un control bastante exhaustivo de las referencias y antecedentes de todo el personal que entra a formar parte de la misma.

Los empleados tienen conocimiento del carácter confidencial de parte de la información que se maneja en la empresa, así como sobre el *tratamiento* que deben seguir con los *datos de carácter personal* de clientes, proveedores y colaboradores. Por otro lado, el documento de seguridad según exige la LOPD no ha sido actualizado desde hace varios años. No se están contemplando las medidas para la protección de la seguridad de la información cuando un empleado cesa en su puesto de trabajo. Esto se ha debido probablemente al bajo nivel de rotación de personal que hay en la organización.

En relación a los *activos* de la empresa, no existe *inventario* ni *identificación* de los mismos. Tampoco se ha establecido una normativa para la utilización de los mismos dentro o fuera de la organización.

Los *controles de acceso físico* son básicos. La empresa dispone de 2 puertas de entrada, con cerraduras de seguridad, pero sin sistema de alarma o circuito de videovigilancia con registro de imágenes/eventos. En cuanto al control de acceso en el interior de la empresa, no se ha establecido restricción alguna, por lo que cualquier empleado puede acceder a cualquier zona sin limitaciones. No existen áreas seguras protegidas por controles perimetrales.

Los *controles de acceso lógico* (principalmente al ERP de la empresa) son muy básicos. Actualmente existen 3 tipos de usuarios que acceden al sistema; jcarlos, ventas y soporte. Con el primero de ellos (jcarlos) accede indistintamente el administrador de la empresa y la persona encargada de la administración. Con el usuario “ventas” acceden los 4 empleados restantes (ventas en el mostrador, comercial externo y almacén). Por último, el usuario “soporte” está destinado al personal externo que mantiene el ERP. Destacar que las claves asignadas a estos usuarios no cumplen los requisitos básicos de seguridad y nunca se cambian.

No existe *clasificación de la información* según su nivel de confidencialidad y nunca se utilizan procedimientos de cifrado para el envío y/o almacenamiento de información alguna.

Los equipos y sistemas que contienen información no tienen *medidas anti-robo*. Se dispone de medidas de protección contra incendios, pero no adecuadas para equipos electrónicos. Dada la antigüedad de las instalaciones, los locales de trabajo no están preparados contra *inundaciones*. Existe un sistema de

alimentación ininterrumpida, pero solamente cubre el servidor central. El resto de equipos disponen de una línea específica preparada para cortes de alimentación, aunque no está habilitada.

E l *cableado* de las instalaciones es antiguo, pero cumple con las medidas básicas de seguridad, en cuanto a aislamiento y conectividad. En algún caso los terminales de red están deteriorados.

E l *mantenimiento de los equipos* lo lleva una empresa externa y apena se producen indisponibilidad, ya que son reparados en menos de 72 horas. Cuando los equipos dejan de ser útiles, son almacenados en la propia empresa. Nunca se han retirado de las instalaciones.

No existe *política de usuario desatendido* ni de *puesto de trabajo despejado* y *pantalla limpia*. En cuanto a la *protección contra software malicioso*, sólo el puesto del gerente dispone de esta medida. Este se actualiza periódicamente con los parches de seguridad suministrados por los fabricantes.

La empresa dispone de una *política de copias de seguridad*. Se realizan 2 copias diarias de Gestión y Contabilidad a un servidor remoto. Una copia semanal del equipo de administración y dos copias anuales de toda la base de datos de gestión y contabilidad. Ninguna de las copias es cifrada.

En cuanto a la *seguridad de las comunicaciones*, los dos enrutadores de los que dispone la empresa utilizan la configuración por defecto. No se han establecido medidas de seguridad adicionales. La única precaución es que el acceso inhalámbrico de los dispositivos del personal y visitantes se hace a través del router que no está conectado a la *intranet* de la empresa. Se podría considerar como una especie de segregación básica de redes.

El dispositivo móvil utilizado en labores comerciales fuera de la empresa dispone de una contraseña de acceso al terminal. La seguridad es baja, puesto que se ha implementado con un código numérico de 4 dígitos.

Ningún proveedor tiene acceso a los sistemas de información de la empresa para compartir información, por lo que de momento no ha requerido medidas de seguridad adicionales.

No existe gestión de incidentes de seguridad de la información. Hasta la fecha no se ha producido ningún evento de este tipo. Tampoco existe un plan de continuidad de negocio, establecido para casos de crisis o desastre.

En cuanto al cumplimiento normativo, la empresa cumple con los requisitos básicos exigidos por la LOPD. Actualmente está iniciando los procesos de adecuación al nuevo Reglamento Europeo de protección de datos.

En el **Anexo X** se incluye una auditoría previa en un marco *SOA (Statement of Applicability - Declaración de Aplicabilidad).* **Anexo XI**

5. Plan de Acción

El nivel de seguridad de la información que tiene esta organización es totalmente insuficiente. Por consiguiente, es necesario elaborar un plan de acción que incremente este nivel hasta un umbral de seguridad razonable. Con la consecución de este plan de acción y la consiguiente implantación de este S.G.S.I, el sistema de información quedará preparado para conseguir la certificación ISO/IEC 27001.

Áreas de Actuación

Todos los departamentos de la empresa deben estar involucrados en la implantación del SGSI, ya que interactúan de un modo u otro con el sistema de información y afectan directamente en su seguridad. La dirección de la organización debe estar totalmente convencida e implicada en el proyecto.

El personal Freelance al que se ha externalizado alguno de los servicios también deben estar involucrados en estas actuaciones.

Aquellos proveedores y clientes que interactúen en modo alguno con el sistema de información, también deben integrarse en este proceso.

Propuestas de actuaciones

A continuación se muestra una tabla con los cinco puntos, a desarrollar, que formarán parte del plan director:

Id	Objetivo	Comentario
OBJ1	Implantación de un Sistema de Gestión de la Seguridad de la Información para FCA.	Se pretende preparar e implantar un SGSI para la mejora de la seguridad y posible certificación.
OBJ2	Actualización y ampliación de la red corporativa.	Valorar la posibilidad de incorporación de nuevos equipos en aquellos casos en los que las actualizaciones no soporten los existentes.
OBJ3	Establecer un plan de contingencia ante desastres para asegurar la continuidad de negocio.	Implantar los elementos que sean necesarios para dar continuidad a la actividad en caso de que el único servidor existente en la empresa falle.
OBJ4	Establecer un plan de concienciación y formación continua desde el inicio del proyecto de implantación.	Con esto se pretende que la implantación del SGSI sea lo menos traumática posible y que los miembros de la empresa se impliquen activamente en todo el proceso.
OBJ5	Optimizar el uso del ERP	Actualmente, el ERP está infrautilizado por la mayoría de los miembros del equipo de FCA.

6. Política de Seguridad

El **Anexo II** contiene el conjunto de normas y procedimientos establecidos por la empresa FCA para regular el uso de la información y de los sistemas que la tratan. La finalidad de esta política de seguridad es mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma. Como parte del ciclo PDCA (Plan-Do-Check-Act), se actualizará a través de diferentes versiones.

7. Procedimiento Auditorías Internas

El **Anexo III** se definen las reglas básicas para la realización de la auditoría, entre las que estarán la selección del equipo auditor, la planificación, los elementos que se utilizan para llevarla a cabo y las actividades de seguimiento. Como en el caso anterior, este documento se actualizará a través de diferentes versiones en función de los cambios que se vayan produciendo.

8. Gestión de indicadores

En el **Anexo IV** se incluye una relación detallada de los indicadores de gestión de la seguridad de la información propuestos para la empresa FCA. La finalidad de estos indicadores es la de medir la efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información. Servirán como control para la adopción de decisiones de mejora continua. Del mismo modo que en casos anteriores, este documento se actualizará a través de diferentes versiones en función de los indicadores que se estén aplicando.

9. Procedimiento de revisión directiva

Uno de los principales factores que influyen en que la implantación de un SGSI sea exitosa es la implicación de la alta dirección de la organización. En el **Anexo V** se presenta una relación de las diferentes tareas que tiene encomendadas. Dichas tareas también pueden evolucionar a lo largo del tiempo, por lo que se establecerán versiones también para este documento.

10. Gestión roles y responsabilidades

En el **Anexo VI** se presenta una relación de roles y responsabilidades en materia de seguridad de la información, alineados con las premisas del SGSI. Se ha separado según las diferentes áreas operativas que hay actualmente en FCA. Dicha clasificación puede variar notablemente en función del tiempo y de la evolución de la organización (tamaño, etc.). Por este motivo se presentarán diferentes versiones en función de lo anteriormente indicado.

11. Metodología de Análisis de Riesgos

Para el análisis de riesgos adoptaremos la metodología ***Magerit*** que, de forma resumida, se basa en la realización de dos grandes tareas:

- El *Análisis de Riesgos*, que tiene en cuenta los activos, amenazas y salvaguardas. En función de estos, se hace una estimación del impacto y del riesgo final para la organización. Para éste análisis se han confeccionado una serie de tablas adjuntas en los correspondientes anexos y otra serie de tablas que se muestran a continuación, con la identificación de cada elemento que interviene en las diferentes valoraciones del análisis de riesgos.
- El *Tratamiento de los Riesgos*, que consistirá en la ejecución de una propuesta de mejora de la seguridad, con aquellas actividades encaminadas a mitigar al máximo la situación de riesgo.

La primera tabla sirve de base para la estimación numérica (no en porcentaje) de la probabilidad de que ocurra una determinada amenaza sobre los activos relacionados con el SGSI. Se ha clasificado en función de la ocurrencia temporal de la amenaza, con tres valores umbrales (año, mes y semana).

Tabla para estimar la PROBABILIDAD de ocurrencia de una determinada amenaza	
Valor	**Descripción**
1 = Baja	La amenaza se materializa a lo sumo una vez al año.
2 = Media	La amenaza se materializa a lo sumo una vez al mes.
3 = Alta	La amenaza se materializa a lo sumo una vez a la semana.

La segunda tabla sirve de base para la estimación numérica del impacto que provocaría la materialización de una determinada amenaza sobre un activo específico. Se ha clasificado el daño provocado, según el nivel de gravedad, con tres valores (irrelevante, relevante, grave).

Tabla para estimar el IMPACTO provocado por la materialización de la amenaza	
Valor	**Descripción**
1 = Bajo	El daño derivado no tiene consecuencias relevantes para la organización.
2 = Medio	El daño derivado tiene consecuencias reseñables para la organización.
3 = Alto	El daño derivado tiene consecuencias graves para la organización.

La tercera tabla establece el umbral de riesgo para la organización, cruzando los valores de probabilidad de amenaza y el impacto provocado por la materialización de la misma.

Tabla con los criterios establecidos para la aceptación del RIESGO	
Valor	**Descripción**
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a tratarlo.

Finalmente, en función de los valores de estas tablas, procedemos a valorar el riesgo final al que están sometidos los diferentes activos. En función de los resultados obtenidos, la dirección de la organización valorará su tratamiento.

- Los niveles de riesgo entre 1 y 2 se consideran bajos y por tanto la organización puede tomar la decisión de aceptarlos.
- Los niveles de riesgo entre 3 y 4 son significativos y se debe valorar su tratamiento.
- Los niveles de riesgo superiores a 4 son altamente significativos y obligatoriamente deben ser tratados, a través de la aplicación de determinados controles.
- Un nivel 9 de riesgo es imperativo su tratamiento, al tratarse de un riesgo crítico para la organización.

Tabla de riesgo

Impacto			
Alto	3	6	9
Medio	2	4	6
Bajo	1	2	3
	Baja	Media	Alta
	Probabilidad		

Inventario y valoración de activos

En el **Anexo I** se presenta un tabla con la relación de activos vinculados a la gestión de la seguridad de la información y cuyas columnas tienen el siguiente significado:

- *Ámbito*: Hace referencia al área (física o lógica) donde queda clasificado el activo. Siguiendo los estándares de la serie 27000 de las ISO/IEC, estos serían los siguientes: *instalaciones, hardware, aplicaciones, datos, red, servicios, equipamiento auxiliar y personal*.
- *Id*: Identificador único para ese activo. Está compuesto de 1 carácter alfabético que hace referencia al ámbito de forma: *(I)nstalaciones, (H)ardware, (A)plicaciones, (D)atos, (R)ed, (S)servicios, (E)quipamiento auxiliar, (P)ersonal* y otro numérico asignado en orden ascendente a cada activo (1...N).
- *Activo*: Nombre asignado al activo. En algunos casos se utiliza la abreviatura utilizada en el campo tecnológico, con una breve explicación entre paréntesis del equipo, sistema o servicio referido.
- *Valor*: Hace referencia a la importancia del activo para la organización y pueden estimarse como muy bajo, bajo, medio, alto y muy alto. Esta clasificación denota el grado de importancia que ocasionaría la perdida o deterioro de ese activo.

Valoración de los activos en función de las dimensiones de seguridad

En el mismo anexo, se presenta una tabla que muestra la anterior valoración del activo y otra valoración adicional, incidiendo sobre cada una de las dimensiones de la seguridad de la información.

En las dos tablas que preceden a dicha valoración, se muestran cuales son las dimensiones de seguridad de la información y un criterio de valoración numérica que representa el daño que ocasionaría a la organización la violación de esa dimensión.

Las tres primeras columnas de la tabla ya han sido descritas en el inventario y valoración de activos. Las columnas 4 a 8 representan cada una de las dimensiones de la seguridad (Autenticidad, Confidencialidad, Integridad, Disponibilidad, Trazabilidad) y su valor numérico hace referencia al daño anteriormente descrito.

Análisis de amenazas

En el **Anexo VII** se presenta una tabla que describe, en diferentes categorías, cada una de las amenazas identificadas para el sistema de información. En la parte derecha de la tabla, que hace referencia a cada dimensión de la seguridad, se han marcado con una "x" las que se pueden ver afectadas. Las categorías han sido marcadas en diferentes colores y pueden ser de los siguientes tipos:

- *Color gris*: Amenazas de origen natural.
- *Color verde*: Amenazas de origen humano (intencionadas).
- *Color amarillo*: Amenazas del entorno (origen industrial).
- *Color rojo*: Amenazas sobre el hardware o el software.
- *Color azul*: Amenazas de origen humano (no intencionadas).
- *Color naranja*: Otras amenazas (insiders y outsiders).

A continuación se identifican y describen cada una de las columnas que conforman la tabla:

- *Id*: Identificador único de la amenaza, compuesto por tres caracteres alfabéticos (AMZ) y un número correlativo en orden ascendente (1..N).
- *Descripción*: Identificación de la amenaza.
- *Dimensión*: Compuesta por 5 columnas, cada una de las cuales corresponde a una dimensión de la seguridad de la información (Autenticidad, Confidencialidad, Integridad, Disponibilidad, Trazabilidad).

Análisis del riesgo

En el **Anexo VIII** se presenta la tabla de Análisis de Riesgos, en la que se relacionan de los activos involucrados en el SGSI, las amenazas sobre cada uno de ellos, la probabilidad de ocurrencia de dichas amenazas, el impacto provocado por su materialización y el riesgo final observado.

A continuación de identifica y describe cada una de las columnas de la tabla:

- *Activo*: Identificador alfanumérico del activo y su nombre.
- *Amenaza*: Identificador alfanumérico de la amenaza y su nombre.
- *Probabilidad*: De ocurrencia de esa amenaza, que se clasificará en: 1=Baja, 2=Media, 3=Alta (Tabla para estimar la probabilidad de ocurrencia de una determinada amenaza).

- *Impacto*: Provocado por la materialización de esa amenaza, siendo: 1=Bajo, 2=Medio, 3=Alto (Tabla para estimar el impacto provocado por la materialización de la amenaza).
- *Riesgo*: Estimación del riesgo existente para la organización, en función de la probabilidad de ocurrencia de una amenaza y la materialización de la misma. (Tabla con los criterios establecidos para la aceptación del riesgo).

12. Proyecto de mejora de la seguridad

El **Anexo IX** contiene los diferentes proyectos con propuestas de mejora de la seguridad para FCA. Este documento se mantendrá actualizado a través de diferentes versiones e inicialmente contempla las siguientes áreas:

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

13. Auditoría de cumplimiento

Las propuestas de proyecto han sido implementadas y hemos llegado al punto en el que debemos verificar que están siendo efectivas. Esto se lleva a cabo a través de una auditoría interna, en el que se comprueba el estado actual de los controles de la ISO27002:2013. El resultado de esta auditoría, proporciona información consistente sobre el punto en el que se encuentra el SGSI de cara a una certificación sobre la norma ISO/IEC 27001.
En el **Anexo XI** se presentan las diferentes fases del proceso de auditoría y a través de los diferentes controles ISO/IEC 27002:2013 se muestran las no conformidades encontradas. Finalmente se hace una comparativa de los resultados obtenidos con el estado de madurez de los controles al inicio del proyecto (CMM).
Una vez realizada la auditoría, podemos afirmar que las propuestas de proyecto para la mejora de la seguridad de la información en la empresa FCA han hecho evolucionar el sistema hacia un modelo mucho más dinámico y seguro. Gran parte de las medidas adoptadas y controles implantados han hecho dar un salto cuantitativo y cualitativo en lo que a seguridad de la información se refiere, pero todavía sigue habiendo un número significativo de *no conformidades* encontradas (*4 menores y 2 mayores*).
Con la implantación del presente SGSI y tras la realización de ésta auditoría interna, se puede afirmar que la seguridad de la información en la empresa FCA puede mejorar notablemente, sobre todo en aquellas áreas y activos en los que hasta la fecha era inexistente.

14. Conclusiones

El proyecto de implantación de un SGSI en la empresa FCA surge como necesidad de aumentar el nivel de seguridad de la información en un sistema automatizado con casi 30 años de funcionamiento. Las particularidades de sus nuevas relaciones comerciales con la administración exigen un revisión exhaustiva de la casi inexistente política de seguridad corporativa.

Con la implantación de este SGSI se pretende reducir los riesgos derivados de incidentes de seguridad sobre aquellos activos en los que hasta la fecha es inexistente. Adicionalmente se intenta conseguir una mejora de la imagen corporativa de la empresa frente a la administración y otras empresas del sector estratégico con las que se puede llegar a establecer relaciones comerciales.

Partimos de una situación inicial en el que la empresa cuenta con dos sedes, de las cuales actualmente sólo una dispone de sistema de información. La otra sede es utilizada como almacén de mercancía y exposición de maquinaria.

Tras efectuar un inventario y clasificación de activos se procede a la delimitar las tareas de cada uno de los departamentos en lo que a seguridad de la información se refiere.

Se establecen 5 objetivos principales: implantación de un SGSI, actualización de la red corporativa, creación de un plan de contingencia ante desastres para garantizar la continuidad del negocio y optimizar el actual ERP.

A través de la metodología *Magerit* se procede a realizar un análisis y evaluación de riesgos, para posteriormente presentar una serie de proyectos de mejora de la seguridad de la información.

Finalmente se procede a la realización de una auditoría interna para verificar el grado de cumplimiento de los 114 controles contemplados en la norma ISO 27002:2013. Finalizado este proceso, se detectan 6 *"no conformidades"* de las cuales 4 son menores y 2 mayores. Sobre el mismo informe se proponen las acciones correctoras oportunas, asignándoles un responsable de aplicación.

En este momento finaliza el primer ciclo PDCA del SGSI. Este es el punto de partida para la mejora continua de la seguridad de la información en la empresa FCA, que será versionada en posteriores documentos.

14. Glosario

ACIDT: Son las siglas de las dimensiones de seguridad de la información, es decir; (A)utenticidad, (C)onfidencialidad, (I)ntegridad, (D)isponibilidad y (T)razabilidad.

ADSL: Asymmetric Digital Subscriber Line o Bucle de Abonado Digital Asimétrico es una técnica de transmisión que, aplicada sobre los bucles de abonado de la red telefónica, permite la transmisión de datos a alta velocidad.

B2C: es la abreviatura de la expresión Business-to-Consumer y se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o consumidor final.

BACKUP: Copia y archivo de datos de un equipo informático con la finalidad de poder utilizarla para restaurar la información original ante una eventual pérdida de datos.

CMM: El Modelo de Madurez de Capacidades o CMM (Capability Maturity Model), es un modelo de evaluación de los procesos de una organización.

ERP: Los sistemas de Planificación de Recursos Empresariales (en inglés: Enterprise Resource Planning) son los sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía en la producción de bienes o servicios.

ETHERNET: Es un estándar de redes de área local para ordenadores. Define las características de cableado, la señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos.

FCA: Empresa cliente de implantación del SGSI.

GANTT: El diagrama de Gantt es una herramienta gráfica cuyo objetivo es exponer el tiempo de dedicación previsto para diferentes tareas o actividades a lo largo de un tiempo total determinado.

GB: Un gigabyte (GB) es una unidad de almacenamiento de información equivalente a 10^9 bytes.

HUB: Un hub o concentrador es un dispositivo que canaliza el cableado de una red para ampliarla y repetir la misma señal a través de diferentes puertos.

INTRANET: Red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. Suele ser interna, en vez de pública como internet, por lo que solo los miembros de esa organización tienen acceso a ella.

ISO: Es la Organización Internacional para la Estandarización (en inglés: International Organization for Standardization), que regula una serie de normas para fabricación, comercio y comunicación, en todas las ramas industriales. Se conoce por ISO tanto a la Organización como a las normas establecidas por la misma para estandarizar los procesos de producción y control en empresas y organizaciones internacionales.

ISP: Internet Service Provider o Proveedor de Servicios de Internet.

KNOW HOW: Forma de transferencia de tecnología. Se ha empezado a utilizar habitualmente en los últimos tiempos en el ámbito del comercio internacional para denominar a los conocimientos preexistentes, no siempre académicos, que incluyen técnicas, información secreta, teorías e incluso datos privados, como clientes o proveedores.

LOPD: Ley Orgánica de Protección de Datos.

MAGERIT: Metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información.

MALWARE: Abreviatura de *"Malicious software"*, término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

PDCA: El ciclo de Deming, también conocido como círculo PDCA (del inglés plan-do-check-act, esto es, planificar-hacer-verificar-actuar), es una estrategia de mejora continua de la calidad en cuatro pasos muy utilizado por los sistemas de gestión de la calidad (SGC) y los sistemas de gestión de la seguridad de la información (SGSI).

PRL: La prevención de riesgos laborales (PRL) es la disciplina que busca promover la seguridad y salud de los trabajadores mediante la identificación, evaluación y control de los peligros y riesgos asociados a un entorno laboral.

RACK: Soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de cualquier fabricante.

RDSI: Red Digital de Servicios Integrados (en inglés: ISDN, Integrated Services Digital Network). Facilita conexiones digitales, extremo a extremo, para proporcionar una amplia gama de servicios y a la que los usuarios acceden a través de un conjunto de interfaces normalizados.

ROL: Término que proviene del inglés role y está vinculado a la función o papel que cumple alguien o algo.

ROOT: El superusuario o *"root"* es el nombre convencional de la cuenta de usuario que posee todos los derechos en el sistema de información.

ROUTER: Dispositivo que se encarga de enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes.

RRHH: Los recursos humanos de una empresa (RRHH) es una función y/o departamento del área de gestión y administración de empresas que organiza y maximiza el desempeño del capital humano, con el fin de aumentar su productividad.

RTC: La Red Telefónica Conmutada (RTC) se define como el conjunto de elementos constituido por todos los medios de transmisión y conmutación necesarios para enlazar a voluntad dos equipos terminales mediante un circuito físico, específico para la comunicación.

SAI: Un Sistema de Alimentación Ininterrumpida (SAI) (en inglés: Uninterruptible Power Supply), es un dispositivo que gracias a sus baterías puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.

SGSI: Un Sistema de Gestión de la Seguridad de la Información (SGSI) (en inglés: Information Security Management System, ISMS) es un conjunto de políticas de administración de la seguridad de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

SOA: Statement of Applicability o Declaración de Aplicabilidad es un documento que enumera los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001.

SOCIAL MEDIA: Los medios de comunicación sociales (en inglés: social media) son plataformas de comunicación en línea donde el contenido es creado por los propios usuarios mediante el uso de las tecnologías web, que facilitan la edición, la publicación y el intercambio de información.

SSH: **S**ecure **SH**ell, (en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

TB: Un terabyte (TB) es una unidad de almacenamiento de información equivalente a 10^{12} bytes.

TELNET: **Tel**ecommunication **Net**work, es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

USB: Un sistema de almacenamiento Universal Serial Bus (USB) es un tipo de dispositivo de almacenamiento de datos e información, normalmente utilizado como copia de respaldo.

15. Bibliografía

Implantación de un SGSI en la empresa. INCIBE
https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

Portal ISO27001 en español
http://iso27000.es/index.html

Guía de seguridad CCN-STIC-815. ENS. Métricas e indicadores
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/525-ccn-stic-815-indicadores-y-metricas-en-el-ens/file.html

Implementación efectiva de un SGSI ISO 27001 - ISACA
https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposición%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

MAGERIT. Versión 3.0. Método, catálogo de elementos y guía de técnicas. Portal Pae.
https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WS2vUFIryDU

AENOR. Norma UNE-ISO/IEC 27001. Noviembre 2014
http://www.aenor.es/aenor/normas/iso/fichanormaiso.asp?codigo=054534#.WS2w1FIryDU

AENOR. Norma UNE-ISO/IEC 27002:2013
http://www.aenor.es/aenor/normas/iso/fichanormaiso.asp?codigo=054533#.WS2w71IryDU

Política de seguridad de la información
https://web.ua.es/es/consejo-gobierno/documentos/consejo-de-gobierno-28-06-2013/punto-7-2-politica-seguridad-informacion-ua.pdf

Modelo de capacidad de madurez (CMM)
http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/garcia_r_ci/capitulo5.pdf

Informe de auditoría interna para un SGSI según ISO/IEC 27001:2013
http://es.presidencia.gov.co/oci/DocumentosOCI/AEG2016-SGSI.pdf

Revisión del SGSI por la dirección
http://www.electroucayali.com.pe/ElectroUcayali/index.php/transparencia-estandar1/category/349-documentacion-de-seguridad-de-la-informacion?download=1357:a-9-3-revision-del-sgsi-por-la-direccion

Anexo I. Inventario y valoración activos

Versión → v01-0517. A continuación se presenta una tabla con el inventario de los activos vinculados a la información y su valor según clasificación *Magerit*:

Ámbito	Id	Activo	Valor
Instalaciones	I1	Tienda – Sede 1	Alto
	I2	Almacén 1 - Sede 1	Medio
	I3	Almacén 2 - Sede 1	Medio
	I4	Oficina - Sede 1	Muy alto
	I5	Nave almacén y exposición - Sede 2	Bajo
	I6	Vehículo comercial	Bajo
Hardware	H1	Servidor	Muy alto
	H2	PC Gerente	Muy alto
	H3	PC,s ventas	Bajo
	H4	Ordenadores portátiles	Alto
	H5	Dispositivos móviles (smartphone,s y tablet,s)	Medio
	H6	Impresoras	Muy bajo
	H7	Unidades de respaldo	Muy alto
	H8	Hub (Concentrador)	Alto
	H9	Router,s (Encaminador)	Alto
Aplicaciones	A1	ERP (Gestión y Contabilidad)	Muy alto
	A2	ERP (Solución movilidad)	Muy alto
	A3	Sistemas operativos	Medio
	A4	Gestor de correo electrónico	Bajo
	A5	Aplicaciones web	Bajo
	A6	Software Antimalware	Muy alto
	A7	Suite ofimática y otras aplicaciones	Alto
	A8	Autobackup remoto	Muy alto
Datos	D1	Bases de datos	Muy alto
	D2	Información en soporte digital	Alto
	D3	Información en soporte papel	Alto
Red	R1	ADSL,s (Voz + Datos)	Medio
	R2	Servicio 3G (Datos)	Medio
	R3	Servicio 4G (Voz + Datos)	Medio
	R4	LAN (Red de Área Local)	Medio
	R5	WIFI (Red inalámbrica)	Bajo
Servicios	S1	WWW (Servicio web)	Alto
	S2	SSH (Acceso remoto al servidor)	Muy alto
	S3	EMAIL (Correo electrónico)	Muy alto
	S4	FTP (Transferencia de ficheros)	Alto

Ámbito	Id	Activo	Valor
Servicios	S5	FILE (Almacenamiento de ficheros)	Alto
	S6	PKI (Infraestructura de clave pública – firma digital)	Muy alto
	S7	IDM (Gestión identidades en usuarios del sistema)	Medio
Equipamiento aux.	E1	Equipos de climatización	Muy bajo
	E2	Cableado eléctrico y de red	Bajo
	E3	Mobiliario	Bajo
	E4	Caja de seguridad	Muy alto
	E5	SAI (Sistema de alimentación ininterrumpida)	Medio
Personal	P1	Operadores internos	Alto
	P2	Operadores externos	Alto
	P3	Soporte externo (subcontratas)	Medio
	P4	Clientes	Medio
	P5	Proveedores	Medio

Valoración de activos en función de las dimensiones de seguridad

A continuación se procederá a la valoración de los activos en función de su criticidad sobre las 5 dimensiones de la Seguridad de la Información. La siguiente tabla explica brevemente en que consisten estas dimensiones:

Dimensión	Significado
(A)utenticidad	Garantía de la identidad de usuarios y autoría de una determinada acción.
(C)onfidencialidad	Garantía del acceso a la información sólo por personal autorizado.
(I)ntegridad	Garantía de que la información y sus procesos no son manipulados.
(D)isponibilidad	Garantía de que la información es accesible cuando es necesaria.
(T)razabilidad	Garantía de reproducción de una determinada secuencia de acciones.

Ahora se presenta la escala de valoración que utilizaremos sobre cada activo y el correspondiente criterio a aplicar:

Valor	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

A continuación presentamos la tabla resumen de valoración de los activos y los aspectos críticos de los mismos (sobre las 5 dimensiones de seguridad).

Ámbito	Id	Valor	Aspectos críticos – Dimensiones seguridad				
			A	C	I	D	T
Instalaciones	I1	Alto	5	9	9	6	6
	I2	Medio	3	0	5	5	6
	I3	Medio	3	0	5	5	6
	I4	Muy alto	9	9	9	9	9
	I5	Bajo	3	3	3	3	3
	I6	Bajo	6	7	7	5	5
Hardware	H1	Muy alto	9	9	9	10	9
	H2	Muy alto	9	9	9	9	9
	H3	Bajo	6	6	9	6	3
	H4	Alto	6	9	9	6	6
	H5	Medio	3	3	3	6	3
	H6	Muy bajo	0	0	0	3	0
	H7	Muy alto	9	9	9	9	6
	H8	Alto	0	0	0	6	3
	H9	Alto	0	0	0	6	3
Aplicaciones	A1	Muy alto	9	9	9	9	9
	A2	Muy alto	9	9	9	9	9
	A3	Medio	3	3	6	6	3
	A4	Medio	6	6	8	8	6
	A5	Medio	8	8	8	6	6
	A6	Muy alto	9	3	6	9	9
	A7	Alto	6	6	6	8	3
	A8	Muy alto	9	9	9	9	9
Datos	D1	Muy alto	8	8	9	9	8
	D2	Alto	8	8	8	8	8
	D3	Alto	8	8	8	8	8
Red	R1	Medio	6	6	6	6	6
	R2	Medio	6	6	6	6	6
	R3	Medio	6	6	6	6	6
	R4	Medio	3	6	6	9	0
	R5	Bajo	3	3	3	3	0
Servicios	S1	Alto	8	6	6	6	6
	S2	Muy alto	9	9	9	6	6
	S3	Muy alto	9	9	9	9	9
	S4	Alto	9	9	8	8	6

Ámbito	Id	Valor	Aspectos críticos – Dimensiones seguridad				
			A	C	I	D	T
Servicios	S5	Alto	8	6	6	8	6
	S6	Muy alto	9	9	9	9	9
	S7	Medio	3	6	3	3	6
Equipamiento aux.	E1	Muy bajo	0	0	0	0	0
	E2	Bajo	2	2	2	2	2
	E3	Bajo	1	1	1	1	1
	E4	Muy alto	8	8	9	8	9
	E5	Medio	1	1	1	1	1
Personal	P1	Alto	6	8	8	6	8
	P2	Alto	6	8	8	6	8
	P3	Medio	8	8	8	8	9
	P4	Medio	8	6	6	8	6
	P5	Medio	8	3	3	4	4

Un aspecto importante a tener en cuenta es la valoración individual que se ha hecho de cada activo sobre las 5 dimensiones de seguridad a las que está sometido. No todas las dimensiones afectan de igual modo a un activo y por ello es importante analizar los resultados de forma individual.

Anexo II. Política de Seguridad

Versión → v01-0517. A través de la política de seguridad que se presenta a continuación se pretende garantizar la confidencialidad, integridad y disponibilidad de la información de FCA. La empresa pone a disposición de todos sus empleados el presente documento con la finalidad de que conozcan y asuman esta política como el conjunto de normas de obligado cumplimiento que se exponen a continuación:

Principios generales de la Política de Seguridad

- Se debe mantener un nivel apropiado de seguridad para proteger la información de la empresa y los sistemas automatizados/manuales que la contienen.
- En la seguridad de la información deben estar involucrados todos los miembros de la organización, sin excepción alguna por razón de cargo o responsabilidad. Toda esta normativa es de obligado cumplimiento.
- La presente política de seguridad afecta a todos los equipos y sistemas conectados a la red corporativa. Se incluyen también aquellos dispositivos personales que utilizan la red de FCA para la obtención de servicios web (banca electrónica personal, servicios de ocio, etc). Toda la información corporativa que no esté en soporte digital y sea considerada sensible está incluida en la presente política de seguridad.

Responsabilidades en la Gestión de la Seguridad de la Información

- La dirección y autoridad en materia de seguridad de la información recae en la dirección de la empresa. La orientación y aplicación de medidas en dicha materia está externalizada en las dos empresas que proporcionan soporte TIC.
- Existen tres categorías de usuario con acceso al sistema de información: jcarlos, ventas y soporte. La primera de ellas (jcarlos) tiene carácter de administrador pero sin privilegios de “root”. La segunda (ventas) tiene carácter de usuario (con restricciones sobre parte del ERP) y es utilizada por el equipo de ventas y almacén. La tercera (soporte) tiene carácter de administrador y los máximos privilegios (root). Es utilizada por el equipo que proporciona el soporte y mantenimiento del ERP. Este equipo ha sido el que también lo ha diseñado e implantado.
- La información de la empresa debe clasificarse según su grado de confidencialidad y protegerse adecuadamente, con independencia del soporte en el que esté almacenada (papel o digital). Se propone dos categorías para toda esta información: uso general y confidencial. No se considera necesario que estén etiquetadas como tal, pero si que se custodien bajo diferentes medidas de seguridad.
- La responsabilidad de que se lleven a cabo las copias de seguridad recae en la dirección de la empresa, aunque la implantación y supervisión periódica de las mismas (verificación del estado, contenido y pruebas de restauración) sea responsabilidad de las empresas de soporte TIC.

- Las copias de seguridad tendrán la siguiente periodicidad:
  - Autobackup: Este tipo de copia de respaldo está programado para que vuelque el contenido del ERP, sobre un servidor remoto, dos veces al día (12h y 18h). No se considera necesario cifrar el contenido, por lo que las copias son completamente operativas.
  - Semanal: programada para que a las 10h de cada sábado lance una copia de seguridad, del equipo de dirección, creando una imagen a través de una aplicación nativa del propio sistema operativo. Se alternarán 2 discos externos y dicha copia se custodiará fuera de la empresa.
  - Anual: se realizan 2 copias en diferentes dispositivos de todo el contenido del ERP (anual incremental). Estas copias se realizan los últimos días del año y se custodiarán fuera de la empresa.
  - En aquellos casos en que las copias se efectúen sobre dispositivos USB externos, se procederá a la desconexión, de estos dispositivos del equipo. al finalizar la copia. Con esto se pretende evitar la propagación de malware cuando un punto de la red ha sido comprometido.

Control de acceso a la información corporativa y de carácter personal

- El acceso a la información corporativa será proporcionado por la dirección de la empresa según “la necesidad de saber”, que tenga cada empleado, para el desempeño de sus funciones. La propia dirección será la encargada de asignar y retirar estos privilegios según las circunstancias operativas de cada momento.
- Identificadores de usuario y contraseñas. Se mantendrán los tres tipos de usuario (categorías) establecidos desde la implantación del ERP. Las contraseñas deben tener entre 8 y 12 caracteres y renovarán según el siguiente procedimiento:
  - Usuario “ventas”. Renovación anual. Los 4 primeros caracteres serán el año en curso y los 6 siguientes el usuario con la última letra en mayúsculas. Todos los miembros del equipo de ventas utilizarán el mismo nombre de usuario y contraseña, ya que los equipos de venta al público son utilizados indistintamente por todos los miembros de la empresa. La segregación de operaciones en el ERP, por razón de usuario, se efectúa a través de un número de “agente” lo que permite consultar en todo momento el “log” de transacciones e identificar a la persona física que las ha efectuado.
  - Usuario “jcarlos”. Renovación anual. Los 7 primeros caracteres corresponderán al nombre de usuario con la primera letra en mayúsculas, seguido de los 4 dígitos del año en curso.
  - Usuario “soporte”. La periodicidad en la renovación y confección de la contraseña será responsabilidad del equipo de soporte. La empresa no tiene acceso a estos datos.
- Cualquier miembro de la empresa está obligado a guardar el debido secreto sobre la identificación del usuario y la contraseña que esté

operativa en cada momento, incluso durante un periodo de 2 años, en el caso de que cese en su puesto de trabajo.

- La empresa que realiza el soporte del ERP será la encargada del proceso CRUD (Create, Update, Delete) de usuarios y contraseñas. La dirección podrá realizar igualmente este proceso.

Aspectos relacionados con el personal

- *Contrato de confidencialidad*: Todos los empleados de la organización deberán leer, entender, aceptar y firmar el correspondiente contrato de confidencialidad en el que se incluye:
  - Mención a la existencia de un documento de seguridad de obligado cumplimiento, según establece la LOPD de carácter personal. Este documento será actualizado en función de las exigencias del nuevo reglamento Europeo en esta materia.
  - Mención a la obligatoriedad de mantener la confidencialidad de toda la información corporativa a la que tenga acceso en el desarrollo de sus tareas. Esta obligatoriedad se mantendrá durante los dos años, en caso de cesar en su puesto de trabajo.
  - Mención a las medidas que debe adoptar para garantizar la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso en el desarrollo de sus funciones.
- *Modalidad de teletrabajo*: No está contemplada esta modalidad. Unicamente la dirección de la empresa puede autorizar la salida de dispositivos para labores comerciales. Solo se contempla esta modalidad en la persona que realiza labores de visita a clientes de la empresa, dos días por semana. En este caso, se autoriza la salida de un dispositivo móvil tipo “smartphone” y otro tipo “tablet”, con información corporativa.
- *Protección contra robos*: Todos los equipos portables, unidades de volcado de seguridad y documentación de carácter confidencial en sus diferentes formatos (digital extraible o papel) deberán estar custodiados bajo llave, en armarios o cajas de seguridad con acceso restringido a la dirección o personal autorizado. En caso de la existencia de unidades USB que contengan información sensible, deberá cifrarse su contenido.
- *Derecho a la vigilancia y auditoría*: La dirección se reserva el derecho a inspeccionar, en cualquier momento, cualquier equipo propiedad de la empresa y correo electrónico corporativo, a fin de verificar el cumplimiento de esta normativa y detectar posibles violaciones de seguridad. Esta inspección podrá realizarse sin la autorización del usuario auditado y no incluye sus dispositivos de uso personal ni siquiera cuando utilicen la infraestructura de red corporativa para conectarse a Internet.
- *Uso personal de los sistemas informáticos*: Con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información, no está permitido el uso de ningún elemento del sistema de información de la empresa para uso personal. Como excepción, se autoriza el uso ocasional de una de las redes WiFi corporativas para la conexión a

Internet de los dispositivos personales de los empleados, en su tiempo de descanso.

- *Aplicaciones que comprometen la seguridad*: No está permitido, en ningún tipo de dispositivo (personal o corporativo) la instalación y utilización de aplicaciones que vulneren la seguridad de la red, para la obtención de privilegios de acceso (contraseñas) y con la intención de acceder al sistema. Tampoco está permitido el análisis e interceptación de las comunicaciones (voz y datos) o cualquier otro tipo de sistema cuyo objetivo sea evadir las medidas de protección del sistema de información. Estas conductas son consideradas violaciones graves de esta normativa interna y podrán ser sancionadas.

Control de la seguridad en la red corporativa

- *Conexiones internas*: Los equipos de trabajo de la empresa trabajan en doble modalidad. Por un lado utilizan un emulador, sobre un sistema operativo Windows, para conectarse al servidor y entrar en el ERP para la gestión comercial. Por otro lado, funcionan como terminales independientes conectados a un "hub" que a su vez tiene salida a Internet a través de un enrutador facilitado por el ISP (Internet Service Provider – Proveedor de Servicios de Internet – Movistar). La información corporativa, en ningún momento se almacena en uno de estos equipos. Unicamente se almacena en el servidor central. No está permitido, sin autorización de la dirección, la conexión a Internet desde ningún puesto de trabajo de las zonas de ventas o almacén.
- *Conexiones externas*: La única conexión que procede del exterior es la efectuada por la empresa de soporte del ERP vía protocolo SSH (Secure Shell). Este protocolo usa técnicas de cifrado que hacen que la información que circula por la red pública, lo haga de manera no legible. Actualmente no está permitido ningún otro tipo de conexión externa a la red corporativa.

Control contra el software malicioso

- La red corporativa trabaja sobre un servidor con sistema operativo Suse Linux. Inicialmente no se contempla la instalación de software anti-malware en este equipo. El resto de terminales en red sólo utilizan el sistema operativo anfitrión para el arranque del emulador que permite el inicio de sesiones contra el servidor, por lo que no se hace necesaria la actualización del sistema ni la instalación de antivirus.
- No está permitida la introducción e instalación de ningún software en el servidor central sin aprobación de la dirección. En cualquier caso, las actualizaciones del sistema, parches de seguridad y otros elementos necesarios para el correcto funcionamiento del ERP, serán efectuadas por el personal de soporte externo o bajo autorización expresa de la dirección..
- El equipo de dirección, que también está conectado al servidor central, dispone de software antimalware propietario completamente actualizado.
- Esta totalmente prohibido la conexión de dispositivos USB a cualquiera de los equipos de red, sin autorización de la dirección o supervisión de alguno de los miembros de soporte.

- En caso de producirse una infección por virus en alguno de los equipos, este debe desconectarse/aislarse de la red corporativa hasta que personal técnico habilitado pueda proceder a su análisis y eliminación. Este hecho quedará registrado en el correspondiente formulario del documento de seguridad LOPD.
- En caso de que el servidor central se viese afectado, se pondrá en conocimiento de la empresa de soporte para que proceda a la restauración de la última copia (limpia de virus) procedente del autobackup.

Controles sobre licencias de software base y otras aplicaciones

- Todo el software instalado en el sistema de información dispone de licencia en unos de los siguientes formatos:
  - Sistemas Windows y aplicaciones ofimáticas. Licencia comercial.
  - Dispositivos móviles: Licencia comercial iOS y Android (GNU).
  - Servidor Suse Linux Enterprise Server (SLES). Licencia comercial.
  - Software ERP CX. Licencia monoempresa hasta 10 usuarios.
  - Software iPreventa. Licencia monoempresa de 1 usuario.
  - Software Autobackup. Licencia monoempresa de 1 equipo.

Seguridad de los equipos

- En la medida en que la operativa habitual lo permita, los equipos que estén al alcance del público deben cumplir con las siguientes premisas:
  - *Política de puesto de trabajo despejado*: debe adoptarse las medidas oportunas para que no haya información sensible cerca de los puesto de trabajo en ausencia del personal de la empresa.
  - *Política de pantalla limpia*: en aquellos casos en los que el puesto esté desatendido, debe habilitarse la protección de la pantalla mediante contraseña para todos aquellos equipos cuya información sea visible por personas ajenas a la empresa.
  - *Seguridad de los equipos fuera de las instalaciones*: es el caso de aquellos dispositivos móviles que contienen información corporativa y son utilizados por el equipo comercial en las visitas a clientes. Será responsabilidad del usuario, la custodia del terminal y la utilización de medidas de bloqueo mediante contraseña.
  - *Reutilización de equipos o eliminación segura de la información contenida en los mismos*: Antes de proceder a la reutilización de un equipo por personal ajeno a la empresa o el desecho de algún componente o soporte que contenga información corporativa, debe procederse a realizar un borrado seguro a través del *"Método Gutman"*. Este procedimiento consiste en escribir sobre los datos originales una serie de 35 diferentes patrones, de tal forma que sea extremadamente difícil (para efectos prácticos, imposible) saber el contenido original.

Anexo III. Auditorías Internas

Versión → v01-0517. Para el correcto mantenimiento del SGSI, independientemente de los requisitos impuestos por la norma ISO/IEC27001:2013, se propone la realización de una auditoría interna anual que contemple los siguientes puntos:

Alcance y objetivo de la auditoría

El alcance de la auditoría está limitado a los todos los sistemas de información del empresa, así como el personal con acceso a los mismos. En concreto se relacionan los siguientes:

- *Red corporativa*: servidor central, puestos de trabajo, equipos portátiles y dispositivos móviles, unidades extraíbles de backup, otros dispositivos USB de bajo almacenamiento, hub, enrutadores, cableado, puntos de acceso telefónico e impresoras.
- *Personal*: grado de cumplimiento de la política de seguridad en cuanto a los procedimientos empleados por el personal de la empresa para garantizar la confidencialidad, integridad y disponibilidad de la información.
- *Información sensible no automatizada*: grado de cumplimiento de las medidas de seguridad para toda aquella información confidencial en soporte papel.

El objetivo de la auditoría es mejorar el nivel de seguridad de la información de una forma dinámica y periódica.

Fecha y lugar de realización de la auditoría

Como fecha, para la realización de las *auditoría anual*, se propone la segunda quincena del mes de Diciembre y con una *duración estimada* de *3 días*. De estos 3 días se reservará media jornada para reunirse con la dirección. En caso de que no pudiese ser realizada en esta fecha, se propone como alternativa la primera semana del mes de Agosto.

Posteriormente, *se reservarán 4 días más* para las siguientes tareas:

- 1 día para la revisión de los controles ISO/IEC 27002. Confección del SOA (Statement of Applicability . Declaración de Aplicabilidad).
- 1 día para la revisión de toda la documentación generada.
- 2 días para la elaboración del informe de auditoría.

La auditoría se llevará a cabo “in situ”, en las instalaciones de FCA. Primero se realizará en la sede principal y posteriormente en la segunda ubicación (actualmente no operativa).

Equipo auditor

Dada la dimensión de la empresa, no se considera necesario que el equipo auditor esté compuesto por más de una persona. En cualquier caso, podrá ser requerido el apoyo del personal de soporte para llevar acabo la auditoría.

Al equipo auditor se le requerirán conocimientos y experiencia en las siguientes áreas:

- Políticas y organización de la seguridad.
- Gestión de activos y sus políticas de uso.
- Gestión de recursos humanos.
- Seguridad física y del entorno.
- Aspectos técnicos de la auditoría aplicables a la organización.
- Gestión de incidentes de seguridad.
- Continuidad de negocio según estándares tipo BS 25999.
- Normativa sobre cumplimiento legal, aplicable en cada momento.
- Norma ISO/IEC 27001 (en profundidad).
- Planificación de auditorías periódicas, tipos y metodologías.
- Análisis de riesgos y metodologías.
- Ciclo de Demming.

Equipo de empresa presente en la auditoría

En el proceso de auditoría deberán estar presentes todos los miembros de la organización. En caso de no ser posible, deberán participar: el director de la empresa, 1 miembro de administración, 1 miembro del equipo de ventas/comercial, el encargado del almacén y 1 miembro del soporte TIC.

Criterios de auditoría

Serán aplicados los criterios contemplados en la norma ISO/IEC 27001:2013.

Anexo IV. Gestión de Indicadores

Versión → v01-0517. A continuación se presenta una relación con aquellos indicadores que se han seleccionado para controlar el funcionamiento de las medidas de seguridad de la información implantadas en FCA:

Indicador	**Política de seguridad de la información**
Descripción	Revisión de las políticas en materia de seguridad de las TIC
Control de seguridad	Revisión a intervalos planificados o cambios importantes
Formula de medición	Nº de veces/año que se actualiza la política de seguridad
Unidades de medida	Número de revisiones
Frecuencia de medición	Anual
Valor umbral	>=1 (generará alarma si el valor es 0)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Organización de seguridad de la información**
Descripción	Contacto con grupos de interés especial
Control de seguridad	Contacto periódico con especialistas en seguridad TIC
Formula de medición	N.º de veces/año que se tienen reuniones informativas
Unidades de medida	Número de reuniones
Frecuencia de medición	Trimestral
Valor umbral	>=4 (generará alarma si el número es inferior)
Responsable de la medición	Dirección de la empresa

Indicador	**Conexión de dispositivos móviles en la empresa**
Descripción	Revisión de la seguridad de los dispositivos móviles
Control de seguridad	Seguridad en el uso de estos dispositivos en la empresa
Formula de medición	N.º de veces/año que se chequean y actualizan
Unidades de medida	Número de revisiones
Frecuencia de medición	Mensual
Valor umbral	>=6 (generará alarma si el número es inferior)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Recursos humanos: Antes de la incorporación**
Descripción	Investigación de referencias anteriores
Control de seguridad	Comprobación de las referencias del candidato
Formula de medición	Si/No
Unidades de medida	1 = Si / 0 = No
Frecuencia de medición	Única
Valor umbral	1 (generará alarma si el valor es 0)
Responsable de la medición	Dirección de la empresa

Indicador	**Recursos humanos: Durante el empleo**
Descripción	Cumplimiento de las políticas de seguridad
Control de seguridad	Verificación de su cumplimiento por parte del personal
Formula de medición	N.º de verificaciones por empleado y año
Unidades de medida	Veces por empleado/año
Frecuencia de medición	Trimestral
Valor umbral	>=4 (generará alarma si el número es inferior)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Gestión de activos: Inventario**
Descripción	Inventario de activos que integran el sistema de información
Control de seguridad	Revisión/actualización periódica de la relación de activos
Formula de medición	N.º veces que se actualiza el inventario/año
Unidades de medida	Número de actualizaciones
Frecuencia de medición	Semestral
Valor umbral	>=1 (generará alarma si el valor es 0)
Responsable de la medición	Personal de administración o responsable TIC

Indicador	**Gestión de activos: Clasificación de la información**
Descripción	Etiquetado y clasificación de la información corporativa
Control de seguridad	Etiquetado de la información sensible de la empresa
Formula de medición	N.º documentos etiquetados/total de documentos sensibles
Unidades de medida	% documentos
Frecuencia de medición	Semanal
Valor umbral	>=80% (generará alarma si el valor es inferior)
Responsable de la medición	Personal de administración o dirección

Indicador	**Gestión de activos: Manipulación de soportes**
Descripción	Gestión de soportes extraíbles durante su ciclo de vida
Control de seguridad	Verificación periódica del estado del soporte
Formula de medición	N.º de veces que se chequea soporte/año
Unidades de medida	Número de chequeos
Frecuencia de medición	Semestral
Valor umbral	>=1 (generará alarma si el valor es 0)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Gestión de activos: Eliminación segura**
Descripción	Borrado seguro de información previo al desecho del soporte
Control de seguridad	Realización de un borrado seguro de su contenido
Formula de medición	N.º de veces que realiza un borrado seguro
Unidades de medida	Número de operaciones borrado/año
Frecuencia de medición	Anual
Valor umbral	>=1 (generará alarma si el valor es 0)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Control de acceso: Instalaciones**
Descripción	Revisión de las medidas de control de acceso al negocio
Control de seguridad	Verificación de las medidas de seguridad en el acceso
Formula de medición	N.º de veces que revisan los controles de acceso físico
Unidades de medida	Número de comprobaciones
Frecuencia de medición	Trimestral
Valor umbral	>=1 (generará alarma si el valor es 0)
Responsable de la medición	Dirección de la empresa

Indicador	**Control de acceso: Redes y servicios de red**
Descripción	Revisión periódica de los accesos a la red corporativa
Control de seguridad	Verificación y análisis de los logs de acceso a la red
Formula de medición	N.º consultas a ficheros de log/año
Unidades de medida	Número accesos al log
Frecuencia de medición	Mensual
Valor umbral	>=6 (generará alarma si el valor es inferior)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Control de acceso: Gestión de contraseñas**
Descripción	Renovación periódica de las contraseñas de acceso
Control de seguridad	Cambio de todas las contraseñas de acceso al sistema
Formula de medición	N.º de cambios por contraseña y año
Unidades de medida	Número de modificaciones
Frecuencia de medición	Trimestral (generará alarma si el valor es 0)
Valor umbral	>=1
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Política de controles criptográficos**
Descripción	Uso de la criptografía en información confidencial
Control de seguridad	Cifrado de la información sensible antes de ser almacenada
Formula de medición	Si/No
Unidades de medida	1 = Si / 0 = No
Frecuencia de medición	Anual
Valor umbral	1 (generará alarma si el valor es 0)
Responsable de la medición	Dirección de la empresa con apoyo del soporte TIC

Indicador	**Seguridad física: Perímetro de seguridad**
Descripción	Acceso físico a las instalaciones
Control de seguridad	Comprobación de medidas de seguridad física perimetral
Formula de medición	Si/No
Unidades de medida	1 = Si / 0 = No
Frecuencia de medición	Anual
Valor umbral	1 (generará alarma si el valor es 0)
Responsable de la medición	Dirección de la empresa

Indicador	**Seguridad física de los equipos: ambientales**
Descripción	Medidas de protección contra desastres naturales
Control de seguridad	Plan de contingencia para la continuidad del negocio
Formula de medición	Si/No
Unidades de medida	1 = Si / 0 = No
Frecuencia de medición	Anual
Valor umbral	1 (generará alarma si el valor es 0)
Responsable de la medición	Dirección de la empresa

Indicador	**Seguridad física de los equipos: robo**
Descripción	Medidas de protección contra el robo de equipamiento
Control de seguridad	Comprobación de la situación y estado de los equipos
Formula de medición	Si/No
Unidades de medida	1 = Si / 0 = No
Frecuencia de medición	Anual
Valor umbral	1 (generará alarma si el valor es 0)
Responsable de la medición	Dirección de la empresa

Indicador	**Seguridad lógica de los equipos: actualizaciones**
Descripción	Actualizaciones y parches de seguridad de los fabricantes
Control de seguridad	Frecuencia de actualización del software base y aplicaciones
Formula de medición	N.º actualizaciones por año/nº total de aplicaciones
Unidades de medida	% aplicaciones
Frecuencia de medición	Trimestral
Valor umbral	>=80% (generará alarma si el valor es inferior)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Seguridad lógica de los equipos: política antimalware**
Descripción	Medidas de protección contra el software malicioso
Control de seguridad	Comprobación de las actualizaciones y firmas de virus
Formula de medición	N.º de actualizaciones realizadas/300
Unidades de medida	% de actualizaciones
Frecuencia de medición	Semanal
Valor umbral	100% (generará alarma si el valor es inferior)
Responsable de la medición	Dirección de la empresa

Indicador	**Seguridad lógica de los equipos: política antimalware**
Descripción	Medidas de protección contra el software malicioso
Control de seguridad	Comprobación de las actualizaciones y firmas de virus
Formula de medición	N.º de actualizaciones realizadas/365
Unidades de medida	% de actualizaciones
Frecuencia de medición	Semanal
Valor umbral	>=85% (generará alarma si el valor es inferior)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Seguridad lógica de los equipos: copias de seguridad**
Descripción	Política de copias de seguridad locales y remotas
Control de seguridad	Integridad de las copias de seguridad
Formula de medición	N.º restauraciones exitosas/n.º total de copias realizadas
Unidades de medida	% Copias de seguridad
Frecuencia de medición	Diaria (autobackup remoto) y Semanal (copia local dirección)
Valor umbral	>=80% (generará alarma si el valor es inferior)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Gestión de incidentes de seguridad de la información**
Descripción	Registro de los incidentes relacionados con información
Control de seguridad	Resolución de incidentes de seguridad de la información
Formula de medición	N.º incidentes resueltos en (<24 h)/total incidentes reportados
Unidades de medida	% incidentes
Frecuencia de medición	Mensual
Valor umbral	>=70% (generará alarma si el valor es inferior)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Gestión de la continuidad de negocio**
Descripción	Verificación de la disponibilidad de la información
Control de seguridad	Análisis de las incidencias que afecten a la disponibilidad
Formula de medición	N.º días de indisponibilidad información/365
Unidades de medida	% días
Frecuencia de medición	Mensual
Valor umbral	>=85% (generará alarma si el valor es inferior)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Cumplimiento normativa legal de protección de datos**
Descripción	Verificar el grado de cumplimiento de las medidas RLOPD
Control de seguridad	Documento de seguridad actualizado y aplicado
Formula de medición	Si/No
Unidades de medida	1 = Si / 0 = No
Frecuencia de medición	Anual
Valor umbral	1 (generará alarma si el valor es 0)
Responsable de la medición	Responsable de seguridad TIC

Indicador	**Revisiones de SGSI**
Descripción	Programa de actualizaciones periódicas y auditorías internas
Control de seguridad	Estado de actualización del SGSI
Formula de medición	N.º actualizaciones del SGSI por año
Unidades de medida	Actualizaciones
Frecuencia de medición	Anual
Valor umbral	>=1 generará alarma si el valor es 0)
Responsable de la medición	Dirección de la empresa

Anexo V. Revisión por la Dirección

Versión → v01-0517. La dirección de la empresa debe comprometerse con la implantación, monitorización, revisión y mejora del Sistema de Gestión de Seguridad de la Información. Para ello, en este proceso de revisión y mejora continua, el papel de la dirección debe incluir las siguientes tareas:

- Analizar los resultados proporcionados por los indicadores de control.
- Analizar y poner en marcha los cambios relevantes (internos y externos) que afecten al SGSI.
- Analizar los resultados obtenidos en las auditorías internas.
- Aprobar y colaborar en la implantación de las medidas correctivas.
- Designar los recursos necesarios para la anterior medida.
- Observar el grado de cumplimiento de los objetivos del SGSI.
- Evaluar la información obtenida en las reuniones periódicas con las partes involucradas en el alcance del SGSI.
- Analizar los resultados obtenidos en la evaluación y posterior tratamiento del riesgo.
- Aprobar el acta final que contemple las nuevas acciones y acuerdos establecidos en materia de seguridad de la información.

Anexo VI. Roles y Responsabilidades

Versión → v01-0517. A continuación se presenta una relación de roles y responsabilidades, en lo que al SGSI se refiere, sobre cada área de la empresa:

Área: Dirección	
Rol	Fundador de FCA y Gerente de la empresa.
Nombre	JCPP
Responsabilidades	• Aprobación del proyecto de implantación SGSI. • Determinación del alcance y objetivos del SGSI. • Asignación de recursos para el SGSI. • Aprobación de la política de seguridad. • Programación y supervisión de auditorías. • Gestión de cambios en el SGSI. • Aprobación de la documentación del SGSI.

Área: Administración	
Rol	Tareas de administración.
Nombre	VNF
Responsabilidades	• Cumplimiento política seguridad. • Actualización documentación SGSI. • Apoyo auditoría interna.

Área: Ventas/Comercial/Almacén	
Rol	Personal de ventas, comercial y almacén.
Nombre	AG1, AG2, AG3, AG4
Responsabilidades	• Integración en el SGSI. • Cumplimiento política de seguridad. • Control y mantenimiento de equipos. • Notificación de incidentes.

Área: Soporte TIC	
Rol	Soporte del ERP y coordinación del SGSI.
Nombre	CVM, JGK
Responsabilidades	• Implantación de controles. • Reporte del resultado de los indicadores. • Actualización de equipos y sistemas. • Auditoría anual.

Anexo VII. Análisis de las amenazas

Versión → v01-0517. A continuación se presenta una tabla descriptiva con las diferentes amenazas que pueden afectar a cada activo, en cada una de sus dimensiones. Esta clasificación se ha efectuado con metodología *Magerit 3.0*.

Id.	Descripción	Dimensión				
		A	C	I	D	T
AMZ1	Fuego				X	
AMZ2	Daños por agua				X	
AMZ3	Desastres naturales				X	
AMZ4	Fuga de información		X			X
AMZ5	Introducción de información falsa	X		X		X
AMZ6	Alteración de la información			X		X
AMZ7	Corrupción de la información			X	X	
AMZ8	Destrucción de la información				X	X
AMZ9	Interceptación de la información (escucha)		X			
AMZ10	Corte del suministro eléctrico				X	
AMZ11	Condiciones inadecuadas de temperatura o humedad				X	
AMZ12	Fallo de servicios de comunicaciones				X	X
AMZ13	Interrupción de otros servicios y suministros esenciales				X	
AMZ14	Desastres industriales				X	
AMZ15	Degradación de los soportes de almacenamiento de información				X	
AMZ16	Difusión de software dañino		X	X	X	X
AMZ17	Errores de mantenimiento/Actualización de programas (software)			X	X	X
AMZ18	Errores de mantenimiento/Actualización de equipos (hardware)				X	X
AMZ19	Caída del sistema por sobrecarga				X	
AMZ20	Pérdida de equipos		X		X	
AMZ21	Indisponibilidad de equipos				X	X
AMZ22	Abuso de privilegios de acceso		X	X	X	X
AMZ23	Acceso no autorizado		X	X		X
AMZ24	Errores de los usuarios		X	X	X	X
AMZ25	Errores del administrador		X	X	X	X
AMZ26	Errores de configuración			X		X
AMZ27	Denegación de servicio				X	
AMZ28	Robo		X		X	
AMZ29	Indisponibilidad del personal				X	X
AMZ30	Extorsión		X	X	X	
AMZ31	Ingeniería social (picaresca)		X	X	X	

Anexo VIII. Análisis de los riesgos

Versión → v01-0517. A continuación se presenta la tabla final en la que se incluye, para cada activo, la probabilidad de ocurrencia de cada amenaza, el impacto generado por la ocurrencia de la misma y el riesgo final estimado.

Activo	Amenaza	Probabilidad	Impacto	Riesgo
I1 (Tienda)	AMZ1 (Fuego)	1	2	2
I1 (Tienda)	AMZ2 (Daños por agua)	1	2	2
I1 (Tienda)	AMZ28 (Robo)	2	2	4
I2, I3 (Almacén)	AMZ1 (Fuego)	1	1	1
I2, I3 (Almacén)	AMZ2 (Daños por agua)	1	1	1
I2, I3 (Almacén)	AMZ28 (Robo)	1	2	2
I4 (Oficina)	AMZ1 (Fuego)	2	3	6
I4 (Oficina)	AMZ2 (Daños por agua)	1	3	3
I4 (Oficina)	AMZ28 (Robo)	2	3	6
I5 (Nave)	AMZ1 (Fuego)	1	1	1
I5 (Nave)	AMZ2 (Daños por agua)	1	1	1
I5 (Nave)	AMZ28 (Robo)	1	1	1
I6 (Vehículo)	AMZ28 (Robo)	3	1	3
H1 (Servidor)	AMZ4 (Fuga información)	1	1	1
H1 (Servidor)	AMZ7 (Corrupción información)	1	3	3
H1 (Servidor)	AM17 (Errores actualización software)	1	3	3
H1 (Servidor)	AMZ19 (Sobrecarga del sistema)	1	3	3
H1 (Servidor)	AMZ23 (Acceso no autorizado)	2	3	6
H1 (Servidor)	AMZ24 (Errores de los usuarios)	1	3	3
H1 (Servidor)	AMZ25 (Errores del administrador)	1	3	3
H2 (PC Gerente)	AMZ4 (Fuga información)	1	3	3
H2 (PC Gerente)	AMZ7 (Corrupción información)	2	3	6
H2 (PC Gerente)	AMZ16 (Difusión software dañino)	3	3	9
H2 (PC Gerente)	AMZ17 (Errores actualización software)	1	3	3
H2 (PC Gerente)	AMZ23 (Acceso no autorizado)	2	3	6
H2 (PC Gerente)	AMZ24 (Errores de los usuarios)	1	3	3
H2 (PC Gerente)	AMZ25 (Errores del administrador)	1	3	3
H3 (PC,s Ventas)	AMZ5 (Información falsa)	2	3	6
H3 (PC,s Ventas)	AMZ17 (Actualizaciones software)	2	2	4
H3 (PC,s Ventas)	AMZ18 (Actualizaciones hardware)	2	2	4
H3 (PC,s Ventas)	AMZ24 (Errores de los usuarios)	3	3	9
H4 (Portátiles)	AMZ7 (Corrupción información)	2	3	6
H4 (Portátiles)	AM17 (Errores actualización software)	1	3	3
H4 (Portátiles)	AMZ20 (Pérdida de equipos)	2	3	6
H4 (Portátiles)	AMZ28 (Robo)	2	3	6

Activo	Amenaza	Probabilidad	Impacto	Riesgo
H5 (Disp.Móviles)	AM17 (Errores actualización software)	1	3	3
H5 (Disp.Móviles)	AMZ20 (Pérdida de equipos)	2	3	6
H5 (Disp.Móviles)	AMZ28 (Robo)	2	3	6
H6 (Impresoras)	AMZ18 (Actualizaciones hardware)	2	2	4
H7 (Uds. Backup)	AMZ7 (Corrupción información)	2	3	6
H7 (Uds. Backup)	AMZ20 (Pérdida de equipos)	1	3	3
H7 (Uds. Backup)	AMZ28 (Robo)	1	3	3
H8 (Hub)	AMZ12 (Fallo servicio comunicaciones)	3	3	9
H9 (Router,s)	AMZ12 (Fallo servicio comunicaciones)	3	2	6
A1 (ERP)	AMZ24 (Errores de los usuarios)	3	2	6
A1 (ERP)	AMZ25 (Errores del administrador)	1	3	3
A2 (ERP)	AMZ24 (Errores de los usuarios)	3	2	6
A2 (ERP)	AMZ25 (Errores del administrador)	1	3	3
A3 (S.O)	AMZ17 (Actualizaciones software)	2	3	6
A4 (Correo)	AMZ9 (Interceptación información)	3	2	6
A5 (Web)	AMZ27 (denegación de servicio)	1	3	3
A6 (Antivirus)	AMZ17 (Actualizaciones software)	3	3	9
A7 (Ofimática)	AMZ16 (Difusión software dañino)	3	2	6
A7 (Ofimática)	AMZ17 (Actualizaciones software)	2	3	6
A8 (Autobackup)	AMZ12 (Fallo servicio comunicaciones)	3	3	9
D1 (Bases datos)	AMZ7 (Corrupción de la información)	1	3	3
D2 (Info. digital)	AMZ4 (Fuga información)	1	3	3
D2 (Info. digital)	AMZ7 (Corrupción de la información)	1	3	3
D3 (Info.papel)	AMZ4 (Fuga información)	1	3	3
D3 (Info.papel)	AMZ23 (Acceso no autorizado)	2	3	6
D3 (Info.papel)	AMZ28 (Robo)	2	3	6
R1 (ADSL)	AMZ12 (Fallo servicio comunicaciones)	3	2	6
R2 (Servicio 3G)	AMZ12 (Fallo servicio comunicaciones)	1	2	2
R3 (Servicio 4G)	AMZ12 (Fallo servicio comunicaciones)	1	3	3
R4 (LAN)	AMZ21 (Indisponibilidad equipos)	2	2	4
R5 (WiFi)	AMZ23 (Acceso no autorizado)	3	3	9
S1 (Servicio web)	AMZ27 (denegación de servicio)	1	3	3
S2 (SSH)	AMZ12 (Fallo servicio comunicaciones)	3	1	1
S3 (Correo)	AMZ12 (Fallo servicio comunicaciones)	2	3	6
S4 (Servicio FTP)	AMZ12 (Fallo servicio comunicaciones)	2	1	2
S5 (FILE)	AMZ16 (Difusión software dañino)	1	3	3
S6 (PKI)	AMZ22 (Abuso privilegios)	1	3	3
S6 (PKI)	AMZ28 (Robo)	1	3	3
S7 (IDM)	AMZ25 (Errores del administrador)	1	1	1

Activo	Amenaza	Probabilidad	Impacto	Riesgo
E1 (Climatizac.)	AMZ10 (Corte suministro eléctrico)	1	1	1
E2 (Cableado)	AMZ18 (Errores de mantenimiento)	1	3	3
E3 (Mobiliario)	AMZ1 (Fuego)	1	2	2
E3 (Mobiliario)	AMZ2 (Daños por agua)	1	2	2
E4 (Caja fuerte)	AMZ28 (Robo)	3	3	9
E5 (SAI)	AMZ21 (Errores mantenimiento)	1	3	3
P1 (Op. internos)	AMZ4 (Fuga de información)	1	2	2
P1 (Op. internos)	AMZ16 (Difusión software dañino)	1	3	3
P1 (Op. internos)	AMZ23 (Acceso no autorizado)	1	2	2
P1 (Op. internos)	AMZ29 (Indisponibilidad personal)	2	2	4
P1 (Op. internos)	AMZ30 (Extorsión)	1	1	1
P1 (Op. internos)	AMZ31 (Ingeniería social)	2	3	6
P2 (Op. externos)	AMZ20 (Pérdida de equipos)	3	2	6
P2 (Op. externos)	AMZ28 (Robo)	3	2	6
P2 (Op. externos)	AMZ29 (Indisponibilidad personal)	2	2	4
P2 (Op. externos)	AMZ30 (Extorsión)	1	1	1
P2 (Op. externos)	AMZ31 (Ingeniería social)	2	3	6
P3 (Soporte ext.)	AMZ4 (Fuga de información)	1	3	3
P3 (Soporte ext.)	AMZ29 (Indisponibilidad personal)	1	3	3
P3 (Soporte ext.)	AMZ30 (Extorsión)	1	1	1
P3 (Soporte ext.)	AMZ31 (Ingeniería social)	1	1	1
P4 (Clientes)	AMZ5 (Información falsa)	3	2	6
P4 (Clientes)	AMZ28 (Robo)	1	3	3
P5 (Proveedores)	AMZ4 (Fuga de información)	1	2	2
P5 (Proveedores)	AMZ5 (Información falsa)	1	2	2

A continuación, a modo de resumen, vamos a presentar el análisis de riesgos para cada uno de los ámbitos que intervienen en la gestión de la seguridad de la información:

- Para las ***Instalaciones***, los riesgos más notables que deben tratarse son los derivados de la amenaza de fuego y robo en la oficina, ya que es donde se encuentran gran parte de los activos de información (servidor, caja fuerte y ficheros de gestión y administración). Se aconseja también, aunque con menor prioridad, el tratamiento del riesgo de los activos con valoración “amarilla”. El riesgo de los activos con valoración “verde” es asumido por la organización.
- Para el ***Hardware***, los riesgos críticos que se deben tratar de forma inmediata son la difusión de malware en el equipo gerente, los errores de los usuarios (empleados) en los equipos de ventas y la caída del hub de la red corporativa. Como riesgos altos que también requieren tratamiento están: los accesos no autorizados al servidor y al equipo del

gerente, la corrupción y/o fuga de información en el equipo del gerente, la introducción de información falsa en los equipos de ventas, la corrupción de información en equipos portátiles, la pérdida o robo de equipos portátiles y dispositivos móviles y caída del router que da salida a la red corporativa. De igual modo, se aconseja también el tratamiento del riesgo de los activos con valoración “amarilla”.

- Para las ***Aplicaciones***, los riesgos críticos, de inmediato tratamiento, son los derivados de la no actualización del software antivirus y el fallo de comunicación en el servicio de autobackup. Como riesgos altos que requieren urgente tratamiento están: los errores de usuarios sobre el ERP, actualizaciones del sistema operativo y paquetes ofimáticos, la interceptación de correos electrónicos y la difusión de malware a través de la red corporativa. Se aconseja también, aunque con menor prioridad, el tratamiento del riesgo de los activos con valoración “amarilla”.
- Para los ***Datos***, se deben tratar con urgencia los riesgos derivados del acceso no autorizado o el robo de documentación en papel, que contenga datos de carácter personal o confidencial. De igual modo, se aconseja también el tratamiento del riesgo de los activos con valoración “amarilla”.
- Para la ***Red***, se debe tratar inmediatamente (riesgo crítico) los accesos nos autorizados a través de la WiFi y con urgencia (riesgo alto) la caída de las comunicaciones a través del router conectado a la red corporativa. Se aconseja también, aunque con menor prioridad, el tratamiento del riesgo de los activos con valoración “amarilla”. El riesgo de los activos con valoración “verde” es asumido por la organización.
- Para los ***Servicios***, se considera urgente el tratamiento del riesgo derivado del fallo de comunicaciones en el servicio de correo electrónico. Se aconseja también, aunque con menor prioridad, el tratamiento del riesgo de los activos con valoración “amarilla”. El riesgo de los activos con valoración “verde” es asumido por la organización.
- Para el ***Equipamiento Auxiliar***, se considera crítico el riesgo de robo sobre la caja fuerte y por tanto se debe priorizar su tratamiento. Se aconseja también, aunque con menor prioridad, el tratamiento del riesgo de los activos con valoración “amarilla”. El riesgo de los activos con valoración “verde” es asumido por la organización.
- Para el ***Personal*** de la organización, se considera urgente el tratamiento de los riesgos derivados de la pérdida o robo de equipos, la ingeniería social sobre los miembros internos o externos (prestadores de servicio) de la organización y la introducción de información falsa por parte de los clientes. Se aconseja también, aunque con menor prioridad, el tratamiento del riesgo de los activos con valoración “amarilla”. El riesgo de los activos con valoración “verde” es asumido por la organización.

Anexo IX. Propuestas de proyectos

Versión → v01-0517. Una vez identificadas las principales amenazas sobre los activos, relacionados con el sistema de información, y determinado el riesgo e impacto derivado de la materialización de dichas amenazas, se presentan las siguientes propuestas de proyectos de mejora integral de la seguridad de la información.

Recomendaciones para la mejora de la seguridad de la información

Partimos de cada uno de los ámbitos de la organización y para cada amenaza, en función del nivel de impacto de materialización, se propone una recomendación de mejora.

Las recomendaciones se establecen en función de los siguientes niveles de riesgo:

- *Riesgo bajo (verde)*: Se considera que las medidas implantadas actualmente por la organización son suficientes o el riesgo es tan bajo que es asumido por la misma.
- *Riesgo medio (amarillo)*: Se considera conveniente revisar las medidas de seguridad implantadas, aunque no de forma prioritaria.
- *Riesgo alto (amarillo)*: Es necesario aplicar las recomendaciones que se indican de forma sistemática y periódica.
- *Riesgo crítico (rojo)*: Es imperativo aplicar las recomendaciones propuestas por presentar un grave riesgo para la organización.

PPT-01-INS Proyecto de mejora para la seguridad de las instalaciones

Se proponen las siguientes medidas para la mejora de la seguridad de los activos relacionados con la información y sus sistemas:

- Para la **AMZ28 en I1** (Amenaza por robo en tienda – Riesgo Medio): Como medida adicional a las ya establecidas se propone la instalación de una alarma perimetral con conexión a central de seguridad e instalación de un servidor de grabación para conectar a las cámaras de video-vigilancia ya presentes.
  - Dominio ISO27001-2013: A.11 (Seguridad física y ambiental).
  - Previsión temporal: a corto plazo
  - Personal asignado: externo a la empresa.
  - Estimación económica: 2.000 €.

- Para la **AMZ1 en I4** (Amenaza por fuego en oficina – Riesgo Alto): Se propone la instalación de un detector de humos y un sistema de extinción de incendios manual, específico para equipos electrónicos.
  - Dominio ISO27001-2013: A.11 (Seguridad física y ambiental).
  - Previsión temporal: a corto plazo.
  - Personal asignado: externo a la empresa.
  - Estimación económica: 500 €.

- Para la **AMZ2 en I4** (Daños por agua en oficina – Riesgo Medio): Revisión periódica (trimestral) del estado de las canalizaciones y desagües sobre el perímetro de la oficina.
  - Dominio ISO27001-2013: A.11 (Seguridad física y ambiental).
  - Previsión temporal: a medio plazo.
  - Personal asignado: externo a la empresa.
  - Estimación económica: 300 €.

- Para la **AMZ28 en I4** (Amenaza por robo en oficina – Riesgo Alto): Se propone la instalación una alarma perimetral con conexión a central de seguridad e instalación de un servidor de grabación para conectar a las cámaras de video-vigilancia ya presentes. Adicionalmente se propone la instalación de una cámara de video-vigilancia en la oficina.
  - Dominio ISO27001-2013: A.11 (Seguridad física y ambiental).
  - Previsión temporal: a corto plazo.
  - Personal asignado: externo a la empresa.
  - Estimación económica: ya contemplada anteriormente.

- Para la **AMZ28 en I6** (Amenaza por robo en vehículo – Riesgo Medio): Se propone que toda la información de carácter confidencial o personal, en soporte manual o automatizado, sea custodiada por la persona que utiliza el vehículo en zonas de estacionamiento públicas, o en tránsito. Para ello, las portará personalmente en sus desplazamientos fuera del vehículo.
  - Dominio ISO27001-2013: A.11 (Seguridad física y ambiental).
  - Previsión temporal: a corto plazo
  - Personal asignado: todos los empleados con acceso al vehículo.
  - Estimación económica: 0 €.

PPT-02-HDW Proyecto de mejora para la seguridad del hardware

Se proponen las siguientes medidas para la mejora de la seguridad de la información en los dispositivos hardware:

- Para la **AMZ7 en H1** (Amenaza por corrupción de información – Riesgo Medio), la **AMZ17 en H1** (Errores en la actualización de software – Riesgo Medio) y la **AMZ19 en H1** (Sobrecarga del sistema – Riesgo Medio): Se propone la verificación y prueba de restauración de la última copia de seguridad, actualización del software de base bajo demanda, monitorización periódica de las tareas que se ejecutan en el servidor y del nivel de carga de trabajo en el mismo. De igual modo se chequeará que la cantidad de espacio libre en el disco principal de almacenamiento no sea inferior al 15%.
  - Dominio ISO27001-2013: A.16 (Gestión de incidentes de S.I).
  - Previsión temporal: a medio plazo.
  - Personal asignado: miembros de soporte externo.
  - Estimación económica: incluida en cuota de soporte.

- Para la **AMZ23 en H1** (Amenaza por acceso no autorizado al servidor – Riesgo Alto): Se propone el chequeo periódico de todos los usuarios conectados al servidor, haciendo especial hincapié a las conexiones remotas a través de conexiones SSH, Telnet o similar. Se aconseja la revisión aleatoria de los "log" de conexión para detectar posibles conductas sospechosas.
  - Dominio ISO27001-2013: A.9 (Control de acceso).
  - Previsión temporal: a corto plazo.
  - Personal asignado: soporte externo y gerencia.
  - Estimación económica: incluida en cuota de soporte.

- Para la **AMZ24 en H1** (Amenaza por errores de los usuarios sobre el servidor – Riesgo Medio): Se asume como posible el borrado accidental de albaranes, tickets o facturas por parte de los usuarios en la operativa diaria. No se proponen medidas adicionales para impedir el borrado de otro tipo de información ya que los usuarios carecen de privilegios para efectuar voluntariamente un borrado parcial o total del contenido del servidor.
  - Dominio ISO27001-2013: A.12 (Seguridad de las operaciones).
  - Previsión temporal: a medio plazo.
  - Personal asignado: todos los miembros de la organización.
  - Estimación económica: 0 €.

- Para la **AMZ25 en H1** (Amenaza por errores del administrador sobre el servidor – Riesgo Medio): Se descarta la posibilidad de que el administrador interno del sistema (jcarlos) pueda llegar a efectuar un borrado total del contenido almacenado en el servidor. En el improbable caso de que esto ocurriese se propone la restauración remota de una de una de las últimas copias de seguridad diarias (de las 12 horas o de las 18 horas).
  - Dominio ISO27001-2013: A.12 (Seguridad de las operaciones).
  - Previsión temporal: a corto plazo.
  - Personal asignado: gerente de la empresa.
  - Estimación económica: 0 €.

- Para la **AMZ4 en H2** (Amenaza por fuga de información en el PC Gerente – Riesgo Medio): Existe la posibilidad de que personal ajeno a la empresa acceda a este equipo y pueda extraer información vía USB, DVD, o red. Para ello se propone la incorporación de una contraseña de autenticación a nivel de arranque del sistema. También se aconseja la incorporación del desbloqueo de pantalla por contraseña tras un tiempo de inactividad. Se descarta la posibilidad de exfiltración de información de forma remota, ya que sólo el personal de soporte tiene acceso a este equipo.
  - Dominio ISO27001-2013: A.6 (Organización de la S.I).
  - Previsión temporal: a largo plazo.
  - Personal asignado: miembros de soporte externo.
  - Estimación económica: incluida en la cuota de soporte.

- Para la **AMZ7 en H2** (Amenaza por corrupción de información en el PC Gerente – Riesgo Alto) y la **AMZ16 en H2** (Amenaza por difusión de software dañino en el PC Gerente – Riesgo Crítico): Se propone, además de la copia de seguridad semanal, la realización de copias de seguridad diaria sobre ciertas carpetas de uso habitual y la desconexión, tras la copia, de los dispositivos destino.
  - Dominio ISO27001-2013: A.12 (Seguridad de las operaciones).
  - Previsión temporal: a largo plazo.
  - Personal asignado: personal de soporte y gerente.
  - Estimación económica: 0 €.

- Para la **AMZ17 en H2** (Amenaza por errores de actualización de software en equipo gerente – Riesgo Medio): Se propone la actualización semanal del software de base, así como del resto de aplicaciones instaladas en el equipo.
  - Dominio ISO27001-2013: A.8 (Gestión de activos).
  - Previsión temporal: a largo plazo.
  - Personal asignado: personal de soporte externo.
  - Estimación económica: incluida en cuota de soporte.

- Para la **AMZ23 en H2** (Amenaza por acceso no autorizado al equipo del gerente – Riesgo Alto): Se propone la incorporación de una contraseña de autenticación a nivel de arranque del sistema. También se aconseja la incorporación del desbloqueo de pantalla por contraseña tras un tiempo de inactividad.
  - Dominio ISO27001-2013: A.9 (Control de accesos).
  - Previsión temporal: a corto plazo.
  - Personal asignado: personal de soporte externo y gerente.
  - Estimación económica: incluida en cuota de soporte.

- Para la **AMZ5 en H3** (Introducción de información falsa en los equipos de venta al público – Riesgo Alto): Se da por hecho que la introducción de información falsa se realiza de manera involuntaria y por tanto tiene la consideración de información errónea. Para mitigar esta amenaza se propone el entrenamiento/actualización periódica del personal en el uso de las diferentes opciones de la aplicación CX_Gestion.
  - Dominio ISO27001-2013: A.12 (Seguridad de las operaciones).
  - Previsión temporal: a largo plazo.
  - Personal asignado: miembros del equipo de ventas.
  - Estimación económica: 0 €.

- Para la **AMZ17 en H3** (Actualizaciones de software en los equipos de ventas – Riesgo Medio): Estos equipos trabajan contra el servidor, por lo que no se considera indispensable la actualización del mismo, máxime cuando son sistemas muy antiguos que carecen de soporte). No obstante se aconseja la realización de un proyecto de actualización a medio plazo.
  - Dominio ISO27001-2013: A.8 (Gestión de activos).
  - Previsión temporal: a largo plazo.

- Personal asignado: personal de soporte externo.
- Estimación económica: incluida en cuota de soporte.

- Para la **AMZ18 en H3** (Actualización del hardware en los equipos de ventas – Riesgo Medio): Se propone la renovación completa de todos los equipos de ventas por su elevada antigüedad.
  - Dominio ISO27001-2013: A.8 (Gestión de activos).
  - Previsión temporal: a medio plazo.
  - Personal asignado: miembros de soporte externo.
  - Estimación económica: 3.000 €.

- Para la **AMZ24 en H3** (Errores de los usuarios en los equipos de ventas – Riesgo Crítico): Mismo caso de la AMZ5 en H3. Adicionalmente se propone, durante el proceso de verificación de la facturación mensual, la comprobación de datos erróneos e identificación del usuario para que efectúe las correcciones oportunas en un futuro.
  - Dominio ISO27001-2013: A.12 (Seguridad de las operaciones).
  - Previsión temporal: a largo plazo.
  - Personal asignado: personal del equipo de ventas.
  - Estimación económica: 0 €.

- Para la **AMZ27 en H4** (Corrupción de la información en los equipos portátiles – Riesgo Alto): Se propone la realización de copias de seguridad semanales del contenido de estos equipos, ya que actualmente no se están realizando.
  - Dominio ISO27001-2013: A.12 (Seguridad en las operaciones).
  - Previsión temporal: a medio plazo.
  - Personal asignado: todo el personal que utilice al equipo.
  - Estimación económica: incluida en la cuota de soporte.

- Para la **AMZ20 en H4** (Pérdida de equipos portátiles - Riesgo Alto) y la **AMZ28 en H4** (Robo de equipos portátiles - Riesgo Alto): Se propone que estos equipos estén almacenados bajo llave, en la oficina, y la custodia durante la salida de los mismos sea responsabilidad del personal a su cargo. En cualquier caso, estos dispositivos permanecerán siempre a la vista del usuario y bajo ningún concepto quedarán apoyados sobre mostradores o mesas auxiliares al alcance de personal ajeno a la organización.
  - Dominio ISO27001-2013: A.11 (Seguridad física y ambiental).
  - Previsión temporal: a largo plazo.
  - Personal asignado: todo el personal con acceso al equipo.
  - Estimación económica: 0 €.

- Para la **AMZ20 en H5** (Pérdida de dispositivos móviles - Riesgo Alto) y la **AMZ28 en H4** (Robo de dispositivos móviles - Riesgo Alto): Se proponen las mismas medidas que para el caso anterior. Adicionalmente, si el usuario es propietario de alguno de estos dispositivos, deberá responsabilizarse de que no se mantiene información corporativa o de

carácter personal (que afecte al desarrollo de su trabajo) en su dispositivo móvil.
  - Dominio ISO27001-2013:A.11 (Seguridad física y ambiental).
  - Previsión temporal: a largo plazo.
  - Personal asignado: todo el personal que tenga uno asignado.
  - Estimación económica: 0 €.

- Para la **AMZ7 en H7** (Corrupción de la información en las unidades auxiliares de backup – Riesgo Alto): Se propone la verificación de la integridad de las unidades a través de un proceso de restauración de la copia de seguridad sobre otro dispositivo USB o máquina virtual situada en un equipo externo a la red corporativa.
  - Dominio ISO27001-2013: A.12 (Seguridad de las operaciones).
  - Previsión temporal: a medio plazo.
  - Personal asignado: miembros de soporte externo.
  - Estimación económica: incluido en la cuota de soporte.

- Para la **AMZ12 en H8** (Fallo comunicaciones a través del HUB – Riesgo Crítico): Se propone la adquisición de otro dispositivo idéntico al instalado a modo de respaldo para aquellos casos en los que se pueda producir una caída de la red, provocada por un fallo físico del concentrador.
  - Dominio ISO27001-2013: A.13 (Seguridad de las comunicaciones).
  - Previsión temporal: a medio plazo.
  - Personal asignado: miembros de soporte externo.
  - Estimación económica: incluido en la cuota de soporte.
  -
- Para la **AMZ12 en H9** (Fallo comunicaciones a través del Router – Riesgo Alto): Dado que el ISP es el encargado de sustituir y mantener los dispositivos de enrutamiento, se propone que en caso de fallo de uno de los routers, y con objeto de dar continuidad al servicio, éste sea sustituido por el otro que hay instalado (sólo en caso de que el router averiado sea el que da salida a la red corporativa). En caso de que el router averiado sea el auxiliar, se esperará a su reemplazo por parte del proveedor de servicios de Internet.
  - Dominio ISO27001-2013: A.13 (Seguridad de las comunicaciones).
  - Previsión temporal: a corto plazo.
  - Personal asignado: servicio asistencia técnica del ISP.
  - Estimación económica: incluido en la cuota de mantenimiento.

PPT-03-APP Proyecto de mejora para la seguridad de las Aplicaciones

Se proponen las siguientes medidas para la mejora de la seguridad de la información en las aplicaciones de la organización:

- Para la **AMZ24 en A1** (Errores de los usuarios sobre el ERP Gestión y Contabilidad – Riesgo Alto) y la AMZ24 en A2 (Errores de los usuarios sobre el ERP Solución Movilidad – Riesgo Alto): Se propone la realización de formación continua en la jornada semanal de control que

se lleva a cabo los viernes por la tarde. Los asistentes a dicha jornada serán los encargados de comunicar al resto del personal los cambios, nuevas normativas y políticas de utilización del ERP.
  - Dominio ISO27001-2013: A.8 (Gestión de activos)
  - Previsión temporal: a largo plazo.
  - Personal asignado: todos los usuarios del ERP.
  - Estimación económica: según programa de formación.

- Para la **AMZ17 en A3** (Actualizaciones de Software/Sistema Operativo – Riesgo Alto): Se propone que el responsable de soporte externo del ERP se encargue de actualizar el sistema operativo del servidor a demanda de las alertas de seguridad que vayan surgiendo. Estas actualizaciones se efectuarán, al menos, una vez al año. En cuanto a las actualizaciones de los SO del resto de equipos, incluidos los portátiles y dispositivos móviles, se efectuarán a demanda de las nuevas versiones que vayan apareciendo. Este proceso se efectuará, al menos, con una periodicidad trimestral.
  - Dominio ISO27001-2013: A.11 (Seguridad física y del entorno).
  - Previsión temporal: a medio plazo.
  - Personal asignado: equipo de soporte del ERP.
  - Estimación económica: incluida en la cuota de mantenimiento.

- Para la **AMZ9 en A4** (Interceptación de la información contenida en correos electrónicos – Riesgo Alto): Se propone la verificación periódica del estado de las cuentas de correo, en que dispositivos están instalados y el cambio de las contraseñas de dichas cuentas con una periodicidad no superior a los 6 meses.
  - Dominio ISO27001-2013: A.10 (Criptografía).
  - Previsión temporal: a medio plazo.
  - Personal asignado: miembros del equipo de soporte externo.
  - Estimación económica: incluida en cuota de soporte.

- Para la **AMZ17 en A6** (Actualización del software anti-malware – Riesgo Crítico): Se propone la verificación diaria de que las firmas de virus están actualizadas, de que la versión de la aplicación es la última suministrada por el fabricante y de que el servicio está activo desde el arranque de los equipos. En cuanto a la configuración de seguridad y privacidad, se verificará, al menos una vez al año, que los parámetros están correctamente configurados.
  - Dominio ISO27001-2013: A.12 (Seguridad en las operaciones).
  - Previsión temporal: a corto plazo.
  - Personal asignado: miembros del equipo de soporte externo.
  - Estimación económica: incluida en cuota de soporte.

- Para la **AMZ16 en A7** (Difusión de software dañino a través de aplicaciones incluidas en paquetes ofimáticos – Riesgo Alto) y la **AMZ17 en A7** (Actualizaciones del software de paquetes ofimáticos – Riesgo Alto): Se propone la incorporación de los parches de seguridad, a través de las actualizaciones proporcionadas por el fabricante. La periodicidad

de estas actualizaciones irá en función de los parches publicados por los fabricantes.
    - Dominio ISO27001-2013: A.12 (Seguridad en las operaciones).
    - Previsión temporal: a corto plazo.
    - Personal asignado: miembros del equipo de soporte externo.
    - Estimación económica: incluida en cuota de soporte.

- Para la **AMZ12 en A8** (Fallo de comunicaciones en el servicio de Autobackup – Riesgo Crítico: Se propone la realización/sincronización de 2 copias de seguridad remotas, a mitad de cada una de las jornadas (mañana y tarde, por ejemplo a las 12h y a las 18h).
    - Dominio ISO27001-2013: A.12 (Seguridad en las operaciones).
    - Previsión temporal: a largo plazo.
    - Personal asignado: miembros del equipo de soporte externo.
    - Estimación económica: incluida en cuota de soporte.

PPT-04-DTS Proyecto de mejora para la seguridad de los datos

Se proponen las siguientes medidas para la mejora de la seguridad de la información contenida en las bases de datos:

- Para la **AMZ23 en D3** (Acceso no autorizado a la información en soporte papel – Riesgo Alto) y **AMZ28 en D3** (Robo de información en soporte papel – Riesgo Alto): Se propone el almacenamiento y custodia de dicha información en armarios bajo llave y/o en la oficina. Aquella información que sea necesaria en la zona de ventas no estará al alcance de los clientes.
    - Dominio ISO27001-2013: A.11 (Seguridad física y del entorno).
    - Previsión temporal: a largo plazo.
    - Personal asignado: todos los miembros de la organización.
    - Estimación económica: 0 €.

PPT-05-NTW Proyecto de mejora para la seguridad de la red

Se proponen las siguientes medidas para la mejora de la seguridad de la información que circula a través de la red corporativa e Internet:

- Para la **AMZ12 en R1** (Fallo en el servicio de comunicaciones ADSL – Riesgo Alto): Se propone el mantenimiento de una línea adicional de voz y datos para alternar en caso de caída del servicio.
    - Dominio ISO27001-2013: A.15 (Relación con proveedores).
    - Previsión temporal: a largo plazo.
    - Personal asignado: gerente de la organización.
    - Estimación económica: incluida en la cuota mensual de servicios.

- Para la **AMZ23 en R5** (Acceso no autorizado a través de la red inhalámbrica – Riesgo Crítico): Se propone la revisión periódica de la configuración del firmware del router ADSL que está conectado a la red corporativa.

- Dominio ISO27001-2013: A.15 (Seguridad física y del entorno).
- Previsión temporal: a medio plazo.
- Personal asignado: miembros del equipo de soporte.
- Estimación económica: incluida en la cuota mensual de servicios.

PPT-06-SRV Proyecto de mejora para la seguridad de los Servicios

Se proponen las siguientes medidas para la mejora de la seguridad de la información en los servicios:

- Para la **AMZ12 en S3** (Fallo en el servicio de comunicaciones de correo electrónico – Riesgo Alto): Se propone el chequeo periódico de la capacidad del servidor de correo y la configuración de una cuenta de correo en otro servidor diferente al del dominio corporativo.
  - Dominio ISO27001-2013: A.15 (Relación con proveedores).
  - Previsión temporal: a largo plazo.
  - Personal asignado: miembro del equipo de soporte externo.
  - Estimación económica: incluida en la cuota mensual de servicios.

PPT-07-AUX Proyecto de mejora de seguridad en equipamiento auxiliar

Se proponen las siguientes medidas para la mejora de la seguridad de la información en el equipamiento auxiliar:

- Para la **AMZ28 en E4** (Robo en la Caja Fuerte – Riesgo Crítico): Se propone la realización de una copia de seguridad de la información contenida en la misma y su almacenamiento/custodia fuera de las instalaciones.
  - Dominio ISO27001-2013: A.11 (Seguridad física y del entorno).
  - Previsión temporal: a medio plazo.
  - Personal asignado: gerente de la organización.
  - Estimación económica: 200 €.

PPT-08-PRS Proyecto de mejora de seguridad en el personal

Se proponen las siguientes medidas para la mejora de la seguridad de la información en lo que respecta al personal de la organización:

- Para la **AMZ31 en P1** Ataques de Ingeniería Social contra los operadores internos de la organización – Riesgo Alto): Se propone la realización de jornadas de formación periódicas para concienciarlos de estos riesgos.
  - Dominio ISO27001-2013: A.7 (Seguridad de los Recursos Humanos).
  - Previsión temporal: a largo plazo.
  - Personal asignado: todos los miembros de la organización.
  - Estimación económica: según programa de formación.

- Para la **AMZ20 en P2** (Pérdida de equipos por parte de los operadores externos de la organización – Riesgo Alto) y **AMZ28 en P2** (Robo a los

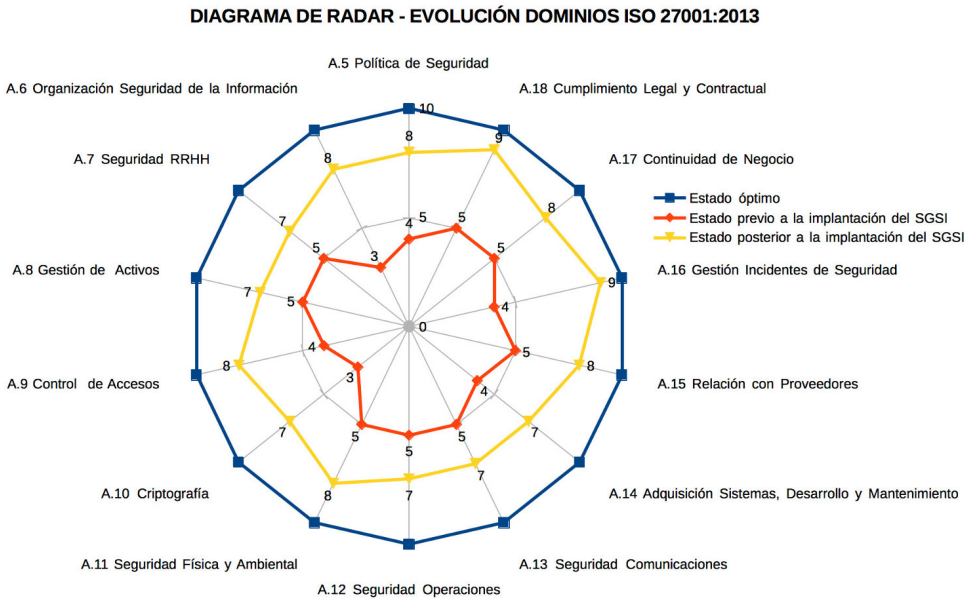
operadores externos de la organización – Riesgo Alto): Se propone la implantación de medidas anti-hurto para el personal que trabaje fuera de la empresa y la contratación de seguros para el equipamiento portable, así como la obligación, para este personal, de revisar periódicamente las políticas de utilización de recursos de la empresa.

- Dominio ISO27001-2013: A.7 (Seguridad de los Recursos Humanos).
- Previsión temporal: a largo plazo.
- Personal asignado: todos los miembros de la organización que trabajen fuera de la misma.
- Estimación económica: 1.000 € al año.

- Para la **AMZ31 en P2** (Ataques de Ingeniería Social contra los operadores externos de la organización – Riesgo Alto): Se propone la realización de jornadas de formación periódicas para concienciarlos de estos riesgos.
  - Dominio ISO27001-2013: A.7 (Seguridad de los Recursos Humanos).
  - Previsión temporal: a largo plazo.
  - Personal asignado: todos los miembros de la organización.
  - Estimación económica: según programa de formación.

- Para la **AMZ25 en P4** (Suministro de información falsa por parte de los clientes – Riesgo Alto): Se propone la verificación de todos su datos personales y profesionales, así como de cualquier otro tipo de información que suministren en su relación comercial con la empresa.
  - Dominio ISO27001-2013: A.7 (Seguridad de los Recursos Humanos).
  - Previsión temporal: a largo plazo.
  - Personal asignado: todo el personal de la organización.
  - Estimación económica: 0 €.

A continuación se muestra un *diagrama de radar* con la evolución de los diferentes dominios de la ISO27001:2013, desde el estado inicial de la seguridad de la información en la organización hasta la completa implantación del Sistema de Gestión de Seguridad de la Información.



Anexo X. Declaración de Aplicabilidad

Versión → v01-0517. Como punto de partida de los trabajos se ha realizado un análisis para determinar las áreas de mejora que habría que abordar, de acuerdo con la Norma ISO 27002:2013.

A.5 Políticas de seguridad de la información			
A.5.1 Directrices de gestión de la seguridad de la información			
Objetivo: Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas pertinentes.			**¿Aplicado?**
A.5.1.1	Políticas para la seguridad de la información	*Control* Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	NO
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	NO

A.6 Organización de la seguridad de la información			
A.6.1 Organización interna			
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.			**¿Aplicado?**
A.6.1.1	Roles y responsabilidades en seguridad de la información	*Control* Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	NO
A.6.1.2	Segregación de tareas	*Control* Las funciones 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.	NO

A.6.1.3	Contacto con las autoridades	*Control* Deben mantenerse los contactos apropiados con las autoridades pertinentes.	NO
A.6.1.4	Contacto con grupos de interés especial	*Control* Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.	NO
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	NO

A.6.2 Los dispositivos móviles y el teletrabajo			
Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.			**¿Aplicado?**
A.6.2.1	Política de dispositivos móviles	*Control* Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	NO
A.6.2.2	Teletrabajo	*Control* Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	NO

A.7 Seguridad relativa a los recursos humanos			
A.7.1 Antes del empleo			
Objetivo: Para asegurarse de que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones encomendadas.			**¿Aplicado?**
A.7.1.1	Investigación de antecedentes	*Control* La comprobación de antecedentes de todos los candidatos al trabajo se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos.	SI

A.7.1.2	Términos y condiciones del empleo	*Control* Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.	NO

A.7.2 Durante el empleo			
Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.			**¿Aplicado?**
A.7.2.1	Responsabilidades de gestión	*Control* La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	NO
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	*Control* Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	NO
A.7.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	NO

A.7.3 Finalización del empleo o cambio en el puesto de trabajo			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.			**¿Aplicado?**
A.7.3.1	Responsabilidades ante la finalización o cambio	*Control* Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	NO

A.8 Gestión de activos			
A.8.1 Responsabilidad sobre los activos			
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.			**¿Aplicado?**
A.8.1.1	Inventario de activos	*Control* Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.	NO
A.8.1.2	Propiedad de los activos	*Control* Todos los activos que figuran en el inventario deben tener un propietario.	NO
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	NO
A.8.1.4	Devolución de activos	*Control* Todos los empleados y terceras partes deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	NO

A.8.2 Clasificación de la información			
Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.			**¿Aplicado?**
A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	NO
A.8.2.2	Etiquetado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	NO

A.8.2.3	Manipulado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema adoptado por la organización.	NO

A.8.3 Manipulación de los soportes			
Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.			**¿Aplicado?**
A.8.3.1	Gestión de soportes extraíbles	*Control* Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	NO
A.8.3.2	Eliminación de soportes	*Control* Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.	NO
A.8.3.3	Soportes físicos en tránsito	*Control* 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.	NO

A.9 Control de acceso			
A.9.1 Requisitos de negocio para el control de acceso			
Objetivo: Limitar el acceso a los recursos de tratamiento de información y a la información.			**¿Aplicado?**
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	NO
A.9.1.2	Acceso a las redes y a los servicios de red	*Control* Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	SI

A.9.2 Gestión de acceso de usuario			
Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.			**¿Aplicado?**
A.9.2.1	Registro y baja de usuario	*Control* Debe implantarse un procedimiento formal de registro y retirada de usuarios que posibilite la asignación de derechos de acceso.	NO
A.9.2.2	Provisión de acceso de usuario	*Control* Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	NO
A.9.2.3	Gestión de privilegios de acceso	*Control* La asignación y el uso de privilegios de acceso debe estar restringida y controlada.	SI
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	*Control* La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	NO
A.9.2.5	Revisión de los derechos de acceso de usuario	*Control* Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	NO
A.9.2.6	Retirada o reasignación de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	NO

A.9.3 Responsabilidades del usuario			
Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.			**¿Aplicado?**
A.9.3.1	Uso de la información secreta de autenticación	*Control* Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	NO

A.9.4 Control de acceso a sistemas y aplicaciones			
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.			**¿Aplicado?**
A.9.4.1	Restricción del acceso a la información	*Control* Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	SI
A.9.4.2	Procedimientos seguros de inicio de sesión	*Control* Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.	SI
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas para la gestión de contraseñas deben ser interactivos y con contraseñas seguras y robustas.	NO
A.9.4.4	Uso de utilidades con privilegios del sistema	*Control* Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	SI
A.9.4.5	Control de acceso al código fuente de los programas	*Control* Se debe restringir el acceso al código fuente de los programas.	SI

A.10 Criptografía			
A.10.1 Controles criptográficos			
Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y / o integridad de la información.			**¿Aplicado?**
A.10.1.1	Política de uso de los controles criptográficos	*Control* Desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.	NO
A.10.1.2	Gestión de claves	*Control* Se debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	NO

A.11 Seguridad física y del entorno			
A.11.1 Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.			**¿Aplicado?**
A.11.1.1	Perímetro de seguridad física	*Control* Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.	NO
A.11.1.2	Controles físicos de entrada	*Control* Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	NO
A.11.1.3	Seguridad de oficinas, despachos y recursos	*Control* Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.	NO
A.11.1.4	Protección contra las amenazas externas y ambientales	*Control* Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	NO
A.11.1.5	El trabajo en áreas seguras	*Control* Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.	NO
A.11.1.6	Áreas de carga y descarga	*Control* Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.	NO

A.11.2 Seguridad de los equipos			
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.			**¿Aplicado?**
A.11.2.1	Emplazamiento y protección de equipos	*Control* Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.	SI
A.11.2.2	Instalaciones de suministro	*Control* Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	NO
A.11.2.3	Seguridad del cableado	*Control* El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.	SI
A.11.2.4	Mantenimiento de los equipos	*Control* Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	NO
A.11.2.5	Retirada de materiales propiedad de la empresa	*Control* Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	SI
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	*Control* Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	SI
A.11.2.7	Reutilización o eliminación segura de equipos	*Control* Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.	NO

A.11.2.8	Equipo de usuario desatendido	*Control* Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.	NO
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	*Control* Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	NO

A.12 Seguridad de las operaciones			
A.12.1 Procedimientos y responsabilidades operacionales			
Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.			**¿Aplicado?**
A.12.1.1	Documentación de procedimientos de los operación	*Control* Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de usuarios.	NO
A.12.1.2	Gestión de cambios	*Control* Los cambios en la organización, los procesos de negocio, instalaciones y los sistemas que afectan a la seguridad de información deben ser controlados.	NO
A.12.1.3	Gestión de capacidades	*Control* Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	NO
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	*Control* Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema.	NO

A.12.2 Protección contra el software malicioso (malware)			
Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.			**¿Aplicado?**
A.12.2.1	Controles contra el código malicioso	*Control* Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	SI

A.12.3 Copias de seguridad			
Objetivo: Evitar la pérdida de datos			**¿Aplicado?**
A.12.3.1	Copias de seguridad de la información	*Control* Se deben realizar backup,s de la información, del software y del sistema y se deben verificar periódicamente.	SI

A.12.4 Registros y supervisión			
Objetivo: Registrar eventos y generar evidencias.			**¿Aplicado?**
A.12.4.1	Registro de eventos	*Control* Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	NO
A.12.4.2	Protección de la información de registro	*Control* Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	NO
A.12.4.3	Registros de administración y operación	*Control* Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	NO
A.12.4.4	Sincronización del reloj	*Control* Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.	NO

A.12.5 Control del software en explotación			
Objetivo: Asegurar la integridad del software en explotación.			**¿Aplicado?**
A.12.5.1	Instalación del software en explotación	*Control* Se deben implementar procedimientos para controlar la instalación del software en explotación.	NO

A.12.6 Gestión de la vulnerabilidad técnica			
Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.			**¿Aplicado?**
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	NO
A.12.6.2	Restricción en la instalación de software	*Control* Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	NO

A.12.7 Consideraciones sobre la auditoria de sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.			**¿Aplicado?**
A.12.7.1	Controles de auditoría de sistemas de información	*Control* Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	NO

A.13 Seguridad de las comunicaciones			
A.13.1 Gestión de la seguridad de redes			
Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.			**¿Aplicado?**
A.13.1.1	Controles de red	*Control* Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	NO

A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	NO
A.13.1.3	Segregación en redes	*Control* Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.	NO

A.13.2 Intercambio de información			
Objetivo: Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.			**¿Aplicado?**
A.13.2.1	Políticas y procedimientos de intercambio de información	*Control* Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	NO
A.13.2.2	Acuerdos de intercambio de información	*Control* Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	NO
A.13.2.3	Mensajería electrónica	*Control* La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	NO
A.13.2.4	Acuerdos de confidencialidad o no revelación	*Control* Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación	NO

A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información			
A.14.1 Requisitos de seguridad en sistemas de información			
Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.			**¿Aplicado?**
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	*Control* Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	NO
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	*Control* La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.	NO
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	*Control* La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción mensaje no autorizadas.	NO

A.14.2 Seguridad en el desarrollo y en los procesos de soporte			
Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.			**¿Aplicado?**
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	NO
A.14.2.2	Procedimiento de control de cambios en sistemas	*Control* La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.	NO

A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	*Control* Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.	NO
A.14.2.4	Restricciones a los cambios en los paquetes de software	*Control* 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.	NO
A.14.2.5	Principios de ingeniería de sistemas seguros	*Control* Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	NO
A.14.2.6	Entorno de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	NO
A.14.2.7	Externalización del desarrollo de software	*Control* El desarrollo de software externalizado debe ser supervisado y controlado por la organización.	NO
A.14.2.8	Pruebas funcionales de seguridad de sistemas	*Control* Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	NO
A.14.2.9	Pruebas de aceptación de sistemas	*Control* Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	NO

A.14.3 Datos de prueba			
Objetivo: Asegurar la protección de los datos de prueba			**¿Aplicado?**
A.14.3.1	Protección de los datos de prueba	*Control* Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.	NO

A.15 Relación con proveedores			
A.15.1 Seguridad en las relaciones con proveedores			
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			**¿Aplicado?**
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	*Control* Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.	NO
A.15.1.2	Requisitos de seguridad en contratos con terceros	*Control* Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor.	NO
A.15.1.3	Cadena de suministro de tecnología de la información y de comunicaciones	*Control* Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	NO

A.15.2 Gestión de la provisión de servicios del proveedor			
Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores			**¿Aplicado?**
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	*Control* Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor	NO

A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	*Control* Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.	NO

A.16 Gestión de incidentes de seguridad de la información			
A.16.1 Gestión de incidentes de seguridad de la información y mejoras			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.			**¿Aplicado?**
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	NO
A.16.1.2	Notificación de los eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	NO
A.16.1.3	Notificación de puntos débiles de la seguridad	*Control* Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen.	NO
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	*Control* Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	NO
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	NO

A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	*Control* El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.	NO
A.16.1.7	Recopilación de evidencias	*Control* La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.	NO

A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio			
A.17.1 Continuidad de la seguridad de la información			
Objetivo: La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de continuidad de negocio de la organización.			**¿Aplicado?**
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	NO
A.17.1.2	Implementar la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	NO
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	NO

A.17.2 Redundancias.			
Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.			**¿Aplicado?**
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	*Control* Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	NO

A.18 Cumplimiento			
A.18.1 Cumplimiento de los requisitos legales y contractuales			
Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.			**¿Aplicado?**
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	*Control* Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.	NO
A.18.1.2	Derechos de propiedad intelectual (DPI)	*Control* Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	NO
A.18.1.3	Protección de los registros de la organización	*Control* Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.	NO
A.18.1.4	Protección y privacidad de la información de carácter personal	*Control* Deber garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	SI

A.18.1.5	Regulación de los controles criptográficos	*Control* Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	NO

A.18.2 Revisiones de la seguridad de la información			
Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.			**¿Aplicado?**
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de seguridad de la información y su implantación (objetivos de control, controles, políticas, procesos y 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 seguridad.	NO
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	*Control* Los directivos 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 y cualquier otro requisito de seguridad aplicable	NO
A.18.2.3	Comprobación del cumplimiento técnico	*Control* Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	NO

Anexo XI. Auditoría de cumplimiento

Versión → v01-0517. La presente auditoría interna evalúa el estado de la seguridad de la información para la empresa FCA una vez aplicadas las propuestas de proyectos. Esta consta de los siguientes apartados:

- Objetivo.
- Alcance.
- Equipo auditor.
- Documentación de referencia.
- Metodología utilizada.
- Procedimiento y control de pruebas.
- No conformidades.

Objetivo de la Auditoría

Verificar el cumplimiento de los 114 controles contenidos en 14 dominios de la norma ISO / IEC 27002:2013 y evaluar su estado de madurez sobre el Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa. En el caso particular de FCA, nos centraremos en los siguientes:

Dominios ISO/IEC 27002:2013 evaluados en la empresa FCA	
Id	**Descripción**
A.5	Políticas de seguridad de la información
A.6	Organización de la seguridad de la información
A.7	Seguridad de los recursos humanos
A.8	Gestión de los activos
A.9	Control de acceso
A.11	Seguridad física y del entorno
A.12	Seguridad de las operaciones
A.13	Seguridad de las comunicaciones
A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información
A.16	Gestión de incidentes de seguridad de la información
A.17	Gestión de la continuidad de negocio
A.18	Cumplimiento

Efectividad	CMM	Significado
0%	L0	Inexistente
10%	L1	Inicial/Ad-hoc
50%	L2	Reproducible, pero intuitivo
90%	L3	Proceso definido
95%	L4	Gestionado y medible
100%	L5	Optimizado

Dicha evaluación será porcentual y se tomará como referencia el Modelo de Madurez de la Capacidad (CMM) descrito en la tabla que se presenta en la siguiente página y cuyo significado es el siguiente:

L0 (Inexistente) → Hay una carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.

L1 (Inicial/Ad/Hoc) → La organización en este nivel no dispone de un ambiente estable para el desarrollo y mantenimiento de software. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado de los proyectos es impredecible.

L2 (Reproducible) → En este nivel la organización dispone de unas prácticas institucionalizadas de gestión de proyectos, existen unas métricas básicas y un razonable seguimiento de la calidad. La relación con subcontratistas y clientes está gestionada sistemáticamente.

L3 (Proceso definido) → Además de una buena gestión de proyectos, a este nivel la organización dispone de correctos procedimientos de coordinación entre grupos, formación del personal, técnicas de ingeniería más detalladas y un nivel más avanzado de métricas en los procesos.

L4 (Gestionado y medible) → La organización dispone de un conjunto de métricas significativas de calidad y productividad, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El software resultante es de alta calidad.

L5 (Optimizado) → La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Alcance de la Auditoría

El alcance de la presente auditoría está delimitado por el conjunto de activos de la empresa FCA que están relacionados con su sistema de información. Son todos aquellos que forman parte del inventario inicial de activos e incluye tanto a los recursos humanos, como técnicos e instalaciones. Con la evolución del ciclo PDCA, y por tanto del SGSI, el alcance se verá modificado, incluyendo adicionalmente toda la información correspondiente a resultados de auditorías anteriores y actualizaciones en el plan director de seguridad.

Equipo auditor

El equipo auditor estará formado por los siguientes miembros:

- Un auditor jefe.
- Un especialista en gestión y auditoría de la seguridad
- Un experto técnico en sistemas y redes.

Dada la dimensión de la empresa FCA, El especialista y experto técnico pueden ser la misma persona, asumiendo el auditor jefe el rol de gestión.

Documentación de referencia

Para la realización de la presente auditoría se ha tomado como base la siguiente documentación:

- Norma UNE ISO/IEC 27001:2013. Versión Noviembre 2014. Castellano.
- Norma UNE ISO/IEC 27002:2013. Versión Julio de 2015. Castellano.
- Modelo de Madurez de Capacidades o CMM. Castellano.
- MAGERIT v.3.0. Castellano.
- Guía de apoyo a la implantación de un SGSI del INCIBE. Castellano.

Metodología utilizada

La metodología empleada para la realización de la presente auditoría se basa en la evaluación del cumplimiento de los controles contemplados en la Norma UNE ISO/IEC 27002:2013 y contemplando el Modelo de Madurez de la capacidad (CMM).

Procedimiento y control de pruebas

La documentación aportada y evaluada, para la realización de la presente auditoría ha sido la siguiente:

- Política de seguridad de la empresa FCA.
- Análisis de riesgos a través de la metodología MAGERIT v.3.
- Verificación del cumplimiento de los 114 controles ISO/IEC 27002:2013.
- Evaluación del estado de madurez mediante el modelo de madurez de la capacidad (CMM) y presentado a continuación.

No conformidades

A continuación se presenta la relación de seis *no conformidades* encontradas durante la realización de la presente auditoría:

Identificador: NC-01	**Fecha inicio: 19/05/2017**	**Fecha fin:**
Descripción Inexistencia de un proceso disciplinario por incumplimiento de la política de seguridad.		
Tipo de no conformidad: Menor.		
Afectación ISO/IEC 27002:2013		
Control A.7.2.3 Proceso disciplinario durante empleo.	**Dominio** A.7 Seguridad relativa a los RRHH.	
Acción correctora Actualización del documento base con la política de seguridad corporativa.		
Responsable asignado: Responsable de RRHH.		

Identificador: NC-02	Fecha inicio: 19/05/2017	Fecha fin:
Descripción Inexistencia de un sistema de gestión de contraseñas para el acceso al ERP.		
Tipo de no conformidad: Menor.		
Afectación ISO/IEC 27002:2013		
Control A.9.4.3 Sistema de gestión de contraseñas.	**Dominio** A.9 Control de acceso.	
Acción correctora Implantación de un sistema manual de gestión periódica de contraseñas.		
Responsable asignado: Responsable de soporte TIC.		

Identificador: NC-03	Fecha inicio: 19/05/2017	Fecha fin:
Descripción Falta de controles físicos de acceso a las instalaciones y fallo en las políticas de equipo desatendido, puesto despejado y pantalla limpia.		
Tipo de no conformidad: Menor.		
Afectación ISO/IEC 27002:2013		
Control A.11.1.2 Controles físicos e entrada. A.11.2.8 Equipos de usuario desatendido. A.11.2.9 Puesto despejado y pantalla limpia.	**Dominio** A.11 Seguridad física y del entorno.	
Acción correctora Instalación de una alarma para el control perimetral, con detectores de presencia y conexión a central de seguridad. Activación de protección de pantalla con contraseña a los 5 minutos de inactividad en los puestos de la oficina (servidor y pc gerente). Documentación fuera de los mostradores de venta, en los cajones habilitados a la izquierda y cierre con llave en la oficina ante la ausencia del personal.		
Responsable asignado: Equipo de ventas, administración y gerente.		

Identificador: NC-04	Fecha inicio: 19/05/2017	Fecha fin:
Descripción Inexistencia de registros de eventos de seguridad de la información. No se realiza semestralmente la sincronización de reloj en el servidor ni en los equipos de ventas. No existe una mínima gestión de vulnerabilidades técnicas.		
Tipo de no conformidad: Menor.		
Afectación ISO/IEC 27002:2013		
Control A.12.4.1 Registro de eventos. A.12.4.4 Sincronización del reloj. A.12.6.1 Gestión vulnerabilidades técnicas.	**Dominio** A.12 Seguridad de las operaciones.	
Acción correctora Implantación de un registro manual de eventos para su posterior notificación. Obligatoriedad de sincronización del reloj en el servidor entre las 24 y 48 horas posteriores al cambio horario. Revisión periódica y resolución, por parte del personal de soporte TIC, de las vulnerabilidades técnicas encontradas en el sistema de información.		
Responsable asignado: Responsable de administración y personal externo de soporte TIC.		

Identificador: NC-05	Fecha inicio: 19/05/2017	Fecha fin:
Descripción Mínima seguridad en los servicios de red y ausencia de acuerdos para favorecer el intercambio seguro de información a través de mensajería electrónica.		
Tipo de no conformidad: Mayor.		
Afectación ISO/IEC 27002:2013		
Control A.13.1.2 Seguridad de los servicios de red. A.13.2.2 Acuerdos intercambio información. A.13.2.3 Mensajería electrónica.	**Dominio** A.13 Seguridad de las comunicaciones	
Acción correctora Bastionado del servidor y cortafuegos. Cifrado de comunicaciones con información sensible.		
Responsable asignado: Personal externo de soporte TIC.		

Identificador: NC-06	Fecha inicio: 19/05/2017	Fecha fin:
Descripción Inexistencia de un sistema formal y normalizado para la gestión y respuesta ante incidentes de seguridad de la información. No está contemplada la recopilación de evidencias, para su posterior análisis, tras un evento que afecte a la seguridad del sistema de información.		
Tipo de no conformidad: Mayor.		
Afectación ISO/IEC 27002:2013		
Control A.16.1.2 Notificación eventos de seguridad. A.16.1.3 Notificación de puntos débiles. A.16.1.5 Respuesta ante incidentes. A.16.1.7 Recopilación de evidencias.	**Dominio** A.16 Gestión de incidentes de seguridad de la información.	
Acción correctora Revisión y adecuación del plan director de seguridad para contemplar la respuesta ante incidentes de seguridad y adquisición de posibles evidencias para su posterior análisis.		
Responsable asignado: Gerente y personal externo de soporte TIC.		

Podemos concluir que tras la realización de la auditoría interna, se han encontrado 8 no conformidades, que deben ser tratadas:

- ***6 No Conformidades Menores*** que deben ser resueltas en un plazo no superior a los 6 meses y han afectado a los siguientes dominios:
  - No conformidad en 1 control sobre los Recursos Humanos.
  - No conformidad en 1 control sobre el Control de Acceso.
  - No conformidad en 3 controles sobre Seguridad Física y del Entorno.
  - No conformidad en 3 controles sobre la Seguridad en operaciones.
- ***2 No Conformidades Mayores*** que deben ser resueltas de forma inmediata y están clasificadas de la siguiente forma:
  - No conformidad en 3 controles realizados sobre la Seguridad en las Comunicaciones.
  - No conformidad en 4 controles realizados sobre la gestión de incidentes de Seguridad de la Información.

Anexo XII. Evaluación estado del CMM

A continuación se presenta una tabla con la evaluación del estado de madurez de la seguridad de la información, para FCA, en base a los 14 dominios y 114 controles contemplados en la ISO 27002:2013.

A.5 Políticas de seguridad de la información		
A.5.1 Directrices de gestión de la seguridad de la información		**CMM**
A.5.1.1	Políticas para la seguridad de la información	10%
A.5.1.2	Revisión de las políticas para la seguridad de la información	0%

La implantación de políticas para la SI está en su estado inicial, con la implantación del presente Sistema de Gestión de Seguridad de la información. Este documento corresponde al primer ciclo *PDCA (Plan-Do-Check-Act)* y por ello no se ha dado por iniciado el procedimiento de revisión de dichas políticas.

A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		**CMM**
A.6.1.1	Roles y responsabilidades en seguridad de la información	30%
A.6.1.2	Segregación de tareas	30%
A.6.1.3	Contacto con las autoridades	0%
A.6.1.4	Contacto con grupos de interés especial	60%
A.6.1.5	Seguridad de la información en la gestión de proyectos	80%
A.6.2 Los dispositivos móviles y el teletrabajo		**CMM**
A.6.2.1	Política de dispositivos móviles	70%
A.6.2.2	Teletrabajo	80%

Los roles, responsabilidades y segregación de tareas están establecidos de manera informal. No existe contacto alguno con autoridades pero si con grupos de interés especializados en seguridad de la información, a través del personal de soporte externalizado. Actualmente hay dos proyectos en marcha y la seguridad en su gestión está siendo documentada. Existe una clara política de utilización de dispositivos móviles en la empresa y para modalidad teletrabajo.

A.7 Seguridad relativa a los recursos humanos		
A.7.1 Antes del empleo		**CMM**
A.7.1.1	Investigación de antecedentes	95%
A.7.1.2	Términos y condiciones del empleo	50%
A.7.2 Durante el empleo		**CMM**
A.7.2.1	Responsabilidades de gestión	10%
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	50%
A.7.2.3	Proceso disciplinario	0%
A.7.3 Finalización del empleo o cambio en el puesto de trabajo		**CMM**
A.7.3.1	Responsabilidades ante la finalización o cambio	40%

La labor de investigación a los candidatos que optan por un puesto en la organización está perfectamente definida y las condiciones para el desarrollo de la actividad están más o menos claras, aunque no formalmente establecidas.

Las responsabilidades de gestión, durante el desempeño del empleo, están en un estado inicial de implantación. No existe un proceso disciplinario formal, pero si se ha comunicado, de forma directa, a cada uno de los empleados las normas de seguridad que deben cumplir en cuanto a la seguridad de la información.

Todos los miembros de la organización tienen clara su responsabilidad en cuanto a la privacidad y confidencialidad de la información durante el desarrollo de su puesto de trabajo, siendo conocedores que esta responsabilidad continua por un período de 3 años en caso de abandonar la organización.

A.8 Gestión de activos		
A.8.1 Responsabilidad sobre los activos		**CMM**
A.8.1.1	Inventario de activos	80%
A.8.1.2	Propiedad de los activos	20%
A.8.1.3	Uso aceptable de los activos	60%
A.8.1.4	Devolución de activos	95%
A.8.2 Clasificación de la información		**CMM**
A.8.2.1	Clasificación de la información	5%
A.8.2.2	Etiquetado de la información	5%
A.8.2.3	Manipulado de la información	50%
A.8.3 Manipulación de los soportes		**CMM**
A.8.3.1	Gestión de soportes extraibles	60%
A.8.3.2	Eliminación de soportes	95%
A.8.3.3	Soportes físicos en tránsito	95%

Existe un inventario de activos establecido, aunque la propiedad de los mismos no ha sido asignada todavía. La utilización correcta de los activos está documentada según exige el RLOPD y el proceso de devolución de activos está perfectamente definido.

Actualmente no se ha considerado necesario la clasificación ni etiquetado de información, porque no hay información sensible al alcance de ninguna persona excepto el Gerente de la organización. Si existe un proceso, aunque informal, de manipulación de información sensible, que es aplicado en la organización.

Existe un procedimiento informal para la gestión de soportes extraibles y tanto la eliminación segura de la información que contienen como el tránsito de los mismos está formalmente controlada por el personal de soporte externo.

A.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		**CMM**
A.9.1.1	Política de control de acceso	10%
A.9.1.2	Acceso a las redes y a los servicios de red	90%
A.9.2 Gestión de acceso de usuario		**CMM**
A.9.2.1	Registro y baja de usuario	90%
A.9.2.2	Provisión de acceso de usuario	40%
A.9.2.3	Gestión de privilegios de acceso	95%
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	0%
A.9.2.5	Revisión de los derechos de acceso de usuario	0%
A.9.2.6	Retirada o reasignación de los derechos de acceso	80%
A.9.3 Responsabilidades del usuario		**CMM**
A.9.3.1	Uso de la información secreta de autenticación	10%
A.9.4 Control de acceso a sistemas y aplicaciones		**CMM**
A.9.4.1	Restricción del acceso a la información	90%
A.9.4.2	Procedimientos seguros de inicio de sesión	50%
A.9.4.3	Sistema de gestión de contraseñas	0%
A.9.4.4	Uso de utilidades con privilegios del sistema	95%
A.9.4.5	Control de acceso al código fuente de los programas	95%

No existe una política formal de control de accesos, aunque si se controla el acceso al servidor corporativo y red interna. Los procesos CRUD de usuarios se realizan formalmente, aunque no se revisan periódicamente los derechos de acceso. El uso de información secreta apenas está contemplado.

Hay restricciones claras a cierto tipo de información y procedimientos de inicio de sesión pero no demasiado seguros (no está contemplado un sistema de gestión de contraseñas). El acceso al código fuente de los programas y el uso de privilegios “root” está únicamente habilitado para el personal de soporte TIC.

A.11 Seguridad física y del entorno		
A.11.1 Áreas seguras		**CMM**
A.11.1.1	Perímetro de seguridad física	50%
A.11.1.2	Controles físicos de entrada	0%
A.11.1.3	Seguridad de oficinas, despachos y recursos	0%
A.11.1.4	Protección contra las amenazas externas y ambientales	40%
A.11.1.5	El trabajo en áreas seguras	0%
A.11.1.6	Áreas de carga y descarga	80%
A.11.2 Seguridad de los equipos		**CMM**
A.11.2.1	Emplazamiento y protección de equipos	90%
A.11.2.2	Instalaciones de suministro	50%
A.11.2.3	Seguridad del cableado	90%
A.11.2.4	Mantenimiento de los equipos	5%
A.11.2.5	Retirada de materiales propiedad de la empresa	70%
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	80%
A.11.2.7	Reutilización o eliminación segura de equipos	95%
A.11.2.8	Equipo de usuario desatendido	5%
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	5%

El perímetro físico de las instalaciones tiene una seguridad aceptable pero debe mejorar notablemente. No existen controles de acceso de tipo alguno en cualquier instalación ni áreas de trabajo seguras. Las áreas de carga y descarga están bien controladas. Por otro lado, existe una protección razonable contra amenazas externas y ambientales, también mejorables.

En cuanto a la seguridad de los equipos, destacar un buen emplazamiento y protección, así como un buen cableado. El mantenimiento de los equipos es claramente insuficiente. Destaca la inexistente política de puesto de trabajo despejado y pantalla limpia. La seguridad de los equipos fuera de las instalaciones es buena y la reutilización/eliminación está bien gestionada.

A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operacionales		**CMM**
A.12.1.1	Documentación de procedimientos de los operación	10%
A.12.1.2	Gestión de cambios	10%
A.12.1.3	Gestión de capacidades	0%
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	0%
A.12.2 Protección contra el software malicioso (malware)		**CMM**
A.12.2.1	Controles contra el código malicioso	100%
A.12.3 Copias de seguridad		**CMM**
A.12.3.1	Copias de seguridad de la información	100%
A.12.4 Registros y supervisión		**CMM**
A.12.4.1	Registro de eventos	5%
A.12.4.2	Protección de la información de registro	95%
A.12.4.3	Registros de administración y operación	5%
A.12.4.4	Sincronización del reloj	5%
A.12.5 Control del software en explotación		**CMM**
A.12.5.1	Instalación del software en explotación	95%
A.12.6 Gestión de la vulnerabilidad técnica		**CMM**
A.12.6.1	Gestión de las vulnerabilidades técnicas	0%
A.12.6.2	Restricción en la instalación de software	95%
A.12.7 Consideraciones sobre la auditoria de sistemas de información		**CMM**
A.12.7.1	Controles de auditoría de sistemas de información	10%

Únicamente la protección contra *malware* y la gestión de *backup,s* está optimizada. Destacar la protección de la información de registro, la instalación del software de explotación y las restricciones sobre dicha instalación.

A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de redes		**CMM**
A.13.1.1	Controles de red	50%
A.13.1.2	Seguridad de los servicios de red	0%
A.13.1.3	Segregación en redes	5%
A.13.2 Intercambio de información		**CMM**
A.13.2.1	Políticas y procedimientos de intercambio de información	10%
A.13.2.2	Acuerdos de intercambio de información	5%
A.13.2.3	Mensajería electrónica	0%
A.13.2.4	Acuerdos de confidencialidad o no revelación	70%

Hay un proceso claro, no formalizado, de controles de red, aunque la seguridad de los servicios no está contemplada ni hay una segregación de red. Únicamente se ha derivado la entrada de conexiones *wifi* a otro *router* que no está conectado al *hub* de la red corporativa.

Las políticas para el intercambio de información están siendo contempladas en el SGSI, pero en un estado muy inicial. No existen acuerdos para el intercambio seguro de información corporativa pero si de carácter personal.

Existen acuerdos de confidencialidad firmados por los empleados de la organización, según exige el RLOPD, pero han sido actualizados con las últimas incorporaciones a la empresa.

A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.14.1 Requisitos de seguridad en sistemas de información		**CMM**
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	5%
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	10%
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	95%
A.14.2 Seguridad en el desarrollo y en los procesos de soporte		**CMM**
A.14.2.1	Política de desarrollo seguro	0%
A.14.2.2	Procedimiento de control de cambios en sistemas	0%
A.14.2.3	Revisión técnica de aplicaciones tras efectuar cambios en el S.O	95%
A.14.2.4	Restricciones a los cambios en los paquetes de software	95%
A.14.2.5	Principios de ingeniería de sistemas seguros	0%
A.14.2.6	Entorno de desarrollo seguro	0%
A.14.2.7	Externalización del desarrollo de software	95%
A.14.2.8	Pruebas funcionales de seguridad de sistemas	95%
A.14.2.9	Pruebas de aceptación de sistemas	0%
A.14.3 Datos de prueba		**CMM**
A.14.3.1	Protección de los datos de prueba	0%

Los requisitos de seguridad en el sistema de información de la empresa es casi inexistente, pero en proceso de implantación. Si se está contemplando de manera formal la protección de las transacciones entre el ERP y otros sistemas externos a la organización.

No se ha establecido política de seguridad alguna en cuanto al desarrollo de aplicaciones, porque está externalizado. Por otro lado, los procesos de soporte del ERP si han sido externalizados y se puede garantizar la seguridad de la información en los mismos (revisiones, control de cambios y pruebas funcionales).

No se puede asegurar internamente la seguridad de los datos de pruebas porque es tarea del personal de soporte externo a la organización.

A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		**CMM**
A.16.1.1	Responsabilidades y procedimientos	10%
A.16.1.2	Notificación de los eventos de seguridad de la información	10%
A.16.1.3	Notificación de puntos débiles de la seguridad	10%
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	10%
A.16.1.5	Respuesta a incidentes de seguridad de la información	10%
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	10%
A.16.1.7	Recopilación de evidencias	0%

Los procedimientos para gestionar la respuesta ante incidentes que afecten a la seguridad de la información no están definidos, aunque van a ser contemplados en esta primera versión del SGSI.

No existen tampoco procedimientos para la notificación de incidentes ni de vulnerabilidades encontradas, aunque también está contemplada su implantación a corto plazo.

Hasta la fecha no se ha evaluado ni clasificado evento de seguridad alguno. Si está contemplado su implantación a medio plazo. Como no se ha producido ni registrado incidente de seguridad alguno, el mecanismo de respuesta ante los mismos es inexistente o está en una fase muy inicial. Por el mismo motivo, no se ha recopilado evidencia alguna, aunque se considera conveniente contemplar esta posibilidad.

A.17 Aspectos seguridad de información para la gestión de la continuidad del negocio		
A.17.1 Continuidad de la seguridad de la información		**CMM**
A.17.1.1	Planificación de la continuidad de la seguridad de la información	10%
A.17.1.2	Implementar la continuidad de la seguridad de la información	10%
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la S.I.	10%
A.17.2 Redundancias.		**CMM**
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	60%

El proceso de planificación de la continuidad en la seguridad de la información no está contemplado actualmente aunque si se considera necesario ponerlo en marcha.

La implementación de procesos para proporcionar continuidad en la seguridad de la información es nulo o está en un estado muy inicial. Por el mismo motivo, los controles de evaluación de seguridad de la información son inexistentes aunque están siendo contemplados a medio plazo.

La disponibilidad de los recursos para el tratamiento de la información, así como la propia información está garantizada, aunque su grado de madurez no sea el deseado.

A.18 Cumplimiento		
A.18.1 Cumplimiento de los requisitos legales y contractuales		**CMM**
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	30%
A.18.1.2	Derechos de propiedad intelectual (DPI)	0%
A.18.1.3	Protección de los registros de la organización	30%
A.18.1.4	Protección y privacidad de la información de carácter personal	90%
A.18.1.5	Regulación de los controles criptográficos	60%
A.18.2 Revisiones de la seguridad de la información		**CMM**
A.18.2.1	Revisión independiente de la seguridad de la información	90%
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	50%
A.18.2.3	Comprobación del cumplimiento técnico	10%

Los requisitos legales y contractuales se están cumpliendo de forma sistemática, aunque los procedimientos para el cumplimiento de los mismos no estén actualizados.

Como no existen derechos de propiedad intelectual no se ha implementado procedimiento alguno para garantizar los requisitos legales, regulatorios y contractuales.

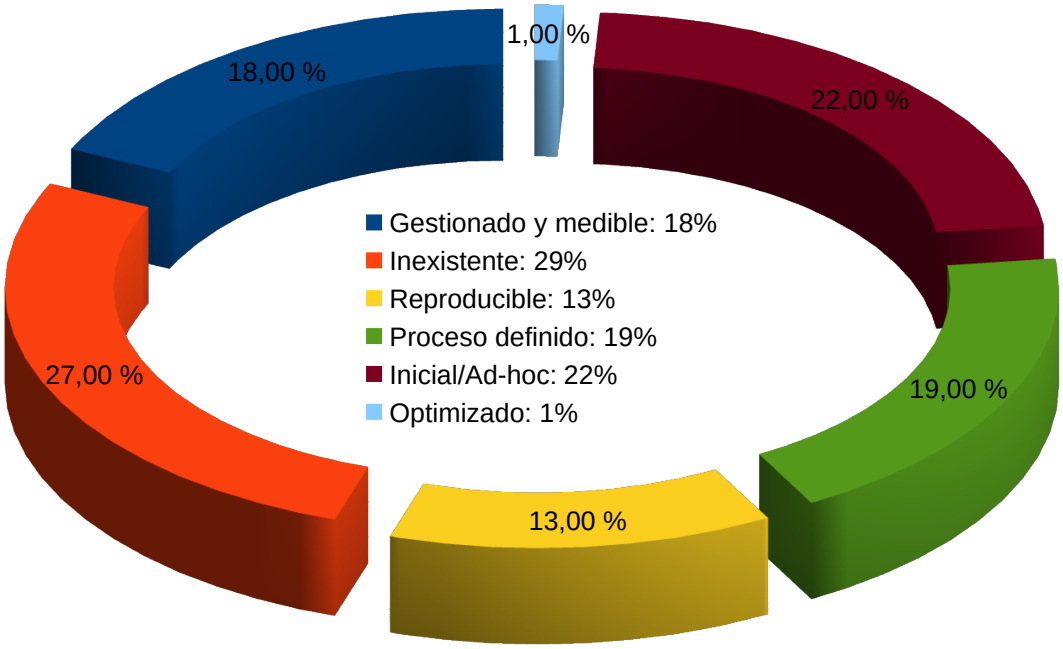
Cualquier registro disponible en el sistema de información está replicado en las copias de seguridad aunque no se ha verificado la integridad de las mismas. Está totalmente garantizada la privacidad y protección de los datos, según exige el RLOPD.

Los controles criptográficos son correctos en lo que a firma electrónica y transacciones con los organismos públicos se refiere.

Está contemplada, desde principios de año, los procesos para la revisión independiente de la seguridad de la información, a través de las empresas que proporcionan el soporte técnico a la organización.

Las normas y políticas de seguridad se cumplen de manera informal, ya que actualmente no está totalmente implantado el SGSI. Por este motivo, tampoco se puede garantizar que los sistemas de información estén siendo auditados periódicamente, aunque si está contemplado en el siguiente ciclo del SGSI.

Finalmente presentamos un gráfico circular con el ***Modelo de Madurez de la Capacidad*** *(CMM - Capability Maturity Model)* aplicado a los ***controles ISO 27002:2013***, con una aproximación por porcentajes obtenidos en cada uno de los dominios evaluados.



A modo de resumen, se puede llegar a las siguientes conclusiones sobre el estado de madurez de los controles auditados:

- Únicamente el 1% de los controles verificados ha dado como resultado un proceso optimizado.
- El 18% de los controles han dado como resultado procedimientos bien gestionados, medibles y analizables.
- Otro 19% de los controles muestran procesos que se han implantado y documentado aunque han sido comunicados de manera informal.
- Un 13% de los controles nos indican que se puede verificar su cumplimiento pero de forma intuitiva (no práctica).
- El 27% de los controles se encuentran en un estado inicial de implantación y por tanto de no cumplimiento.
- Hay un 22% de controles inexistentes o que no se están cumpliendo sistemáticamente, bien porque no tiene sentido su implantación, bien porque no se han implementado correctamente.