Elaboración SGSI Seguridad365 (Presentación a la Dirección)

Programa:	MISTIC
Empresa:	Seguridad365
Prueba:	TFM (Memoria)
Fecha:	21 de diciembre de 2018
Alumno:	José Alberto Catalá Hernansáiz
Universidad:	Universidad Oberta de Cataluña
Consultor:	Antonio José Segovia Henares

Resumen

Elaboración del plan de implementación de un Sistema de Gestión de Seguridad de la Información para Seguridad365. Compañía dedicada a la prestación de servicios de seguridad privada.

El proyecto se ha desarrollado de forma incremental y se ha vertebrado en seis fases, y dando como resultado los siguientes entregables:

- Informe Análisis Diferencial
- Esquema Documental ISO/IEC 27001
- Análisis de Riesgos
- Plan de Proyectos
- Auditoría de Cumplimiento
- Presentación de resultados

Para la elaboración del SGSI he utilizado la norma ISO/IEC 27001:2013. Para la elaboración del Análisis de Riesgo he utilizado la metodología Magerit.

Como resultado, la compañía Seguridad365 cuenta con un SGSI y estaría preparada para la certificación en la norma ISO/IEC 27001.

Metodología

- **Fase I** • Situación actual: Contextualización, objetivos y análisis diferencial
- **Fase II** • Sistema de Gestión Documental
- **Fase III** • Análisis de riesgos
- **Fase IV** • Propuesta de Proyectos
- **Fase V** • Auditoría de Cumplimiento
- **Fase VI** • Presentación de resultados

Situación Actual – Contexto Normativo

Seguridad 365

Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

La familia de normas ISO/IEC 27000 recoge distintas normas, siendo las siguientes las más representativas para el desarrollo del SGSI y las que se aplicarán para el desarrollo de este.

- ISO/IEC 27001. Contiene las especificaciones para la implantación del SGSI. Proviene en origen de la BS 7799-2:2002. Desde entonces ha pasado por distintas versiones, siendo su última versión vigente la ISO/IEC 27001:2013.
- ISO/IEC 27002. Contiene el código de buenas prácticas en la gestión de la Seguridad de la Información. Proviene de la BS 7799 parte 1 y la ISO/IEC 17799. Como la ISO/IEC 27001 ha sido actualizada, siendo la versión vigente la ISO/IEC 27002:2013.

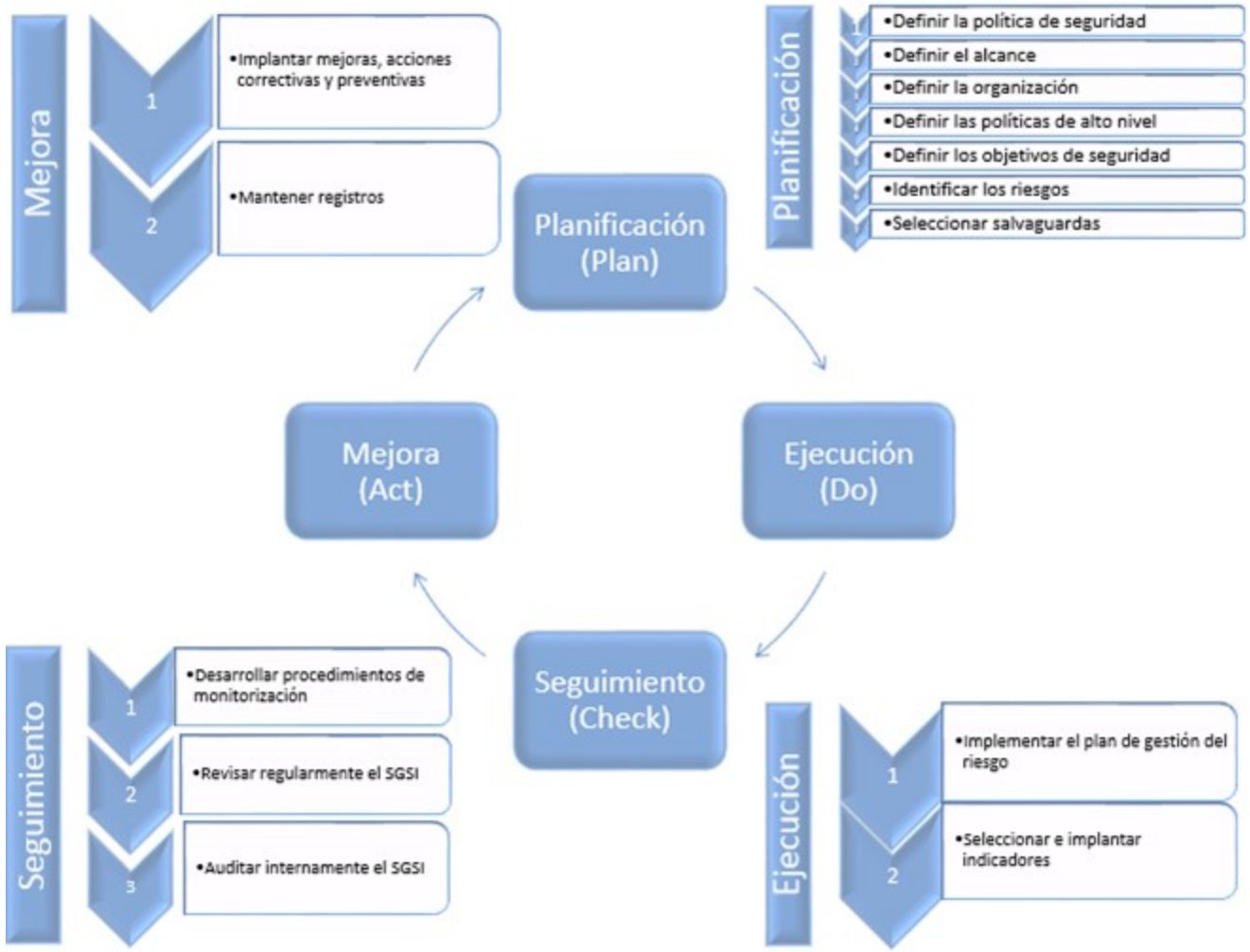
Norma (ISO/IEC 27001:2013)	
4.	CONTEXTO DE LA ORGANIZACIÓN
5.	LIDERAZGO
6.	PLANIFICACIÓN
7.	SOPORTE
8.	OPERACIÓN
9.	EVALUACIÓN DEL DESEMPEÑO
10.	MEJORA

CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)	
5.	POLÍTICA DE SEGURIDAD
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
8.	GESTIÓN DE ACTIVOS
9.	CONTROL DE ACCESOS
10.	CIFRADO
11.	SEGURIDAD FÍSICA Y AMBIENTAL
12.	SEGURIDAD EN LA OPERATIVA
13.	SEGURIDAD EN LAS TELECOMUNICACIONES
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN
15.	RELACIONES CON SUMINISTRADORES
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN
17.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
18.	CUMPLIMIENTO

Situación Actual – Plan de proyecto

Seguridad 365

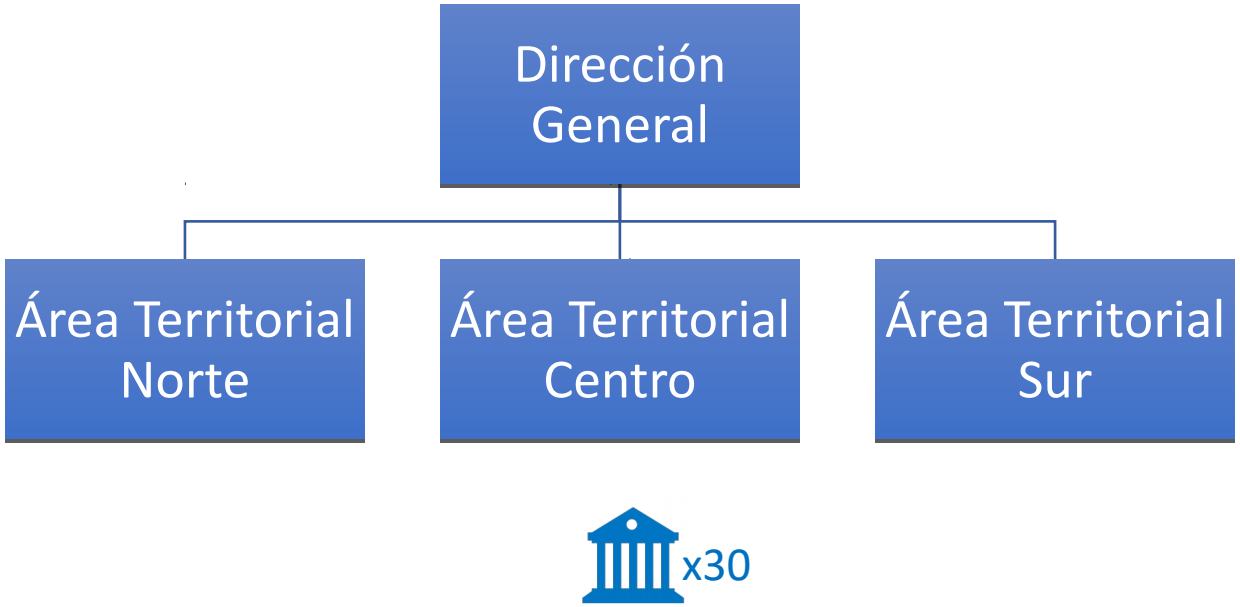
Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI



Situación Actual – Contexto de Seguridad365

Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

Seguridad365 es una compañía de carácter nacional líder en el sector de la Seguridad Privada. Su personal tiene una marcada vocación de servicio que permite alcanzar un alto nivel de excelencia y calidad de servicio. Su porfolio de servicios y soluciones es amplio y la permite dar cobertura a gran variedad de clientes y sectores empresariales.



Situación Actual – Contexto de Seguridad365

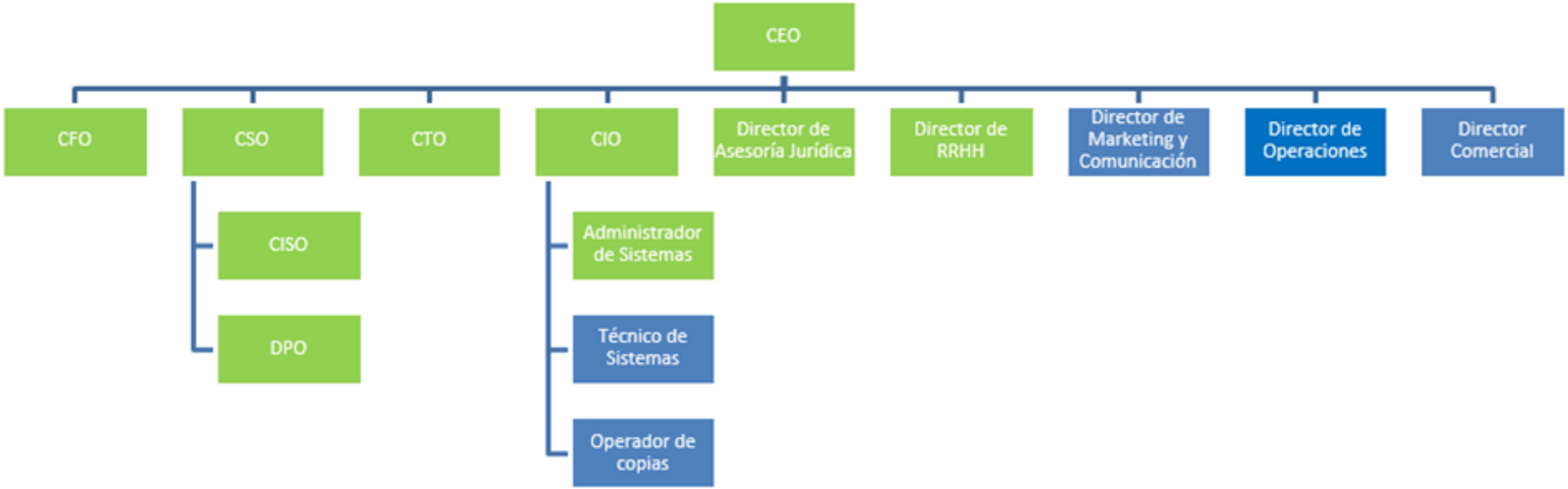
Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

Soportado por:

- Gestión contable/financiera a través del ERP Navision de Microsoft.
- Gestión de Nominas a través de PeopleSoft.
- Gestión de turnos de personal operativo a través de ProPlan365.
- Correo electrónico a través de Exchange
- Sistema de recepción de gestión de señales de los sistemas instalados a través de MasterCentral.
- Control de Operativo en Clientes a través de Guadian365
- Portal del Empleado
- Otros sistemas de menos calada pero igualmente necesarios.

Situación Actual – Contexto de Seguridad365

Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

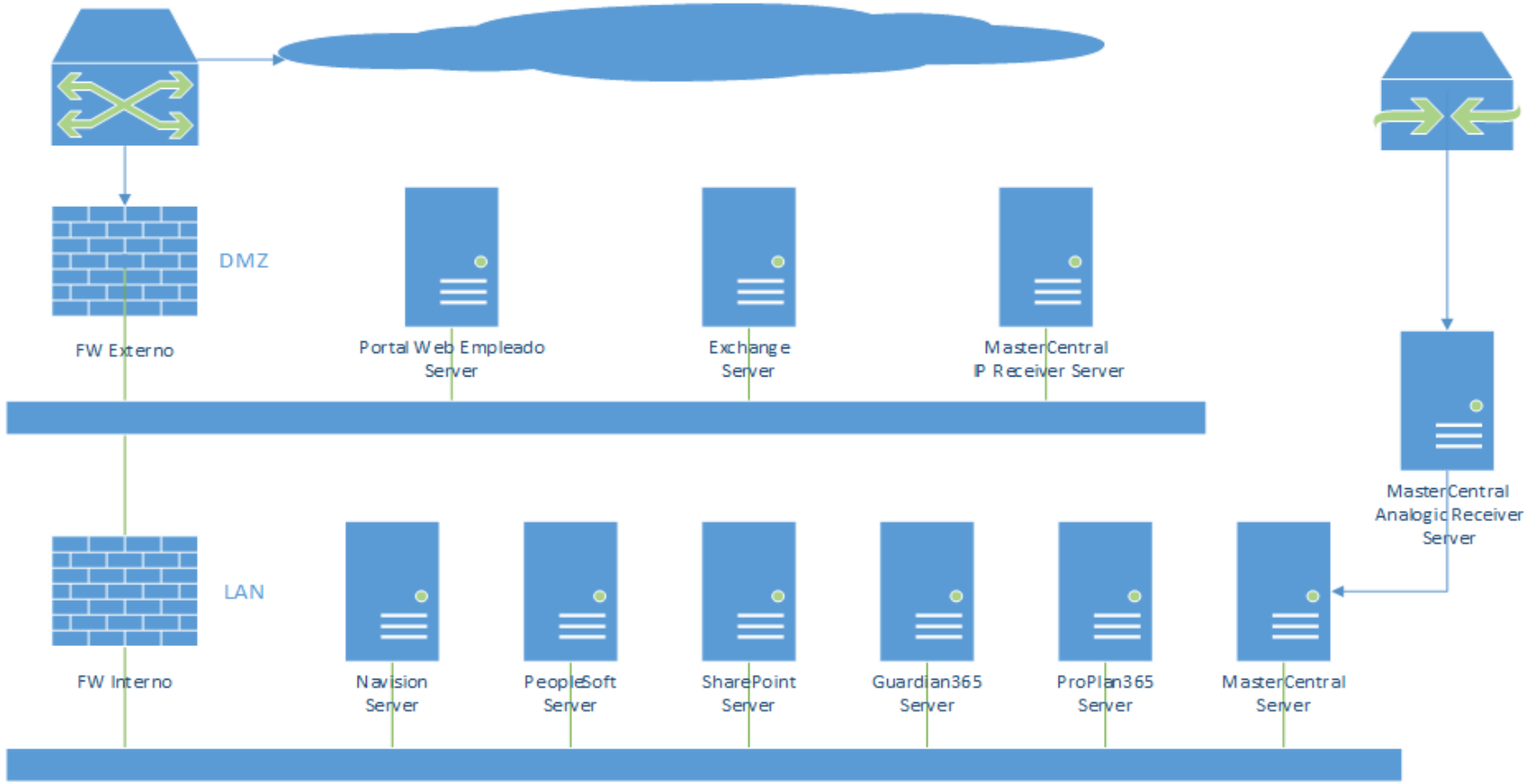


Situación Actual – Contexto de Seguridad365

Seguridad 365

Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

Esquema de red básico



Situación Actual – Mapa de Procesos

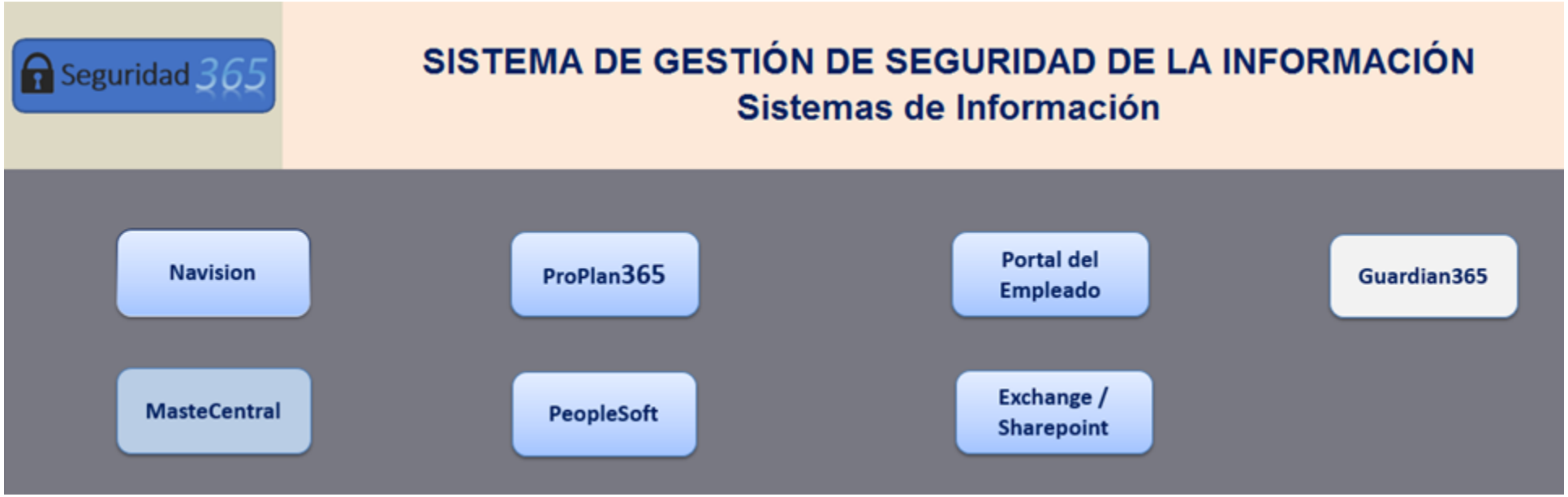
Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

Procesos de negocio principales y de soporte

Situación Actual – Mapa de Procesos

Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

Sistemas de Información que soportan los procesos de negocio



Situación Actual – Mapa de Procesos

Seguridad 365

Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

Navision

DIMENSIONES DE SEGURIDAD

Confidencialidad			Integridad			Disponibilidad		
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Muy alta	Alta	Alta	Muy alta	Muy alta	Alta	Muy alta	Alta	Baja

ProPlan365

DIMENSIONES DE SEGURIDAD

Confidencialidad			Integridad			Disponibilidad		
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Muy alta	Alta	Alta	Muy alta	Alta	Alta	Muy alta	Alta	Media

PeopleSoft

DIMENSIONES DE SEGURIDAD

Confidencialidad			Integridad			Disponibilidad		
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Muy alta	Alta	Alta	Muy alta	Muy alta	Alta	Muy alta	Alta	Media

Portal del Empleado

DIMENSIONES DE SEGURIDAD

Confidencialidad			Integridad			Disponibilidad		
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Baja	Media	Alta	Baja	Alta	Alta	Baja	Baja	Baja

Exchange / Sharepoint

DIMENSIONES DE SEGURIDAD

Confidencialidad			Integridad			Disponibilidad		
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Alta	Alta	Muy alta	Alta	Alta	Muy alta	Muy alta	Alta	Baja

MasterCentral

DIMENSIONES DE SEGURIDAD

Confidencialidad			Integridad			Disponibilidad		
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Alta	Muy alta	Alta	Muy alta	Muy alta	Alta	Muy alta	Muy alta	Muy alta

Guardian365

DIMENSIONES DE SEGURIDAD

Confidencialidad			Integridad			Disponibilidad		
Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Media	Alta	Alta	Media	Alta	Alta	Baja	Baja	Baja

Situación Actual – Objetivos del Plan Director

Seguridad 365

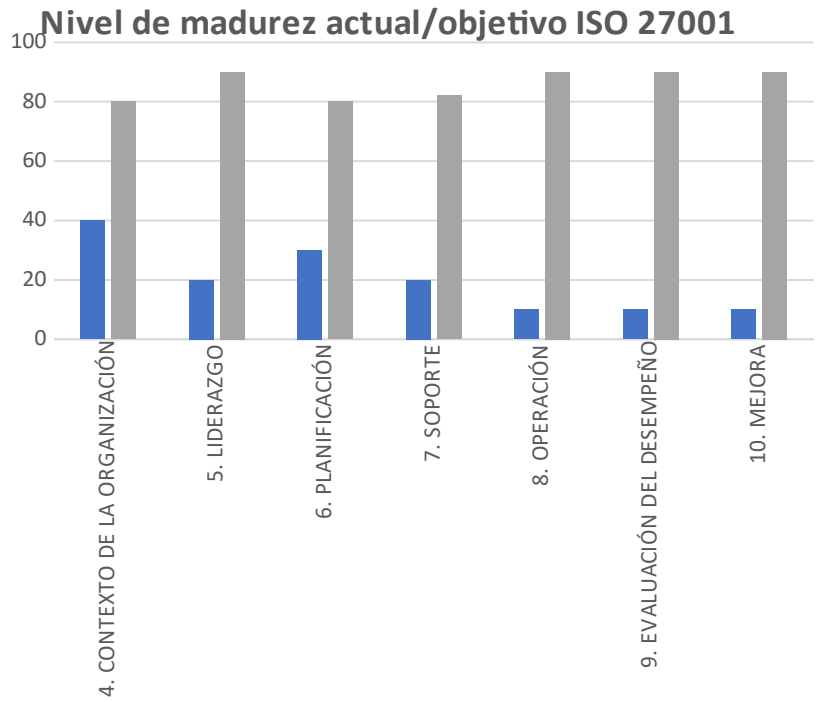
Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

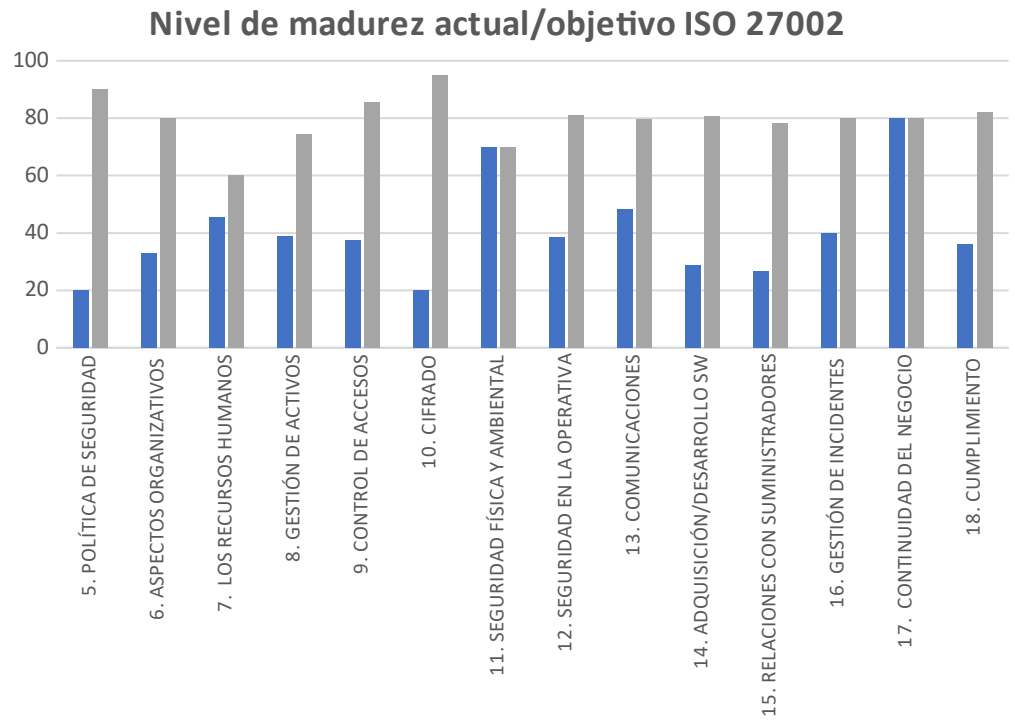
Seguridad365 pese a no presta servicios de seguridad gestionada IT para sus clientes, está muy sensibilizada con la protección de su información y la de sus clientes. Tratándose de una compañía del sector de la seguridad privada, su sensibilidad es si cabe mayor, pues está acostumbrada a realizar análisis de riesgos para sus clientes y conoce el impacto negativo que tiene cualquier incidente de seguridad.

Situación Actual – Análisis Diferencial

Fase I | Fase II | Fase III | Fase IV | Fase V | Fase VI

Resumen ejecutivo del Análisis Diferencial





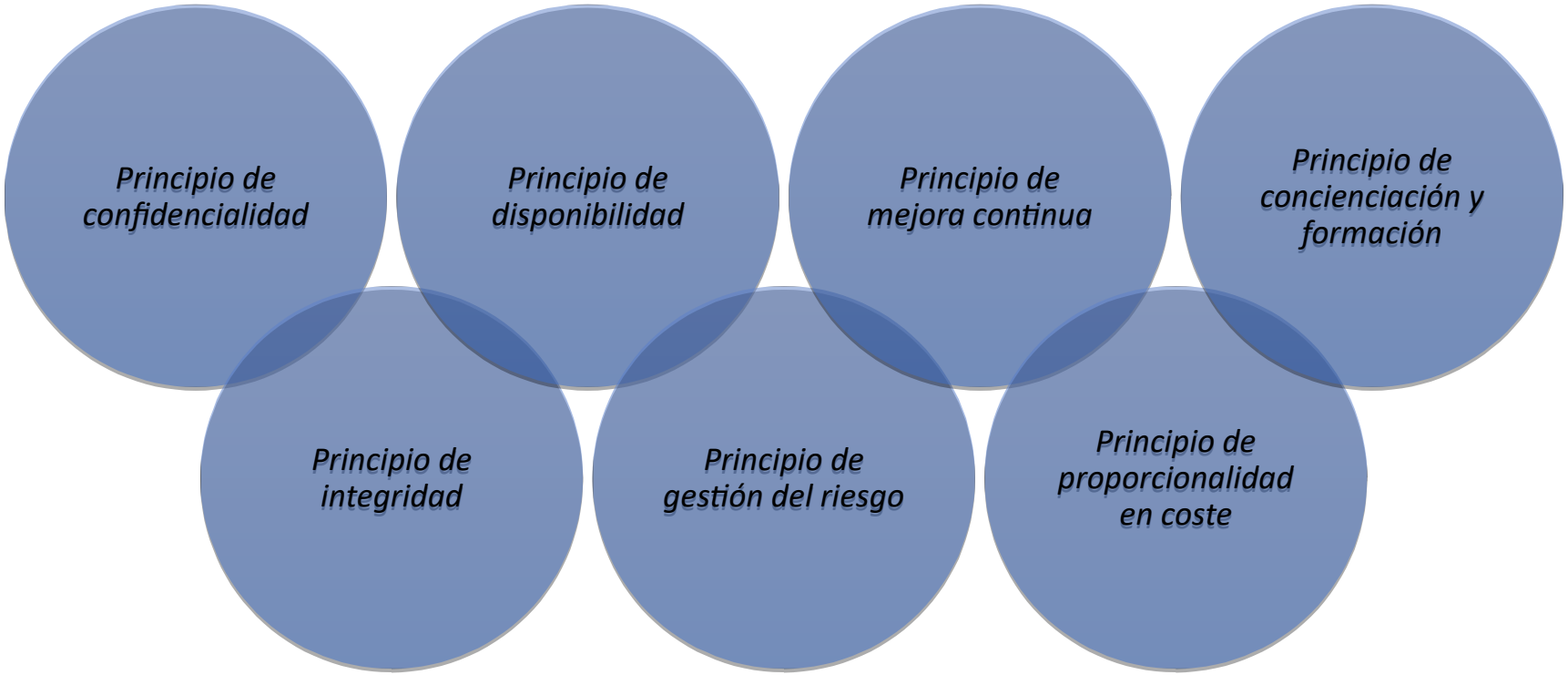
* Para mayor detalle, ver el epígrafe 1.7 y el Anexo II de la Memoria.

Sistema de Gestión Documental – Política de Seguridad

Seguridad 365

Fase I | **Fase II** | Fase III | Fase IV | Fase V | Fase VI

Principios de desarrollo de la Política de Seguridad



Sistema de Gestión Documental – Proc. Audit. Internas

Seguridad 365

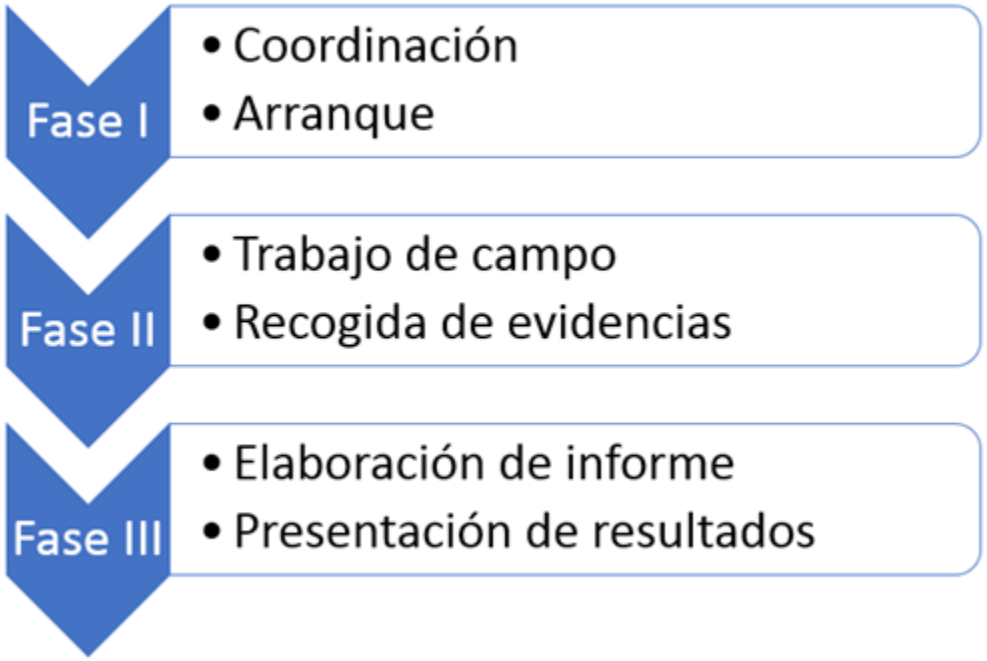
Fase I | **Fase II** | Fase III | Fase IV | Fase V | Fase VI

Metodología

Alcance	El alcance de las auditorías internas se circunscribirá a los procesos identificados en el mapa de procesos de la compañía.
Objetivo	El objetivo será verificar el cumplimiento de lo establecido en el SGSI.
Periodicidad	La periodicidad de la auditoría interna será de carácter anual, realizándose durante el primer semestre del año.
Programa de auditoría	Se ha diseñado un Programa de Auditoría basado en ciclos de 3 años. De esta manera, se revisa una parte del sistema cada año, completando un ciclo completo al tercer año.
Equipo auditor	El equipo auditor estará formado por la Dirección de Seguridad. Recayendo el liderazgo sobre la figura del CISO.

Sistema de Gestión Documental – Proc. Audit. Internas

Fases de Auditoría Interna



Sistema de Gestión Documental – Gestión de Indicadores

Seguridad 365

Fase I | **Fase II** | Fase III | Fase IV | Fase V | Fase VI

Indicadores fijados

CÓDIGO	NOMBRE	DOMINIO	MÉTRICA	PERIODICIDAD	UMBRAL	OBJETIVO	RESPONSABLES
SGSI1	Formación	Personal	Trabajadores que han recibido formación específica en materia de seguridad de la información	Anual	90%	100%	Comité de Seguridad
SGSI2	Umbral de Riesgo	Riesgos	Riesgos por encima del umbral establecido tras análisis (estado potencial) y tratamiento (estado residual)	Anual	5%	0%	CISO
SGSI3	Logs	Control de Acceso	Sistemas/aplicaciones con acceso a datos sensibles sobre los que se realiza registro y alerta periódica de logs de acceso (referido a los Administradores)	Anual	90%	100%	Sistemas
SGSI4	Bajas		Ratio de cuentas de usuario para las que se ha solicitado baja que aún siguen activas	Mensual	5%	0%	Sistemas
SGSI5	Mantenimiento de Sistemas en CPDs	Seguridad Física	Sistemas sometidos a revisión de mantenimiento/inspección	Anual	90%	100%	Resp. Inmuebles
SGSI6	IPS	Comunicaciones	Falsos positivos/negativos detectados por el IPS (Sistema de Detección de Intrusión)	Mensual	95%	100%	Sistemas
SGSI7	Antivirus		Equipos sin antivirus o desactualizado		< 10%	< 5%	

* Para mayor detalle, ver Ilustración 19. Tabla Gestión de Indicadores de la memoria

Sistema de Gestión Documental – Proc. Revisión Dirección

Fase I | **Fase II** | Fase III | Fase IV | Fase V | Fase VI

Esta labor se ha de hacer con una periodicidad anual y ha de reflejar la evolución que ha tenido el Sistema durante este último año. De la misma manera que se realiza un Análisis Diferencial en el proceso de elaboración del SGSI, anualmente se tiene que conocer cuál es el estado con respecto a la revisión anterior. De esta manera, el informe deberá contener los siguientes aspectos:

- Estado de las acciones tomadas en la revisión anterior y su evolución.
- Cambios producidos en la organización que puedan afectar al SGSI. Por ejemplo, la existencia de nuevos procesos de negocio o activos.
- Informes relativos a las no conformidades que hubieran podido producir, acciones correctivas, indicadores relativos al cumplimiento con el sistema, resultado de auditorías internas/externas y cumplimiento con los objetivos de seguridad fijados.
- Apreciaciones del Comité de Seguridad.
- Evolución del plan de tratamiento de riesgos
- Oportunidades de mejora.

Sistema de Gestión Documental – Declaración Aplicabilidad

Seguridad 365

Fase I | **Fase II** | Fase III | Fase IV | Fase V | Fase VI

Medidas	SGSI	Aplica/No aplica	Justificación
Norma (ISO/IEC 27001:2013)			
4.	CONTEXTO DE LA ORGANIZACIÓN	Aplica	
4.1.	Comprensión de la organización y de su contexto.	Si	La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información.
4.2.	Compresión de las necesidades y expectativas de las partes interesadas.	Si	La organización debe determinar las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información; y los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.
4.3.	Determinación del alcance del sistema de gestión de seguridad de la información.	Si	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.
4.4.	Sistema de gestión de seguridad de la información (SGSI).	Si	La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información, de acuerdo con los requisitos de esta norma internacional.
5.	LIDERAZGO	Aplica	
5.1.	Liderazgo y compromiso.	Si	La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información.
5.2.	Política.	Si	La alta dirección debe establecer una política de seguridad de la información.

* Para mayor detalle, Anexo III de la memoria

Sistema de Gestión Documental – Metodología AR

Seguridad 365

Fase I | **Fase II** | Fase III | Fase IV | Fase V | Fase VI

Se fija la metodología para la realización del Análisis de Riesgos

Análisis de Riesgos – Identificación y Valoración de Activos

Seguridad 365

Fase I | Fase II | **Fase III** | Fase IV | Fase V | Fase VI

Inventario de Sistemas de Información y Activos asociados				
Ámbito	Clúster	Descripción	Activo Subordinado	Dependencia
Hardware	C1	Clúster de Servidores	Host	Muy Alta
	C1	Servidor de Base de Datos	SGBD	Muy Alta
	C1	Balanceador de Carga	Equipo virtual	Muy Alta
	C1	Sistema de Almacenamiento	Host	Muy Alta
	C1	Sistema Backup	Servicio de respaldo	Media
Aplicación	C1	Servidor de aplicaciones	Servidor de aplicaciones	Media
	C1	Servidores virtuales de aplicación	Granjas virtuales	Muy Alta
	C1	Servidor de base de datos	SGBD	Baja
Red	C1	Red interna	LAN	Media
	C1	Red externa	DMZ	Baja
Hardware	C2	Servidores físicos SQL	Host	Muy Alta
	C2	Sistema Back-Up	Servicio de respaldo	Muy Alta
Aplicación	C2	Servidor SQL	SGBD	Muy Alta
Red	C2	Red interna	LAN	Muy Alta
Personal	C1, C2	Desarrolladores	Personal	Media
	C1, C2	Técnicos de sistemas	Administradores	Muy Alta
	C1, C2	Usuarios de negocio	Usuarios internos	Muy Alta
Instalaciones	C1, C2	CPD principal	Locales protegidos	Muy Alta

Agrupación de Activos	
Sistema de Información	Clúster
Navision	C1
ProPlan365	C1
Portal del Empleado	C1
Guardian365	C1
PeopleSoft	C1
MasterCentral	C2
Exchange/SharePoint	C1

	Grados de Dependencia	
100%	Muy alta	Sería imposible trabajar en el activo dependiente
75%	Alta	Sería muy difícil trabajar en el activo dependiente
50%	Media	Se podría trabajan en el activo dependiente, pero con muchas dificultades.
25%	Baja	Se podría trabajan en el activo dependiente, no siendo su modo de operación óptimo.
0%	Muy Baja	No tienen ninguna afectación.

Análisis de Riesgos – Identificación y Valoración de Activos

Seguridad 365

Fase I | Fase II | **Fase III** | Fase IV | Fase V | Fase VI

Dimensión	Descripción
Confidencialidad	Revelación de información a personas no autorizadas
Integridad	Modificación de información por alguien no autorizado. Incluye el borrado o eliminación de datos.
Disponibilidad	Imposibilidad de acceso a la información o uso del servicio por parte del personal autorizado cuando lo necesita.
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Criterio	Descripción
Negocio	Perdidas económicas, daño para el negocio
Imagen	Daño reputacional/pérdida de imagen y confianza
Legal	Incumplimiento legal, normativo o regulatorio

	Valores posibles por cada Dimensión / Criterio	
9-10	**Muy alto**	Daño muy grave a la organización
7 - 9	**Alto**	Daño grave a la organización
4 - 6	**Medio**	Daño importante a la organización
1 - 3	**Bajo**	Daño menor a la organización
0	**Muy Bajo**	Despreciable irrelevante a efectos prácticos

Análisis de Riesgos – Identificación y Valoración de Activos

Seguridad 365

Fase I | Fase II | **Fase III** | Fase IV | Fase V | Fase VI

Tabla de Valoración de Activos

Sistema de Información	Confidencialidad			Integridad			Disponibilidad			Trazabilidad		
	Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal	Negocio	Imagen	Legal
Navision	MA	A	A	MA	A	A	MA	A	B	A	A	A
Guardian365	M	A	A	M	A	A	B	B	B	A	A	A
ProPlan365	MA	A	A	MA	A	A	MA	A	M	A	A	A
PeopleSoft	MA	A	A	MA	A	A	MA	A	M	A	A	A
Exchange/SharePoint	A	A	MA	A	A	MA	MA	A	B	A	A	A
Portal del Empleado	B	M	A	B	A	A	B	B	B	B	M	A
MasterCentral	A	MA	A	MA	MA	A	MA	MA	MA	A	A	A

Análisis de Riesgos – Identificación y Valoración de Amenazas

Seguridad 365

Fase I | Fase II | **Fase III** | Fase IV | Fase V | Fase VI

Basado en Magerit V3

Escala de Frecuencia

VALOR		CRITERIO
100%	Muy frecuente (MF)	La amenaza aparece a diario
75%	Frecuente (FR)	La amenaza aparece mensualmente
50%	Normal (No)	La amenaza aparece una vez al año
25%	Poco frecuente (PF)	La amenaza aparece cada varios años
0%	Nunca (NU)	La amenaza nunca aparece

Escala de Degradación

VALOR		CRITERIO
100%	Total	El activo resulta totalmente inservible
75%	Alta	Prácticamente inservible
50%	Media	Funcionalmente degradado, rendimiento bajo
25%	Baja	Ligera degradación que no impide el funcionamiento
0%	Despreciable	Activo en perfecto estado

* Para mayor detalle, ver Anexo IV de la memoria

Análisis de Riesgos – Identificación y Valoración de Amenazas

Seguridad 365

Fase I | Fase II | **Fase III** | Fase IV | Fase V | Fase VI

Extracto Tabla de Amenazas y Valoración sobre Activos

TABLA DE AMENAZAS Y VALORACIÓN SOBRE ACTIVOS							
Tipología	**Amenazas**		**Frec.**	**Conf.**	**Integ.**	**Disp.**	**Traz.**
[N] Desastres Naturales	N1	Fuego	PF	Baja	Baja	Total	Baja
	N2	Daños por agua	PF	Baja	Baja	Alta	Baja
[I] Origen Industrial	I1	Fuego	PF	Baja	Baja	Total	Baja
	I2	Daños por agua	PF	Baja	Baja	Alta	Baja
	I5	Avería de origen físico / lógico	FR	Baja	Baja	Total	Baja
	I6	Corte del suministro eléctrico	NO	Baja	Baja	Alta	Baja
	I7	Condiciones inadecuadas T/H	NO	Baja	Baja	Alta	Baja
	I8	Fallo de comunicaciones	NO	Media	Media	Total	Media
	I9	Interrupción otros servicios	FR	Baja	Baja	Total	Baja
	I10	Degradación soportes	NO	Baja	Baja	Alta	Baja

....

* Para mayor detalle, ver Ilustración 32. Tabla de Amenazas y Valoración sobre Activos de la memoria

Análisis de Riesgos – Mapa de Riesgos

Seguridad 365

Fase I | Fase II | **Fase III** | Fase IV | Fase V | Fase VI

Método de valoración

Se denomina riesgo a la medida del daño probable sobre el sistema de información. El riesgo se mide a través de una función del impacto y la frecuencia:

Riesgo = ℜ (impacto, frecuencia)

RIESGO		PROBABILIDAD				
		Muy Baja	Baja	Media	Alta	Muy Alta
IMPACTO	Muy Alto	5	6,25	7,5	8,75	10
	Alto	3,75	5	6,25	7,5	8,75
	Medio	2,5	3,75	5	6,25	7,5
	Bajo	1,25	2,5	3,75	5	6,25
	Muy Bajo	0	1,25	2,5	3,75	5

Análisis de Riesgos – Mapa de Riesgos

Seguridad 365

Fase I | Fase II | **Fase III** | Fase IV | Fase V | Fase VI

Extracto tabla de Riesgo Actual

Tipología	Amenazas		Activo						
			Navision	Guardian365	ProPlan365	PeopleSoft	Exchange / SharePoint	Portal del Empleado	MasterCentral
[N] Desastres Naturales	N1	Fuego	0,79	0,48	0,85	0,85	0,79	0,4	1,02
	N2	Daños por agua	0,69	0,44	0,73	0,73	0,69	0,36	0,86
[I] Origen Industrial	I1	Fuego	0,79	0,48	0,85	0,85	0,79	0,4	1,02
	I2	Daños por agua	0,69	0,44	0,73	0,73	0,69	0,36	0,86
	I5	Avería de origen físico / lógico	2,38	1,45	2,54	2,54	2,38	1,2	3,05
	I6	Corte del suministro eléctrico	1,38	0,89	1,46	1,46	1,38	0,72	1,72
	I7	Condiciones inadecuadas T/H	1,38	0,89	1,46	1,46	1,38	0,72	1,72
	I8	Fallo de comunicaciones	2,34	1,62	2,45	2,45	2,34	1,29	2,81
	I9	Interrupción otros servicios	2,38	1,45	2,54	2,54	2,38	1,2	3,05
	I10	Degradación soportes	1,38	0,89	1,46	1,46	1,38	0,72	1,72

* Para mayor detalle, ver ilustración 34. Tabla de Riesgo Actual de la memoria

Análisis de Riesgos – Mapa de Riesgos

Seguridad 365

Fase I | Fase II | **Fase III** | Fase IV | Fase V | Fase VI

Extracto tabla de Riesgo Residual

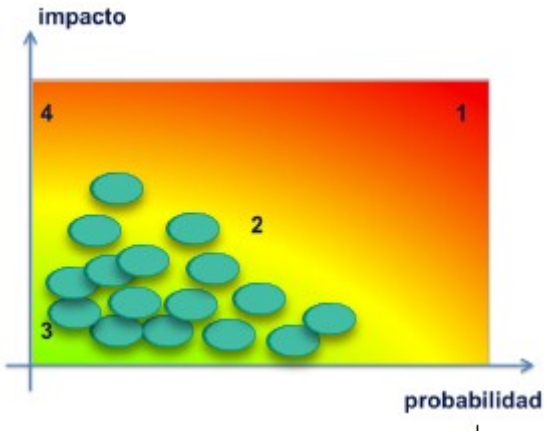
Tipología	Amenazas		Activo						
			Navision	Guardian365	ProPlan365	PeopleSoft	Exchange / SharePoint	Portal del Empleado	MasterCentral
[N] Desastres Naturales	N1	Fuego	0,24	0,14	0,26	0,26	0,24	0,24	0,31
	N2	Daños por agua	0,21	0,13	0,22	0,22	0,21	0,22	0,26
[I] Origen Industrial	I1	Fuego	0,24	0,14	0,26	0,26	0,24	0,24	0,31
	I2	Daños por agua	0,21	0,13	0,22	0,22	0,21	0,22	0,26
	I5	Avería de origen físico / lógico	0,71	0,44	0,76	0,76	0,71	0,36	0,92
	I6	Corte del suministro eléctrico	0,41	0,27	0,44	0,44	0,41	0,22	0,52
	I7	Condiciones inadecuadas T/H	0,41	0,27	0,44	0,44	0,41	0,22	0,52
	I8	Fallo de comunicaciones	0,70	0,49	0,74	0,74	0,70	0,39	0,84
	I9	Interrupción otros servicios	0,71	0,44	0,76	0,76	0,71	0,36	0,92
	I10	Degradación soportes	0,41	0,27	0,44	0,44	0,41	0,22	0,52

* Para mayor detalle, ver Ilustración 35. Tabla de Riesgo Residual de la memoria

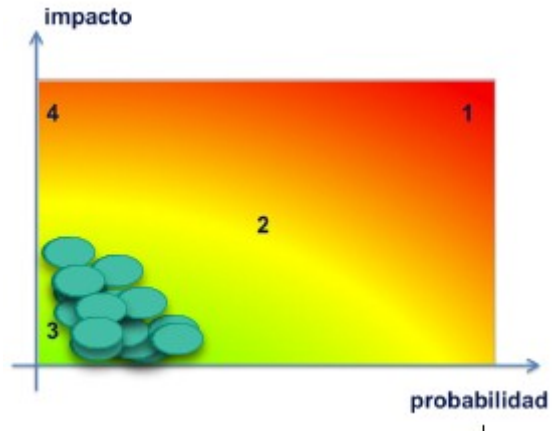
Análisis de Riesgos – Mapa de Riesgos

Fase I | Fase II | **Fase III** | Fase IV | Fase V | Fase VI

Conclusiones



Zona de Riesgo Actual



Zona de Riesgo Residual

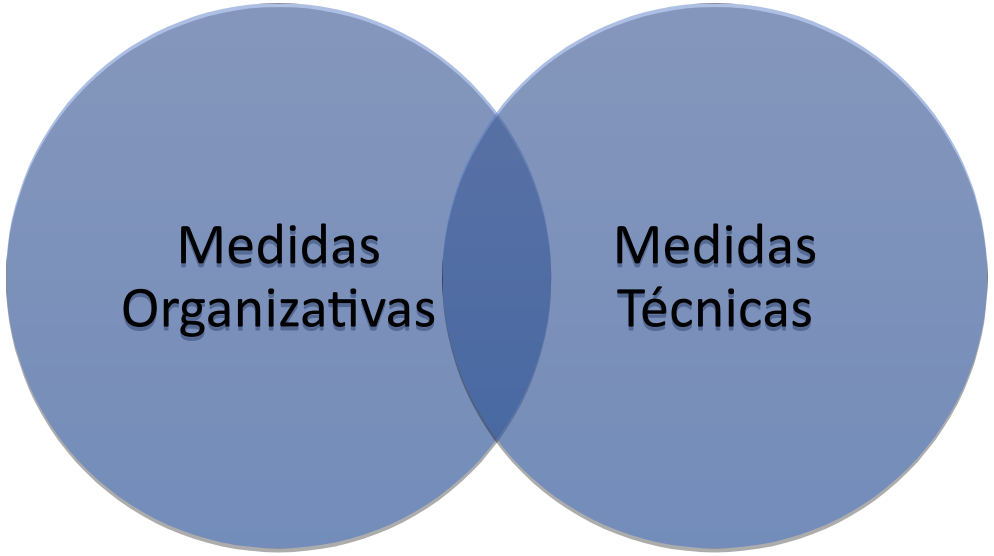
* Para mayor detalle, ver Ilustración 35. Tabla de Riesgo Residual de la memoria

Propuestas de Mejora

Seguridad 365

Fase I | Fase II | Fase III | **Fase IV** | Fase V | Fase VI

Tipos de medidas de mejora



Propuestas de Mejora

Fase I | Fase II | Fase III | **Fase IV** | Fase V | Fase VI

Ejemplo de proyecto de mejora en el ámbito organizativo

Código: **MO-1**	*Proyecto:* **Plan de formación y concienciación a empleados**	
Presupuesto: N/A - Recursos propios	*Inicio: 3/12/2018*	*Fin: 1/2/2019*
Apartado Normativo 4. Contexto de la Organización 5. Liderazgo 7. Soporte *Controles* Políticas de Seguridad (5.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Elaborar un plan formativo y de capacitación de los empleados para el tratamiento adecuado de los sistemas de información. Incluye una campaña de concienciación del tratamiento de los datos de compañía y en particular de los datos de carácter personal.		
Objetivos: Incorporar acciones formativas genéricas al plan de formación de la compañía. Contratar cursos específicos para personal técnico y/o de compliance (sistemas de Gestión) Elaborar y difundir boletines periódicos de seguridad, buscando el impacto inmediato		
Responsable: • Director de RRHH	*Miembros implicados:* • CEO • CISO • Responsable de formación	

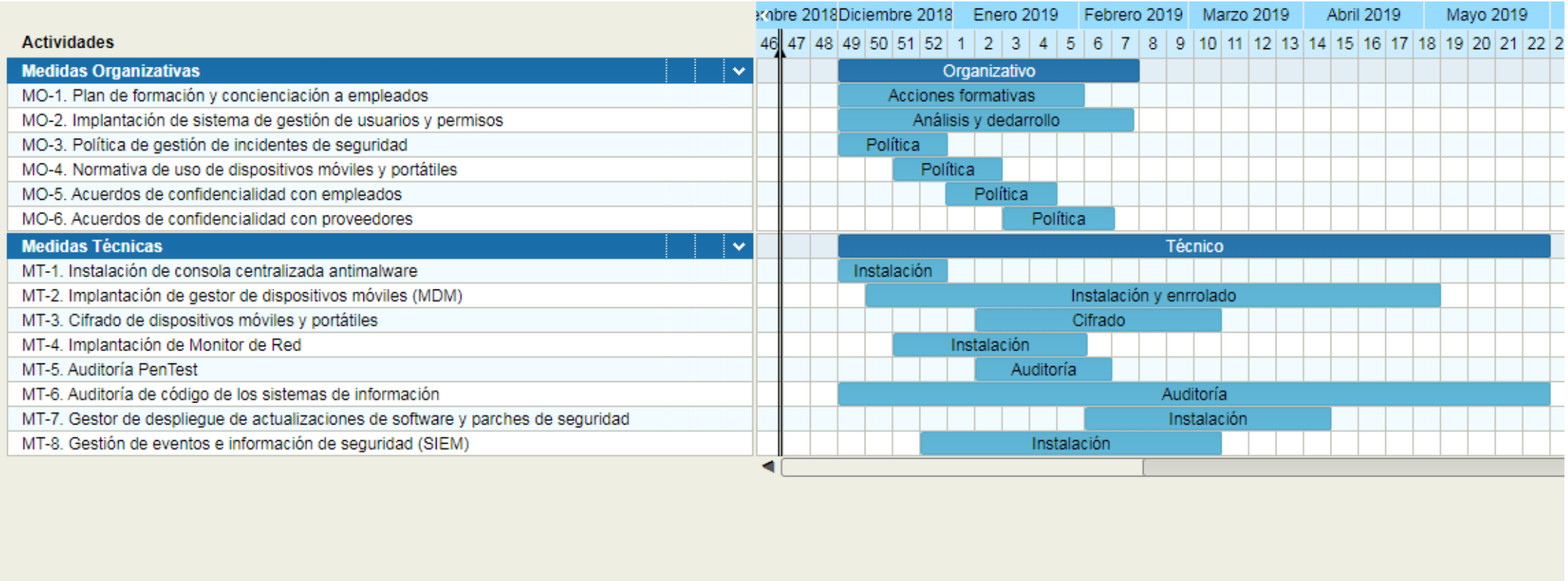
* Para mayor detalle, ver epígrafe 4.1 de la memoria

Propuestas de Mejora – Plan de Ejecución

Seguridad 365

Fase I | Fase II | Fase III | **Fase IV** | Fase V | Fase VI

Cronograma de proyectos



Auditoria de Cumplimiento

Seguridad 365

Fase I | Fase II | Fase III | Fase IV | **Fase V** | Fase VI

Metodología

Norma (ISO/IEC 27001:2013)	
4.	CONTEXTO DE LA ORGANIZACIÓN
5.	LIDERAZGO
6.	PLANIFICACIÓN
7.	SOPORTE
8.	OPERACIÓN
9.	EVALUACIÓN DEL DESEMPEÑO
10.	MEJORA

Aspectos relativos a las directrices dadas en la norma ISO/IEC 27001:2013

CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)	
5.	POLÍTICA DE SEGURIDAD
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
8.	GESTIÓN DE ACTIVOS
9.	CONTROL DE ACCESOS
10.	CIFRADO
11.	SEGURIDAD FÍSICA Y AMBIENTAL
12.	SEGURIDAD EN LA OPERATIVA
13.	SEGURIDAD EN LAS TELECOMUNICACIONES
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN
15.	RELACIONES CON SUMINISTRADORES
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN
17.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
18.	CUMPLIMIENTO

Aspectos relativos a los dominios y controles de la norma ISO/IEC 27002:2013

Auditoria de Cumplimiento

Fase I | Fase II | Fase III | Fase IV | **Fase V** | Fase VI

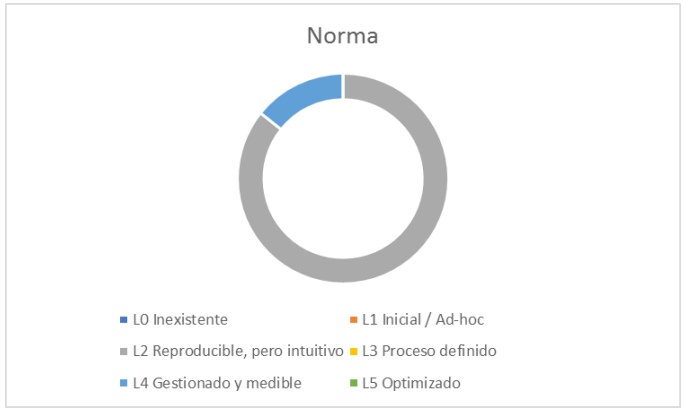
Medidas	SGSI	Actual		Inicial	
		Madurez	%	Madurez	%
Norma (ISO/IEC 27001:2013)					
4.	CONTEXTO DE LA ORGANIZACIÓN	L2	88 %	L1	40 %
5.	LIDERAZGO	L4	95 %	L1	20 %
6.	PLANIFICACIÓN	L2	85 %	L1	30 %
7.	SOPORTE	L2	78 %	L1	20 %
8.	OPERACIÓN	L2	72 %	L1	10 %
9.	EVALUACIÓN DEL DESEMPEÑO	L2	76 %	L1	10 %
10.	MEJORA	L2	83 %	L1	10 %
CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)					
5.	POLÍTICA DE SEGURIDAD	L4	97 %	L1	20 %
6.	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD	L2	86 %	L1	33 %
7.	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	L3	94 %	L1	46 %
8.	GESTIÓN DE ACTIVOS	L2	82 %	L1	39 %
9.	CONTROL DE ACCESOS	L2	68 %	L1	38 %
10.	CIFRADO	L2	80 %	L1	20 %
11.	SEGURIDAD FÍSICA Y AMBIENTAL	L4	95 %	L2	70 %
12.	SEGURIDAD EN LA OPERATIVA	L2	76 %	L1	39 %
13.	SEGURIDAD EN LAS TELECOMUNICACIONES	L2	84 %	L1	48 %
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	L2	58 %	L1	29 %
15.	RELACIONES CON SUMINISTRADORES	L3	93 %	L1	27 %
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	L2	69 %	L1	40 %
17.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	L4	98 %	L2	80 %
18.	CUMPLIMIENTO	L2	75 %	L1	36 %

* Para mayor detalle, ver epígrafe 4.1 de la memoria

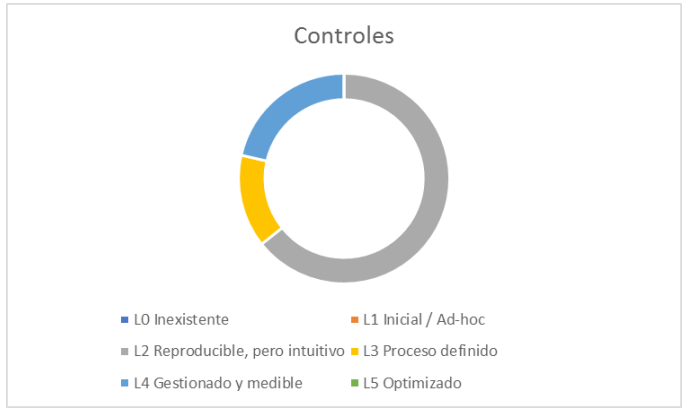
		Norma	Controles
L0	Inexistente	0	0
L1	Inicial / Ad-hoc	0	0
L2	Reproducible, pero intuitivo	6	9
L3	Proceso definido	0	2
L4	Gestionado y medible	1	3
L5	Optimizado	0	0

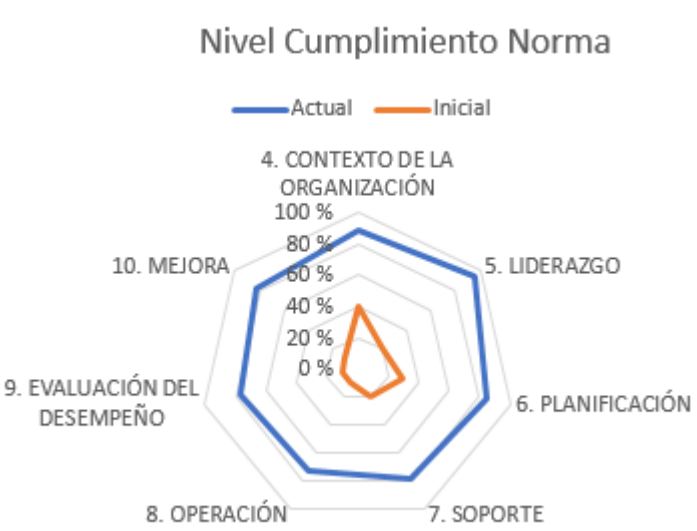
Auditoria de Cumplimiento

Fase I | Fase II | Fase III | Fase IV | **Fase V** | Fase VI

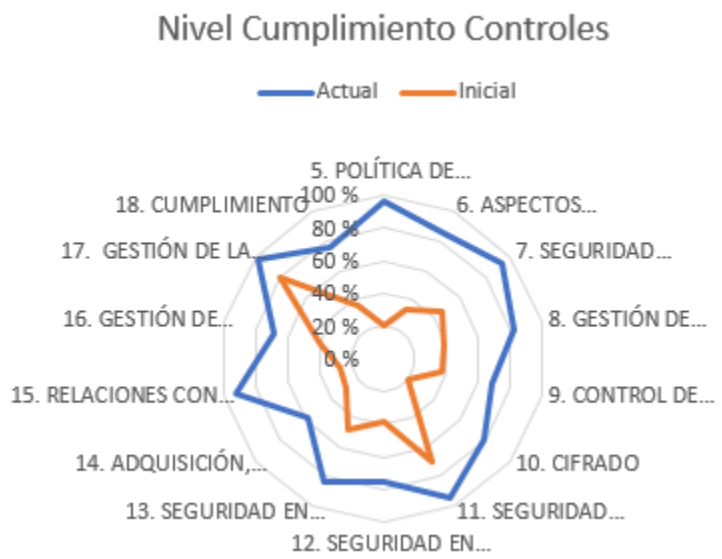


Madurez





Nivel de cumplimiento



Auditoria de Cumplimiento

Seguridad 365

Fase I | Fase II | Fase III | Fase IV | **Fase v** | Fase VI

Medidas	SGSI	Tipo	Comentario
Norma (ISO/IEC 27001:2013)			
4.	CONTEXTO DE LA ORGANIZACIÓN		
4.3.	Determinación del alcance del sistema de gestión de seguridad de la información.	Punto de mejora	Es recomendable definir más claramente el alcance en relación a las interfaces y dependencias entre las actividades realizadas por la organización y las realizadas por otras organizaciones. Esto debe quedar documentado claramente en la política de Seguridad.
5.	LIDERAZGO		
5.1.	Liderazgo y compromiso.	Punto de mejora	Aunque el compromiso de la Dirección es muy alto, se detecta la falta de asistencia por parte de la Dirección a las reunión del Comité de Seguridad. Sería conveniente demostrar el compromiso de la dirección con la asistencia a este tipo de reuniones.
6.	PLANIFICACIÓN		
6.1.	Acciones para tratar los riesgos y las oportunidades		
6.1.2.	Apreciación de riesgos de seguridad de la información.	Punto de mejora	Aunque se asume que la Dirección es el propietario del riesgo de todos los Sistemas de Información, es aconsejable definir propietarios más concretos. Por ejemplo, en el caso de Navision podría ser el Director Financiero. No obstante, se deja este extremo a criterio del Comité de Seguridad.
7.	SOPORTE		
7.2.	Competencia.	Punto de mejora	En algún caso, no se puede acreditar la realización del curso de concienciación por parte de alguno de los empleados. Se considera que son casos aislados, pero se recomienda poner especial cuidado en el seguimiento de la realización de este tipo de cursos.
8.	OPERACIÓN		
8.1.	Planificación y control operacional.	Observación	La organización debe garantizar que los procesos contratados externamente estén controlados. En este punto se recomienda dejar mejor documentados los procesos realizados por terceros.

CONTROLES DE SEGURIDAD (ISO/IEC 27002:2013)			
9.2.	Gestión de acceso de usuario:		
9.2.2.	Gestión de los derechos de acceso asignados a usuarios.	Observación	Si bien se ha implementado una aplicación para la gestión de accesos de los usuarios a los distintos sistemas de información, este desarrollo es muy incipiente y con varios puntos de mejora. Por ejemplo, se recomienda automatizar la relación jerárquica de los usuarios.
12.	SEGURIDAD EN LA OPERATIVA		
12.4.	Registro de actividad y supervisión:		
12.4.1.	Registro y gestión de eventos de actividad.	Punto de mejora	Se ha instalado una consola para el control del antivirus. No obstante, se detecta un porcentaje muy bajo de ordenadores que no están reportando su situación con relación a su estado de salud.
14.3.	Datos de prueba:		
14.3.1.	Protección de los datos utilizados en pruebas.	No conformidad menor	Se ha instalado una consola para el control del antivirus. No obstante, se detecta un porcentaje muy bajo de ordenadores que no están reportando su situación con relación a su estado de salud.
16.	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN		
16.1.	Gestión de incidentes de seguridad de la información y mejoras:		
16.1.2.	Notificación de los eventos de seguridad de la información.	No conformidad menor	De igual manera se ha diseñado un protocolo y un pequeño desarrollo en la plataforma SharePoint para el registro y notificación de incidentes de seguridad. En el tempo que lleva en marcha no se han registrado incidentes, aunque sí se han registrado incidentes sucedidos con anterioridad a la implantación del SGSI. Se detecta en algún caso haber excedido el tiempo fijado para la notificación de los incidentes a las autoridades competentes.

Presentación de Resultados

Seguridad 365

Fase I | Fase II | Fase III | Fase IV | Fase V | **Fase VI**

- **Memoria descriptiva** (*CatalaHernansaizJoseAlberto_TFM_Memoria.doc)*
- **Resumen Ejecutivo** (*CatalaHernansaizJoseAlberto_TFM_ResumenEjecutivo.pptx)*
- **Presentación a la dirección** (*CatalaHernansaizJoseAlberto_TFM_PresentaciónDirección.pptx)*
- **Concienciación Seguridad de la Información** (*CatalaHernansaizJoseAlberto_TFM_Concienciación.pptx)*
- **Estado de cumplimiento** (*CatalaHernansaizJoseAlberto_TFM_EstadoCumplimiento.pptx)*

Agradecimientos

A mi mujer y mis hijos. Esas personas a las que tanto quiero y las que tanto tiempo he quitado para sacar adelante este Master.

Y como no, a todos los consultores que siempre han tenido unas palabras de ánimo en esos momentos a los que a uno le fallan las fuerzas.

¡¡¡A todos, muchas gracias!!!

Seguridad 365

Gracias

UOC
Universitat Oberta de Catalunya

UAB
Universitat Autònoma de Barcelona

UNIVERSITAT ROVIRA i VIRGILI

UIB
Universitat de les Illes Balears