Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Elaboración de Plan de Implementación de la ISO/IEC 27001:2013

Alumno: Cristóbal Garrido Camargo
Director: Antonio José Segovia Henares

Introducción

- Objetivos TFM:

  Bases para la implantación SGSI acorde a la ISO/IEC 27001:2013

- Organización:

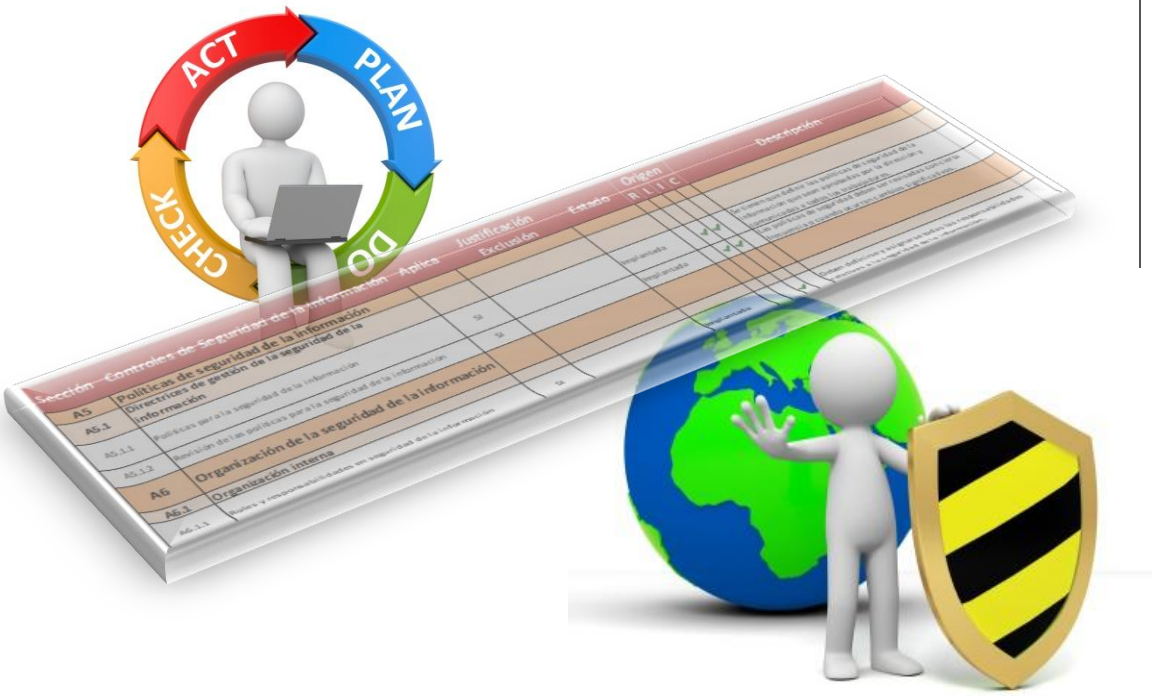
  Multinacional dedicada a servicios medioambientales de reciclaje: RecycleSA

- Presentación:

  Descripción del proceso realizado en el TFM.

Plan Implementación de la ISO/IEC 27001:2013

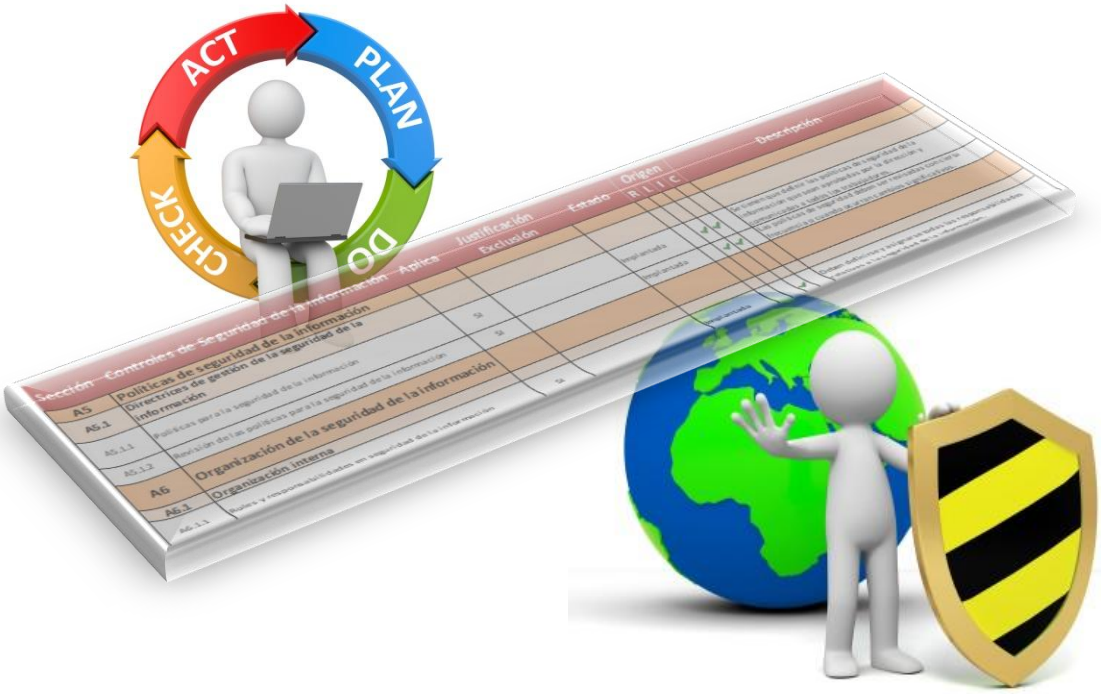
- Contexto.
- Alcance.
- Objetivos.
- Situación inicial.
- Sistema de gestión documental.
- Análisis de riesgos.
- Propuestas de proyectos.
- Auditoría de cumplimiento.
- Resultados y conclusiones



Contexto.

- Alcance.
- Objetivos.
- Situación inicial.
- Sistema de gestión documental.
- Análisis de riesgos.
- Propuestas de proyectos.
- Auditoría de cumplimiento.
- Resultados y conclusiones

Plan Implementación de la ISO/IEC 27001:2013



Contexto. Estructura Organizativa

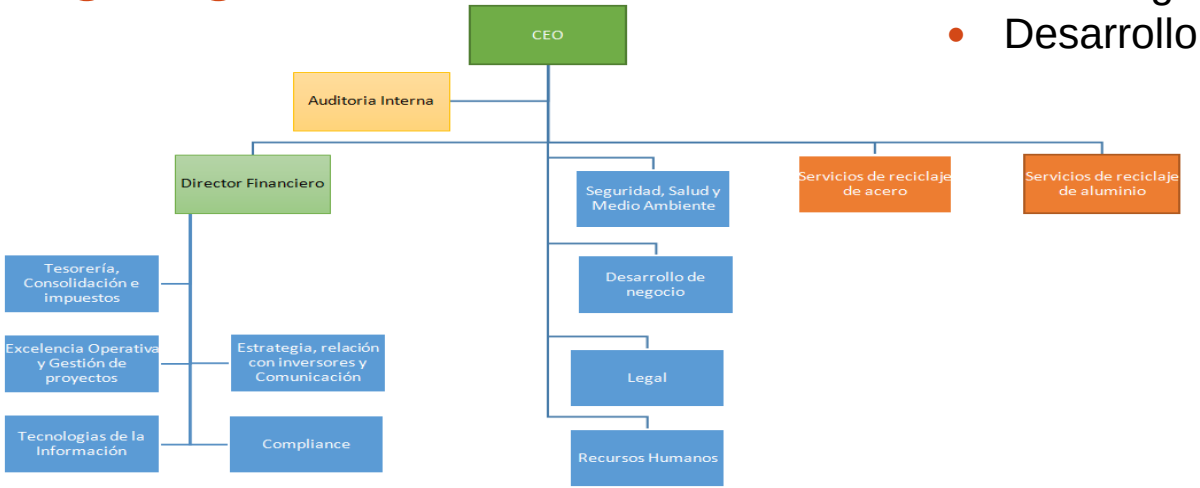
Unidades de negocio

- Reciclaje acero
- Reciclaje aluminio

Servicios adicionales

- Servicios financieros.
- Recursos Humanos.
- Legal.
- Seguridad y Medio Ambiente.
- Tecnologías de la información.
- Desarrollo de negocio

Organigrama

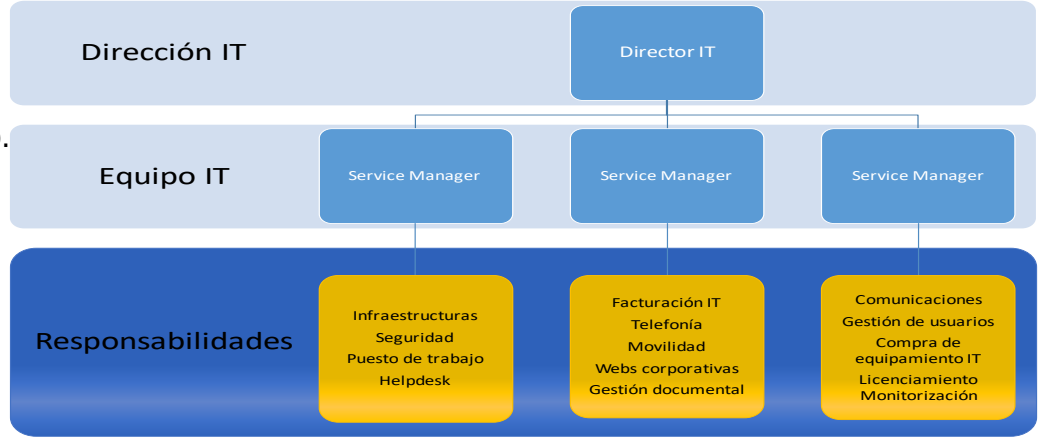


Contexto. Estructura Servicio IT

Servicios IT

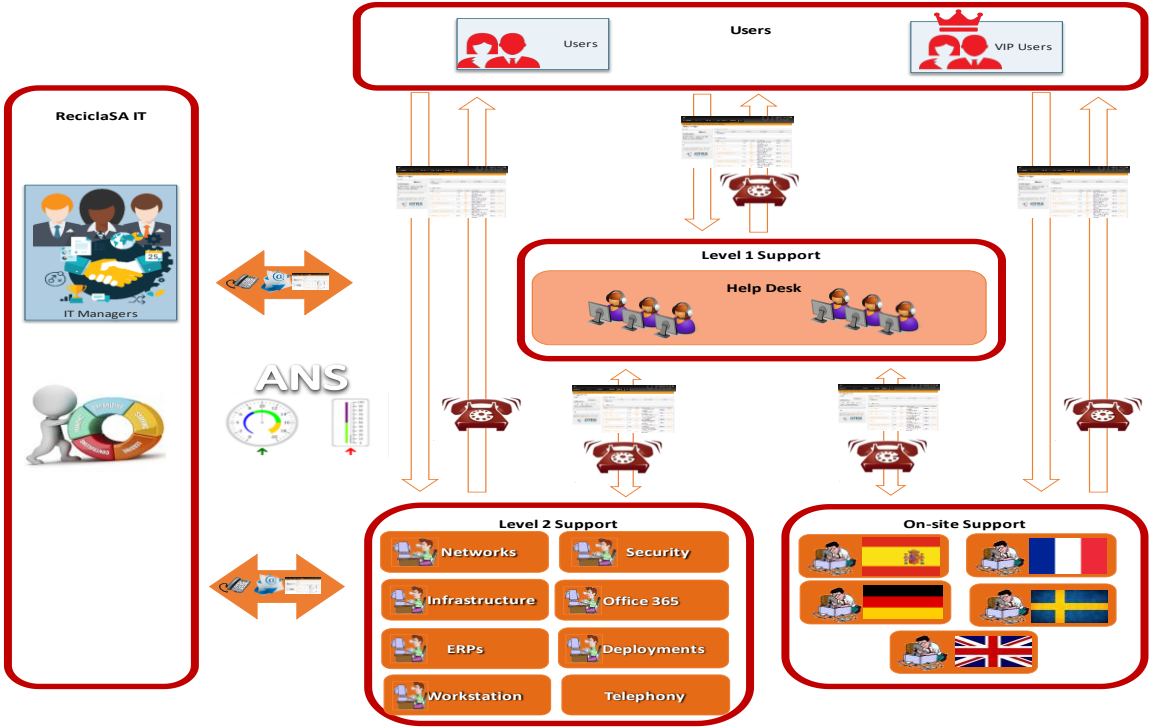
- Servicios de infraestructuras: servidores y almacenamiento.
- Servicios de comunicaciones y redes.
- Servicios de seguridad.
- Servicios de despliegue al puesto de trabajo.
- Servicios Office 365: Correo y Sharepoint.
- Servicios ERP: SAP y Navision.
- Servicios de telefonía.
- Servicios de soporte remoto al puesto de usuario.
- Servicios de soporte on-site.
- Servicios de Helpdesk.

Organigrama Dpto. IT



Contexto. Estructura Servicio soporte IT

Servicios Soporte IT



Contexto. Infraestructura Tecnológica. Sedes

Puestos de trabajo

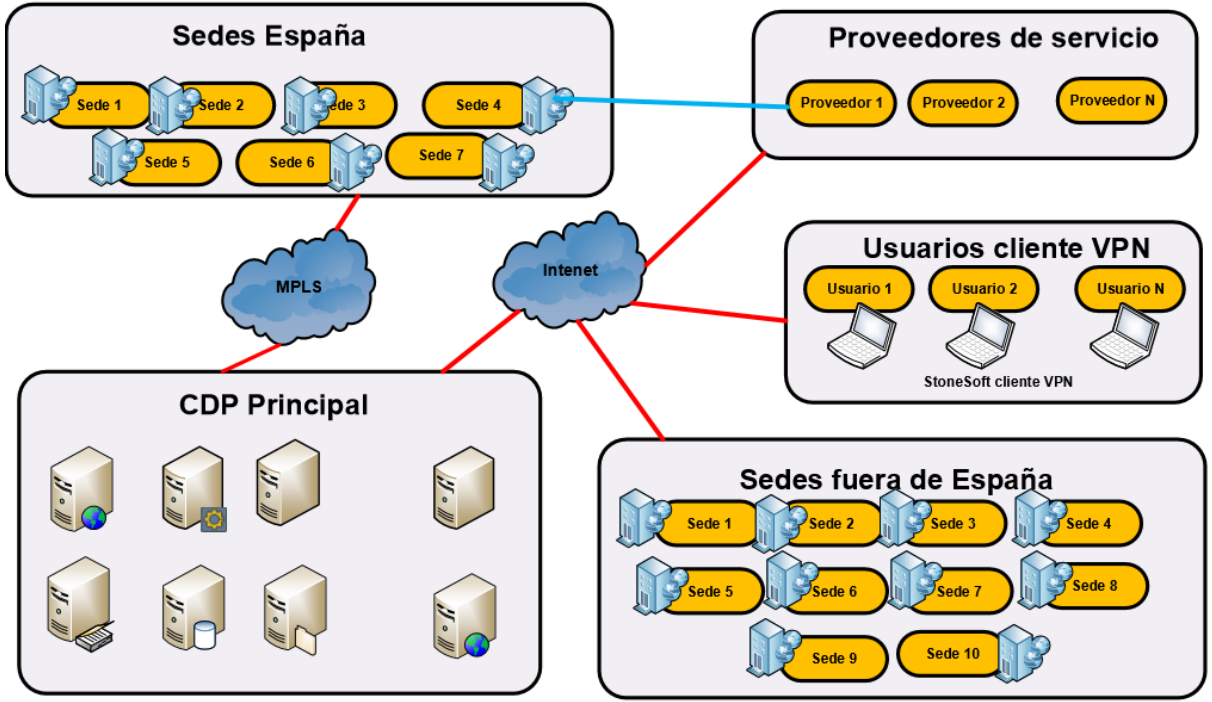
Sedes	PC	Portátil	Total
Alemania	**83**	**81**	**164**
Alemania-Sede 1	16	8	24
Alemania-Sede 2	15	10	25
Alemania-Sede 3	13	5	18
Alemania-Sede 4	14	11	25
Alemania-Sede 5	11	4	15
Alemania-Sede 6	14	43	57
Corea	**17**	**1**	**18**
Corea-Sede 1	17	1	18
España	**113**	**125**	**238**
España-Sede 1		7	7
España-Sede 2	35	44	79
España-Sede 3	31	34	65
España-Sede 4	20	7	27
España-Sede 5	10	15	25
España-Sede 6	3	4	7
España-Sede 7	14	14	28
Francia	**33**	**16**	**49**
Francia-Sede 1	33	16	49
Reino Unido	**14**	**10**	**24**
Reino Unido-Sede 1	14	10	24
Total	**260**	**233**	**493**

Servidores

Ubicación	Servidores Virtuales
Alemania	**18**
Alemania-Sede 1	3
Alemania-Sede 2	2
Alemania-Sede 3	3
Alemania-Sede 4	3
Alemania-Sede 5	3
Alemania-Sede 6	4
Corea	**3**
Corea-Sede 1	3
España	**64**
CPD Principal	56
España-Sede 2	2
España-Sede 4	6
Francia	**4**
Francia-Sede 1	4
Reino Unido	**3**
Reino Unido-Sede 1	3
Suecia	**2**
Suecia-Sede 1	2
Total general	**94**

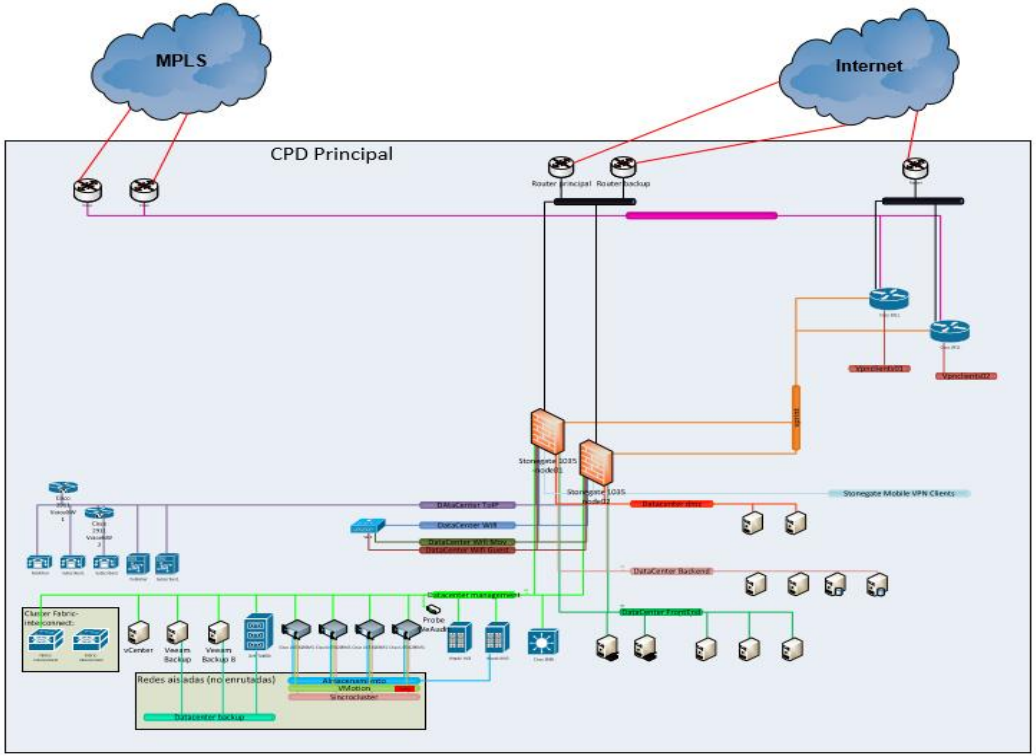
Contexto. Red de comunicaciones

Esquema global de comunicaciones



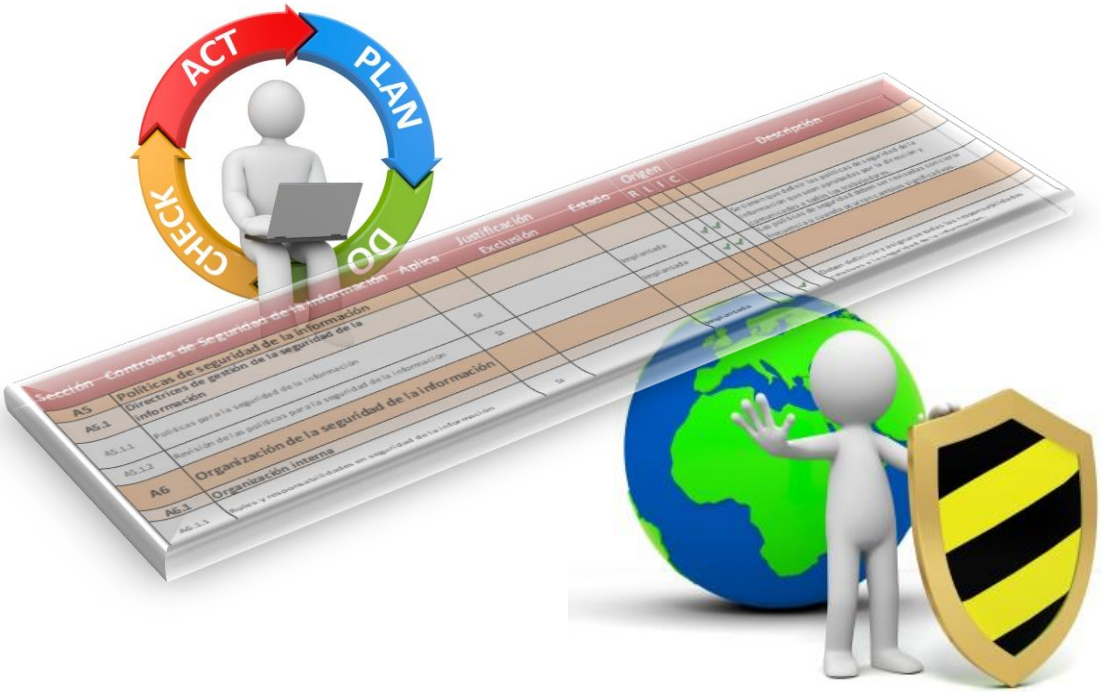
Contexto. Red de comunicaciones

Esquema red CPD principal



Plan Implementación de la ISO/IEC 27001:2013

- Contexto.
- Alcance.
- Objetivos.
- Situación inicial.
- Sistema de gestión documental.
- Análisis de riesgos.
- Propuestas de proyectos.
- Auditoría de cumplimiento.
- Resultados y conclusiones



Alcance SGSI

Sistemas de información

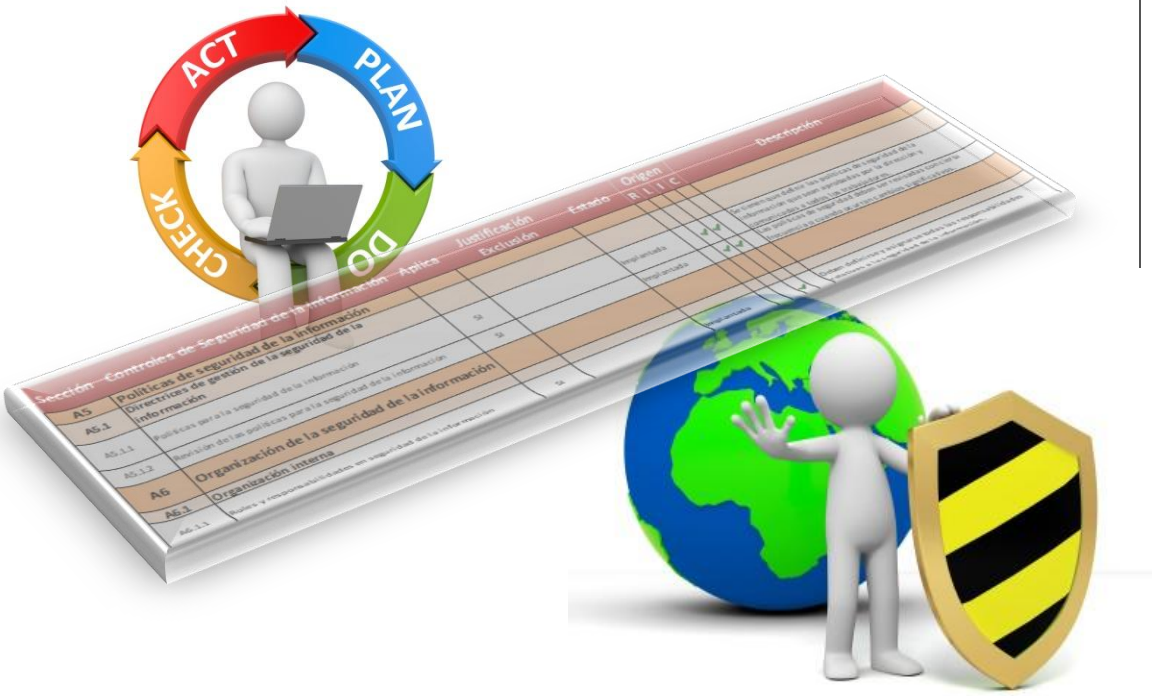
- Relativos a los procesos productivos de RecycleSA: Servicios de reciclaje.
- Servicios financieros.
- Recursos Humanos.
- Legal.
- Seguridad y Medio Ambiente.
- Desarrollo de negocio.
- Tecnologías de la información

Incluye

- Todos los activos relacionados con la información.
- Todos los procesos de negocio y de organización interna.
- Todos los procedimientos que el personal, tanto interno como externo, deben aplicar para la gestión de la información de la organización.

Plan Implementación de la ISO/IEC 27001:2013

- Contexto.
- Alcance.
- **Objetivos.**
- Situación inicial.
- Sistema de gestión documental.
- Análisis de riesgos.
- Propuestas de proyectos.
- Auditoría de cumplimiento.
- Resultados y conclusiones



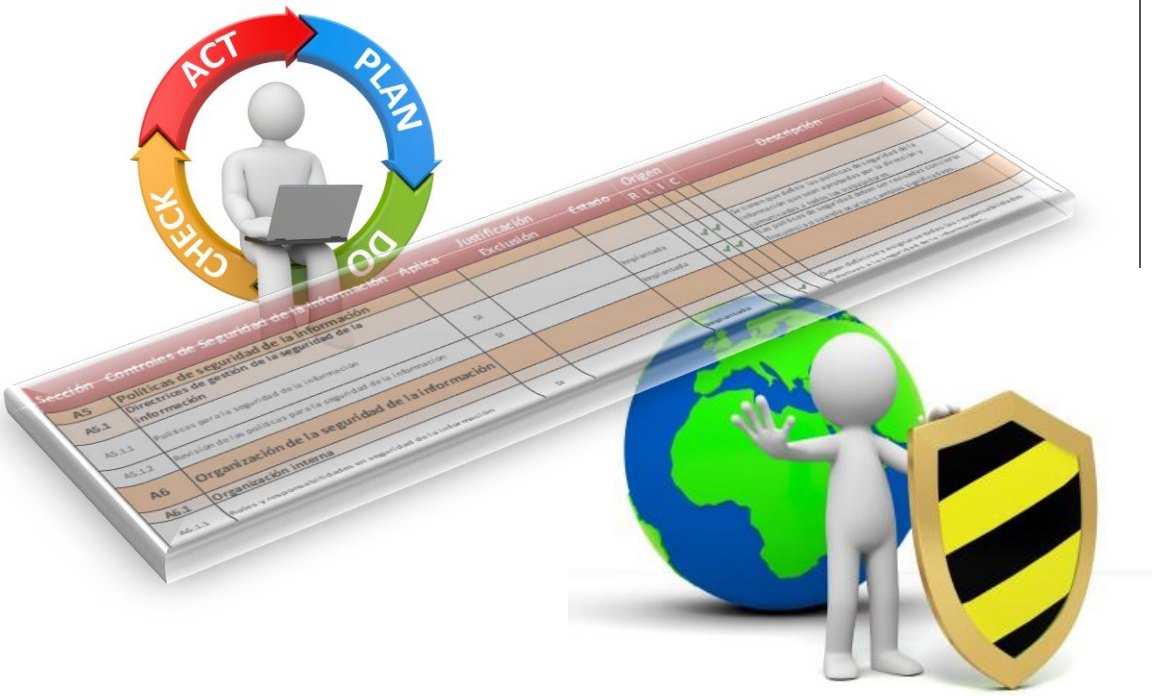
Objetivos

Objetivos Plan Director de Seguridad

- Promover la cultura de la seguridad.
- Involucrar a la Alta Dirección.
- Mejorar en la concienciación y formación del personal.
- Identificar los riesgos y amenazas.
- Definir los procesos y controles para garantizar la seguridad de la información.
- Reducir el riesgo para los activos de la organización.
- Mejorar la disponibilidad , integridad y confidencialidad de la información.
- Definir los roles y responsabilidades en materia de seguridad.
- Adecuar todos los procesos y sistemas al RGPD.
- Conseguir madurez los procesos que permita la expansión segura de la compañía.
- Superar auditorias de segundas partes que puedan requerir clientes e inversores.
- Mejora continua en lo relativo a la seguridad de información.

Plan Implementación de la ISO/IEC 27001:2013

- Contexto.
- Alcance.
- Objetivos.
- **Situación inicial.**
- Sistema de gestión documental.
- Análisis de riesgos.
- Propuestas de proyectos.
- Auditoría de cumplimiento.
- Resultados y conclusiones



Situación inicial. Análisis Diferencial

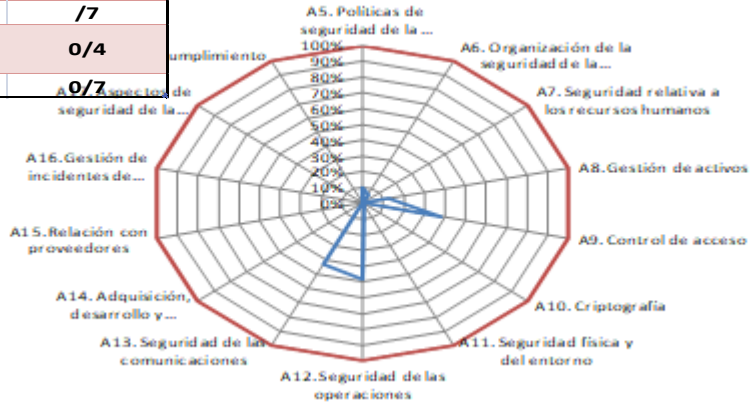
Evaluación madurez: CMM

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

Situación inicial. Análisis Diferencial

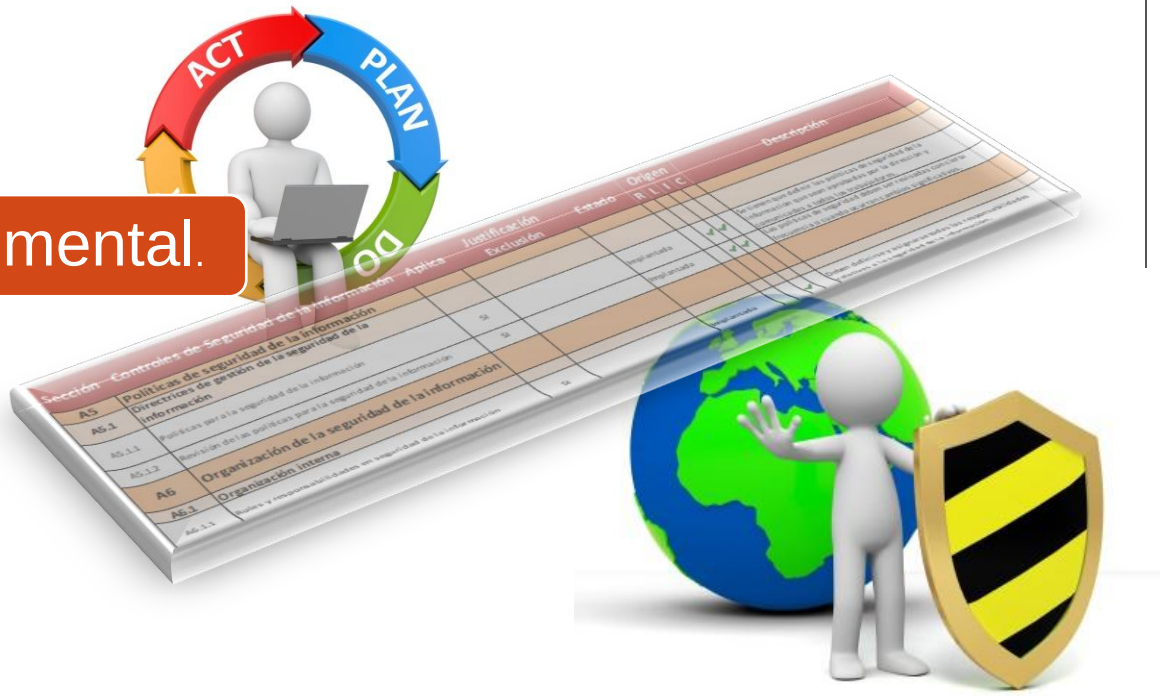
Evaluación efectividad controles ISO/IEC 27002:2013

Controles de Seguridad de la Información	Madurez	Implantados
A5. Políticas de seguridad de la información	10%	2/2
A6. Organización de la seguridad de la información	6%	3/7
A7. Seguridad relativa a los recursos humanos	0%	0/6
A8. Gestión de activos	13%	3/10
A9. Control de acceso	38%	12/14
A10. Criptografía	0%	0/2
A11. Seguridad física y del entorno	1%	2/15
A12. Seguridad de las operaciones	49%	13/14
A13. Seguridad de las comunicaciones	43%	3/7
A14. Adquisición, desarrollo y mantenimiento de los sistemas de información	0%	0/14
A15. Relación con proveedores	0%	0/5
A16. Gestión de incidentes de seguridad de la información	0%	/7
A17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	0%	0/4
A18. Cumplimiento	0%	0/7



Plan Implementación de la ISO/IEC 27001:2013

- Contexto.
- Alcance.
- Objetivos.
- Situación inicial.
- **Sistema de gestión documental.**
- Análisis de riesgos.
- Propuestas de proyectos.
- Auditoría de cumplimiento.
- Resultados y conclusiones



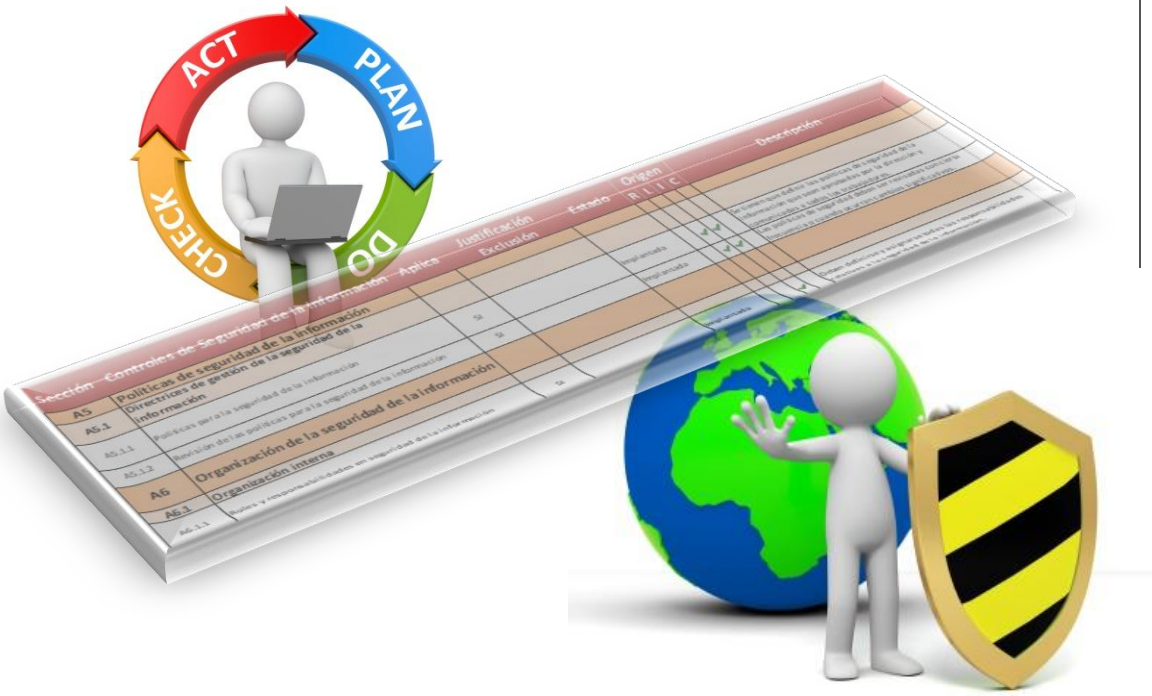
Sistema de gestión documental

Documentos desarrollados

- Política de Seguridad.
- Procedimiento de Auditorías Internas.
- Gestión de Indicadores.
- Procedimiento de Revisión por la Dirección.
- Gestión de Roles y Responsabilidades.
- Metodología de Análisis de Riesgo: Magerit.
- Declaración de Aplicabilidad.

Plan Implementación de la ISO/IEC 27001:2013

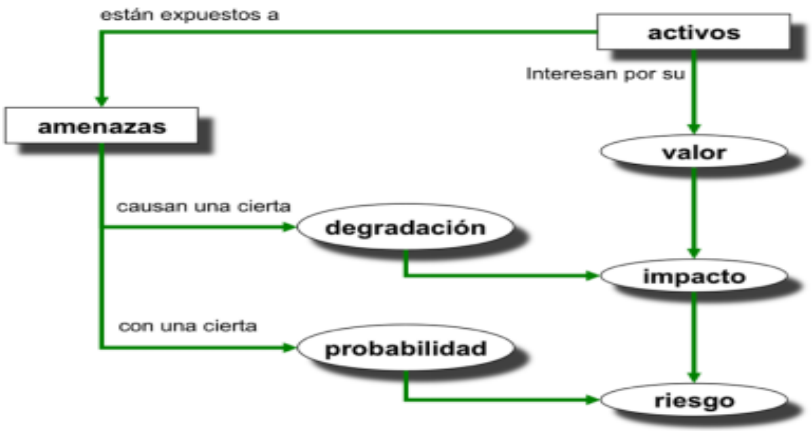
- Contexto.
- Alcance.
- Objetivos.
- Situación inicial.
- Sistema de gestión documental.
- **Análisis de riesgos.**
- Propuestas de proyectos.
- Auditoría de cumplimiento.
- Resultados y conclusiones



Análisis de Riesgos. Metodología Magerit

Pasos

- Determinar los **activos** relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación
- Determinar a qué **amenazas** están expuestos aquellos activos
- Determinar qué **salvaguarda**s hay dispuestas y cuán eficaces son frente al riesgo
- Estimar el **impacto**, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el **riesgo**, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.



Análisis de Riesgos. Metodología Magerit

Activos: Clasificación Magerit

- **Datos** que materializan la información.
- **Servicios auxiliares** que se necesitan para poder organizar el sistema.
- Las **aplicaciones** informáticas (software) que permiten manejar los datos.
- **Los equipos informáticos (hardware)** y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
- **Las personas que explotan u operan** todos los elementos anteriormente citados.

Tipo Activo	Identificador
Instalaciones	L
Hardware	HW
Aplicación/Software	SW
Datos/Información	D
Redes de comunicación	COM
Servicios	S
Soportes de información	M
Equipamiento auxiliar	AUX
Personal	P

Análisis de Riesgos. Valoración activos

Tabla valoración activos

Tipo Activo	ID Activo	Activo	Aspectos críticos				
			A	C	I	D	T
Instalaciones [L]	[L.1]	CPD	9	9	9	10	8
	[L.2]	Sala Técnica Sede	9	7	7	10	3
	[L.3]	Despacho Directivo	8	9	8	7	5
	[L.4]	Oficinas	2	6	7	7	2
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	9	9	9	9	7
	[HW.2]	Firewall CPD	9	9	9	9	7
	[HW.3]	Swithes CPD	8	7	9	9	7
	[HW.4]	Servidores hypervisor Sedes	7	7	7	7	6
	[HW.5]	Switches/routers Sedes	6	6	7	7	6
	[HW.6]	Puntos de acceso Wifi	5	6	5	3	4
	[HW.7]	PCs usuarios	7	7	5	5	6
	[HW.8]	Portátiles usuarios	7	7	5	5	6
	[HW.9]	Dispositivos móviles corporativos	6	6	4	3	6
	[HW.10]	Dispositivos móviles personales	5	6	4	3	6
	[HW.11]	Teléfonos IPs	3	2	2	3	4
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare	8	8	8	9	5
	[SW.2]	Sistema operativos Windows Server	8	8	8	8	5
	[SW.3]	Sistema operativos Linux Server	7	8	7	6	5
	[SW.4]	Software backup: Veeam backup	8	9	8	2	7
	[SW.5]	Sistema operativo Windows 7	6	7	4	7	3
	[SW.6]	Sistema operativo Windows 10	6	7	4	7	3
	[SW.7]	Sistema operativo android	5	6	3	3	3
	[SW.8]	Sistema operativo IOS	5	7	3	3	3
	[SW.9]	Directorio Activo Microsoft	6	6	9	9	6
	[SW.10]	BBDD Microsoft SQL Server	7	8	8	6	7
	[SW.11]	BBDD Oracle	7	8	8	8	7
	[SW.12]	Microsoft SCCM	5	6	4	6	6
	[SW.13]	Herramienta de ticketing: OTRS	5	6	4	8	7
	[SW.14]	Antivirus Symantec	3	3	5	7	6
	[SW.15]	Intranet corporativa	7	8	7	7	7
	[SW.16]	Web corporativa	7	6	9	6	8
	[SW.17]	SAP	8	9	8	8	8
	[SW.18]	Navision	8	9	8	8	8
	[SW.19]	Contaplus	6	7	6	5	5
	[SW.20]	Software puesto usuario: office 365, antivirus, acrobat	3	7	5	5	3
	[SW.21]	Aplicaciones Office 365: Correo, one drive, skype,...	6	8	5	7	6
	[SW.22]	Aplicaciones Sharepoint Office 365	7	8	6	7	6

Tipo Activo	ID Activo	Activo	Aspectos críticos				
			A	C	I	D	T
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos	8	9	8	7	6
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus	9	9	9	8	8
	[D.3]	Bases de datos RRHH	9	9	8	8	8
	[D.4]	LDAP: Directorio Activo Microsoft	7	7	8	9	7
	[D.5]	Copias de seguridad	7	9	7	3	7
Comunicaciones [D]	[COM.1]	Red internet	7	8	8	9	7
	[COM.2]	Red MPLS	7	8	8	8	7
	[COM.3]	Red local CPD	8	9	9	9	7
	[COM.4]	Red local sedes	6	7	7	7	6
	[COM.5]	Red wifi invitados sedes	2	3	3	3	2
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)	3	3	3	4	3
	[COM.7]	Red wifi usuarios	3	7	3	5	3
	[COM.8]	Red telefonía IP	0	0	2	7	0
	[COM.9]	Red telefonía móvil	0	0	2	8	0
Servicios [S]	[S.1]	Servicio ERP	8	9	9	8	7
	[S.2]	Servicio correo	7	9	8	9	7
	[S.3]	Servicio de telefonía	0	3	0	8	0
	[S.4]	Servicio de ficheros	7	8	8	7	7
	[S.5]	Servicio de acceso remoto	6	8	6	6	6
	[S.6]	Servicio de backup	8	9	8	6	8
Soportes de Información [M]	[M.1]	Almacenamiento CPD	9	9	9	9	7
	[M.2]	Almacenamiento Sedes	7	7	7	7	6
	[M.3]	Memorias USB	2	6	3	2	2
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico	0	0	8	9	0
	[AUX.2]	Aire acondicionado Salas técnicas	0	0	7	6	0
	[AUX.3]	Sistemas antiincidencios	0	0	8	8	0
	[AUX.4]	Cableado LAN	0	0	6	9	0
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Financiero	0	0	0	9	0
	[P.2]	Personal TI	0	0	0	8	0
	[P.3]	Personal Proveedor TI	0	0	0	7	0
	[P.4]	Resto de personal	0	0	0	3	0

Análisis de Riesgos. Amenazas

Clasificación

Grupo	Identificador
Desastres Naturales	[N]
De origen Industrial	[I]
Errores y fallos no intencionados	[E]
Ataques Intencionados	[A]

Frecuencia

ID	Vulnerabiliad	Frecuencia
MA	Muy Alta	A diario
A	Alta	Mensualmente
M	Media	Cada 6 meses
B	Baja	Cada año
MB	Muy Baja	Cada 5 años

Impacto

Impacto	ID	Valor
Muy Alto	MA	100%
Alto	A	75%
Medio	M	50%
Bajo	B	20%
Muy Bajo	MB	5%

Análisis de Riesgos. Amenazas

Impactos máximos por grupo de activos

	Impacto				
Activo	A	C	I	D	T
Aplicación/Software [SW]	75%	100%	100%	100%	
Datos/Información [D]	100%	100%	100%	100%	100%
Equipamiento auxiliar [AUX]		20%	20%	100%	
Hardware [HW]		100%	50%	100%	
Instalaciones [L]		20%	20%	100%	
Personal [P]		75%	20%	100%	
Redes de comunicación [COM]	75%	100%	75%	100%	
Servicios [S]	75%	75%	75%	100%	75%
Soportes de información [M]		100%	50%	100%	

Impacto potencial

			Aspectos críticos					Impacto					Impacto potencial				
Tipo Activo	ID Activo	Activo	A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
Instalaciones [L]	[L.1]	CPD	9	9	9	10	8	0%	20%	20%	100%	0%	0,00	1,80	1,80	10,00	0,00
	[L.2]	Sala Técnica Sede	9	7	7	10	3	0%	20%	20%	100%	0%	0,00	1,40	1,40	10,00	0,00
	[L.3]	Despacho Directivo	8	9	8	7	5	0%	20%	20%	100%	0%	0,00	1,80	1,60	7,00	0,00
	[L.4]	Oficinas	2	6	7	7	2	0%	20%	20%	100%	0%	0,00	1,20	1,40	7,00	0,00
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	9	9	9	9	7	0%	100%	50%	100%	0%	0,00	9,00	4,50	9,00	0,00
	[HW.2]	Firewall CPD	9	9	9	9	7	0%	100%	50%	100%	0%	0,00	9,00	4,50	9,00	0,00
	[HW.3]	Swithes CPD	8	7	9	9	7	0%	100%	50%	100%	0%	0,00	7,00	4,50	9,00	0,00
	[HW.4]	Servidores hypervisor Sedes	7	7	7	7	6	0%	100%	50%	100%	0%	0,00	7,00	3,50	7,00	0,00
	[HW.5]	Switches/routers Sedes	6	6	7	7	6	0%	100%	50%	100%	0%	0,00	6,00	3,50	7,00	0,00
	[HW.6]	Puntos de acceso Wifi	5	6	5	3	4	0%	100%	50%	100%	0%	0,00	6,00	2,50	3,00	0,00
	[HW.7]	PCs usuarios	7	7	5	5	6	0%	100%	50%	100%	0%	0,00	7,00	2,50	5,00	0,00

Análisis de Riesgos. Riesgos

Escala cualitativa

Riesgo
Muy Alto
Alto
Medio
Bajo
Muy Bajo

Nivel de riesgo

Nivel de riesgo = Impacto potencial x frecuencia de la amenaza.

Riesgo			Frecuencia				
			Muy Alta	Alta	Media	Baja	Muy Baja
			MA	A	M	B	MB
Impacto	Muy Alto	MA	MA	MA	MA	MA	A
	Alto	A	MA	MA	A	A	M
	Medio	M	A	A	M	M	B
	Bajo	B	M	M	B	B	MB
	Muy Bajo	MB	B	B	MB	MB	MB

Análisis de Riesgos. Riesgos

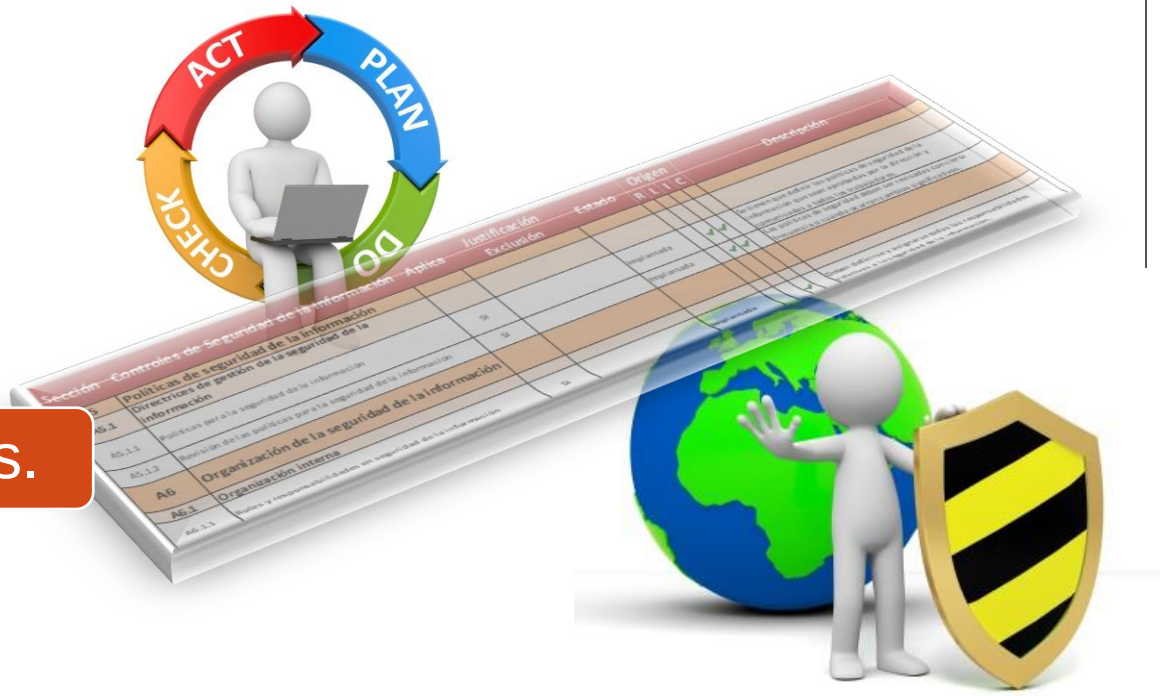
Tabla de Riesgos por activo

Tipo Activo	ID Activo	Activo	Riesgo A	Riesgo C	Riesgo I	Riesgo D	Riesgo T
Instalaciones [L]	[L.1]	CPD	MB	MB	MB	MA	MB
	[L.2]	Sala Técnica Sede	MB	MB	MB	MA	MB
	[L.3]	Despacho Directivo	MB	MB	MB	M	MB
	[L.4]	Oficinas	MB	MB	MB	M	MB
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	B	MA	A	MA	B
	[HW.2]	Firewall CPD	B	MA	A	MA	B
	[HW.3]	Swithes CPD	B	A	A	MA	B
	[HW.4]	Servidores hypervisor Sedes	B	A	M	A	B
	[HW.5]	Switches/routers Sedes	B	A	M	A	B
	[HW.6]	Puntos de acceso Wifi	B	A	M	M	B
	[HW.7]	PCs usuarios	B	A	M	A	B
	[HW.8]	Portátiles usuarios	B	A	M	A	B
	[HW.9]	Dispositivos móviles corporativos	B	A	B	M	B
	[HW.10]	Dispositivos móviles personales	B	A	B	M	B
	[HW.11]	Teléfonos IPs	B	B	B	M	B
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare	A	MA	MA	MA	B
	[SW.2]	Sistema operativos Windows Server	A	MA	MA	MA	B
	[SW.3]	Sistema operativos Linux Server	A	MA	A	A	B
	[SW.4]	Software backup: Veeam backup	A	MA	MA	B	B
	[SW.5]	Sistema operativo Windows 7	A	A	M	A	B
	[SW.6]	Sistema operativo Windows 10	A	A	M	A	B
	[SW.7]	Sistema operativo android	M	A	M	M	B
	[SW.8]	Sistema operativo IOS	M	A	M	M	B
	[SW.9]	Directorio Activo Microsoft	A	A	MA	MA	B
	[SW.10]	BBDD Microsoft SQL Server	A	MA	MA	A	B
	[SW.11]	BBDD Oracle	A	MA	MA	MA	B
	[SW.12]	Microsoft SCCM	M	A	M	A	B
	[SW.13]	Herramienta de ticketing: OTRS	M	A	M	MA	B
	[SW.14]	Antivirus Symantec	M	M	A	A	B
	[SW.15]	Intranet corporativa	A	MA	A	A	B
	[SW.16]	Web corporativa	A	A	MA	A	B
	[SW.17]	SAP	A	MA	MA	MA	B
	[SW.18]	Navision	A	MA	MA	MA	B
	[SW.19]	Contaplus	A	A	A	A	B
	[SW.20]	Software puesto usuario: office 365, antivirus, acrobat	M	A	A	A	B
	[SW.21]	Aplicaciones Office 365: Correo, one drive, skype,...	A	MA	A	A	B
	[SW.22]	Aplicaciones Sharepoint Office 365	A	MA	A	A	B

Tipo Activo	ID Activo	Activo	Riesgo A	Riesgo C	Riesgo I	Riesgo D	Riesgo T
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos	MA	MA	MA	A	A
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus	MA	MA	MA	MA	MA
	[D.3]	Bases de datos RRHH	MA	MA	MA	MA	MA
	[D.4]	LDAP: Directorio Activo Microsoft	A	A	MA	MA	A
	[D.5]	Copias de seguridad	A	MA	A	M	A
Comunicaciones [D]	[COM.1]	Red internet	A	MA	A	MA	B
	[COM.2]	Red MPLS	A	MA	A	MA	B
	[COM.3]	Red local CPD	A	MA	A	MA	B
	[COM.4]	Red local sedes	A	A	A	A	B
	[COM.5]	Red wifi invitados sedes	B	M	M	M	B
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)	M	M	M	M	B
	[COM.7]	Red wifi usuarios	M	A	M	A	B
	[COM.8]	Red telefonía IP	B	B	B	A	B
	[COM.9]	Red telefonía móvil	B	B	B	MA	B
Servicios [S]	[S.1]	Servicio ERP	A	A	A	MA	A
	[S.2]	Servicio correo	A	A	A	MA	A
	[S.3]	Servicio de telefonía	B	M	B	MA	B
	[S.4]	Servicio de ficheros	A	A	A	A	A
	[S.5]	Servicio de acceso remoto	A	A	A	A	A
	[S.6]	Servicio de backup	A	A	A	A	A
Soportes de Información [M]	[M.1]	Almacenamiento CPD	B	MA	A	MA	B
	[M.2]	Almacenamiento Sedes	B	A	M	A	B
	[M.3]	Memorias USB	B	A	B	B	B
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico	B	B	B	MA	B
	[AUX.2]	Aire acondicionado Salas técnicas	B	B	B	A	B
	[AUX.3]	Sistemas antiincendios	B	B	B	MA	B
	[AUX.4]	Cableado LAN	B	B	B	MA	B
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Financiero	B	B	B	MA	B
	[P.2]	Personal TI	B	B	B	MA	B
	[P.3]	Personal Proveedor TI	B	B	B	A	B
	[P.4]	Resto de personal	B	B	B	M	B

Plan Implementación de la ISO/IEC 27001:2013

- Contexto.
- Alcance.
- Objetivos.
- Situación inicial.
- Sistema de gestión documental.
- Análisis de riesgos.
- **Propuestas de proyectos.**
- Auditoría de cumplimiento.
- Resultados y conclusiones



Proyectos. Propuestas

En base a:

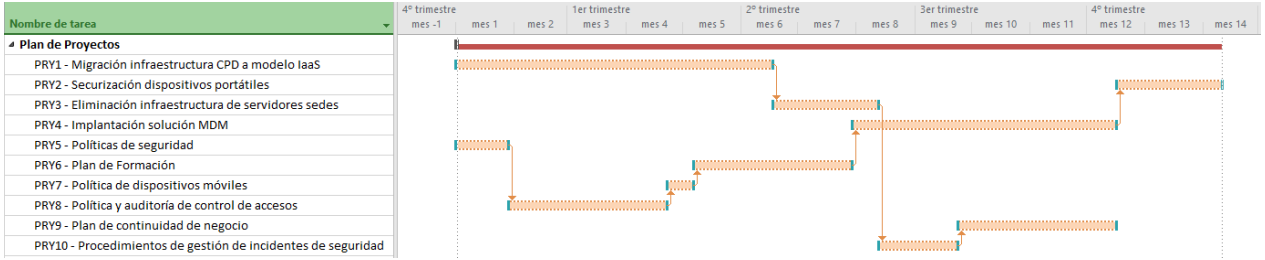
- Análisis de riesgos, amenazas, análisis diferencial.
- Recursos TI limitados.
- Espacio temporal un año.

Ámbto	ID	Proyecto
Tecnológico	PRY1	Migración infraestructura CPD a modelo IaaS
	PRY2	Securización dispositivos portátiles
	PRY3	Eliminación infraestructura de servidores sedes
	PRY4	Implantación solución MDM
Organizativo/Gestión	PRY5	Políticas de seguridad
	PRY6	Plan de Formación
	PRY7	Política de dispositivos móviles
	PRY8	Política y auditoría de control de accesos
	PRY9	Plan de continuidad de negocio
	PRY10	Procedimientos de gestión de incidentes de seguridad

Proyectos. Planificación

Criterios y condicionantes

- Migración CPD ya iniciada.
- Prioridad Política Seguridad
- Políticas de control accesos y dispositivos móviles
- Formación y concienciación previa a proyectos que afecten a los usuarios.



Proyectos. Reducción de impactos

Impactos máximos por grupo de activos

	Impacto				
Activo	A	C	I	D	T
Aplicación/Software [SW]	75%	100%	100%	75%	
Datos/Información [D]	100%	100%	100%	100%	100%
Equipamiento auxiliar [AUX]		20%	20%	100%	
Hardware [HW]		75%	50%	75%	
Instalaciones [L]		20%	20%	75%	
Personal [P]		75%	20%	75%	
Redes de comunicación [COM]	75%	100%	75%	100%	
Servicios [S]	75%	75%	75%	75%	75%
Soportes de información [M]		100%	50%	100%	

Proyectos. Resultados esperados

Evaluación de riesgos

Tipo Activo	ID Activo	Activo	Riesgo A	Riesgo C	Riesgo I	Riesgo D	Riesgo T
Instalaciones [L]	[L.1]	CPD	MB	MB	MB	A	MB
	[L.2]	Sala Técnica Sede	MB	MB	MB	A	MB
	[L.3]	Despacho Directivo	MB	MB	MB	M	MB
	[L.4]	Oficinas	MB	MB	MB	M	MB
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	B	A	A	A	B
	[HW.2]	Firewall CPD	B	A	A	A	B
	[HW.3]	Swithes CPD	B	A	A	A	B
	[HW.4]	Servidores hypervisor Sedes	B	A	M	A	B
	[HW.5]	Switches/routers Sedes	B	A	M	A	B
	[HW.6]	Puntos de acceso Wifi	B	A	M	M	B
	[HW.7]	PCs usuarios	B	A	M	M	B
	[HW.8]	Portátiles usuarios	B	A	M	M	B
	[HW.9]	Dispositivos móviles corporativos	B	A	B	M	B
	[HW.10]	Dispositivos móviles personales	B	A	B	M	B
	[HW.11]	Teléfonos IPs	B	B	B	M	B
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare	A	MA	MA	A	B
	[SW.2]	Sistema operativos Windows Server	A	MA	MA	A	B
	[SW.3]	Sistema operativos Linux Server	A	MA	A	A	B
	[SW.4]	Software backup: Veeam backup	A	MA	MA	B	B
	[SW.5]	Sistema operativo Windows 7	A	A	M	A	B
	[SW.6]	Sistema operativo Windows 10	A	A	M	A	B
	[SW.7]	Sistema operativo android	M	A	M	M	B
	[SW.8]	Sistema operativo IOS	M	A	M	M	B
	[SW.9]	Directorio Activo Microsoft	A	A	MA	A	B
	[SW.10]	BBDD Microsoft SQL Server	A	MA	MA	A	B
	[SW.11]	BBDD Oracle	A	MA	MA	A	B
	[SW.12]	Microsoft SCCM	M	A	M	A	B
	[SW.13]	Herramienta de ticketing: OTRS	M	A	M	A	B
	[SW.14]	Antivirus Symantec	M	M	A	A	B
	[SW.15]	Intranet corporativa	A	MA	A	A	B
	[SW.16]	Web corporativa	A	A	MA	A	B
	[SW.17]	SAP	A	MA	MA	A	B
	[SW.18]	Navision	A	MA	MA	A	B
	[SW.19]	Contaplus	A	A	A	M	B
	[SW.20]	Software puesto usuario: office 365, antivirus,	M	A	A	M	B
	[SW.21]	Aplicaciones Office 365: Correo, one drive, sky	A	MA	A	A	B
	[SW.22]	Aplicaciones Sharepoint Office 365	A	MA	A	A	B

Tipo Activo	ID Activo	Activo	Riesgo A	Riesgo C	Riesgo I	Riesgo D	Riesgo T
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos	A	A	A	M	M
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus	A	A	A	A	A
	[D.3]	Bases de datos RRHH	A	A	A	A	A
	[D.4]	LDAP: Directorio Activo Microsoft	M	M	A	A	M
	[D.5]	Copias de seguridad	M	A	M	B	M
Comunicaciones [D]	[COM.1]	Red internet	M	A	M	A	MB
	[COM.2]	Red MPLS	M	A	M	A	MB
	[COM.3]	Red local CPD	M	A	M	A	MB
	[COM.4]	Red local sedes	M	M	M	M	MB
	[COM.5]	Red wifi invitados sedes	MB	B	B	B	MB
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)	B	B	B	B	MB
	[COM.7]	Red wifi usuarios	B	M	B	M	MB
	[COM.8]	Red telefonía IP	MB	MB	MB	M	MB
	[COM.9]	Red telefonía móvil	MB	MB	MB	A	MB
Servicios [S]	[S.1]	Servicio ERP	M	M	M	M	M
	[S.2]	Servicio correo	M	M	M	M	M
	[S.3]	Servicio de telefonía	MB	B	MB	M	MB
	[S.4]	Servicio de ficheros	M	M	M	M	M
	[S.5]	Servicio de acceso remoto	M	M	M	M	M
	[S.6]	Servicio de backup	M	M	M	M	M
Soportes de Información [M]	[M.1]	Almacenamiento CPD	B	MA	A	MA	B
	[M.2]	Almacenamiento Sedes	B	A	M	A	B
	[M.3]	Memorias USB	B	A	B	B	B
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico	B	B	B	MA	B
	[AUX.2]	Aire acondicionado Salas técnicas	B	B	B	A	B
	[AUX.3]	Sistemas antiincidencios	B	B	B	MA	B
	[AUX.4]	Cableado LAN	B	B	B	MA	B
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Fina	B	B	B	A	B
	[P.2]	Personal TI	B	B	B	A	B
	[P.3]	Personal Proveedor TI	B	B	B	A	B
	[P.4]	Resto de personal	B	B	B	M	B

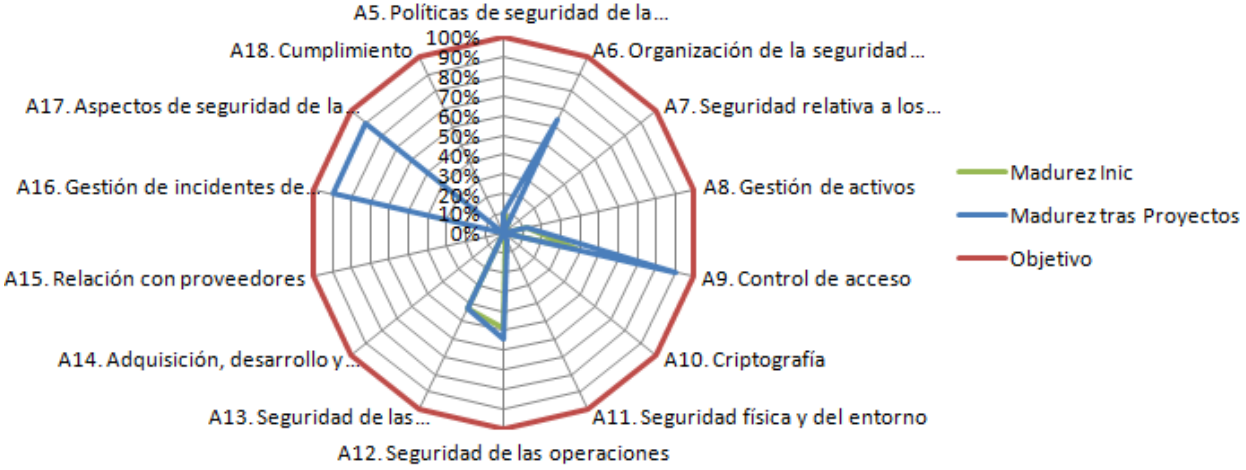
Proyectos. Resultados esperados

Evaluación de efectividad de controles

	Inicial		Tras implantación proyectos	
Controles de Seguridad de la Información	Madurez.	Implantados.	Madurez	Implantados
A5. Políticas de seguridad de la información	10%	2/2	10%	2/2
A6. Organización de la seguridad de la información	6%	3/7	64%	5/7
A7. Seguridad relativa a los recursos humanos	0%	0/6	0%	0/6
A8. Gestión de activos	13%	3/10	13%	3/10
A9. Control de acceso	38%	12/14	90%	13/14
A10. Criptografía	0%	0/2	0%	0/2
A11. Seguridad física y del entorno	1%	2/15	4%	3/15
A12. Seguridad de las operaciones	49%	13/14	54%	13/14
A13. Seguridad de las comunicaciones	43%	3/7	43%	3/7
A14. Adquisición, desarrollo y mantenimiento de los sistemas de información	0%	0/14	0%	0/14
A15. Relación con proveedores	0%	0/5	0%	0/5
A16. Gestión de incidentes de seguridad de la información	0%	0/7	90%	7/7
A17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	0%	0/4	90%	4/4
A18. Cumplimiento	0%	0/7	0%	0/7

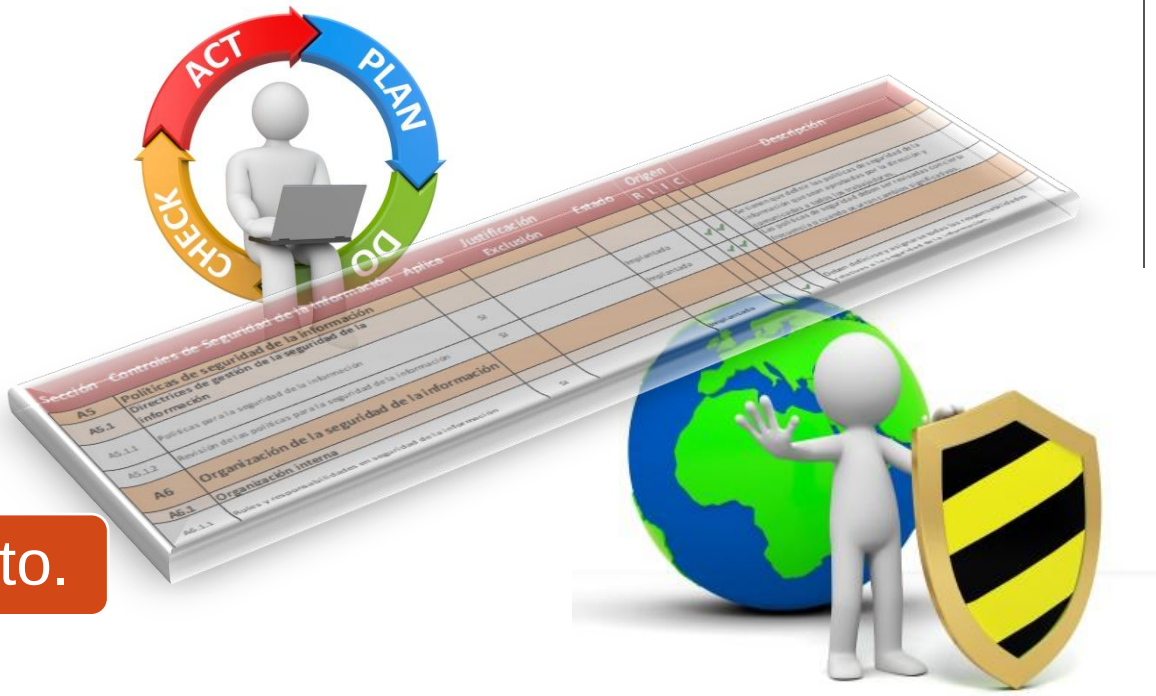
Proyectos. Resultados esperados

Evaluación de efectividad de controles



Plan Implementación de la ISO/IEC 27001:2013

- Contexto.
- Alcance.
- Objetivos.
- Situación inicial.
- Sistema de gestión documental.
- Análisis de riesgos.
- Propuestas de proyectos.
- **Auditoría de cumplimiento.**
- Resultados y conclusiones



Auditoría. Declaración de aplicabilidad

- Previo a la auditoría
- Identifica:
  - Controles que aplican
  - Origen del control
  - Justificación su exclusión
  - Descripción

Código	Orígen
R	Análisis de Riesgos
L	Legal o normativo
I	Requerimiento interno
C	Requerimiento Contractual

Sección	Controles de Seguridad de la Información	Aplica	Justificación Exclusión	Estado	Origen				Descripción
					R	L	I	C	
A5	**Políticas de seguridad de la información**								
A5.1	**Directrices de gestión de la seguridad de la información**								
A5.1.1	Políticas para la seguridad de la información	SI		Implantada		✓	✓		Se tienen que definir las políticas de seguridad de la información que sean aprobadas por la dirección y comunicadas a todos los trabajadores.
A5.1.2	Revisión de las políticas para la seguridad de la información	SI		Implantada		✓	✓		Las políticas de seguridad deben ser revisadas con cierta frecuencia o cuando ocurran cambios significativos.
A6	**Organización de la seguridad de la información**								
A6.1	**Organización interna**								
A6.1.1	Roles y responsabilidades en seguridad de la información	SI		Implantada			✓		Deben definirse y asignarse todas las responsabilidades relativas a la seguridad de la información.
A6.1.2	Segregación de tareas	SI		No implantada		✓	✓		Las funciones y tareas se deben segregar para reducir las modificaciones no autorizadas, no intencionadas o usos indebidos
A6.1.3	Contacto con las autoridades	SI		No implantada		✓	✓		Se deben mantener los contactos apropiados con las autoridades pertinentes en los casos necesarios

Auditoría. Cumplimiento

Codificación del cumplimiento

Código	Valor	Descripción
OK	Cumplimiento	Cumplimiento de los requisitos normativos
NC-	No Conformidad Menor	Desviación minima en relación a los requisitos normativos que no afecta a la eficienca e integraidad del Sistema de Gestión
NC+	No Conformidad Mayor	Incumplimiento de un requisito normativo que vulnera o pone en serio riesgo la integriad del sistema de Gestión

Auditoría. Revisión de requerimientos ISO 27001

No conformidades mayores

Sección	Requerimientos ISO 27001	Cumplimiento	Comentarios
7	**Soporte**		
7.5	Información documentada	NC+	No está documentada toda la información requerida: Requerimientos legales, regulatorios y contractuales, política de seguridad para proveedores y algunos procedimientos operativos de gestión de TI.
8	**Operación**		
8.1	Planificación y control operacional	NC+	No se planifican y controlan acciones para el tratamiento de riesgos.
8.3	Tratamiento de los riesgos de seguridad de la información	NC+	NO hay evidencia de información documentada de los resultados del tratamiento de los riesgos de seguridad
9	**Evaluación del desempeño**		
9.1	Seguimiento, medición, análisis y evaluación	NC+	No están documentadas evidencias de seguimiento, medición, análisis y evaluación del desempeño del sistema de gestión.

No conformidades menores

Sección	Requerimientos ISO 27001	Cumplimiento	Comentarios
4	**Contexto de la organización**		
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	NC-	No están documentados todos los requisitos legales y contractuales.
6	**Planificación**		
6.1	Acciones para tratar los riesgos y oportunidades	NC-	No están documentados los crierios para llevar a cabo las apreciaciones de riesgo.
7	**Soporte**		
7.2	Competencia	NC-	No están documentadas las evidencias de competencias de todos los actores del sistema de gestión de información
8	**Operación**		
8.2	Apreciación de los riesgos de seguridad de la información	NC-	No hay evidencias de de los resultados de apreciación del riesgo.

Auditoría. Revisión de cumplimiento de controles

No conformidades mayores

Se detectan múltiples controles con no conformidades mayores

No conformidades menores

Sección	Controles de Seguridad de la Información	Aplica	Cumplimiento	Comentarios
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.1	Roles y responsabilidades en seguridad de la información	SI	NC-	Las responsabilidades se encuentran definidas conforme a la Política de Seguridad definida, pero no han recibido la formacion adecuada a sus responsabilidades en seguridad.
A7	**Seguridad relativa a los recursos humanos**			
A7.2	**Durante el empleo**			
A7.2.1	Responsabilidades de gestión	SI	NC-	No se notifican a las contratas los requerimientos de la política de seguridad
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	NC-	Planificada formación a empleados. Pero no se verifica que los contratistas tengan la formación adecuada en seguridad
A8	**Gestión de activos**			
A8.1	**Responsabilidad sobre los activos**			
A8.1.2	Propiedad de los activos	SI	NC-	NO se encuentra documentado el propietario de diversos activos

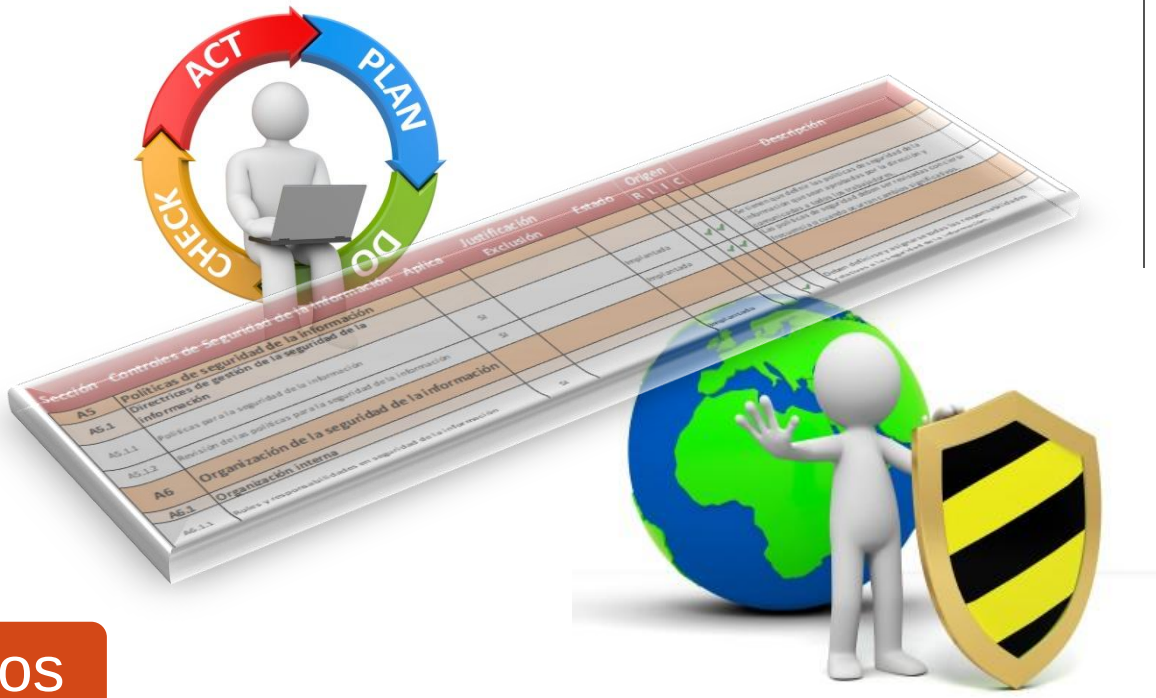
Auditoría. Informe de auditoría

Contiene

- Alcance.
- Criterios.
- Plan de auditoría.
- Registros de auditoría.
- Resultado de auditoria.
- Oportunidades de mejora.
- Planificación futura auditoría.
- Conclusiones.

Plan Implementación de la ISO/IEC 27001:2013

- Contexto.
- Alcance.
- Objetivos.
- Situación inicial.
- Sistema de gestión documental.
- Análisis de riesgos.
- Propuestas de proyectos.
- Auditoría de cumplimiento.



Conclusiones y resultados

Conclusiones

Objetivos alcanzados

- Se ha definido y puesto en marcha un SGSI.
- Se ha definido y desarrollado el esquema documental.
- Se ha definido la metodología y se ha realizado el análisis de riesgos.
- Se han definido y ejecutado diversos proyectos para mejorar la seguridad global de la organización.
- Se ha mejorado la formación y concienciación de todos los empleados de la organización.
- Se han definido los roles y las responsabilidades relativas a la seguridad de la información.
- Se ha definido los indicadores que permitirán evaluar el cumplimiento de los controles de seguridad definidos.

Conclusiones

Aspectos pendientes

- Definir e implementar la política de seguridad de proveedores.
- Definir e implementar procedimientos para la correcta gestión de la seguridad desde el punto de vista de los recursos humanos.
- Definir y desarrollar planes de formación específicos para el personal con responsabilidades en materia de seguridad de la información.
- Identificar las distintas áreas físicas y clasificarlas en función de sus necesidades en cuanto a la seguridad.
- Definir e implementar procedimientos para la autorización de retirada de materiales de las oficinas.
- Corregir las no conformidades detectadas en la auditoría.

MEJORA CONTINUA DEL SGSI

Trabajo de Final de Máster

Gracias por su atención

Cristóbal Garrido Camargo