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

TECNOSOFT

Presentación Dirección

Silvia Zugazaga Echebarria
Alumna MISTIC

Antonio José Segovia Henares
Consultor

Seguridad de la Información:

Seguridad de la Información: Conceptos

- **Activo: Cualquier elemento al cual se le asigna un valor y por lo tanto requiere protección.**

- **Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.**

- **Riesgo: Probabilidad de que una amenaza determinada se materialice produciendo un impacto negativo sobre los activos.**

- **Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo.**

Seguridad de la Información: Conceptos

•**Seguridad de la Información:** Conjunto de medidas preventivas y reactivas que permite resguardar proteger la información. Se ocupa de la información en todas sus formas(oral, impresa, electrónica,..), a diferencia de la seguridad informática, que se ocupa únicamente de la seguridad de los sistemas de información.

•**SGSI:** Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en inglés, Security Management System**.**

Seguridad de la Información: Dimensiones.

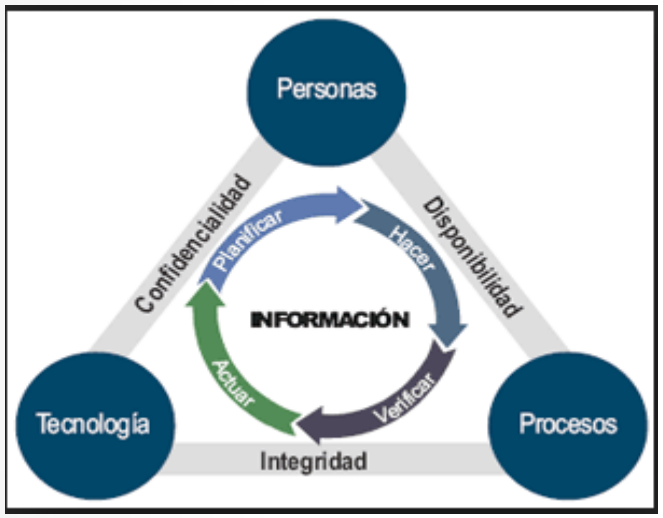
•**Confidencialidad:** Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

•**Disponibilidad:** Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

•**Integridad:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

•**Autenticidad:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
•**Trazabilidad:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Seguridad de la Información: Solución.



Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

- Necesidad
- Metodología
- Situación actual

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Necesidad.

•La información es un activo importante que es necesario proteger.

•Es necesario implantar un Sistema de Gestión de Seguridad de la Información que la proteja adecuadamente.

•La norma ISO/IEC 27001:2013 es un estándar ampliamente reconocido que permite la certificación de la organización.

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Necesidad.

- Concienciación de la necesidad de proteger.
- Compromiso de la Alta Dirección.
- Formación a todos los niveles y en todos los estamentos.
- La seguridad de la información incumbe a toda la Organización.

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Metodología.

La implantación del SGSI se ha llevado a cabo mediante la ejecución de las siguientes fases:

1. Situación actual.
2. Sistema de gestión documental.
3. Análisis de Riesgos.
4. Propuestas de Proyectos.
5. Auditoría del Cumplimiento.
6. Conclusiones.

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Metodología: Situación actual.

1. Contextualización:

- Estructura organizativa.
- Estructuras de servicios TI.
- Usuarios y sedes.
- Infraestructura tecnológica.
- Puesto de trabajo y dispositivos móviles.

Aplicaciones corporativas.
Infraestructura y redes.
Alcance SGSI.

2. Definición de objetivos.

3. Análisis diferencial.

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Metodología: Sistema gestión documental.

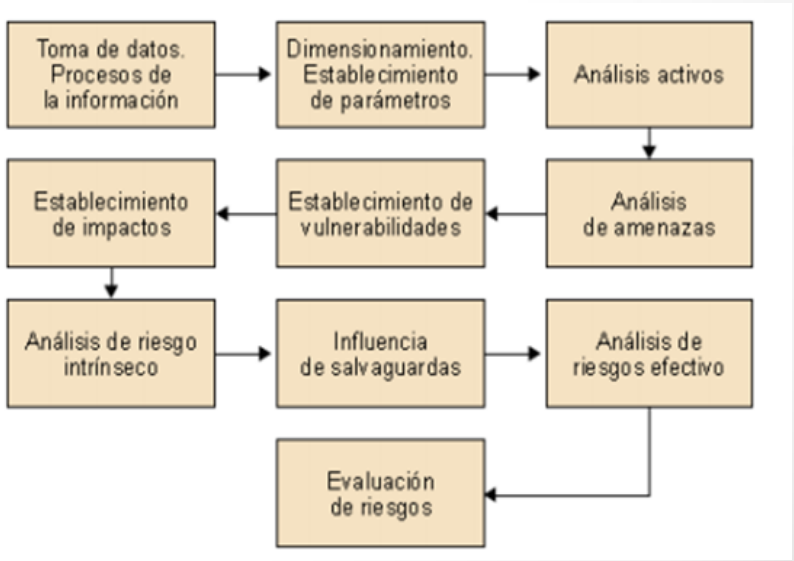
- Política de Seguridad.
- Procedimiento de Auditorías Internas.
- Gestión de Indicadores.
- Procedimiento de Revisión por la Dirección.
- Gestión de Roles y Responsabilidades.
- Metodología de Análisis de Riesgos: MAGERIT.
- Declaración de Aplicabilidad.

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Metodología: Análisis de Riesgos.

MAGERIT

- Determinar activos relevantes para la organización.
- Determinar amenazas de los activos.
- Determinar qué salvaguardas hay dispuestas.
- Estimar el impacto, definido como el daño sobre el activo.
- Estimar el riesgo, definido como el impacto ponderado
- con tasa de ocurrencia de la amenaza.



Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Estimación de riesgos por activo.

Riesgo = Impacto potencial * Frecuencia

Riesgo		Frecuencia				
		MB(0,002)	B(0,005)	M(0,015)	A(0,075)	MA(1)
Impacto	MA(10)	A	MA	MA	MA	MA
	A(7-9)	M	A	A	MA	MA
	M(4-6)	B	M	M	A	A
	B(2-3)	MB	B	B	M	M
	MB(1)	MB	MB	MB	B	B

COD	ACTIVO	Impacto potencial					Frecuencia		Riesgo				
		C	I	D	A	T	F	Valor	C	I	D	A	T
HW1	Equipos de comunicaciones	4.5	1.5	8			M	0,015	0.06	0.02	0.12		
HW2	Robot de cintas	4.5	1.5	8			M	0,015	0.06	0.02	0.12		
HW3	PC del puesto usuario	6	2	2			M	0,015	0.09	0.03	0.03		
HW4	Servidores del CPD principal	2.25	3	6			M	0,015	0.03	0.04	0.09		
HW5	Servidores CPD externalizado.	2.25	3	6			M	0,015	0.03	0.04	0.09		
HW6	Portátiles	6	2.5	3			M	0,015	0.09	0.03	0.04		

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Metodología: Proyectos.

Proyectos propuestos para mitigar los riesgos de seguridad.

En base a:

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

.

CONTROL				Situación inicial	Situación esperada
A.5 Information security policies					
	A.5.1 Management direction for information security				
		A.5.1.1	Policies for information security	4 - Gestionado	5 - Optimizado
		A.5.1.2	Review of the policies for informatio security	4 - Gestionado	5 - Optimizado
A.6 Organization of information security					
	A.6.1 Internal organization				
		A.6.1.1	Information security roles and responsibilities	3 - Definido	4 - Gestionado
		A.6.1.2	Segregation of duties	3 - Definido	4 - Gestionado
		A.6.1.3	Contact with authorities	4 - Gestionado	5 - Optimizado
		A.6.1.4	Contact with special interest groups	0 - No existente	3 - Definido
		A.6.1.5	Information security in project management	0 - No existente	3 - Definido
	A.6.2 Mobile devices and teleworking				
		A.6.2.1	Mobile device policy	0 - No existente	3 - Definido
		A.6.2.2	Teleworking	0 - No existente	3 - Definido
A.7 Human resource security					

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Metodología: Auditoría de cumplimiento.

Declaración de aplicabilidad

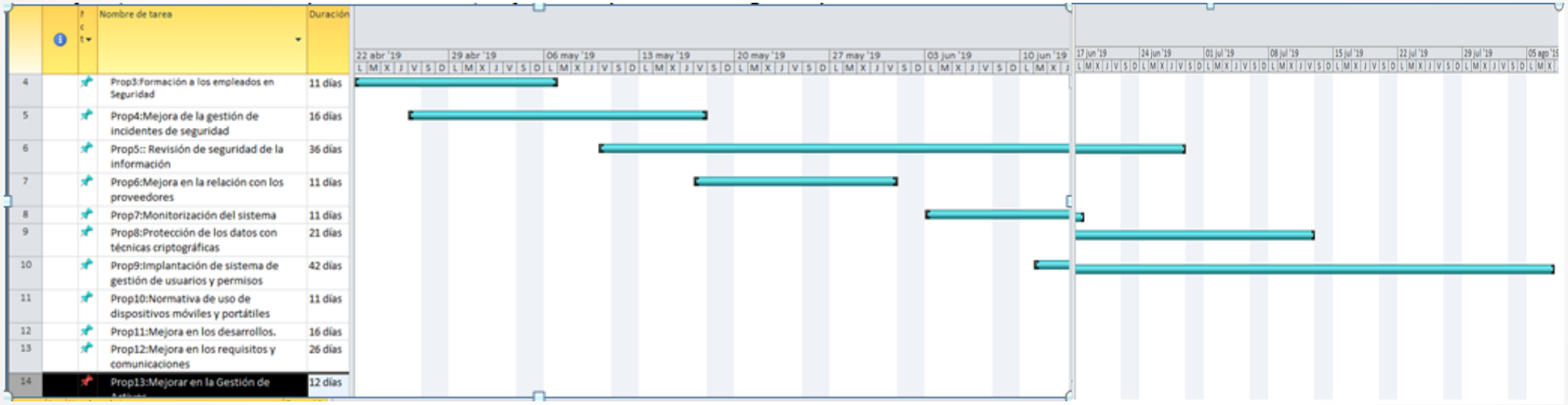
Controles que aplican.
Origen de control.
Justificación de exclusión

Informe de auditoría

Plan de auditoría.
Registros de auditoría.
Resultado de auditoría.
Oportunidades de mejora.
Planificación futura.

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Situación actual. Estado del proyecto



	Nombre de tarea	Duración
4	Prop3:Formación a los empleados en Seguridad	11 días
5	Prop4:Mejora de la gestión de incidentes de seguridad	16 días
6	Prop5:: Revisión de seguridad de la información	36 días
7	Prop6:Mejora en la relación con los proveedores	11 días
8	Prop7:Monitorización del sistema	11 días
9	Prop8:Protección de los datos con técnicas criptográficas	21 días
10	Prop9:Implantación de sistema de gestión de usuarios y permisos	42 días
11	Prop10:Normativa de uso de dispositivos móviles y portátiles	11 días
12	Prop11:Mejora en los desarrollos.	16 días
13	Prop12:Mejora en los requisitos y comunicaciones	26 días
14	Prop13:Mejorar en la Gestión de	12 días

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Evaluación de riesgos.

Estimación de riesgos por activo.

Tipo	Amenaza	Activo	Frec	Valor	A	C	I	D	T
Desastres naturales	Incendio [N1]	Instalaciones [I]	MB	0.005				100	
		Hardware[HW]	MB	0.005				100	
		Cableado eléctrico[COM]	MB	0.005				100	
		Cableado telecomunicaciones[COM]	MB	0.005				100	
		Equipamiento auxiliar[AUX]	MB	0.005				100	
	Inundación [N2]	Instalaciones[I]	MB	0.005				75	
		Hardware[HW]	MB	0.005				75	
		Equipamiento auxiliar[AUX]	MB	0.005				75	
	Tormenta eléctrica [N3]	Hardware [HW]	MB	0.005				75	
		Cableado eléctrico[COM]	MB	0.005				50	
		Equipamiento auxiliar[AUX]	MB	0.005				50	
	Terremoto [N4]	Hardware [HW]	MB	0.005				100	
		Cableado eléctrico[COM]	MB	0.005				100	
		Equipamiento auxiliar[AUX]	MB	0.005				100	

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

Objetivos conseguidos.

- SGSI definido.
- Esquema documental definido necesario para sustentar el SGSI.
- Metodología definida y análisis de riesgos realizado.
- Se han definido y ejecutado diversos proyectos, que han permitido mejorar la seguridad global de la organización.
- Se ha mejorado la formación y concienciación de todos los empleados.
- Se han definido los roles y responsabilidades relativas a seguridad.
- Se han definido indicadores de seguridad definidos.

Implementación de la ISO/IEC 27001:2013 TECNOSOFT.

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 de seguridad de la información.
- Identificar distintas áreas y clasificarlas en función de sus necesidades en cuanto a seguridad.
- Definir e implementar procedimientos para retirada de materiales.

GRACIAS