Trabajo Final de Master (TFM)
Ciberseguridad y Privacidad

Autor: Marc Montemar Parejo
Consultor: Arsenio Tortajada Gallego

Plan Director de Seguridad de la Información de una cadena hotelera

Objetivos

- Reducir riesgos Seguridad de la Información
  - Disponibilidad
  - Confidencialidad
  - Integridad
  - Autenticación y No repudio
- Asegurar cumplimiento legislación vigente
- Asegurar continuidad de negocio

Metodología

Planificación del Proyecto

Fase 1

Situación actual: Contextualización, objetivos y análisis diferencial.

Fase 2

Sistema de Gestión Documental

Fase 3

Análisis de riesgos

Fase 4

Propuesta de Proyectos

Fase 5

Auditoría de cumplimiento

Fase 6

Presentación de resultados y entrega de informes

Planificación del Proyecto

Fase 1

Situación actual: Contextualización, objetivos y análisis diferencial.

Fase 2

Sistema de Gestión Documental

Fase 3

Análisis de riesgos

Fase 4

Propuesta de Proyectos

Fase 5

Auditoría de cumplimiento

Fase 6

Presentación de resultados y entrega de informes

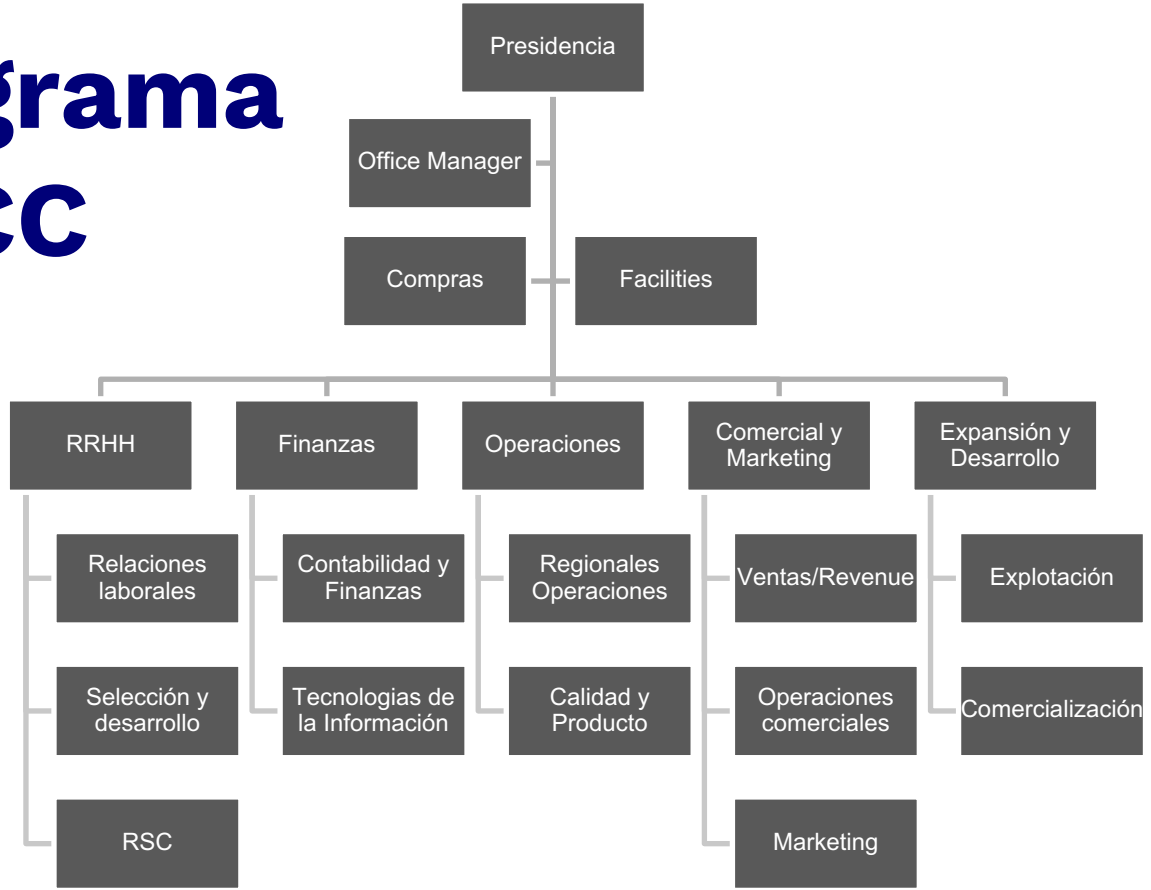
>100 hoteles

Operación y comercialización

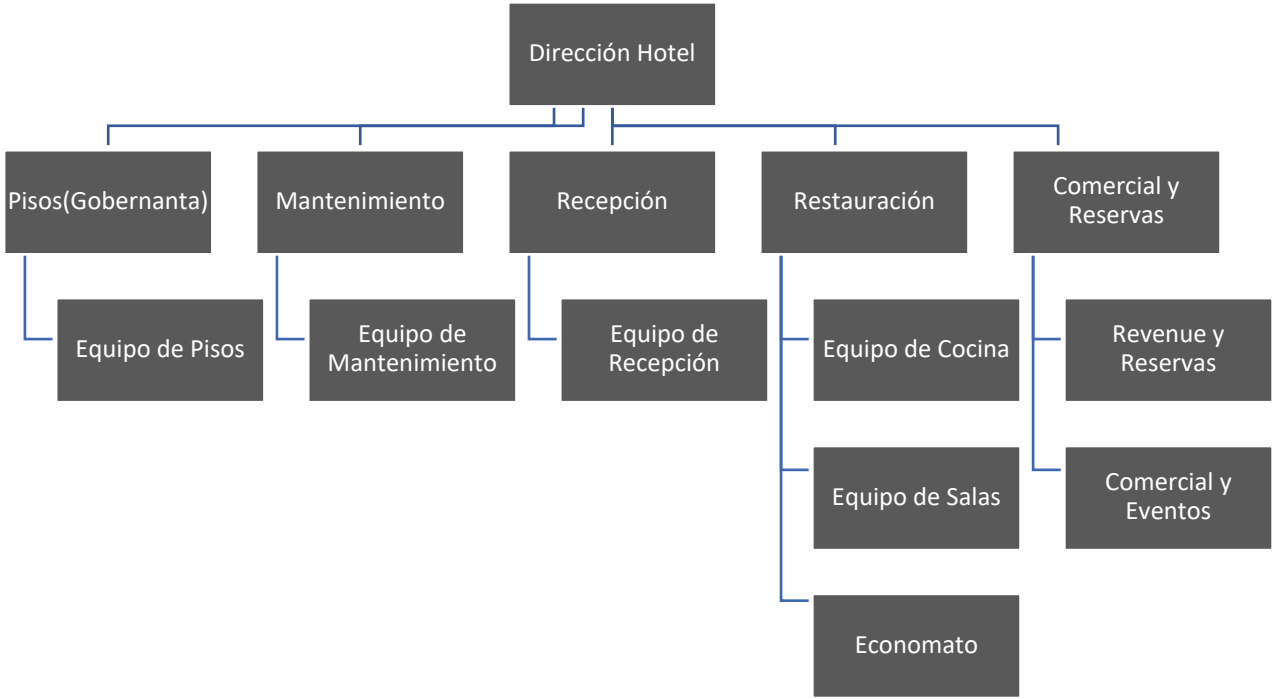
>500 trabajadores

Servicios Centrales y Hoteles

Organigrama SSCC



Organigrama Hotel tipo



Sistemas

PMS

Property Management System. Gestión de Reservas y habitaciones

ERP

Enterprise Resource Planning

Data Warehouse

Almacenamiento de datos para analizar con BI

CRM

Customer Relationship Manager

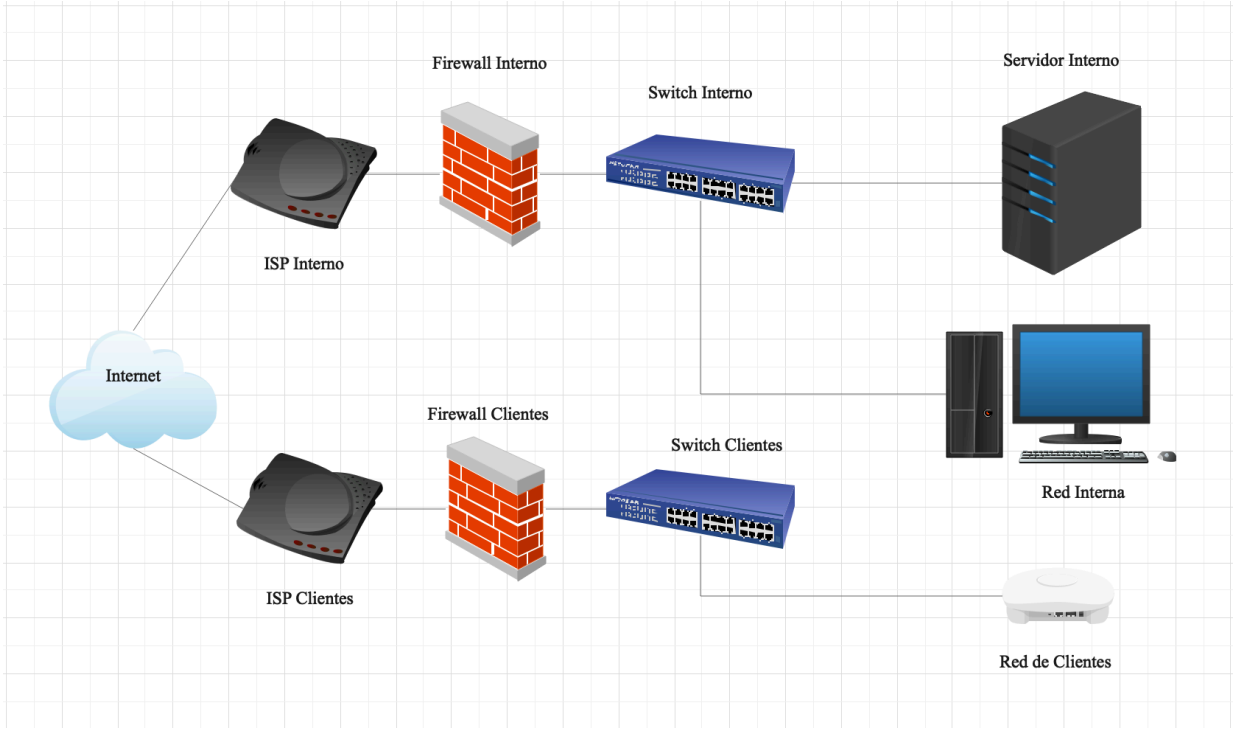
Portal Web Reservas

Permite reservas directas desde la página principal de la cadena hotelera

Wifi Clientes

Puntos de acceso mediante los cuales los clientes acceden a internet

Diagrama de red Hotel

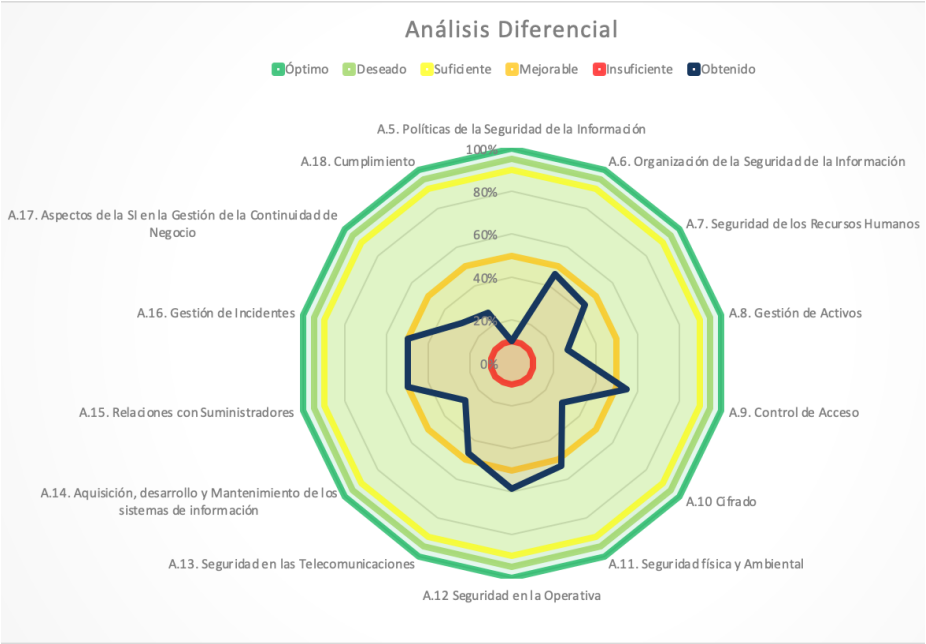


Análisis diferencial ISO 27002

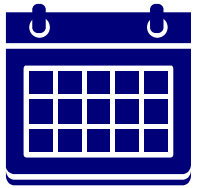
CMM - Significado	Efectividad	Descripción
L0 - Inexistente	0%	Carencia completa de cualquier proveso que reconozcamos. No se ha reconocido que exista nongún problema a resolver.
L1 - Inicial / Ad-hoc	10%	Estado inicial donde el éxito de las actividades de los procesos se basa la mayor parte de las veces en un esfuerzo personal. Los procedimientos su inexistentes o localizados en áreas concretas. No existen plantillas definidas en nivel corporativo.
L2 - Reproducible, pero intuitivo	50%	Los procesos similares se llevan a cabo de manera similar por diferentes personas con la misma tarea. Se normalizan las “buenas practicas” 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.
L3 - Proceso definido	90%	La organización entera participa al proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
L4 - Gestionado y medible	95%	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tiene que tener herramientas para mejorar la calidad y la eficiencia.
L5 - Optimizado	100%	Los procesos están bajo constante mejora. base criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Análisis diferencial ISO 27002

Área	Valor
A.5. Políticas de la Seguridad de la Información	10%
A.6. Organización de la Seguridad de la Información	46%
A.7. Seguridad de los Recursos Humanos	43%
A.8. Gestión de Activos	27%
A.9. Control de Acceso	55%
A.10 Cifrado	30%
A.11. Seguridad física y Ambiental	53%
A.12 Seguridad en la Operativa	59%
A.13. Seguridad en las Telecomunicaciones	47%
A.14. Aquisición, desarrollo y Mantenimiento de los sistemas de información	28%
A.15. Relaciones con Suministradores	50%
A.16. Gestión de Incidentes	50%
A.17. Aspectos de la SI en la Gestión de la Continuidad de Negocio	30%
A.18. Cumplimiento	26%



Planificación



Fase 1

Situación actual: Contextualización, objetivos y análisis diferencial.

Fase 2

Sistema de Gestión Documental

Fase 3

Análisis de riesgos

Fase 4

Propuesta de Proyectos

Fase 5

Auditoría de cumplimiento

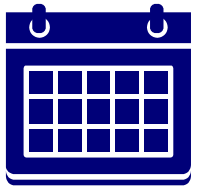
Fase 6

Presentación de resultados y entrega de informes

Sistema de Gestión Documental

- Política de seguridad
- Procedimiento de Auditorías Internas
- Gestión de Indicadores
- Procedimiento de Revisión por Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgos
- Declaración de Aplicabilidad

Planificación del Proyecto



Fase 1

Situación actual: Contextualización, objetivos y análisis diferencial.

Fase 2

Sistema de Gestión Documental

Fase 3

Análisis de riesgos

Fase 4

Propuesta de Proyectos

Fase 5

Auditoría de cumplimiento

Fase 6

Presentación de resultados y entrega de informes

Análisis de Riesgos

- Inventario de Activos
  - Activos SSCC
  - Activos Hotel tipo
- Ámbito de los Activos
  - ☐ Instalaciones
  - ☐ Datos
  - ☐ Servicios
  - ☐ Software
  - ☐ Hardware
  - ☐ Redes de Comunicación
  - ☐ Soportes de Información
  - ☐ Equipamiento Auxiliar
  - ☐ Personas

Valoración Activos

Valoración	Rango en €
Muy Alto	valor > 50.000
Alto	25.000 < valor > 50.000
Medio	10.000 < valor > 25.000
Bajo	3.000 < valor > 10.000
Muy Bajo	valor < 3.000

Valor	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importantea la organización
1-3	Daño menor a la organización
0	Daño irrelevante a la organización

Ámbito	Activo	Valor	Aspectos críticos				
			A	C	I	D	T
Instalaciones	Activo XX	MUY ALTO	8	6	5	6	8

Inventario Activos

Código	Ámbito	Activo	Valor	Aspectos críticos				
				A	C	I	D	T
HL1	Instalaciones[L]	Sala de comunicaciones hoteles	Muy Alto		9	9	9	
HL2	Instalaciones[L]	Archivo físico	Medio		7	7	7	
HL3	Instalaciones[L]	Hotel	Muy Alto		9	9	9	
HD1	Datos[D]	Ficheros	Medio	9	8	8	8	9
HD2	Datos[D]	Datos de clientes	Muy Alto	9	9	9	8	9
HD3	Datos[D]	Datos personal hotel (Nóminas, contratos, datos bancarios,…)	Muy Alto	9	9	9	7	9
HD4	Datos[D]	Procedimientos operativos hotel	Medio	7	7	9	7	7
HD5	Datos[D]	Contratos con proveedores	Medio	6	6	9	6	6
HD6	Datos[D]	Copias de respaldo (backup)	Muy Alto	9	9	9	8	9
HD7	Datos[D]	Datos de validación de credenciales (usuario, password)	Muy Alto	9	9	9	9	9
HS1	Servicios[S]	PMS (Property Management System)	Muy Alto	9	10	10	10	9
HS2	Servicios[S]	APP servicios clientes hotel (Reservas, Room Service,…)	Medio	6	6	6	8	7
HS3	Servicios[S]	Software gestión de incidencias y procedimientos hotel	Medio	6	6	6	6	6
HS4	Servicios[S]	ERP Finanzas	Muy Alto	9	10	9	9	9
HS5	Servicios[S]	CRM	Alto	7	10	7	7	7
HS6	Servicios[S]	Software de feedback de clientes y reputación online	Medio	6	6	6	6	6

Análisis de Amenazas

- Análisis de Amenazas
  - Desastres Naturales
  - De origen Industrial
  - Errores y fallos no intencionados
  - Ataques intencionados

Frecuencia	Rango	Valor
Muy frecuente	Diario	100
Frecuente	Quincenal	75
Frecuencia Media	Mensual	50
Poco frecuente	Trimestral	25
Baja	Semestral	10
Muy baja	Anual	0

Impacto	Valor
Muy alto	100%
Alto	50%
Medio	20%
Bajo	10%
Muy bajo	1%

Catálogo de Amenazas

Amenaza	Dimensión					Tipo de Activo afectado								
	A	C	I	D	T	[L]	[HW]	[SW]	[D]	[Media]	[COM]	[S]	[AUX]	[P]
[N] Desastres naturales														
[N.1] Fuego				x		x	x			x			x	
[N.2] Daños por agua				x		x	x			x			x	
[N.*] Otros desastres naturales				x		x	x			x			x	
[I] De origen industrial														
[I.1] Fuego				x		x	x			x			x	
[I.2] Daños por agua				x		x	x			x			x	
[I.*] Desastres industriales				x		x	x			x			x	
[I.4] Contaminación electromagnética				x			x			x			x	
[I.5] Avería de origen físico o lógico				x										
[I.6] Corte de suministro eléctrico				x			x			x			x	
[I.7] Condiciones inadecuadas de temperatura o humedad				x			x			x			x	
[I.8] Fallo de servicios de comunicaciones				x							x			
[I.9] Interrupción de otros servicios y suministros esenciales				x									x	
[I.10] Degradación de los soportes de almacenamiento de la información				x						x				
[E] Errores y fallos no intencionados.														
[E.1] Errores de los usuarios		x	x	x				x	x	x		x		
[E.2] Errores del administrador		x	x	x				x	x	x		x		
[E.3] Errores de monitorización (log)					x				x					
[E.4] Errores de configuración			x						x					
[E.8] Difusión de SW dañino		x	x	x				x						
[E.9] Errores de [re-]encaminamiento		x						x			x	x		
[E.15] Alteración accidental de la información			x			x		x	x	x	x	x		
[E.18] Destrucción de la información				x		x		x	x	x	x	x		

Valoración base tipo activo

Valoración = Impacto x Frecuencia

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Datos		**100%**	**100%**	**100%**	**100%**	**50%**	**25**	**87,5**	**75**	**40**	**10**
[E] Errores y fallos no intencionados.											
[E.1] Errores de los usuarios	75		20%	20%	20%		0	15	15	15	0
[E.2] Errores del administrador	25		20%	20%	20%		0	5	5	5	0
[E.3] Errores de monitorización (log)	25					20%	0	0	0	0	5
[E.4] Errores de configuración	25			20%			0	0	5	0	0
[E.15] Alteración accidental de la información	25			20%			0	0	5	0	0
[E.18] Destrucción de la información	10				100%		0	0	0	10	0
[E.19] Fugas de información	25		50%				0	12,5	0	0	0
[A] Ataques intencionados											
[A.3]Manipulación de los registros de actividad (log)	0			20%		20%	0	0	0	0	0
[A.4]Manipulación de la configuración	0	50%	50%	50%			0	0	0	0	0
[A.5]Suplantación de la identidad del usuario	25	100%	100%	100%			25	25	25	0	0
[A.6]Abuso de privilegios de acceso	50		20%	20%	20%		0	10	10	10	0
[A.11]Acceso no autorizado	10		100%	50%			0	10	5	0	0
[A.13]Repudio	10			50%		50%	0	0	5	0	5
[A.15]Modificación deliberada de la información	0			100%			0	0	0	0	0
[A.18]Destrucción de información	0				100%		0	0	0	0	0
[A.19]Divulgación de información	10		100%				0	10	0	0	0

Cálculo del Riesgo

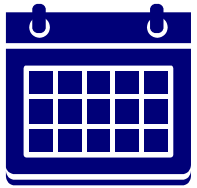
Riesgo = ((Valor activo^2) x (Valor base tipología activo)) / 10

Código	Valor	Aspectos críticos					Impacto x Frecuencia					Valor de Riesgo					
		A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	TOTAL
HL1	Muy Alto		9	9	9		0	50	27,5	2	0	0	405	223	16	0	405
HL2	Medio		7	7	7		0	50	27,5	2	0	0	245	135	10	0	245
HL3	Muy Alto		9	9	9		0	50	27,5	2	0	0	405	223	16	0	405
HD1	Medio	9	8	8	8	9	25	87,5	75	40	10	203	560	480	256	81	560
HD2	Muy Alto	9	9	9	8	9	25	87,5	75	40	10	203	709	608	256	81	709
HD3	Muy Alto	9	9	9	7	9	25	87,5	75	40	10	203	709	608	196	81	709
HD4	Medio	7	7	9	7	7	25	87,5	75	40	10	123	429	608	196	49	608
HD5	Medio	6	6	9	6	6	25	87,5	75	40	10	90	315	608	144	36	608
HD6	Muy Alto	9	9	9	8	9	25	87,5	75	40	10	203	709	608	256	81	709
HD7	Muy Alto	9	9	9	9	9	25	87,5	75	40	10	203	709	608	324	81	709
HS1	Muy Alto	9	10	10	10	9	10	71,5	37	22,95	0	81	715	370	230	0	715
HS2	Medio	6	6	6	8	7	10	71,5	37	22,95	0	36	257	133	147	0	257
HS3	Medio	6	6	6	6	6	10	71,5	37	22,95	0	36	257	133	83	0	257
HS4	Muy Alto	9	10	9	9	9	10	71,5	37	22,95	0	81	715	300	186	0	715
HS5	Alto	7	10	7	7	7	10	71,5	37	22,95	0	49	715	181	112	0	715
HS6	Medio	6	6	6	6	6	10	71,5	37	22,95	0	36	257	133	83	0	257
HS7	Muy Alto	9	7	9	10	9	10	71,5	37	22,95	0	81	350	300	230	0	350
HS8	Alto	9	3	9	6	9	10	71,5	37	22,95	0	81	64	300	83	0	300
HS9	Muy Alto	9	4	9	9	9	10	71,5	37	22,95	0	81	114	300	186	0	300
HS10	Muy Alto	9	10	10	10	9	10	71,5	37	22,95	0	81	715	370	230	0	715
HS11	Muy Alto	7	7	7	10	7	10	71,5	37	22,95	0	49	350	181	230	0	350

NIVEL ACEPTABLE DE RIESGO

- Se establece el nivel aceptable en 700
- Se tratarán todos los riesgos con nivel > 700

Resultados AR



Datos

Financieros, Legales, Contratos, Acuerdos Comerciales, Copias de respaldo, Validación de credenciales, Certificados de clave pública y firmas electrónicas.

Servicios

PMS, ERP, CRM, Servidores Web, Gestión Identidades y Privilegios, Data Warehouse, CPD Externo y BI.

Equipos y Redes

Ordenadores Portátiles, Móviles, Routers, Firewalls, Acceso Wifi.

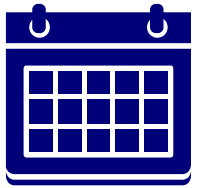
Aplicaciones

Mantener actualizados Sistemas Operativos y Aplicaciones de Servidores y usuarios.

Personas

Directivos, RRHH, Finanzas, Expansión y Operaciones

Planificación del Proyecto



Fase 1

Situación actual: Contextualización, objetivos y análisis diferencial.

Fase 2

Sistema de Gestión Documental

Fase 3

Análisis de riesgos

Fase 4

Propuesta de Proyectos

Fase 5

Auditoría de cumplimiento

Fase 6

Presentación de resultados y entrega de informes

RGPD

Ranking Sanciones RGPD UE

	Country	Date	Fine [€]	Controller/Processor	Quoted Art.	Type
	Filter Column		Filter Column	Filter Column		Filter Column
ETID-23	FRANCE	2019-01-21	50,000,000	Google Inc.	Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 5 GDPR	Insufficient legal basis for data processing
ETID-405	GERMANY	2020-10-01	35,258,708	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
ETID-189	ITALY	2020-01-15	27,800,000	TIM (telecommunications operator)	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing
ETID-58	UNITED KINGDOM	2020-10-16	22,046,000	British Airways	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security
ETID-60	UNITED KINGDOM	2020-10-30	20,450,000	Marriott International, Inc	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security

Fuente: enforcementtracker.com

Propuesta de Proyectos

- Auditoría cumplimiento RGPD.
- Clasificación de la información.
- Definición de política y gestión de permisos de acceso en base a roles.
- Revisión de contratos y regularización de servicios TIC prestados por terceros.
- Procedimiento actualizaciones de software y revisión de logs.
- Procedimiento de copias de seguridad (backup).
- Procedimiento de configuración de equipos.
- Procedimiento de gestión de incidentes de seguridad.
- Auditoría de seguridad de portal web de reservas.
- Auditoría de seguridad de redes y sistemas.
- Plan de formación en Seguridad de la Información.
- Plan de continuidad de negocio.

Propuesta de Proyectos

PSI01-Auditoría cumplimiento RGPD	
Objetivos, descripción y alcance	
El objetivo de este proyecto es analizar si la organización cumple con todo lo establecido en la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD), que adapta la legislación española a la normativa europea, definida por el Reglamento General de Protección de Datos (RGPD).	
Solución propuesta	
Se propone contratar a una empresa externa una auditoría independiente para saber si la empresa cumple con lo establecido en la RGPD y tomar las acciones correspondientes en caso de incumplimiento.	
Fases	
Fase 1- Solicitud de presupuestos.	
Fase 2- Análisis y contratación de propuesta seleccionada.	
Fase 3- Realización de auditoría.	
Fase 4- Presentación de resultados.	
Fase 5- Propuesta de correcciones/mejoras	
Fase 6- Implementación de correcciones/mejoras	
Calendario	
2021	
Fase 1 | Fase 2 | Fase 3 | Fase 4 | Fase 5	Fase 6
Riesgos a mitigar	
Filtración datos clientes, trabajadores y terceras partes.Riesgos asociados a datos, servicios, aplicaciones, equipos, redes y personas.	
Beneficios	
Garantizar el cumplimiento de la legislación vigente para evitar posibles sanciones y evitar fugas de información que pudieran causar un gran daño reputacional para la organización.	
Controles ISO relacionados	
A 18	
Coste	10.000 €

PSI02-Clasificación de la información		
Objetivos, descripción y alcance		
Para trabajar de forma eficiente con la información disponible en la organización, es esencial que ésta se clasifique de forma adecuada. Esto permitirá protegerla frente a posibles amenazas de forma adecuada, así como establecer los permisos de acceso correspondientes en función de los diferentes roles definidos.		
Solución propuesta		
Establecer los criterios de clasificación de la información y revisión de toda la documentación de la organización clasificándola en función de los criterios definidos.		
Fases		
Fase 1- Establecer criterios de clasificación		
Fase 2- Reuniones con los diferentes departamentos para presentación proyecto		
Fase 3- Clasificación de la información		
Fase 4- Establecimiento de roles de acceso a la información		
Calendario		
2021		2022
Fase 1	Fase 2	Fase 4
		Fase 3
Riesgos a mitigar		
Confidencialidad, integridad y disponibilidad de la información (datos).		
Beneficios		
Una correcta clasificación de la información permitirá protegerla de forma adecuada, así como un acceso a la información con los permisos adecuados y evitar duplicidades y acceso a distintas versiones por parte de diferente personas.		
Controles ISO relacionados		
A 8.2		
Coste	Personal interno	

Propuesta de Proyectos

PSI03-Definición de política y gestión de permisos de acceso en base a roles			
Objetivos, descripción y alcance			
El principal objetivo de este proyecto es el de establecer quién debe acceder a qué información y con qué permisos.			
Solución propuesta			
Definición de roles de acceso y de la política de control de acceso a la información asignando los roles correspondientes a cada uno de los usuarios.			
Fases			
Fase 1- Definición de roles de acceso.			
Fase 2- Definición de política de acceso a la información en base a roles			
Fase 3- Asignación de roles a cada uno de los usuarios de la organización			
Fase 4- Asignación de permisos en base a roles			
Calendario			
2021			
Fase 1	Fase 2	Fase 3	Fase 4
Riesgos a mitigar			
Confidencialidad, integridad y disponibilidad de la información (datos).			
Beneficios			
Una correcta definición de roles y de la política de acceso a la información, permitirá protegerla de forma adecuada, así como un acceso a la información con los permisos adecuados.			
Controles ISO relacionados			
A.9			
Coste	Personal interno		

PSI04-Revisión de contratos y regularización de servicios TIC prestados por terceros						
Objetivos, descripción y alcance						
El objetivo de este proyecto es el de revisar todos los contratos relacionados con las TIC prestados por terceros con la finalidad de establecer en los mismos los KPI's necesarios para mitigar y transferir los riesgos relacionados con la Seguridad de la Información de los servicios contratados.						
Solución propuesta						
Revisión de todos los contratos de servicios TIC prestados por terceros, diseñando los KPI's correspondientes para mitigar y transferir los riesgos relativos a la Seguridad de la Información asociados a los mismos, firmando nuevos contratos o añadiendo anexos a los actuales.						
Fases						
Fase 1- Revisión de contratos						
Fase 2- Establecer KPI's						
Fase 3- Negociar inclusión de KPI's en contrato con proveedores						
Fase 4- Inclusión de KPI's en contrato						
Fase 5- Firmar nuevos contratos incluyendo los KPI's						
Calendario						
2021						
Fase 1	Fase 2	Fase 3	Fase 4	Fase 5		
Riesgos a mitigar						
Riesgo relacionado con los servicios prestados por terceros (servicios).						
Beneficios						
Los principales beneficios de este proyecto están relacionados con la mitigación y transferencia de los riesgos asociados a los servicios prestados por terceros.						
Controles ISO relacionados						
A.15						
Coste	Personal interno					

Propuesta de Proyectos

PSI05-Procedimiento actualizaciones de software y revisión de logs							
Objetivos, descripción y alcance							
El objetivo de este proyecto es el de reducir los riesgos relacionados con las vulnerabilidades existentes en las versiones no actualizadas de software.							
Solución propuesta							
Implantación de procedimiento de actualización de software en el que se definan las aplicaciones afectadas así como la periodicidad de revisión de las actualizaciones.							
Fases							
Fase 1- Definición y propuesta de procedimiento							
Fase 2- Revisión y aprobación de procedimiento							
Fase 3- Publicacioón de procedimiento.							
Fase 4- Aplicación de procedimiento							
Calendario							
2021							
Fase 1	Fase 2	Fase 3	Fase 4				
Riesgos a mitigar							
Vulnerabilidades de software no actualizado (aplicaciones).							
Beneficios							
Evitar las amenazas aprovechadas por potenciales atacantes relacionadas con vulnerabilidades conocidas y originadas al no disponer del software actualizado.							
Controles ISO relacionados							
A 11.2.4, A 12.5.1, A 12.6.1							
Coste	Personal interno						

PSI06-Procedimiento de copias de seguridad (backup)							
Objetivos, descripción y alcance							
El objetivo de este procedimiento es el de definir la información de la cual se debe realizar copias de seguridad así como la periodicidad de las copias para cada tipo de información con la finalidad de poder restaurar los sistemas en caso de ocurrencia de incidentes relacionados con la Seguridad de la Información.							
Solución propuesta							
Realización de procedimiento en el que se defina qué información debe disponer de copia de seguridad, así como la periodicidad con la que se deben realizar las copias en función de la importancia de la misma y que se basará en el Objetivo de Punto de Recuperación (RPO) que se haya establecido para cada uno de los procesos de la organización.							
Fases							
Fase 1- Definir qué información debe disponer de copia de seguridad							
Fase 2- Establecer los RPO's para cada tipo de información							
Fase 3- Definición y propuesta de procedimiento							
Fase 4- Revisión y aprobación de procedimiento							
Fase 5- Publicacioón de procedimiento.							
Fase 6- Aplicación de procedimiento							
Calendario							
2021							
Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6		
Riesgos a mitigar							
Riesgo de pérdida de información por falta de backup (datos, servicios y aplicaciones)							
Beneficios							
Permite recuperar información en base a su criticidad para el negocio.							
Controles ISO relacionados							
A 12.3.1							
Coste	Personal interno						

Propuesta de Proyectos

PSI07-Procedimiento de configuración de equipos							
Objetivos, descripción y alcance							
El objetivo principal de la definición de un procedimiento para la configuración de equipos es el de estandarizar dichas configuraciones para disponer de la protección adecuada ante amenazas que puedan producir incidentes relacionados con la Seguridad de la Información.							
Solución propuesta							
Realización de procedimiento que establezca la configuración de los diferentes equipos, tales como ordenadores, routers, firewalls, y cualquier otro equipo relacionado con las TIC utilizando ls mejores prácticas en materia de Seguridad de la Información.							
Fases							
Fase 1- Definición y propuesta de procedimiento							
Fase 2- Revisión y aprobación de procedimiento							
Fase 3- Publicacioón de procedimiento.							
Fase 4- Aplicación de procedimiento							
Calendario							
2021							
Fase 1	Fase 2	Fase 3	Fase 4				
Riesgos a mitigar							
Riesgos relacionados con la configuración de equipos (aplicaciones, equipos y redes).							
Beneficios							
Permite la estandarización de las configuraciones para obtener una protección óptima ante las amenzas relacionadas con la Seguridad de la Información.							
Controles ISO relacionados							
A 9.4, A 11.2.4, A 12.5, A 12.6, A 14.2.4							
Coste	Personal interno						

PSI08-Procedimiento de gestión de incidentes de seguridad							
Objetivos, descripción y alcance							
El objetivo de este proyecto es el de la implantación de un procedimiento de gestión de incidentes, que permita detectar los incidentes relacionados con la seguridad de la información de forma ágil, así como reaccionar de la forma adecuada para su mitigación.							
Solución propuesta							
Creación de procedimiento para la detección y contención de incidentes relacionados con la seguridad de la información.							
Fases							
Fase 1- Definición y propuesta de procedimiento							
Fase 2- Revisión y aprobación de procedimiento							
Fase 3- Publicacioón de procedimiento.							
Fase 4- Aplicación de procedimiento							
Calendario							
2021							
Fase 1	Fase 2	Fase 3	Fase 4				
Riesgos a mitigar							
Riesgos asociados a datos, servicios, aplicaciones, equipos, redes y personas.							
Beneficios							
Permitirá reducir los tiempos de respuesta y de contención ante los incidentes de seguridad que puedan producirse en la organización.							
Controles ISO relacionados							
A 16.1							
Coste	Personal interno						

Propuesta de Proyectos

PSI09-Auditoría de seguridad de portal web de reservas						
Objetivos, descripción y alcance						
El principal objetivo de este proyecto es el de detectar las vulnerabilidades del portal web de reservas con la finalidad de tomar las medidas adecuadas para minimizar los riesgos, protegiendo la información contenida en el mismo, así como garantizando su disponibilidad.						
Solución propuesta						
Se propone contratar a una empresa externa una auditoría independiente de pentesting del portal web para conocer las vulnerabilidades del mismo y tomar las acciones correspondientes para minimizar los riesgos derivados de éste.						
Fases						
Fase 1- Solicitud de presupuestos.						
Fase 2- Análisis y contratación de propuesta seleccionada.						
Fase 3- Realización de auditoría.						
Fase 4- Presentación de resultados.						
Fase 5- Propuesta de correcciones/mejoras						
Fase 6- Implementación de correcciones/mejoras						
Calendario						
2021						
Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6	
Riesgos a mitigar						
iesgo de servicios y aplicaciones, concretamente de los relacionados con el portal wel						
Beneficios						
Permitirá conocer las vulnerabilidades del portal web y tomar las acciones necesarias para mitigar los riesgos existentes, protegiendo al mismo ante las potenciales amenazas.						
Controles ISO relacionados						
A 18.1.3, A.18.1.4, A.18.2						
Coste	5000					

PSI10-Auditoría de seguridad de redes y sistemas						
Objetivos, descripción y alcance						
El principal objetivo de este proyecto es el de detectar las vulnerabilidades en la infraestructura de red de la organización con la finalidad de tomar las medidas adecuadas para minimizar los riesgos asociados a la información que se transmite sobre la misma.						
Solución propuesta						
Se propone contratar a una empresa externa una auditoría independiente para conocer las vulnerabilidades de las infraestructuras de red y de los sistemas de la organización y tomar las acciones correspondientes para minimizar los riesgos relacionados con ello.						
Fases						
Fase 1- Solicitud de presupuestos.						
Fase 2- Análisis y contratación de propuesta seleccionada.						
Fase 3- Realización de auditoría.						
Fase 4- Presentación de resultados.						
Fase 5- Propuesta de correcciones/mejoras						
Fase 6- Implementación de correcciones/mejoras						
Calendario						
2021						
Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6	
Riesgos a mitigar						
Riesgos de infraestructura de red y sistemas.						
Beneficios						
Permitirá conocer las vulnerabilidades de las redes existentes y protegerlas ante las potenciales amenazas.						
Controles ISO relacionados						
A 18.1.3, A.18.1.4, A.18.2						
Coste	5000					

Propuesta de Proyectos

PSI11-Plan de formación en Seguridad de la Información					
Objetivos, descripción y alcance					
Formar a la dirección de la organización en materia de ciberseguridad para que tome conciencia de las vulnerabilidades de la empresa, así como de las amenazas a la que ésta está expuesta y al mismo tiempo se convierta en promotora de la aplicación de las medidas necesarias para protegerse en el ciberespacio.					
Solución propuesta					
Contratación de formación especializada en ciberseguridad que impartirá un experto en la materia.					
Fases					
Fase 1- Búsqueda de formadores y solicitud de presupuestos.					
Fase 2- Análisis y contratación de propuesta seleccionada.					
Fase 3- Impartición de la formación					
Calendario					
2021					
Fase 1	Fase 2	Fase 3			
Riesgos a mitigar					
Riesgo de uso indebido de la información y de los sistemas que la soportan por falta de conocimiento (Personas).					
Beneficios					
Concienciar a la dirección de la necesidad de protegerse frente a las amenazas a las que está sometida la organización en materia de ciberseguridad, lo que ayudará a transmitir al resto de personas de la empresa la necesidad de protección ante estas amenazas .					
Controles ISO relacionados					
A 7.2.2					
Coste	10000				

PSI12-Plan de continuidad de negocio					
Objetivos, descripción y alcance					
El objetivo de este proyecto es el de poder garantizar que la organización pueda continuar y/o restablecer sus procesos en forma, tiempo y coste adecuados ante la ocurrencia de incidentes que afecten a la seguridad de la información.					
Solución propuesta					
Realización de un plan de continuidad de negocio en base al análisis de impacto en el negocio realizado para cada uno de los procesos críticos de la organización y establecimiento de las medidas a tomar ante la materialización de amenazas que puedan afectar a los mismos definiendo los Objetivos de Tiempo de Recuperación (RTO) y el Objetivo del Punto de Recuperación de los datos (RPO).					
Fases					
Fase 1- Revisión con los responsables de departamento de los procesos críticos.					
Fase 2- Realización de Análisis de Impacto en el Negocio (BIA)					
Fase 3- Definición de RTO y RPO					
Fase 4- Definición del plan de respuesta a incidentes					
Fase 5- Realización del Plan de Continuidad de Negocio.					
Calendario					
2021					
Fase 1			Fase 4		
	Fase 2	Fase 3	Fase 5		
Riesgos a mitigar					
Riesgos asociados a datos, servicios, aplicaciones, equipos, redes y personas.					
Beneficios					
Permitirá continuar o restablecer las operaciones de la organización en un tiempo óptimo teniendo en cuenta la relación coste/beneficio de las medidas a tomar.					
Controles ISO relacionados					
A 17					
Coste	Personal interno				

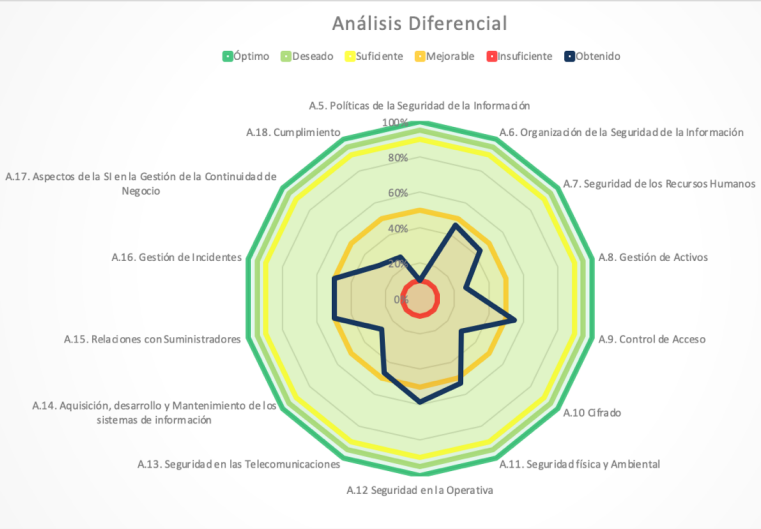
Resumen de Proyectos

Id	Proyecto	2021				2022				Coste
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
PSI01	Auditoría cumplimiento RGPD									10.000 €
PSI02	Clasificación de la información									Personal interno
PSI03	Definición de política y gestión de permisos de acceso en base a roles									Personal interno
PSI04	Revisión de contratos y regularización de servicios TIC prestados por terceros									Personal interno
PSI05	Procedimiento actualizaciones de software y revisión de logs									Personal interno
PSI06	Procedimiento de copias de seguridad (backup)									Personal interno
PSI07	Procedimiento de configuración de equipos									Personal interno
PSI08	Procedimiento de gestión de incidentes de seguridad									Personal interno
PSI09	Auditoría de seguridad de portal web de reservas									5.000 €
PSI10	Auditoría de seguridad de redes y sistemas									5.000 €
PSI11	Plan de formación en Seguridad de la Información									10.000 €
PSI12	Plan de continuidad de negocio									Personal interno

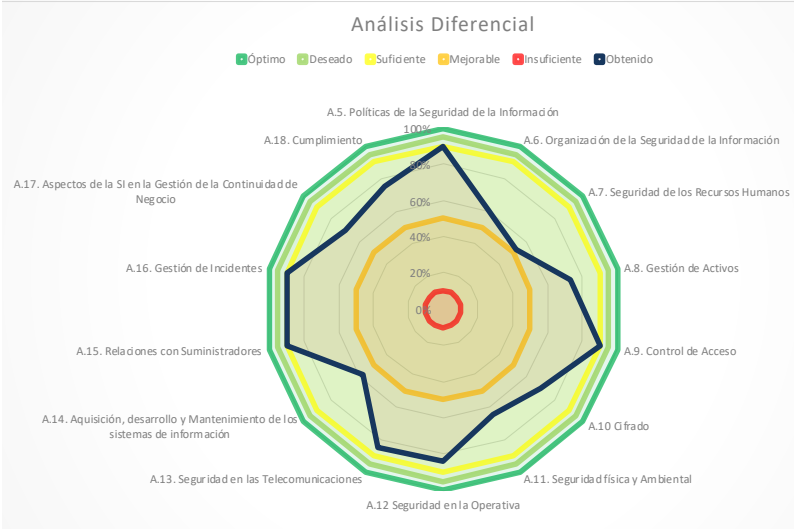
Coste Total	30.000 €

Evolución ISO 27.002

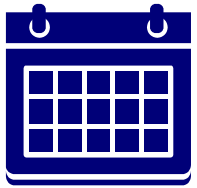
Inicial



Post Proyectos



Planificación del Proyecto



Fase 1

Situación actual: Contextualización, objetivos y análisis diferencial.

Fase 2

Sistema de Gestión Documental

Fase 3

Análisis de riesgos

Fase 4

Propuesta de Proyectos

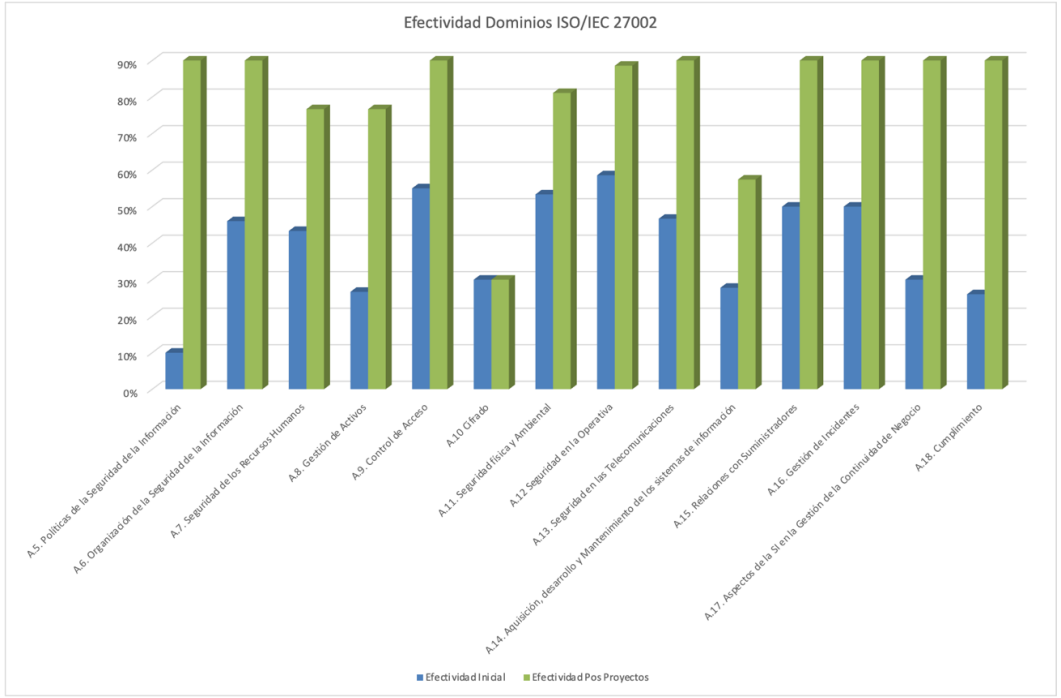
Fase 5

Auditoría de cumplimiento

Fase 6

Presentación de resultados y entrega de informes

Auditoría de cumplimiento

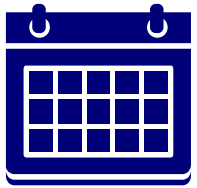


Auditoría de cumplimiento

CONTROL				Cumplimiento
A.7. Seguridad de los Recursos Humanos				
	A.7.1. Antes de la contratación			
		A.7.1.1	Investigación de antecedentes	No
A.8. Gestión de Activos				
	A.8.3. Manejo de medios de soporte			
		A.8.3.1	Gestión de medios de soporte removibles	No
		A.8.3.2	Eliminación de soportes	No
		A.8.3.3	Soportes físicos en tránsito	No
A.10 Cifrado				
	A.10.1 Controles criptográficos			
		A.10.1.1	Política de uso de los controles criptográficos	No
		A.10.1.2	Gestión de claves	No
A.11. Seguridad física y Ambiental				
	A.11.1 Áreas seguras			
		A.11.1.1	Perímetro de seguridad física	No
		A.11.1.6	Áreas de acceso público, carga y descarga	No
	A.11.2 Seguridad de los equipos			
		A.11.2.7	Reutilización o retirada segura de dispositivos de almacenam.	No
A.12 Seguridad en la Operativa				
	A.12.1 Responsabilidades y procedimientos de operación			
		A.12.1.4	Separación de entornos de desarrollo, prueba y producción	No
A.14. Aquisición, desarrollo y Mantenimiento de los sistemas de información				
	A.14.2 Seguridad en los procesos de desarrollo y soporte			
		A.14.2.1	Política de desarrollo seguro de software	No
		A.14.2.6	Seguridad en entornos de desarrollo	No
		A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	No
	A.14.3 Datos de prueba			
		A.14.3.1	Protección de los datos utilizados en prueba	No

Controles ISO 27.002 con No conformidades

Planificación del Proyecto



Fase 1

Situación actual: Contextualización, objetivos y análisis diferencial.

Fase 2

Sistema de Gestión Documental

Fase 3

Análisis de riesgos

Fase 4

Propuesta de Proyectos

Fase 5

Auditoría de cumplimiento

Fase 6

Presentación de resultados y entrega de informes

Conclusiones

- Elaboración Plan Director de Seguridad de la Información
  - ❑ Reducir los riesgos asociados a la seguridad de la información.
  - ❑ Asegurar el cumplimiento de la legislación vigente en materia de protección de datos personales.
  - ❑ Asegurar continuidad de negocio.
- Posibilidad certificación ISO 27.001.

Gracias!