PROJECTE GESTIÓ I AUDITORIA DE LA SEGURETAT 2015-2016

Projecte Final de Postgrau, Elaboració d'un Pla de Seguretat de la Informació

Estudiant: Francesc Lucio Subirachs

Programa: Projecte Final de Postgrau en Seguretat en serveis i aplicacions (PGAS)

Àrea: Sistemes de Gestió de la Seguretat de la Informació

Consultor: Arsenio Tortajada Gallego

Professor responsable de l'assignatura: Carles Garrigues Olivella

Centre: Universitat Oberta de Catalunya

Lliurament: 06/06/2016

INTRODUCCIÓ

- **Projecte de final de postgrau per a la implementació i anàlisi d'un SGSI**
- **Estructurat en fases:**
  - F1. Situació actual
  - F2. Sistema de gestió documental
  - F3. Anàlisi de riscos
  - F4. Proposta de projectes
  - F5. Auditoria de compliment ISO/IEC 27002:2013
  - F6. Presentació de resultats

OBJECTIUS

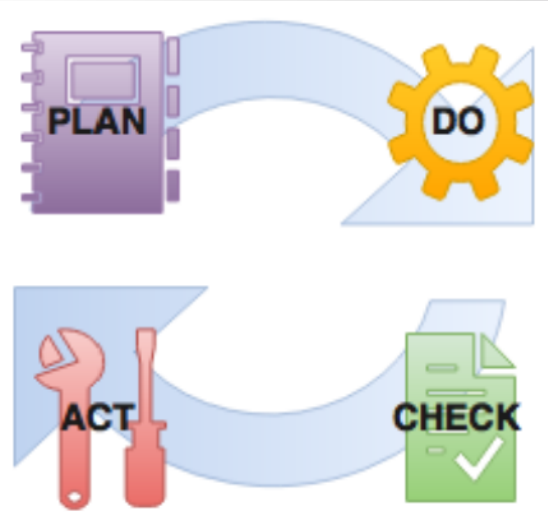
- Generar documentació normativa sobre millors pràctiques en seguretat de la informació
- Definició i objetius de l'empresa i el seu SGSI
- Anàlisi de riscos del SGSI d'una empresa
- Identificació i classificació d'actius, amenaces i vulnerabilitats
- Proposta de projectes de millora
- Avaluació del compliment de la norma ISO
- Elaboració d'un esquema documental

LA NORMA ISO

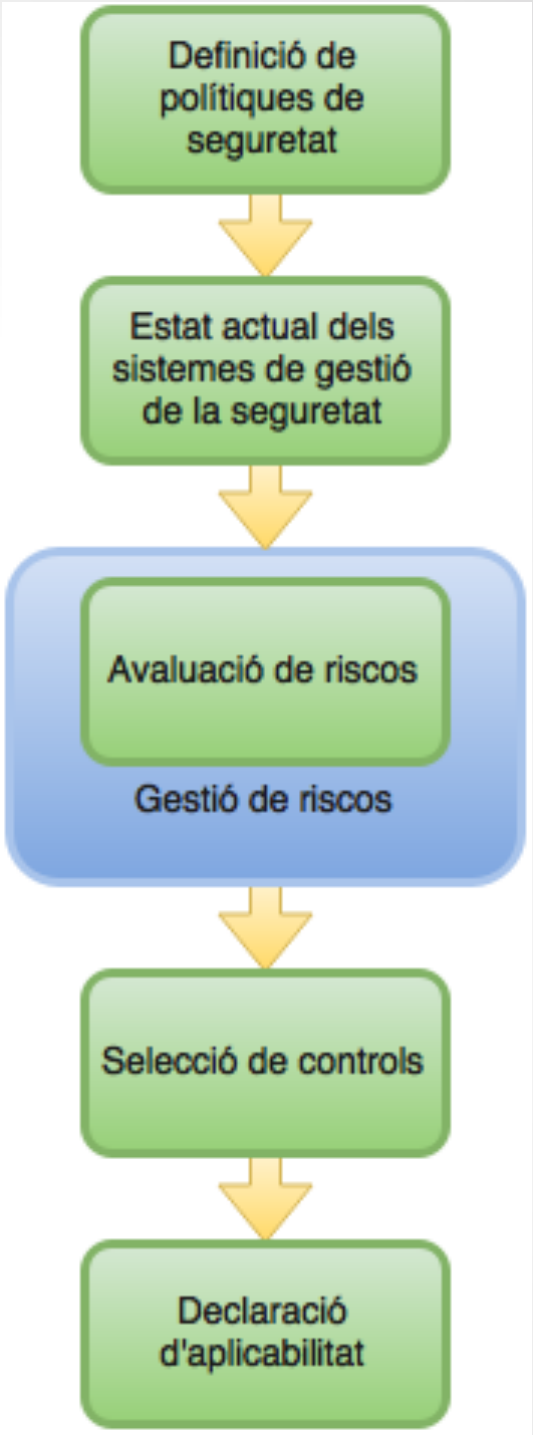
- ISO/IEC27002:2013 “Information technology - Security techniques - Code of practice for information security management”
- Ùltima versió d'un estàndard per a la seguretat de la informació publicat per l'Organització Internacional de Normalització i la Comissió Electrotècnica Internacional
- Aporta recomanacions de les millors pràctiques en al gestió de la seguretat de la informació
- Es basa en el procediment PDCA i l'anàlisi de riscos

SISTEMES GESTORS DE LA SEGURETAT DE LA INFORMACIÓ

- Def.: conjunt de polítiques d'administració de la informació
- Permet gestionar de forma eficient l'accessibilitat de la informació [Confidencialitat, Integritat, Disponibilitat]
- Es centra en els actius que puguin afectar a la informació i al negoci
- Sistema de millora iterativa, segons cicle Deming o PDCA



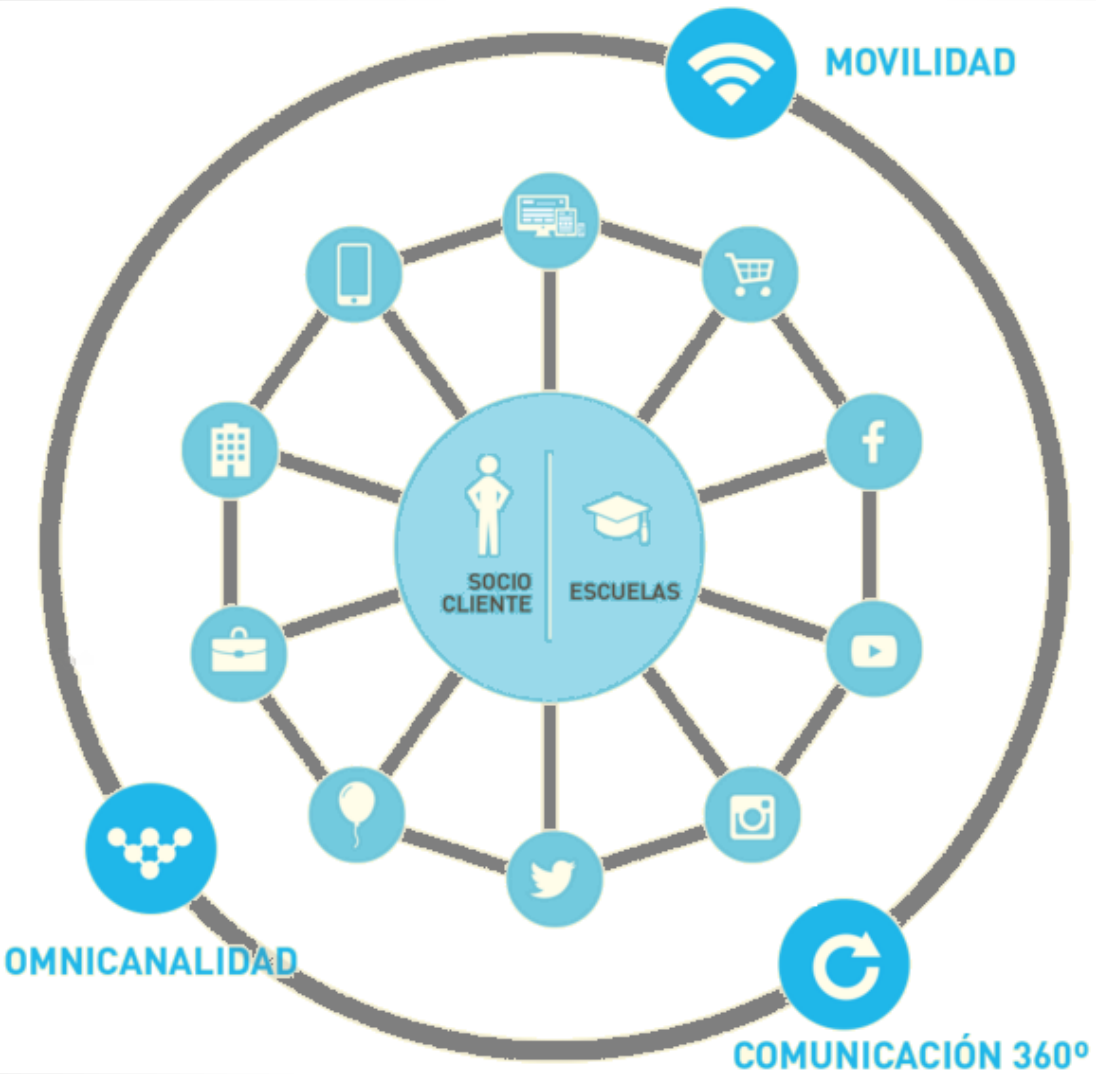
FASES D'UN SGSI



L'EMPRESA

- Activitat: educació, oci i cultura
- Localització: Territori espanyol amb seu a Barcelona
- Clients: Particulars, empreses, escoles i associacions
- Plantilla: 479 empleats + temporers i altres serveis
- Xarxa de venta: 31487 m2
- Capital generat: 82.265.639 €
- Ubicació centre logistic i SSCC: Barcelona i rodalies

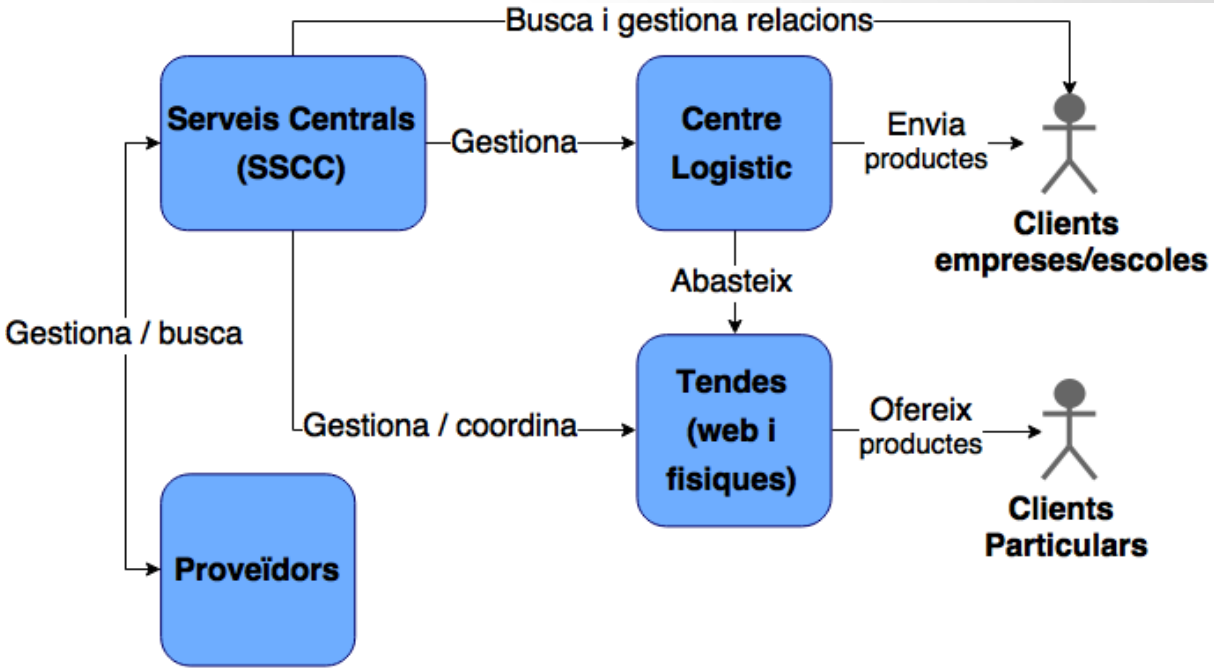
PROJECCIÓ DE FUTUR



- Clients i socis en el centre
- MOBILITAT
- COMUNICACIÓ
- OMNICANALITAT

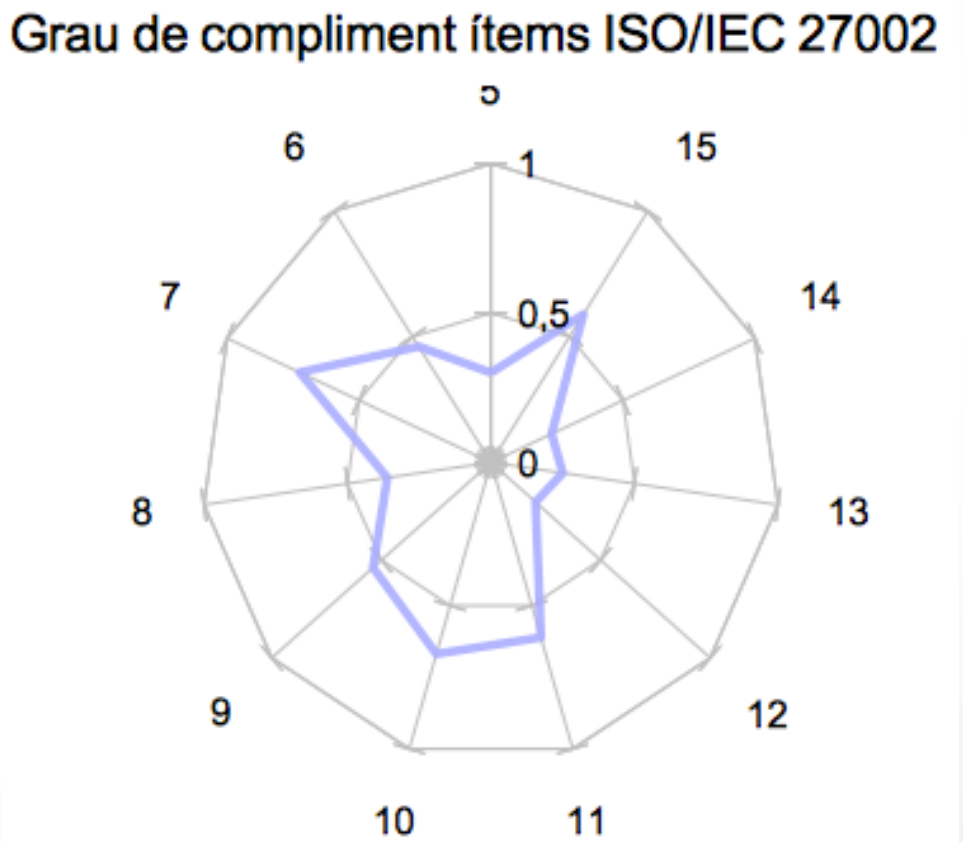
ESTRUCTURA JERÀRQUICA (PER DEPARTAMENTS)

- President
- Director General
- Tendes
- Administració
- RRHH
- Distribució, magatzem proveïdors
- Serveis Informàtics
- Ventes i marketing
- Assessoria jurídica



ANÀLISI DIFERENCIAL I OBJECTIUS DE SEGURETAT

- Definits els objectius que l'empresa vol assolir al llarg del pròxim any
- L'anàlisi diferencial permet coneixer el grau de compliment de la norma en la situació inicial

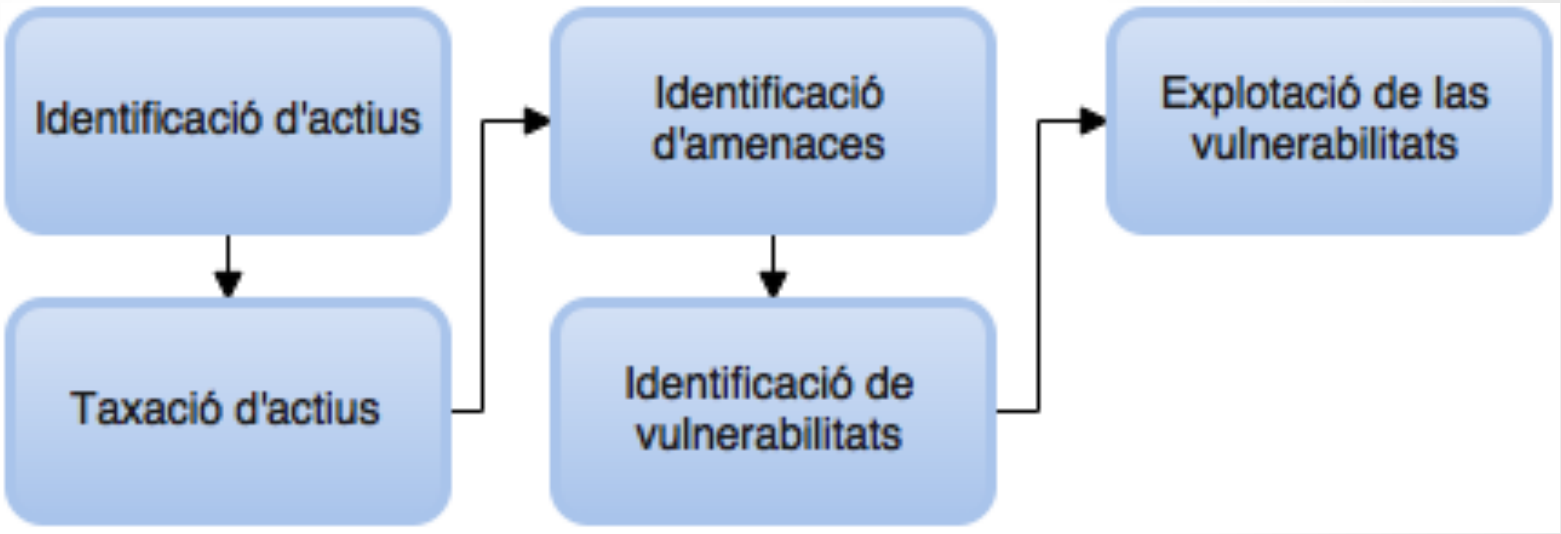


SISTEMA DE GESTIÓ DOCUMENTAL

- **Política de seguretat**
  - La informació com a eix central per a la confiança dels clients
  - Implicació de tot el personal
  - …
- **Assignació de responsabilitats i controls d'accés a la informació**
- **Protocols definits per a incidents concrets**
- **Procediment definit per a auditories internes**
- **Revisió per la direcció**
  - Comitè de seguretat
- **Assignació de rols i responsabilitats**
- **Metodologia d'anàlisi de riscos**

L'ANÀLISI DE RISCOS

- **Metodologia d'anàlisi de riscos:**



- Identificació: actius, amenaces i vulnerabilitats

ID	Actius	Valoració				Amenaces	Probabilitat d'ocurrència	Vulnerabilitat
		Confidencialitat	Integritat	Disponibilitat	Total			
A1	Dades de clients	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en enviaments, accés no autoritzat, control de documents
A2	Dades de proveïdors	A	A	A	A	Plagi, Falsificacio, Alteracio, Privacitat, Destrucció	B,B,B,A,M	Mala organització, errors en enviaments, accés no autoritzat, control de documents

- Declaració d'aplicabilitat

Control ISO + requeriment	Control	comentaris	Grau d'aplicabilitat
5.1 Política de seguretat de la informació.	2		APLICA
5.1.1 Document de política de seguretat de la informació.		Redacció del document de política de seguretat	APLICA
5.1.2 Revisió de la política de seguretat de la informació.		Pla de seguretat	APLICA

- Inventari, classificació i valoració d'actius

Àmbit	Actiu	Valoració
Dades	Dades de clients	6
Dades	Dades de proveïdors	6
Dades	Factures	3
Dades	Tarifes i ofertes	7
Dades	Inventari	3

- Dimensions de seguretat (ACIDA)

Àmbit	Actiu	Valor	Auditabilitat	Confidencialitat	Integritat	Disponibilitat	Autenticitat
Dades	Dades de clients	9,8	10	10	10	9	10
Dades	Dades de proveïdors	8,4	9	10	9	7	7
Dades	Factures	4,2	5	5	6	1	4
Dades	Tarifes i ofertes	4	3	5	6	1	5
Dades	Inventari	2,2	2	2	3	2	2

- Anàlisi d'amenaces (Definides per Magerit)

Amenaces	Identificador Amenaces
Desastres Naturals	DN
D'origen Industrial	OI
Errors i Fallides No Intencionats	NI
Atacs Intencionats	AI

Àmbit	Actiu	Freqüència	Autenticitat	Confidencialitat	Integritat	Disponibilitat	Trassabilitat
Dades	Dades de clients	20	25	45,3	33	30	7,5
	DN					1	
	OI			1		20	
	NI			80	50	40	30
	AI		100	100	80	60	
Dades	Dades de proveïdors	15	25	45,3	30	28	7,5
	DN					1	
	OI			1		20	
	NI			80	50	30	30
	AI		100	100	70	60	

- Calcul de l'impacte potencial

Àmbit	Actiu	Freqüència	Autenticitat	Confidencialitat	Integritat	Disponibilitat	Trassabilitat	Valor	Valoració impacte
Dades	Dades de clients	20	25	45,25	32,5	30,25	7,5	9,8	ALTA
Dades	Dades de proveïdors	15	25	45,25	30	27,75	7,5	8,4	ALTA
Dades	Factures	40	25	45,25	32,5	27,75	15	4,2	MITJA

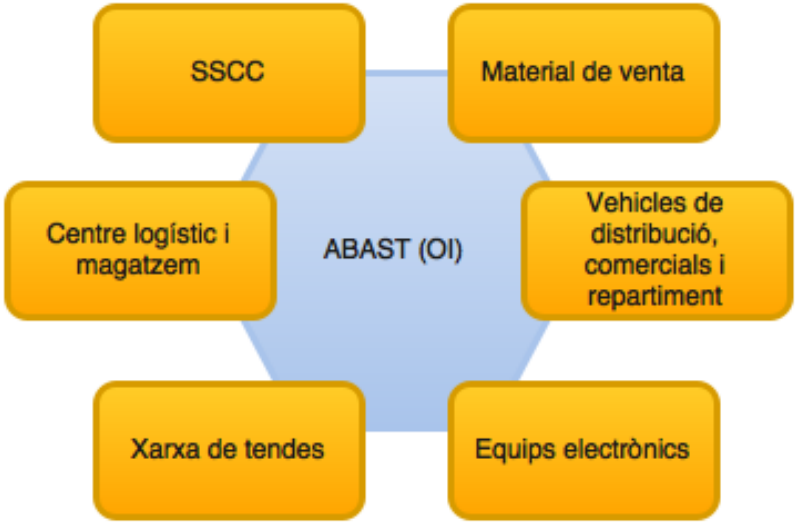
- Determinació del nivell de risc acceptable
  - Tots els actius amb una valoració de l'impacte superior a “mitjà”

PROPOSTA DE PROJECTES

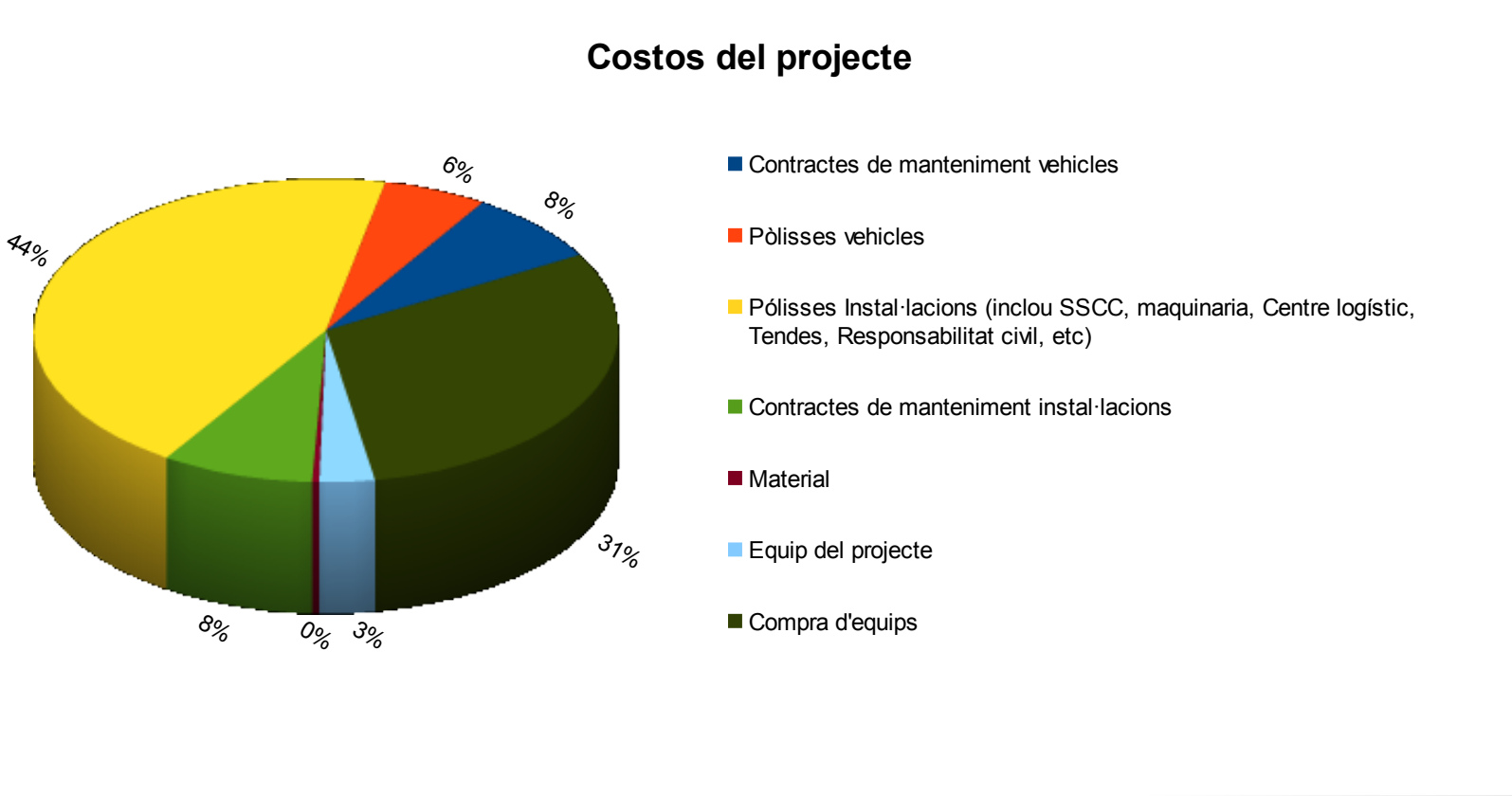
- Objectiu: millorar el nivell de compliment dels controls deifnits per la norma i la seguretat del SGSI
- 3 projectes genèrics enfocats per tipus d'origen dels riscos
  - Desastres naturals o industrials
  - No intencionats
  - Intencionats

MITIGACIÓ DE RISCOS ORIGINATS PER DESASTRES NATURAL O INDUSTRIALS

- **Objectiu**:
  - enfortir i disposar de mesures de prevenció sobre la seguretat ambiental dels locals, edificis, flota de vehicles i actius d'informció.
  - Millorar l'eficiència i la repercusió mediambiental
  - Causar un impacte positiu en la cultura de l'empresa
- **Abast:**



Costos del projecte i temporalitat



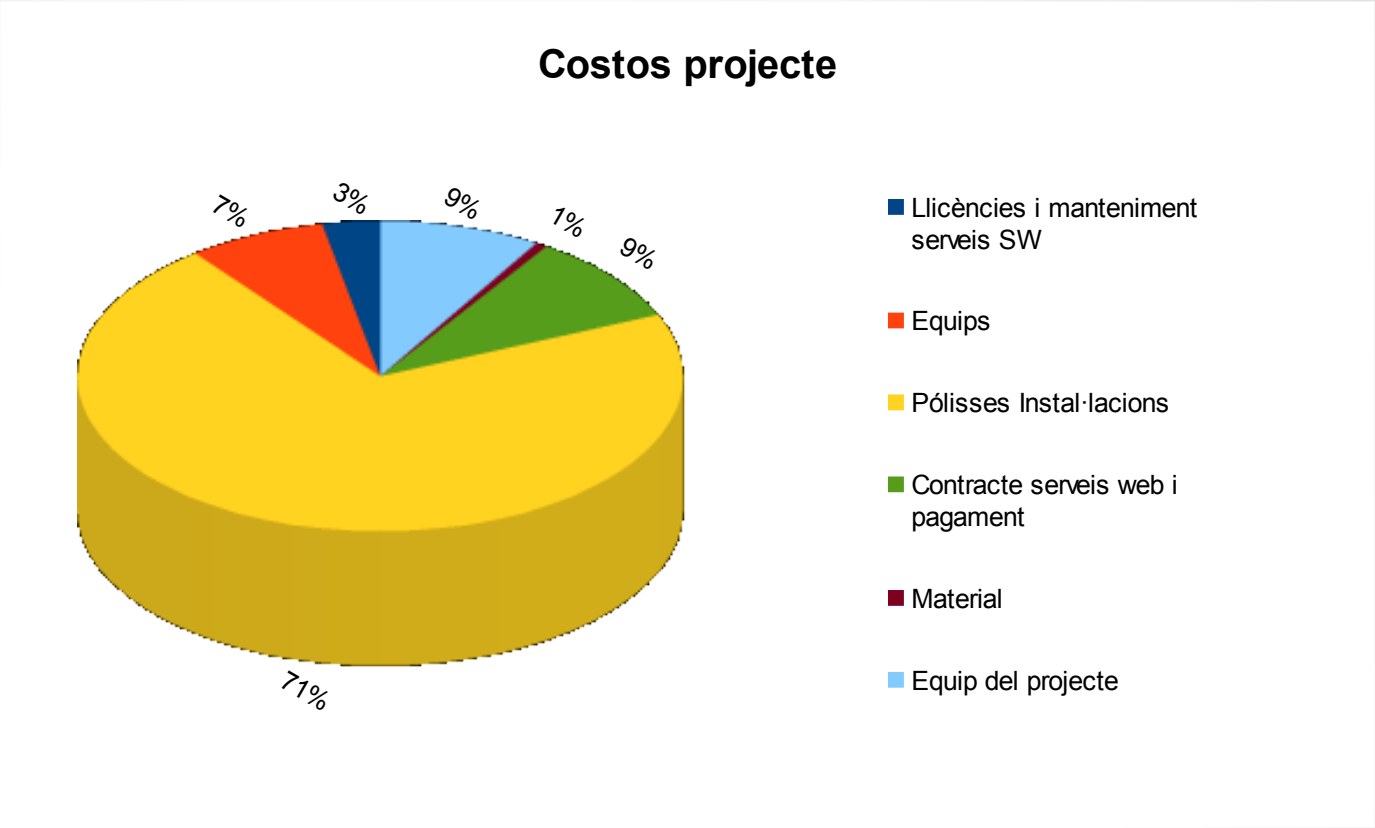
Fases	Any 2016														
	Mes 1				Mes 2				Mes 3				Mes 4		
1															
2															
3															
4															
5															
6															
7															
8															

MITIGACIÓ DE RISCOS D'ORIGEN INVOLUNTARI

- **Objectiu**:
  - enfortir i disposar de mesures de prevenció sobre la seguretat ambiental lògica i física que pugin afectar a actius crítics
  - Millorar la capacitat per evitar, identificar i mitigar riscos

- **Abast:**
  - Tots els actius físics i lògics definits en l'anàlisi de riscos

Costos del projecte i temporalitat

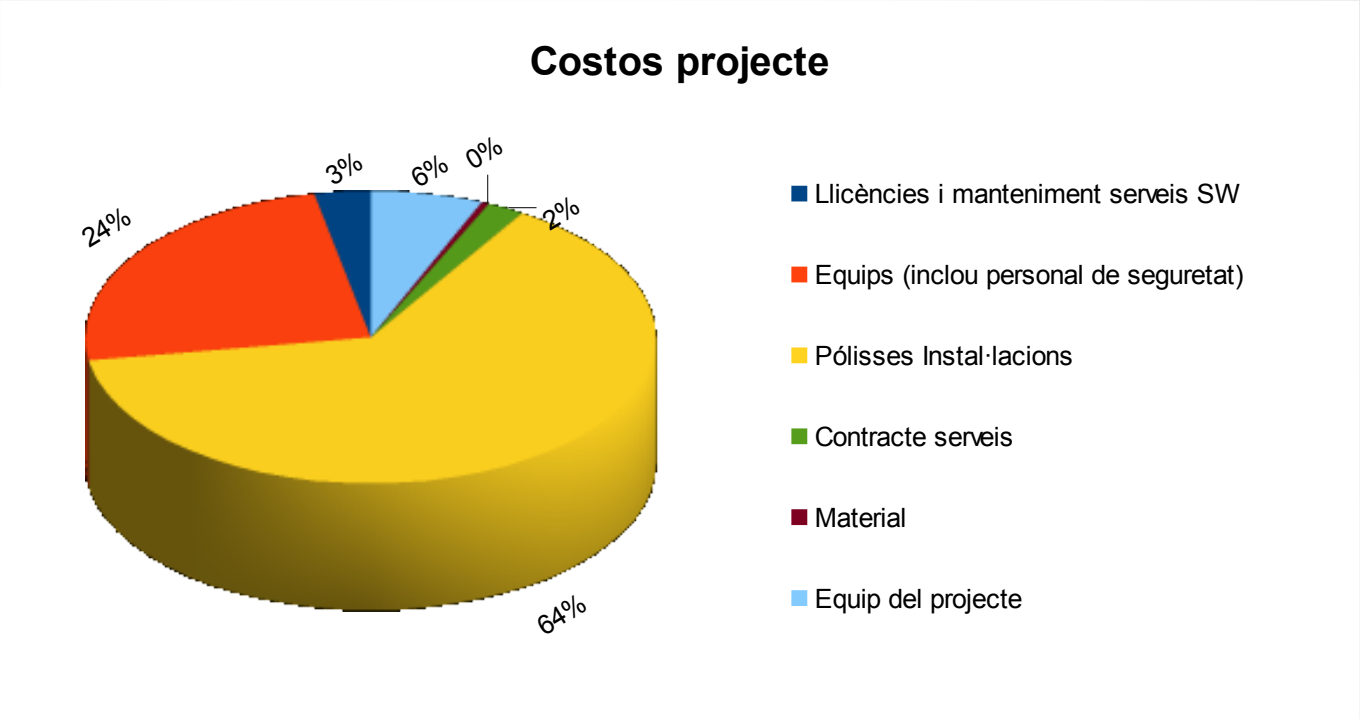


Fases	Any 2016															
	Mes 1				Mes 2				Mes 3				Mes 4			
1																
2																
3																
4																
5																
6																
7																
8																

MITIGACIÓ DE RISCOS D'ORIGEN VOLUNTARI

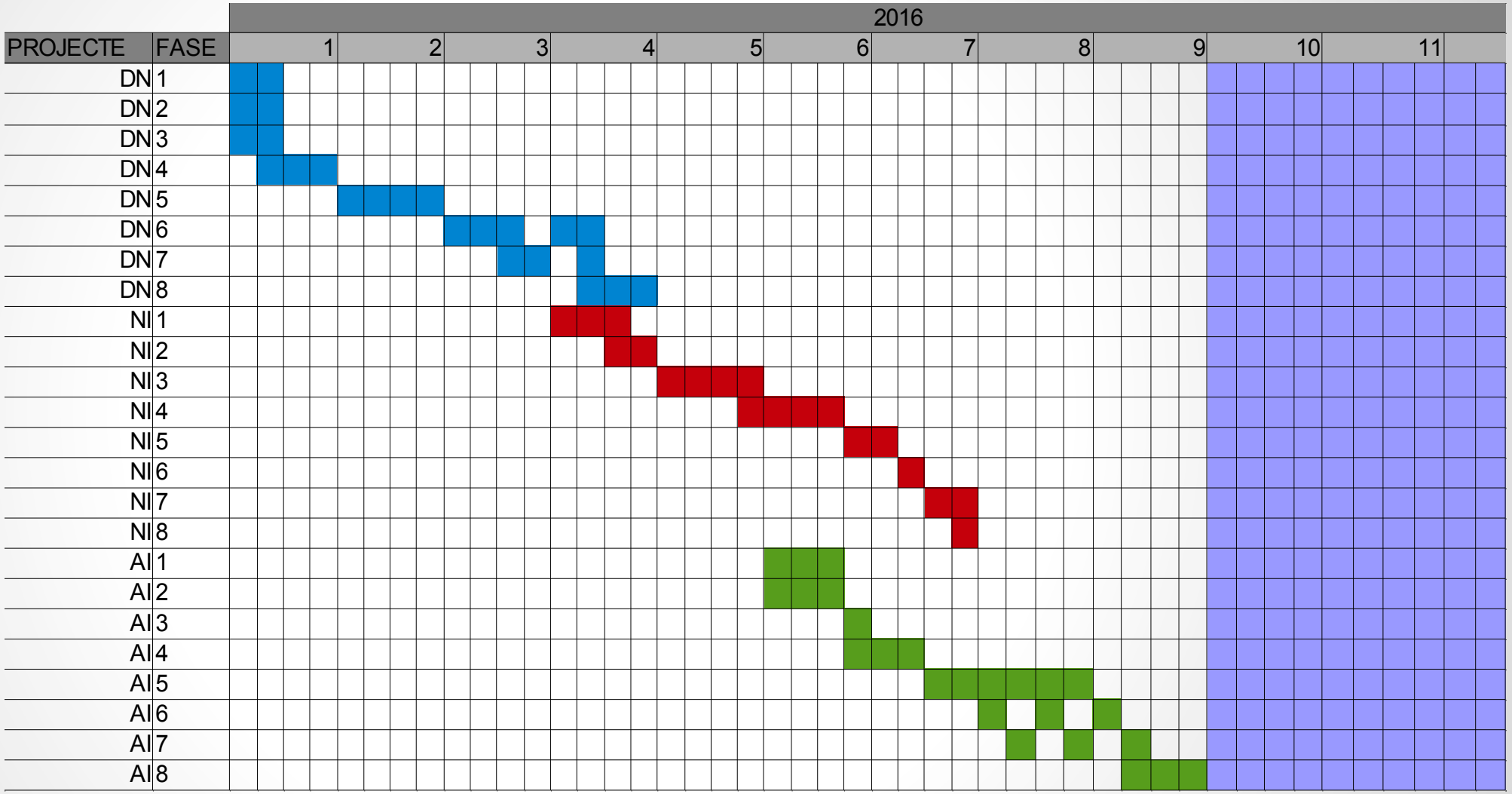
- **Objectiu**:
  - Enfortir i disposar de mesures i controls per a prevenir, actuar i afrontar atacs i altres accions intencionades que persegueixin malmetre els actius físics, lògics i reputacionals de l'empresa
  - Millorar la capacitat per evitar, identificar i minimitzar-ne l'impacte
- **Abast:**
  - Tots els actius físics i lògics definits en l'anàlisi de riscos

Costos del projecte i temporalitat



Fases	Any 2016															
	Mes 1			Mes 2				Mes 3				Mes 4				
1																
2																
3																
4																
5																
6																
7																
8																

PLANIFICACIÓ ANUAL DELS PROJECTES



AUDITORIA DE COMPLIMENT

- **Elaboració de l'informe d'auditoria de compliment**
  - Informació general
  - Execució de l'auditoria
  - Presentació de resultats
  - Conclusions

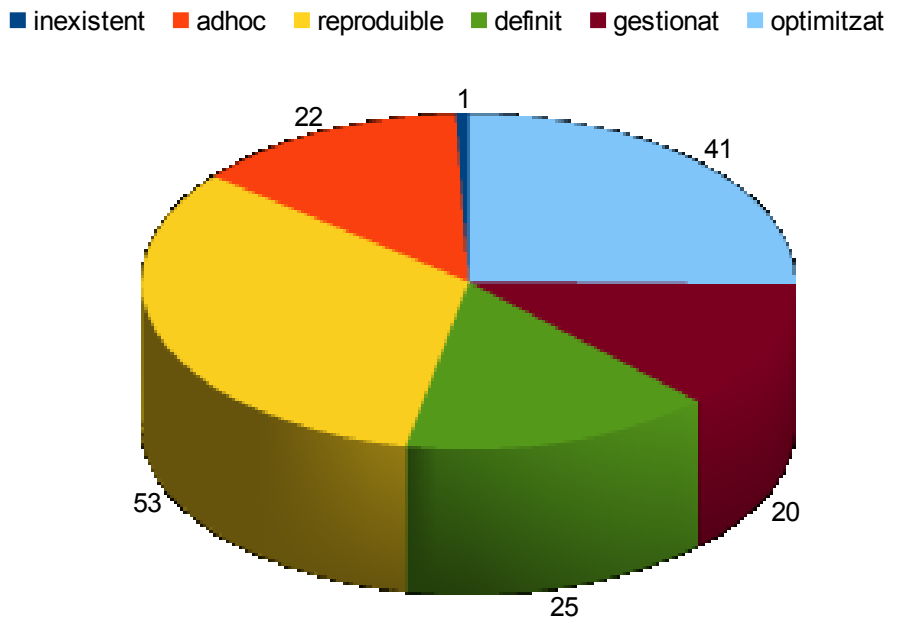
- **Anàlisi de resultats**

RESULTATS

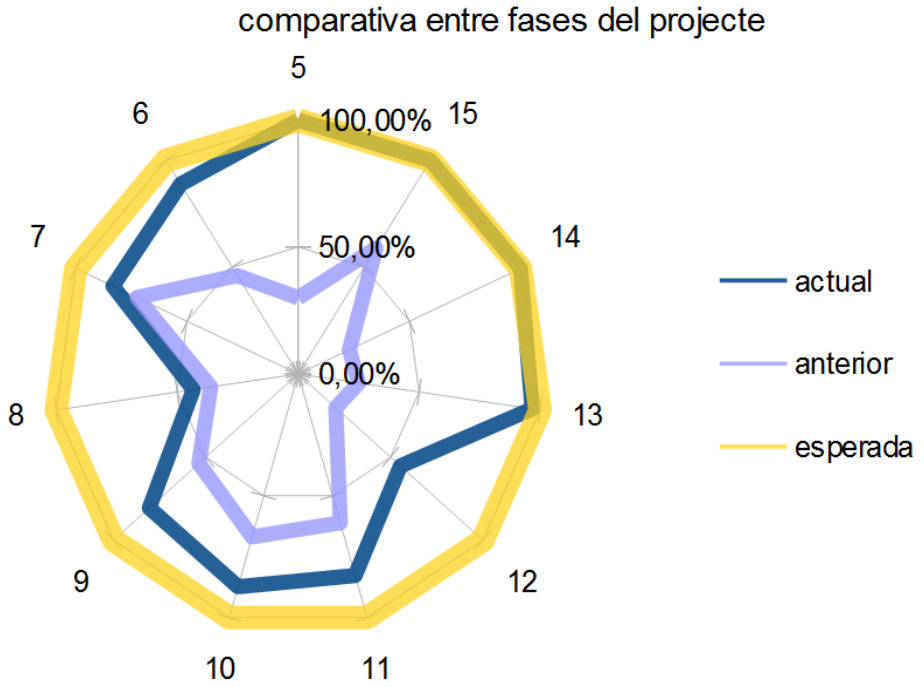
Estat de maduresa	83,48%

ACTUAL – POST PROJECTES	
5.POLÍTICA DE SEGURIDAD.	100,00%
6-ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	88,90%
7.GESTIÓN DE ACTIVOS.	83,33%
8.SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	43,33%
9.SEGURIDAD FÍSICA Y DEL ENTORNO.	80,60%
10.GESTIÓN DE COMUNICACIONES Y OPERACIONES.	87,36%
11.CONTROL DE ACCESO.	82,75%
12.ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	55,36%
13.GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	96,67%
14.GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	100,00%

Estat dels controls per percentatge de maduresa



Maduresa per dominis ISO



CONCLUSIONS

- S'ha assolit els objectius de compliment de la norma ISO per a les consideracions inicials de l'empresa
- S'ha millorat l'estat de seguretat del SGSI
- S'ha realitzat un bloc documental de l'anàlisi de riscos i l'auditoria del SGSI
- S'han proposat projectes que milloren el compliment i adecuació a la norma del SGSI

GRÀCIES PER LA SEVA ATENCIÓ