MISTIC-TREBALL FINAL DE MÀSTER

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

AUTOR: DAVID GONZÁLEZ MAS

CONSULTOR: ARSENIO TORTAJADA GALLEGO

ÀREA DE TREBALL FINAL: SISTEMES DE GESTIÓ DE SEGURETAT DE LA INFORMACIÓ

DATA DE LLIURAMENT: 01/2017

ÍNDEX

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

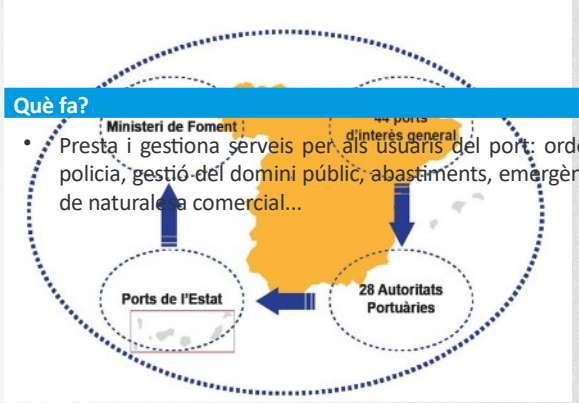
AP ZAPATA

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

Qui és?

- L'Autoritat Portuària de Zapata (APZ), és un organisme de dret públic amb personalitat jurídica i patrimoni propis.
- L'APZ forma part del Sistema Portuari Espanyol, que està format per 44 ports d'interès general, integrats en un total de 28 autoritat portuàries, que depenen de l'organisme públic Ports de l'Estat i que alhora depèn del Ministeri de Foment del Govern d'Espanya.

Què fa?



- Presta i gestiona serveis per als usuaris del port: ordenació, control de tràfic, policia, gestió del domini públic, abastiments, emergències, enllumenat, serveis de naturalesa comercial...

Característiques tècniques

- 543 ha de superfície terrestre
- 18000 ha de làmina d'aigua
- 17 km de línia d'atracada

Tipus de mercaderies

- Càrrega general.
- Sòlids i líquids a lloure.
- Siderúrgics.
- Vehicles.
- Petroquímic.

OBJECTIUS DEL PDSI

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

Per què necessita l'APZ un PDSI?

- Mitjançant el seu PCS, gestiona controls d'accessos que possibiliten l'entrada/sortida d'uns 2000 vehicles de gran volum al recinte portuari.
- Mitjançant el seu PCS, autoritza l'entrada de bucs a port.
- L'APZ gestiona emergències dins del recinte portuari (software + telefonia)
- El PCS, facilita les transaccions d'informació entre els agents portuaris i les administracions i entre els propis agents.
- De forma tradicional s'implementen mesures físiques de seguretat però a nivell lògic tot just es donen les primeres passes.

La pèrdua d'aquests actius d'informació generaria un gran impacte econòmic no només a l'APZ sinó a les empreses i grups d'interès que treballen amb el port.

Objectius del PDSI

- Identificar el riscos als que s'exposen els sistemes d'informació de l'APZ.
- Protegir la informació allotjada en el PCS.
- Protegir el sistema de control d'accessos de possibles atacs que puguin comprometre la seva informació i funcionament.
- Definir un marc de seguretat de la informació dins de l'organització.
- Incrementar el valor competitiu aconseguint una certificació ISO 27000.
- Reduir els costos derivats d'un incident de ciberseguretat.

ANÀLISI INICIAL

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

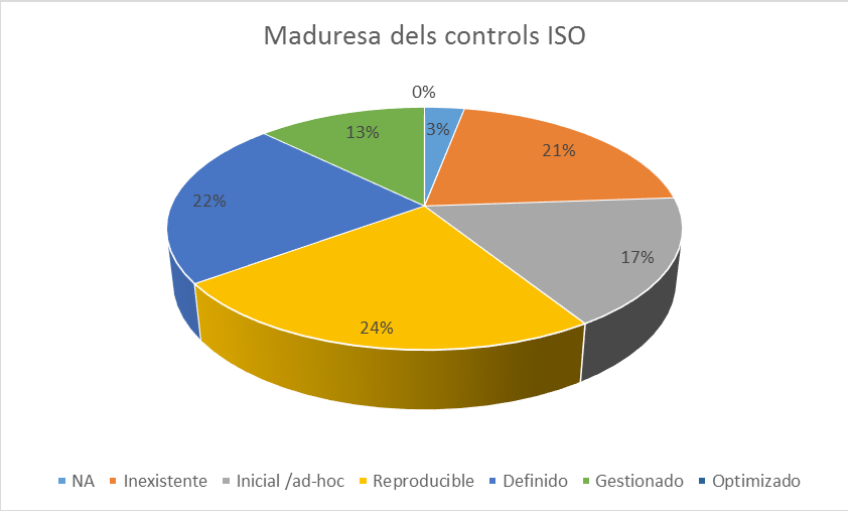
CMM			
EFECTIVITAT	CMM	SIGNIFICAT	DESC
0%	L0	Inexistent	Carènc procés
10%	L1	Inicial / Ad-hoc	Proced localitz
50%	L2	Reproduïble però intuïtiu.	Existei formali experiè
90%	L3	Procés definit	Els prc comun
95%	L4	Gestionat i	Es pot

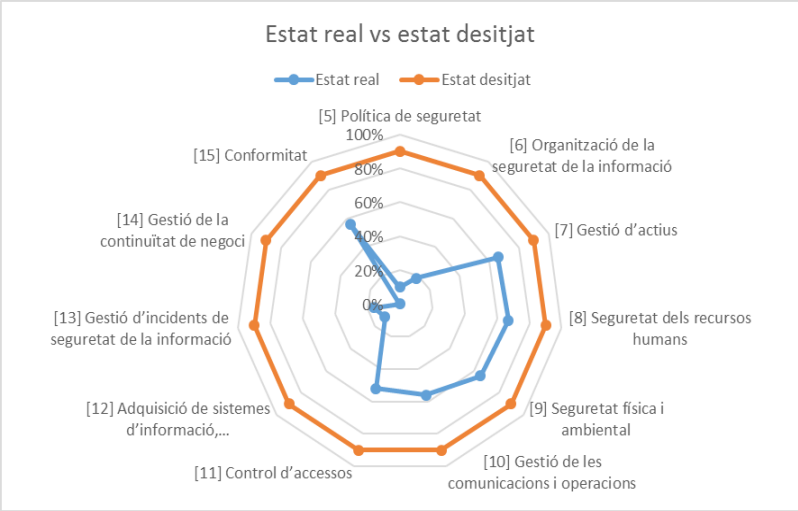
Objectius de control ISO 27002	
[5] Política de seguretat	
[6] Organització de la seguretat de la inform	
[7] Gestió d'actius	
[8] Seguretat dels recursos humans	
[9] Seguretat física i ambiental	
[10] Gestió de les comunicacions i operacio	
[11] Control d'accessos	
[12] Adquisició de sistemes d'informa manteniment	

CAP DELS DOMINIS ASSOLEIX EL 90 %

ANÀLISI INICIAL

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ



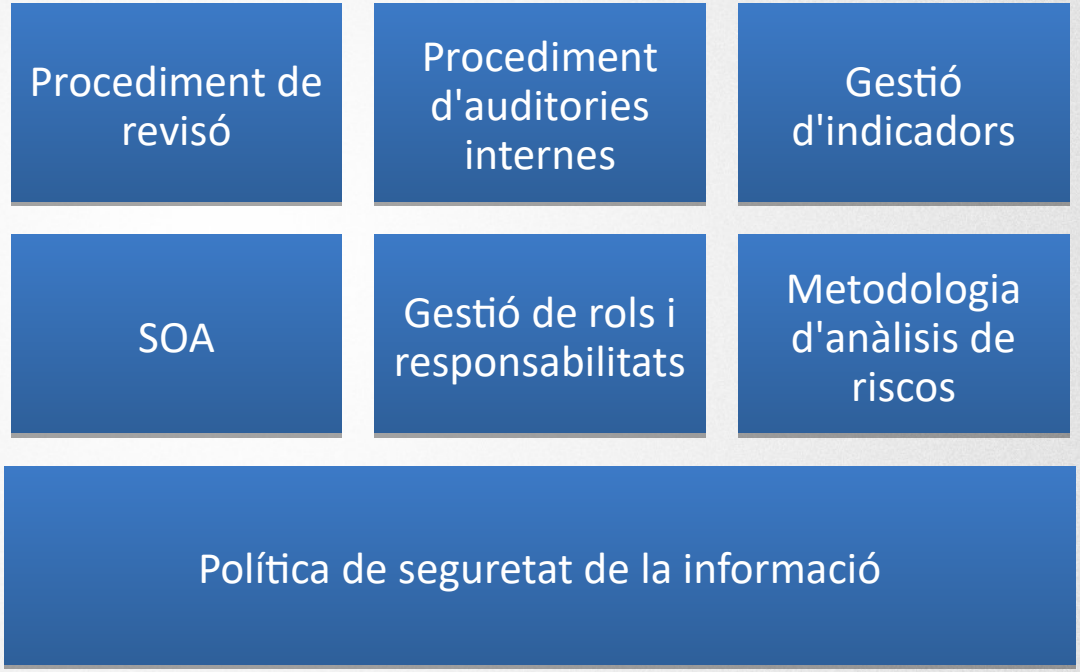


GAIREBÉ EL 50 % DELS CONTROLS ES TROBA EN UN ESTAT DEFINIT O REPRODUIBLE

APZapata

SGSI

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ



ANÀLISI DE RISCOS

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

Metodologia

- MAGERIT v3

Valoració d'actius

Determinar els actius rellevants per a la organització, les seves interrelacions i el seu valor (cost de la pèrdua o degradació de l'actiu).

[HW]	ID	VALOR	C	I	D	A	T	DP
[COM]	COM1	A	5	9	10	9	9	L1,AUX1, AUX6
	COM2	MA	5	7	10	9	10	L1,AUX1, AUX6

Anàlisi d'amenaces

Determinar les amenaces a les que estan exposades els actius identificats.

ID actiu	ID amenaça	F	C	I	D	A	T
COM1 COM2	E.24	FMB			100%		
	A.5	FB	100%	20%		100%	
	A.6	FB	20%	20%	50%		
	A.7	FB	10%	10%	10%		
			100%	100%	100%	100%	

ANÀLISI DE RISCOS

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

Metodologia

- MAGERIT v3

Determinar l'impacte potencial

Determinar l'impacte, definit com el dany sobre l'actiu derivat de la materialització d'una amenaça. $IP = VA * IA$

C	ID	V	VALOR DE L'ACTIU					IMPACTE					IMPACTE POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
C	COM1	A	5	9	10	9	9	100 %	100 %	100 %	100 %		5	9	10	9	0
	COM2	MA	5	7	10	9	10	100 %	100 %	100 %	100 %		5	7	10	9	0

Determinació del risc

Estimar el risc, definit com l'impacte ponderat amb la tassa d'ocurrència de l'amenaça. $RISC = F * IMPACTE$

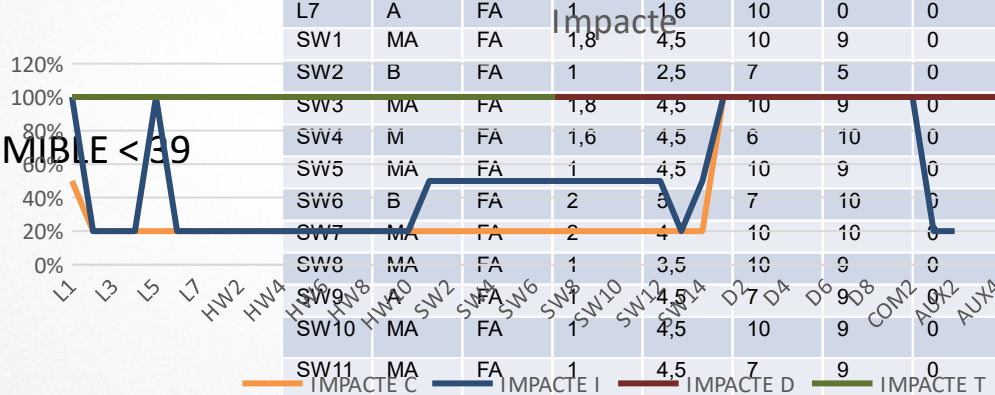
C	ID	V	F	IMPACTE POTENCIAL					RISC				
				C	I	D	A	T	C	I	D	A	T
[COM]	COM 1	A	FB	5	9	10	9	0	0,5	0,9	1	0,9	0
	COM 2	MA	FB	5	7	10	9	0	0,5	0,7	1	0,9	0

ANÀLISI DE RISCOS

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

Resultats

RISC ASSUMIBLE < 39



ID	V	F	IMPACTE POTENCIAL					RISC				
			C	I	D	A	T	C	I	D	A	T
L5	A	FA	0,2	9	7	0	0	2	90	70	0	0
L7	A	FA	1	1,6	10	0	0	10	16	100	0	0
SW1	MA	FA	1,8	4,5	10	9	0	18	45	10	90	0
SW2	B	FA	1	2,5	7	5	0	10	25	70	50	10
SW3	MA	FA	1,8	4,5	10	9	0	18	45	100	90	18
SW4	M	FA	1,6	4,5	6	10	0	16	45	60	100	16
SW5	MA	FA	1	4,5	10	9	0	10	45	100	90	10
SW6	B	FA	2	5	7	10	0	20	50	70	100	20
SW7	MA	FA	2	4	10	10	0	20	40	100	100	20
SW8	MA	FA	1	3,5	10	9	0	10	35	100	90	10
SW9	A	FA	1	4,5	7	9	0	10	45	70	90	10
SW10	MA	FA	1	4,5	10	9	0	10	45	100	90	10
SW11	MA	FA	1	4,5	7	9	0	10	45	70	90	10
SW12	B	FA	1	3,5	7	5	0	10	35	70	50	10
SW13	A	FA	1	3,5	10	7	0	10	35	100	70	10
SW14	A	FA	1	3,5	10	10	0	10	35	100	100	10

PROPOSTES DE MILLORA

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

Pla de formació i conscienciació

Duració: 1 any
Pressupost: 10.000 €

- Executar un pla de formació i conscienciació per a tots els empleats de la Organització.
- Mantenir un grau de conscienciació raonable en matèria de seguretat de la informació.
- Afavorir que el treballador reporti incidents de seguretat quan els detecti.

Definició de l'estructura de seguretat a l'APZ

Duració: 2 mesos
Pressupost: Projecte intern

- Adaptar l'estructura organitzativa per tal de crear un marc de seguretat.

Assignació i classificació d'actius d'informació

Duració: 3 mesos
Pressupost: Projecte intern

- Assignar propietaris i responsabilitats als actius de la Organització.
- Identificar els actius d'informació crítics per a la Organització.
- Establir objectius i responsabilitats vers els responsables dels actius.

Pla CN i resposta a incidents

Duració: 3 mesos
Pressupost: 30.000 €

- Elaboració i documentació dels procediments necessaris per garantir la continuïtat dels sistemes que donen suport a les operacions core de negoci.
- Minimitzar l'impacte d'una interrupció en la continuïtat de les operacions.
- Millorar la imatge de la Organització.
- Establir procediments per donar una resposta adequada als incidents de seguretat.

Implementació validació doble factor

Duració: 6 mesos
Pressupost: 100.000 €

- Assegurar l'autenticitat de la informació introduïda en els sistemes crítics per al negoci.

Reforç elèctric a les instalacions

Duració: 1mes
Pressupost: 60.000 €

- Garantir la continuïtat de les instal·lacions en cas de caiguda de subministrament elèctric.

PROPOSTES DE MILLORA

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

Monitorització se sistemes d'informació

Duració: 1 any
Pressupost: 10.000 €

- Conèixer l'estat en temps real del sistemes d'informació.
- Poder detectar el mes aviat possible una interrupció del servei o un estat anòmal en els sistemes d'informació.
- Establir mecanismes per protegir els registres obtinguts de la monitorització dels sistemes.
- Sincronitzar rellotges.

Redundància de la connexió de dades

Duració: 2 anys
Pressupost: 30.000 €

- Contractar una segona connexió a Internet.

HA per virtualitzadors

Duració: 1 mes
Pressupost: 80.000 €

- Aconseguir alta disponibilitat en els sistemes de virtualització.

Capacitació tècnica personal de sistemes

Duració: 2 anys
Pressupost: 30.000 €

- Reduir les incidències relacionades amb la no disponibilitat dels sistemes motivades per errors de configuració.

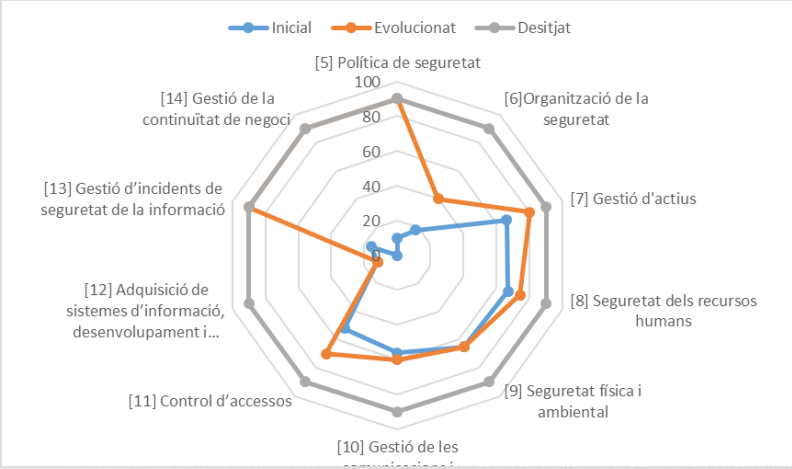
Total: 355.000 € en 2 anys

EVOLUCIÓ DEL RISC

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

Nivell d'acompliment de la norma ISO 27002

DOMINI	PROJECTE	CONTROL
8-Seguretat dels recursos humans	SI-PM-01,SI-PM-10	8.2.2, 8.2.1
6-Organització de la seguretat de la informació	SI-PM-02	6.1
7-Gestió d'actius	SI-PM-03	7.1,7.2
14-Gestió de la continuïtat de negoci	SI-PM-04	14.1
11-Control d'accessos	SI-PM-05, SI-PM-02	11.1,11.3,11.7
9-Seguretat física i ambiental	SI-PM-06,SI-PM-08	9.2.2
10-Gestió de les comunicacions i operacions	SI-PM-07, SI-PM-09	10.10, 10.5
15- Conformitat	SI-PM-02	

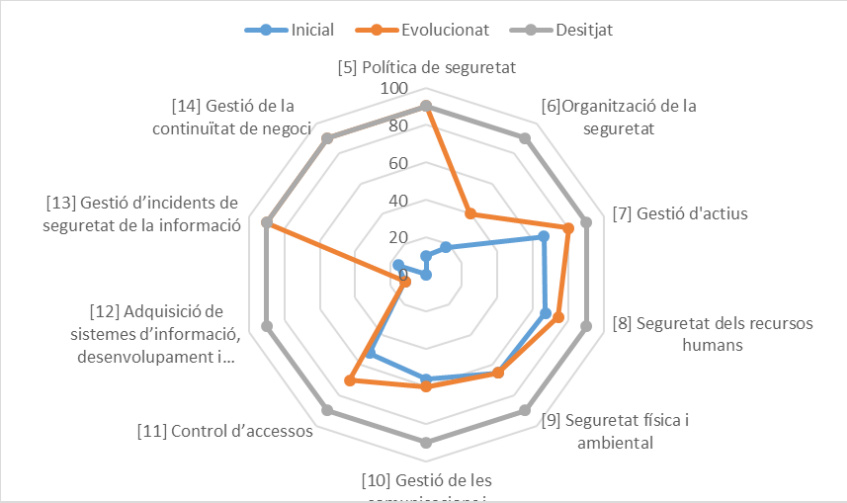


AUDITORIA DE CUMPLIMENT

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

Resum de no conformitats

DOMINI	NO CONFORMITATS	
	MAJORS	MENORS
[A.5] Política de seguretat		
[A.6] Organització de la seguretat de la informació	2	
[A.7] Gestió d'actius		1
[A.8] Seguretat dels recursos humans		1
[A.9] Seguretat física i ambiental		2
[A.10] Gestió de les comunicacions i operacions	1	1
[A.11] Control d'accessos		1
[A.12] Adquisició de sistemes d'informació, desenvolupament i manteniment.	1	
[A.13] Gestió d'incidents de seguretat de la informació		
[A.14] Gestió de la continuïtat de negoci		
[A.15] Conformitat		1



CONCLUSIONS

PLA DIRECTOR DE SEGURETAT DE LA INFORMACIÓ

L'APZ ha donat les primeres passes per implementar un procés de seguretat de la informació a l'organització.

- Identificació dels actius, assignació de propietaris, identificació de riscos.

- Amb una inversió relativament moderada i amb l'elaboració dels procediments i documentació del SGSI s'aconsegueix una bona millora en el grau d'acompliment segons la norma ISO 27002.

- Encara és aviat per afrontar una auditoria de certificació ISO 27001.

GRÀCIES!