




# MISTIC- Màster Interuniversitari en Seguretat de les TIC

## Treball Final de Màster

**Enrique Rubio Rodríguez**

**Maig 2012**

Universitat Rovira i Virgili

UOC
www.uoc.edu

UAB
Universitat Autònoma de Barcelona

# Pla Director de Seguretat de la Informació

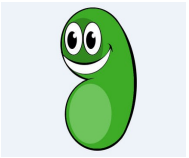

## NUCSSION

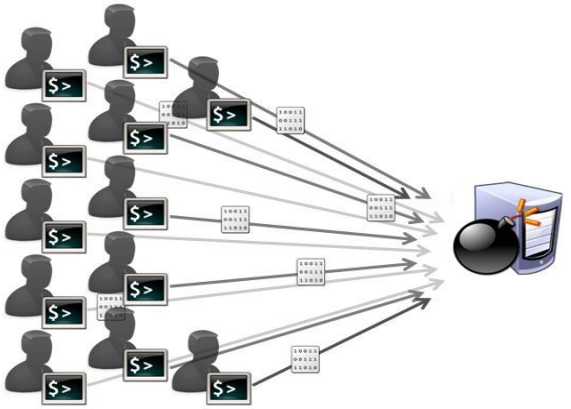
# NUCSSION

## La Seguretat de la Informació

La seguretat als sistemes d'informació es una qüestió clau a totes les organitzacions

Es especialment important en organitzacions com NUCSSION, considerades com a **infraestructura crítica**, pels possibles **impactes** que podria causar un atac sobre els **serveis essencials** que presten a la societat o sobre la **salut de les persones**




Tot el seguit d'amenaces tecnològiques junt amb la probabilitat de comissió d'errors o omissions del personal, risc de treballar amb tercers, etc., fa que sigui necessari adoptar una serie de mesures que minimitzin o eliminin la probabilitat d'ocurrència, redueixin les vulnerabilitats o, directament, suprimeixin riscos concrets.

Per aquest motius, NUCSSION ha dissenyat el **Pla Director de Seguretat de la Informació**, que abasta totes i cada una de les àrees de la empresa, i, especialment, les àrees i sistemes implicats en el control directe de la planta.

# NUCSSION

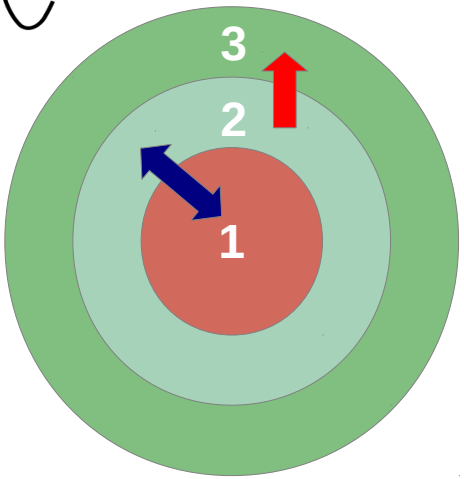
## Pla Director Seguretat Informació




El Pla defineix un model integral de gestió de riscos acord amb els estàndard nacionals i internacionals, així com amb les lleis estatals, internacionals i les normatives específiques del regulador CSN i CNPIC. El model bàsic correspondrà la norma ISO/IEC 27001.

# NUCSSION






| Defensa en profunditat | | Visibilitat nivells |
|---|---|---|
| Xarxa Procés | Nivell 1 – PLCs i equips de Planta | Bidireccional 1<->2 |
| | Nivell 2 – Ordinador de control de processos | |
| Xarxa Gestió | Nivell 3 – Xarxa de Gestió | Unidireccional 2->3 |

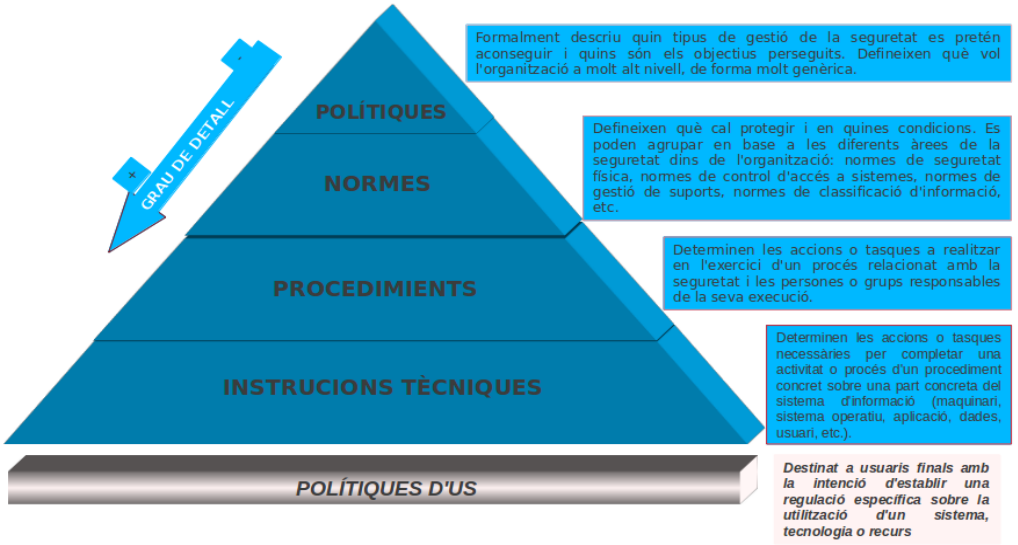
Unidireccionalitat física garantida per dispositius **DataDiode**

D'entre els nou projectes que inclou, destaca el projecte de defensa en profunditat, dirigit a garantir la separació física de les xarxes de gestió i sistemes de control de planta, quedant aquesta ultima com un entorn segur en front d'intents d'accés des de qualsevol punt extern a la mateixa

La protecció està encaminada a protegir la xarxa de sistemes de control, garantint la operació segura del reactor, els accessos il·legals, manipulació de dades, equips i instruments i robatori d'informació confidencial.

# NUCSSION

## Pla Director Seguretat Informació

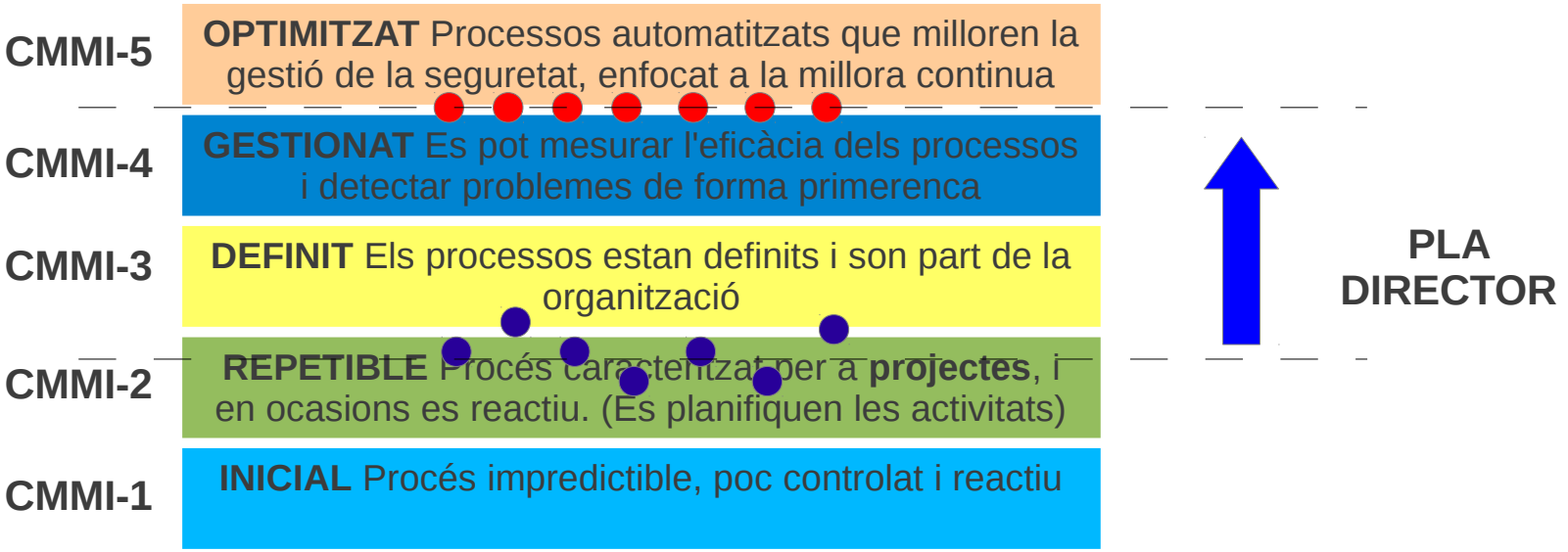



També s'estableix un marc normatiu de seguretat de la Informació i mesures per fomentar la formació i difondre entre tots els treballadors pràctiques d'us responsable i segur de les TIC

El Pla Director de Seguretat de la Informació de NUCSSION garanteix la qualitat i seguretat de tots els serveis TIC aconseguint una gestió eficient dels costos associats.

# NUCSSION

## Pla Director Seguretat Informació
## Objectiu




Definir la **estratègia** en seguretat TIC pel període 2013-2015, identificant i definit les accions a dur a terme, incrementant l'actual nivell de maduresa CMMI.

# NUCSSION

## Pla Director Seguretat Informació
## Avaluació de riscos

| EFECTIVITAT | CMM | SIGNIFICAT | DESCRIPCIÓ |
|---|---|---|---|
| 0% | L0 | Inexistent | Manca completa de qualsevol procés recognoscible.<br>No s'ha reconegut si més no que hi ha un problema a resoldre. |
| 10% | L1 | Inicial / Ad-hoc | Estat inicial on l'èxit de les activitats dels processos es basa la majoria de les vegades en l'esforç personal.<br>Els procediments són inexistents o localitzats en àrees concretes.<br>No hi ha plantilles definides a nivell corporatiu. |
| 50% | L2 | Reproduïble, però intuïtiu | Els processos similars es porten en forma similar per diferents persones amb la mateixa tasca.<br>Es normalitzen les bones pràctiques sobre<br>la base de l'experiència i al mètode.<br>No hi ha comunicació o entrenament<br>formal, les responsabilitats queden a càrrec de cada individu.<br>Es depèn del grau de coneixement de cada individu. |
| 90% | L3 | Proces Definit | L'organització sencera participa en el procés.<br>Els processos estan implantats, documentats i comunicats mitjançant entrenament. |
| 95% | L4 | Gestionat i mesurable | Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos.<br>Es disposa de tecnologia per automatitzar el flux de treball, es tenen eines per millorar la qualitat i l'eficiència. |
| 100% | L5 | Optimitzat | Els processos estan sota constant millora.<br>En base a criteris quantitatius es determinen les desviacions més comuns i s'optimitzen els processos. |

Taula utilitzada per avaluar la maduresa de la seguretat pel que fa als diferents dominis de seguretat i els 133 controls plantejats per la ISO / IEC 27002:2005.

Per poder dur a terme la valoració serà necessari completar cadascú dels següents apartats:

- Identificació i inventari d'actius
- Valoració dels actius
- Relació de la valoració amb les dimensions de la seguretat
- Anàlisi d'amenaces que afecten a cada actiu
- Càlcul de l'impacte potencial de cada amenaça sobre cada actiu

Per tal de no tenir una explosió de dades desmesurada, els actius s'agruparan d'acord a la metodologia **MAGERIT** en les següents categories: (Instal·lacions, Hardware ,Aplicació, Dades, Xarxa, Serveis, Equipament auxiliar, )Personal

Per aquest TFM s'utilitzarà l'anàlisi que proposa MAGERIT en e seu Llibre III (punt 2.1), completant-lo amb una estimació quantitativa, segons les següents categories

| Valor | Importància de l'actiu per l'organització | Justificació de la valoració |
|---|---|---|
| 4 | Molt alta | Es un actiu critic per l'organització, fonamental per la seguretat. El negoci no pot funcionar sense aquest actiu. Per exemple les dades de senyals de planta. |
| 3 | Alta | Es un actiu important per la seguretat, o del que depenen un o més actius crítics. El negoci pot veure reduïda, notablement, la seva activitat si l'actiu no està disponible. Per exemple el un dels PLC que registra senyals de planta. |
| 2 | Mitja | Es un actiu relacionat amb la seguretat o del que depenen actius importants. El negoci pot veure afectada, parcialment, la seva activitat si l'actiu no està disponible. Per exemple el servei de consulta externa de senyals de planta. |
| 1 | Baixa | Es un actiu que en cas de disponibilitat o mal funcionament representa un impacte baix per l'activitat del negoci. Per exemple una estació de consulta d'ODP o un PC d'escriptori |
| 0 | Menyspreable | Es un actiu que en cas de disponibilitat o mal funcionament representa un impacte pràcticament inexistent per l'activitat del negoci. Per exemple, un cable de xarxa o una impressora, ja que poden ser substituïts amb molta rapidesa. Aquest TFM no contempla aquest actius. |

Per cada un dels actius s'ha de mesurar la seva criticitat per cada una de les cinc dimensions de la seguretat de la informació (**ACIDT**): Autenticitat, Confidencialitat, Integritat, Disponibilitat, Traçabilitat.
Aquesta **valoració permetrà**, posteriorment, **avaluar l'impacte que tindrà la materialització d'una amenaça sobre la part de l'actiu exposat** (no cobert per les salvaguardes de cadascuna de les dimensions).

| Valor | Criteri | Justificació |
|---|---|---|
| 10 | Dany molt greu | Implica una interrupció total de les activitats del negoci |
| 7-9 | Dany greu | Implica una interrupció parcial de l'activitat del negoci |
| 4-6 | Dany important | Implica una reducció notable de l'activitat del negoci |
| 1-3 | Dany menor | Implica una reducció menor en l'activitat del negoci |
| 0 | Irrellevant | No te impacte en les activitats del negoci |

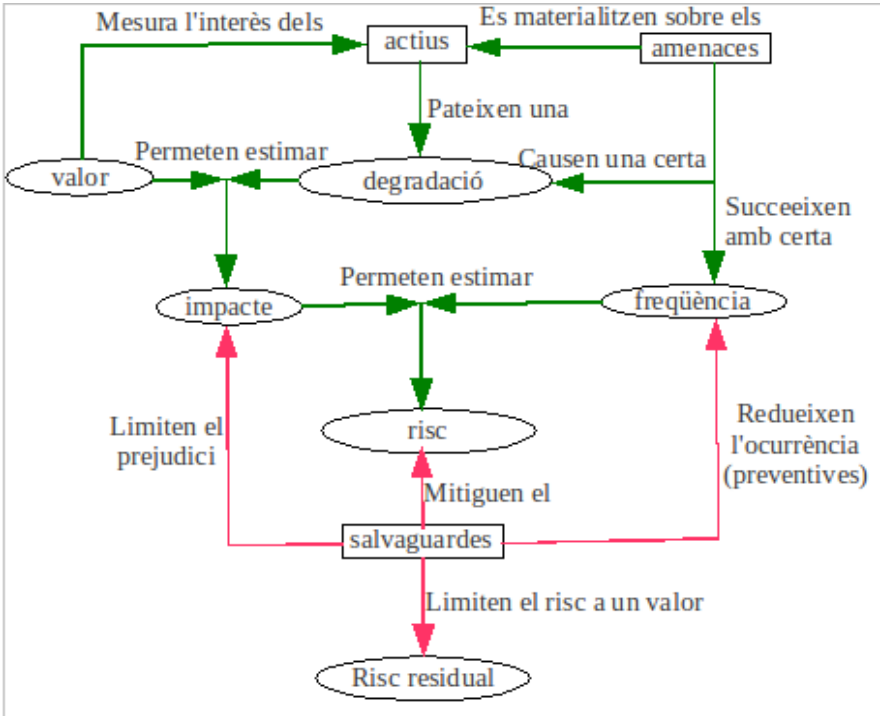
Una **amenaça** es la **probabilitat d'ocurrència d'un esdeveniment o acció que pot produir dany** (material o immaterial) sobre els actius d'informació.
El **dany** sobre un actiu pot afectar qualsevol de les seves dimensions de la seguretat (ACIDT), i serà **proporcional al grau d'exposició a la amenaça (vulnerabilitat)** que el provoca.

Per aquesta avaluació, s'utilitzaran les definides en **MAGERIT** Llibre 2 “Catàleg d'elements” apartat 5. En aquest manual, les amenaces es troben classificades dins els següents grans blocs:

- [N] Desastres naturals
- [I] D'origen industrial
- [E] Errors i fallades no intencionades
- [A] Atacs intencionats

**L'esmentat manual**, a banda de definir amb detall la llista d'amenaces, **indica tant els tipus d'actius com les dimensions de la seguretat afectades per cadascuna**.

Amb el coneixement previ del valor dels actius i de les relacions que existeixen entre ells, es determinarà risc que pot suposar per l'organització la materialització de les amenaces.
Aquesta dada permetrà prioritzar el pla d'acció, i, alhora, avaluar com es modificarà aquest quan s'hagin aplicat les contramesures.
Per donar una idea de conjunt d'on s'utilitzarà cada una de les dades obtingudes, cal revisar el següent esquema inclòs al “Libro_I_Metodo” de la metodologia MAGERIT V2 a la pàgina 132



Un cop identificats els actius i les seves dependències s'ha d'assignar una valoració a cada actiu principal, en cada una de les seves dimensions.
Per cada actiu **principal**, es detallen les valoracions a cada una de les seves dimensions.
Posteriorment, cada actiu **depenent** es relaciona amb els actius principals als que afecta i es calculen els valors per cada una de les dimensions com el màxim valor en cada una de les dimensions dels actius principals.

| **Actiu** | | | **A** | **C** | **I** | **D** | **T** |
|---|---|---|---|---|---|---|---|
| Actiu P1 | | | 2 | 4 | 5 | 4 | 1 |
| Actiu P2 | | | 1 | 7 | 3 | 6 | 2 |
| | **AP1** | **AP2** | | | | | |
| Actiu D1 | 1 | 1 | 2 | 7 | 5 | 6 | 2 |
| Actiu D2 | | 1 | 1 | 7 | 3 | 6 | 2 |
| Actiu D3 | 1 | | 2 | 4 | 5 | 4 | 1 |

Com es pot veure a la taula anterior, els actius principals P1 i P2 presenten els seus valors assignats després de l'entrevista amb els seus propietaris.
Els actius dependents (o subordinats) D1, D2 i D3 expressen la seva relació amb P1 i P2 mitjançant el valor **1** present a les columnes **AP1 i AP2**.

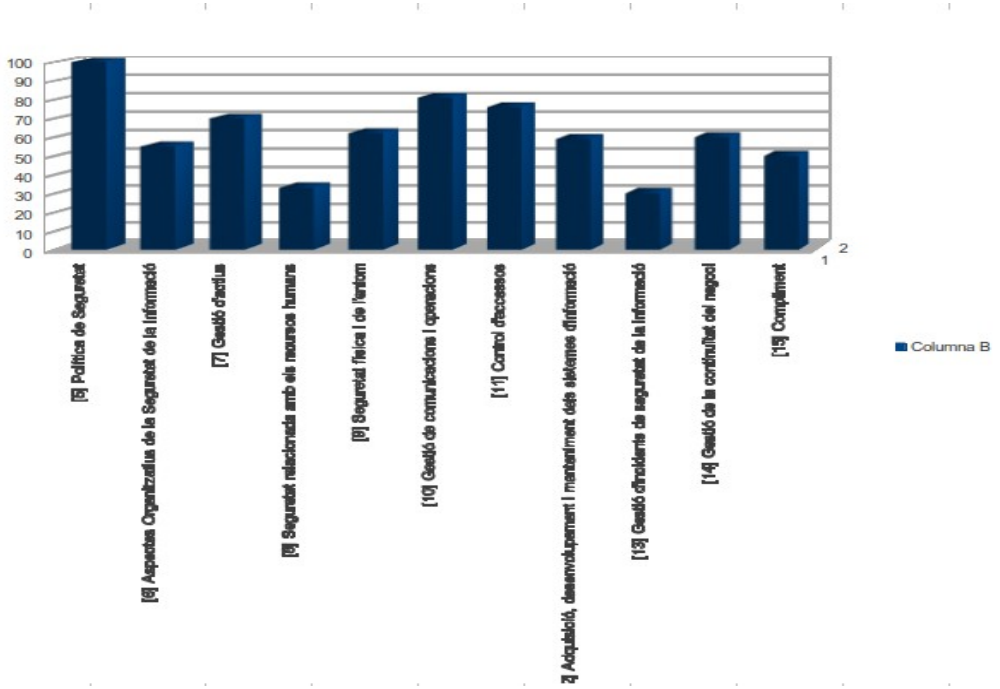
L'estimació del risc es l'ultim pas en el proces d'avaluació de riscos. Per obtenir el risc associat a cada actiu sols queda fer el càlcul per cada actiu i dimensió, prenen el valor de l'impacte i la freqüència d'ocurrència.
Per tal d'obtenir uns valors normalitzats, s'utilitzarà una funció que tornara un enter entre 1 i 7. Aquest valor serà funció de l'impacta i de la freqüència màxima acumulada d'ocurrència d'una amenaça per cada actiu.

| RISC | VALOR MAX. DIMENSIÓ | | | | | VALOR DE L'IMPACTE | | | | | VALOR RISC | | | | | RISC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A | C | I | D | T | A | C | I | D | T | A | C | I | D | T | MÀXIM |
| **ACTIU** | | | | | | | | | | | | | | | | |
| Accés usuaris interns, autenticació i autorització a sistemes | 7 | 7 | 7 | 8 | 7 | 1 | 6 | 7 | 2 | 1 | 2 | 5 | 5 | 3 | 2 | 5 |
| Servidor Active Directory | 7 | 7 | 7 | 8 | 7 | 1 | 7 | 7 | 8 | 1 | 2 | 5 | 5 | 5 | 2 | 5 |
| CPD ODP | 2 | 2 | 8 | 8 | 2 | 0 | 2 | 8 | 8 | 0 | 1 | 2 | 5 | 5 | 1 | 5 |
| Firewall ODP | 2 | 2 | 6 | 4 | 2 | 0 | 2 | 5 | 4 | 2 | 1 | 2 | 4 | 3 | 2 | 4 |

La funció que obté la estimació del risc es la següent:
Al valor de l'impacte de cada dimensió se li suma el valor màxim de la freqüència d'ocurrència(segons taula d'amenaces) mes una constant, en aquest cas 2. El resultat obtingut es divideix per 2. amb aquesta funció el valor mínim obtingut es 2 (1+1+2)/2 i el màxim 8 (10+4+2)/2.
D'aquesta manera s'obtenen resultats normalitzats i uniformes per poder realitzar, posteriorment, les accions pertinents per tal de reduir el risc.

# NUCSSION

## Pla Director Seguretat Informació
## Nivell de compliment actual




El resultat de la fase d'avaluació de riscos ha revelat que el **nivell de compliment actual** es troba en un modest **61 %**, que segons l'escalat anterior el situaria a la part baixa de CMM3.

# Pla Director Seguretat Informació
## Projectes Planificats

| ID | Descripció | Cost | Esforç |
|---|---|---|---|
| P1 | Ampliació de la Política de Seguretat i dels marcs contractuals | 30.000€ | 7 mesos |
| P2 | Millora de la Seguretat Física a les zones d'accés restringit i a les zones de carrega i descarrega | 2.000€ | 2 mesos |
| P3 | Gestió dels drets d'accés | 40.000€ | 6 mesos |
| P4 | Prevenció de l'us indegut dels recursos de tractament de la informació | 40.000€ | 8 mesos |
| P5 | Millora de les polítiques de seguretat | 50.000€ | 12 mesos |
| P6 | Millora de la seguretat del CPD, dels suports (backups i ordinadors portàtils) | 34.500€ | 12 mesos |
| P7 | Millora de la seguretat del software comercial o el desenvolupat a mida | 60.000€ | 12 mesos |
| P8 | Millora entorn desenvolupament NUCSSION | 5.000€ | 6 mesos |
| P9 | Aïllament físic de les xarxes de gestió i procés | 90.000€ | 24 mesos |

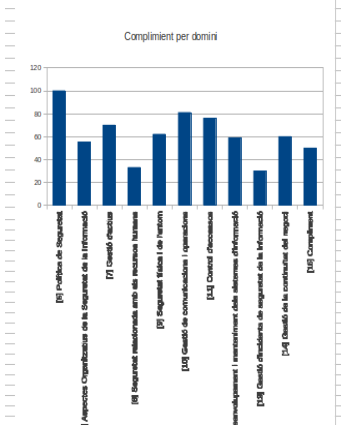
Durant el primer any, implantar aquelles accions correctores de menys cost i que comporten un esforç menor. La implantació d'aquestes accions permetrà incrementar el nivell de compliment fins CMM3 per tots els dominis de seguretat, assolint un nivell de compliment mínim del 80%. durant els anys següents s'implantarà la resta del Pla

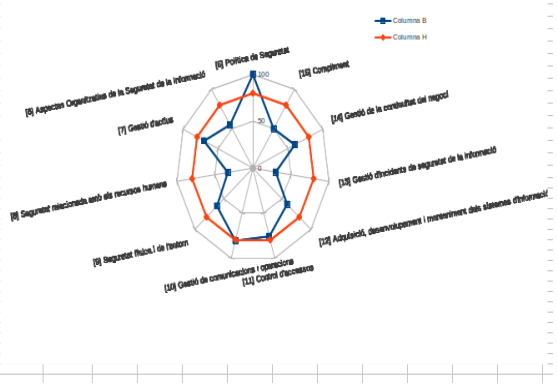
# NUCSSION

# Pla Director Seguretat Informació
# Comparativa primer any

| Domini | %Compliment | CMM | controls aplicables | controls totals | objectiu | |
|---|---|---|---|---|---|---|
| [5] Política de Seguretat | 100 | L5 | 2 | 2 | L3 | 80 |
| [6] Aspectes Organitzatius de la Seguretat de la Informació | 55 | L3 | 10 | 11 | L3 | 80 |
| [7] Gestió d'actius | 70 | L3 | 5 | 5 | L3 | 80 |
| [8] Seguretat relacionada amb els recursos humans | 33 | L2 | 9 | 9 | L3 | 80 |
| [9] Seguretat física i de l'entorn | 62 | L3 | 13 | 13 | L3 | 80 |
| [10] Gestió de comunicacions i operacions | 81 | L3 | 29 | 32 | L3 | 80 |
| [11] Control d'accessos | 76 | L3 | 23 | 25 | L3 | 80 |
| [12] Adquisició, desenvolupament i manteniment dels sistemes d'informac | 59 | L3 | 16 | 16 | L3 | 80 |
| [13] Gestió d'incidents de seguretat de la informació | 30 | L2 | 5 | 5 | L3 | 80 |
| [14] Gestió de la continuïtat del negoci | 60 | L3 | 5 | 5 | L3 | 80 |
| [15] Compliment | 50 | L2 | 10 | 10 | L3 | 80 |

| TOTALS | %Compliment | CMM | controls aplicables | controls totals |
|---|---|---|---|---|
| | 61 | L3 | 127 | 133 |

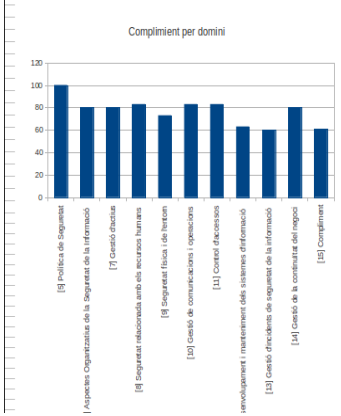


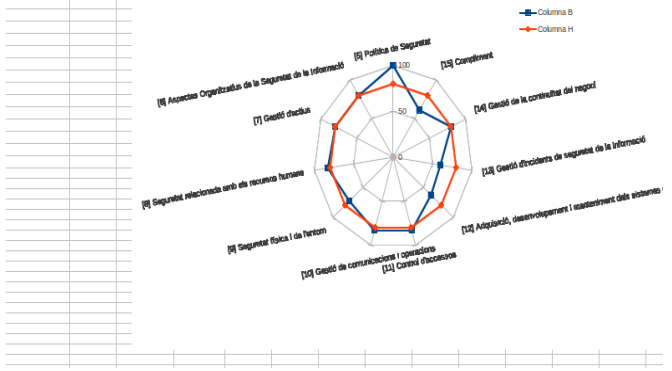




**Situació inicial, abans del primer any d'aplicació de control**

| Domini | %Compliment | CMM | controls aplicables | controls totals | objectiu | |
|---|---|---|---|---|---|---|
| [5] Política de Seguretat | 100 | L5 | 2 | 2 | L3 | 80 |
| [6] Aspectes Organitzatius de la Seguretat de la Informació | 80 | L3 | 10 | 11 | L3 | 80 |
| [7] Gestió d'actius | 80 | L3 | 5 | 5 | L3 | 80 |
| [8] Seguretat relacionada amb els recursos humans | 83 | L3 | 9 | 9 | L3 | 80 |
| [9] Seguretat física i de l'entorn | 73 | L3 | 13 | 13 | L3 | 80 |
| [10] Gestió de comunicacions i operacions | 83 | L3 | 29 | 32 | L3 | 80 |
| [11] Control d'accessos | 83 | L3 | 23 | 25 | L3 | 80 |
| [12] Adquisició, desenvolupament i manteniment dels sistemes d'informació | 63 | L3 | 16 | 16 | L3 | 80 |
| [13] Gestió d'incidents de seguretat de la informació | 60 | L3 | 5 | 5 | L3 | 80 |
| [14] Gestió de la continuïtat del negoci | 80 | L3 | 5 | 5 | L3 | 80 |
| [15] Compliment | 61 | L3 | 9 | 10 | L3 | 80 |

| TOTALS | %Compliment | CMM | controls aplicables | controls totals |
|---|---|---|---|---|
| | 77 | L3 | 126 | 133 |




**Situació després d'aplicar els controls del primer any**

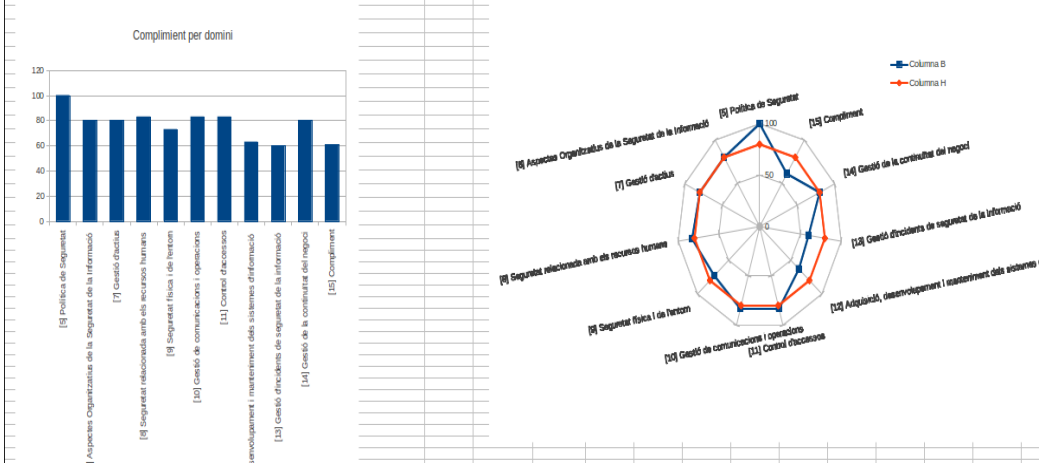
La aplicació de les contramesures implantades durant el primer any, aconseguiran l'objectiu de dur tots els dominis al nivell de compliment CMM3 amb un nivell de compliment proper al 80%

# NUCSSION

# Pla Director Seguretat Informació
# Comparativa anys següents

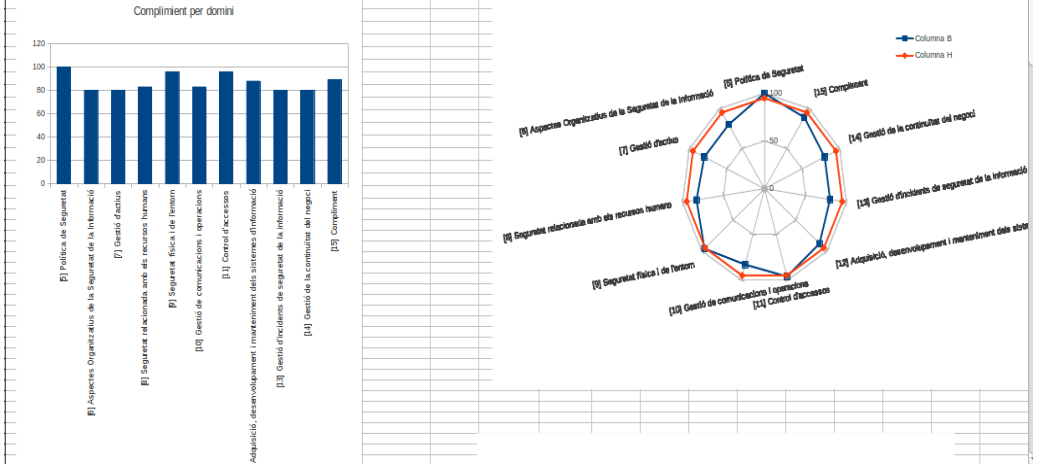
| Domini | %Compliment | CMM | controls aplicables | controls totals | objectiu | |
|---|---|---|---|---|---|---|
| [5] Política de Seguretat | 100 | L5 | 2 | 2 | L3 | 80 |
| [6] Aspectes Organitzatius de la Seguretat de la Informació | 80 | L3 | 10 | 11 | L3 | 80 |
| [7] Gestió d'actius | 80 | L3 | 5 | 5 | L3 | 80 |
| [8] Seguretat relacionada amb els recursos humans | 83 | L3 | 9 | 9 | L3 | 80 |
| [9] Seguretat física i de l'entorn | 73 | L3 | 13 | 13 | L3 | 80 |
| [10] Gestió de comunicacions i operacions | 83 | L3 | 29 | 32 | L3 | 80 |
| [11] Control d'accessos | 83 | L3 | 23 | 25 | L3 | 80 |
| [12] Adquisició, desenvolupament i manteniment dels sistemes d'informació | 63 | L3 | 16 | 16 | L3 | 80 |
| [13] Gestió d'incidents de seguretat de la informació | 60 | L3 | 5 | 5 | L3 | 80 |
| [14] Gestió de la continuïtat del negoci | 80 | L3 | 5 | 5 | L3 | 80 |
| [15] Compliment | 61 | L3 | 9 | 10 | L3 | 80 |

| TOTALS | %Compliment | CMM | controls aplicables | controls totals |
|---|---|---|---|---|
| | 77 | L3 | 126 | 133 |




| Domini | %Compliment | CMM | controls aplicables | controls totals | objectiu | |
|---|---|---|---|---|---|---|
| [5] Política de Seguretat | 100 | L5 | 2 | 2 | L5 | 95 |
| [6] Aspectes Organitzatius de la Seguretat de la Informació | 80 | L3 | 10 | 11 | L5 | 95 |
| [7] Gestió d'actius | 80 | L3 | 5 | 5 | L5 | 95 |
| [8] Seguretat relacionada amb els recursos humans | 83 | L3 | 9 | 9 | L5 | 95 |
| [9] Seguretat física i de l'entorn | 96 | L5 | 13 | 13 | L5 | 95 |
| [10] Gestió de comunicacions i operacions | 83 | L3 | 29 | 32 | L5 | 95 |
| [11] Control d'accessos | 96 | L5 | 23 | 25 | L5 | 95 |
| [12] Adquisició, desenvolupament i manteniment dels sistemes d'informació | 88 | L3 | 16 | 16 | L5 | 95 |
| [13] Gestió d'incidents de seguretat de la informació | 80 | L3 | 5 | 5 | L5 | 95 |
| [14] Gestió de la continuïtat del negoci | 80 | L3 | 5 | 5 | L5 | 95 |
| [15] Compliment | 89 | L3 | 9 | 10 | L5 | 95 |

| TOTALS | %Compliment | CMM | controls aplicables | controls totals |
|---|---|---|---|---|
| | 87 | L3 | 126 | 133 |




**Situació de partida segon any d'aplicació de les contramesures**

**Situació després d'aplicar les darreres contramesures**

La aplicació de les contramesures planificades per els darrers dos anys d'implantació del Pla Director de Seguretat de la Informació,aconseguiran l'objectiu d'apropar dos dimensions mes al nivell CMM5.


La aplicació del cicle de Deming (PDCA), un cop finalitzat el desplegament del Pla Director de Seguretat de la Informació  i després d'uns mesos d'operació, permetrà anar refinant i millorant el Sistema de Gestió de Seguretat de la Informació de NUCSSION.




# MISTIC- Màster Interuniversitari en Seguretat de les TIC

## Treball Final de Màster

**Enrique Rubio Rodríguez**

**Maig 2012**

# MOLTES GRÀCIES