Màster interuniversitari de Seguretat de les tecnologies de la informació i de les comunicacions

Implantació d'un Sistema de Gestió de la Seguretat de la Informació a *PREVENCIÓ S.L.*

Autor: Jordi Querol Gómez de Hinojosa

UAB Universitat Autònoma de Barcelona
UOC www.uoc.edu
Universitat Rovira i Virgili

Escenari de Treball

La empresa té actualment una plantilla d'uns 150 treballadors, entre tècnics de prevenció, metges i infermeres, comercials, administratius i els directors de les diferents àrees.

El personal es troba ubicat en diferents delegacions i en el client final. Per les connexions externes es treballa amb portàtils i a nivell global no es prenen mesures de seguretat suficients per garantir la privacitat de la informació.

Tracta amb dades sensibles associades a la salut dels treballadors de les empreses que contracten els seus serveis.

Subcontracta diferents serveis de vigilància de la salut i laboratoris clínics per poder cobrir els diferents territoris del àmbit nacional.

La empresa es troba immersa en una fase de creixement. Aquest creixement es basa en tres punts:

- **La captació de de nous clients.**
- **L'absorció de serveis de prevenció de menor envergadura.**
- **La incorporació dels serveis de prevenció que es troben en la plantilla de les empreses que contracten el seu servei.**

Les operatives realitzades es basen principalment en el coneixement, en l'experiència i en la maduresa professional de les persones que realitzen les diferents tasques organitzatives, no havent documentació escrita de tots els procediments d'actuació.

Escenari de Treball

L'empresa vol revisar la seva infraestructura tecnològica i que es tingui en compte dins de la definició dels diferents procediments.

La intenció de la empresa és realitzar una despesa moderada, aprofitant el material tecnològic que disposa actualment.

Aquestes mesures de seguretat no es poden definir de manera puntual, tal i com PREVENCIÓ S.L volia en una fase inicial, ja que les necessitats de seguretat varien en funció de:

- **La validació de l'eficiència de les mesures implantades**
- **L'evolució de la organització i de les seves necessitats**
- **L'evolució de les amenaces i dels requisits de la legislació vigent.**

Per poder donar un resultat eficient, proactiu i preventiu és necessari implantar un sistema de gestió de la informació, en el qual:

- **S'analitzi periòdicament l'estat actual de la organització i de les amenaces**
- **Es prioritzi l'aplicació de les mesures de seguretat tenint en compte els riscos**
- **S'adeqüi el pressupost que es pugui destinar anualment a la seguretat.**

Mapa de Ruta

Per part de *AUDITORIA S.L*, amb la col·laboració dels diferents estaments de *PREVENCIÓ S.L* s'ha fet les següents accions:

- **S'ha col·laborat en la elaboració d'un Pla Director, en el que s'ha definit els objectius de seguretat que ha de tenir la organització, i s'ha format el comitè de seguretat encarregat de valorar periòdicament l'estat de seguretat de la organització. S'ha definit com a responsable de seguretat al Director Comercial, que és la persona que actualment realitza les principals tasques dels serveis informàtics de la organització, persona que no té una dedicació en exclusiva a aquestes funcions.**

- **Hem realitzat un anàlisis de riscos intrínsec per valorar els diferents actius de la informació que disposa la organització, i les amenaces que afecten a aquests actius.**

- **La valoració econòmica no s'ha realitzat només en base al seu cost de reposició, sinó que s'ha considerat la dependència que suposa per la resta d'actius d'informació la materialització d'una amenaça sobre aquest element particular.**

- **S'ha utilitzat la metodologia *MAGERIT*, la qual es tracta d'una de les metodologies d'anàlisi de riscos més valorades per la quantificació econòmica que es realitza de les amenaces i per el seu catàleg definit tant a nivell de classificació d'actius, amenaces i salvaguardes.**

- **Per la valoració del risc anual s'ha utilitzat com a criteri principal la dimensió de seguretat més important de cadascun dels actius (Autenticitat, Confidencialitat, Integritat, Disponibilitat i Traçabilitat).**

Mapa de Ruta

Per part de *AUDITORIA S.L*, amb la col·laboració dels diferents estaments de *PREVENCIÓ S.L* s'ha fet les següents accions:

- **S'ha fet una Auditoria de Seguretat seguint la normativa *ISO 27002*, la qual permet valorar d'una manera extensa els diferents controls que intervenen en la seguretat de la informació de qualsevol tipus d'empresa. Aquesta normativa ens permet valorar la maduresa de la nostra organització tant a nivell general com a nivell del diferents controls.**

- **Hem realitzat un anàlisis residual amb les diferents salvaguardes detectades en el anàlisis de riscos per tal de que es pogués valorar la seva eficiència real i tenir-ho en compte en els diferents projectes de millora.**

- **S'han presentat un conjunt de projectes que milloren la seguretat de la informació a *PREVENCIÓ S.L.*,valorant l'impacte individual i el global de tots els projectes.**

- **S'ha fet una estimació econòmica en la reducció de riscos de la organització. S'ha calculat el retorn de la inversió inicial durant 5 anys en base a aquesta reducció de risc i el cost de manteniment de la solució.**

- **S'ha avaluat la influència dels diferents projectes en l'estat de maduresa de la organització.**

Resultats obtinguts: Anàlisi de Riscos

S'han identificat els principals actius d'informació en la organització:

- **Instal·lacions:** Edifici central, Delegacions Territorials,Unitat mòbil
- **Hardware:** PCs de sobretaula, Portàtils, Servidor de correu, Servidor aplicació PREVENET, Router central, Switch Central, Routers delegacions, Blackberries.
- **Aplicacions:** Windows Server, Windows XP, Internet Information Service (IIS), Microsoft SQL Server, PREVENET, Microsoft Exchange Server, NFS, Contasol, Microsoft Office.
- **Dades:** Dades de prevenció, Documentació de formació, Dades de vigilància de la salut, Procediments interns, Dades comptables, Dades comercials, Contractes amb clients, Contractes amb proveïdors.
- **Xarxes**:Connexió externa als servidors centrals, Xarxa Local.
- **Serveis:** Accés a la informació impresa, Recurs de fitxers, Servei de Directoris, Correu electrònic, Accés dades de vigilància de la salut, Accés a dades de prevenció, Pàgina Web de l'empresa.
- **Equipaments auxiliars:** Sistema elèctric.
- **Personal:** Director Comercial, Director de Prevenció, Comercials, Director Mèdic, Infermera central amb experiència, Director financer, Tècnic informàtic, Resta de personal.

Resultats obtinguts: Anàlisi de Riscos

Per la realització de la valoració dels diferents actius a nivell de seguretat s'ha tingut en compte la dependència amb la resta d'actius en cas de que es materialitzi una amenaça.

Les amenaces escollides són les que disposa el catàleg d'elements de *MAGERIT*. Per la valoració del impacte de les diferents amenaces s'ha utilitzat la dimensió de seguretat principal de cadascun dels actius.

En base a aquests criteris, s'ha obtingut l'anàlisi de riscos associat:

Actiu/Amenaces	Valor	Risc Intrínsec Anual
Equipaments Auxiliars	300.000 €	1.315 €
Xarxes	600.000 €	108.921 €
Serveis	650.000 €	42.753 €
Instal·lacions	750.000 €	17.404 €
Personal	1.350.000 €	3.164 €
Dades	1.410.000 €	76.982 €
Hardware	2.250.000 €	174.300 €
Aplicacions	2.700.000 €	428.745 €
Total	**10.010.000 €**	**853.584 €**

Resultats obtinguts: Anàlisi de Riscos

Es pot comprovar que els principals actius als quals recauen un major pes dins de PREVENCIÓ S.L són les aplicacions i el hardware.

Les dades pròpiament també tenen un valor elevat però les actuacions que s'han de realitzar a nivell de seguretat són menors.

Destaca l'impacte que té sobre la seguretat les diferents xarxes.

A nivell de serveis la valoració dels actius i dels riscos associats és menor que en altres categories ja que sòl ser l'últim esglaó de dependències (hi han molt pocs actius que depenguin d'un servei i el seu valor es troba repercutit en la resta d'actius de la informació).

Analitzant l'impacte dels diferents atacs, s'ha observat principalment:

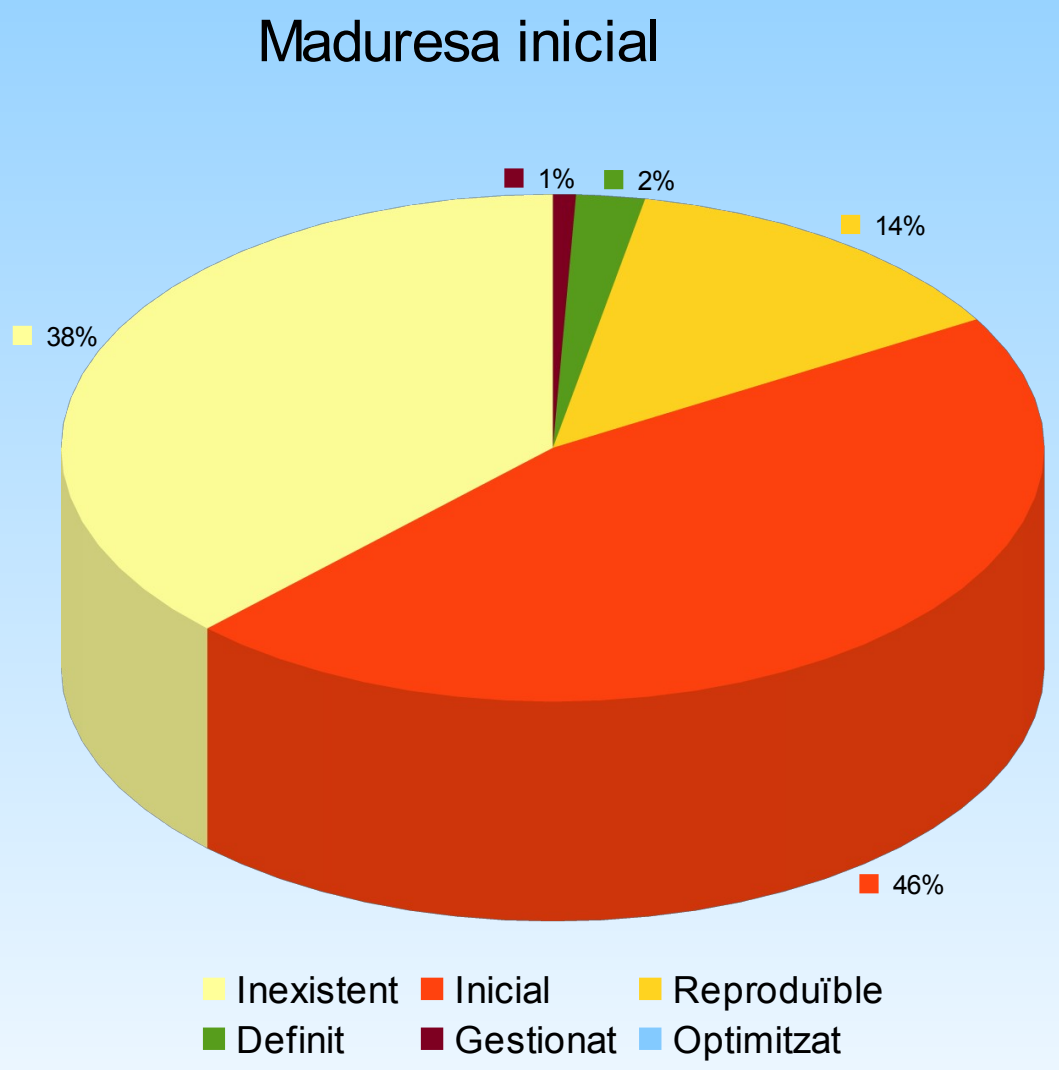
- **Els atacs no autoritzats es produeixen amb una freqüència molt alta en diferents categories d'actius, amb un impacte destacable.**
- **Els riscos associats als errors de configuració del administrador, de manteniment i actualització del software tenen un risc molt alt. Només disposem d'un tècnic un dia a la setmana per realitzar tasques de manteniment i disposem d'un conjunt heterogeni de versions de sistema operatiu i eines ofimàtiques.**
- **A nivell de personal destaquen les deficiències de la organització a nivell de definició de protocols i responsabilitat en les actuacions, que repercuteixen principalment sobre la disponibilitat del servei.**

Resultats obtinguts: Model de Maduresa de la Capacitat (CMM)

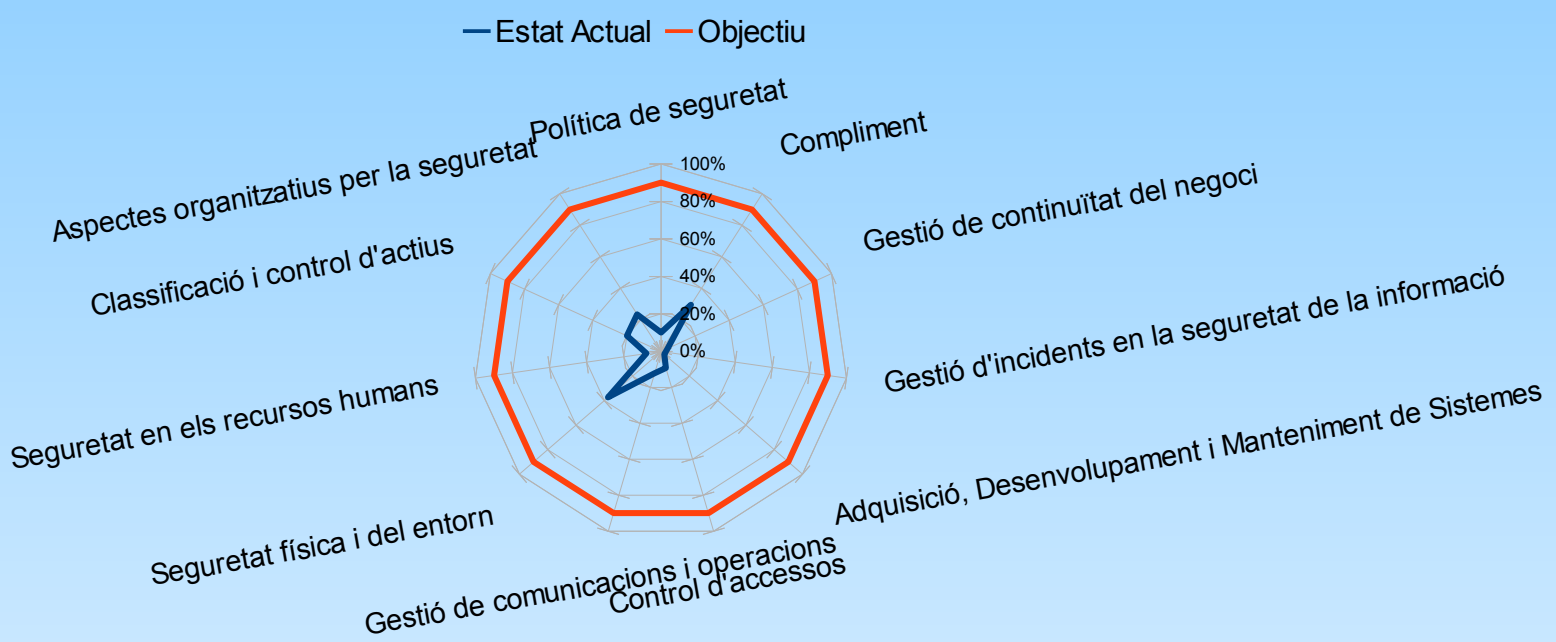
La maduresa dels controls de seguretat es realitzarà a Model de Maduresa de la Capacitat que utilitza *ISO 27002*.

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

Resultats obtinguts: Model de Maduresa de la Capacitat (CMM)



Resultats obtinguts: Model de Maduresa de la Capacitat (CMM)



Podem comprovar que l'estat de maduresa general de PREVENCIO S.L es troba a nivell general en un nivell Inicial segons el model CMM i fins i tot amb un desconeixement alt sobre les mesures de seguretat.

Ens trobem amb una situació freqüent en la petita i mitjana empresa, la qual utilitza el seu servei d'informació com una eina necessària per desenvolupar el seu negoci i no ho han valorat com els actius principals a protegir.

Projectes de millora

Segons l'anàlisi de gestió de riscos, hem de prioritzar les salvaguardes en:

- **Les dades de vigilància de la salut, tant la part informàtica com el servei imprès.**
- **Els equips d'usuari (PCs i portàtils), els quals es comuniquen des de diferents ubicacions, on les mesures de seguretat no es troben sota el control de PREVENCIÓ S.L.Treballem a través d'una xarxa pública, per tant, la comunicació es pot veure compromesa si no realitzem les mesures de seguretat oportunes.**
- **Les aplicacions dels diferents terminals. No disposem d'una infraestructura homogènia i sota un control administratiu necessari.**

En base a la Auditoria de Compliment de la ISO 27002 destaquem els següents aspectes:

- **Hem de definir una política de seguretat. Permetrà a PREVENCIÓ S.L. establir les bases sobre el seu sistema de gestió de la informació.**
- **S'ha de millorar la gestió dels recursos humans i la contractació de serveis. Es requereix un assessorament sobre els diferents aspectes relacionats en la contractació.**
- **PREVENCIO S.L ha de definir els diferents procediments en el que intervinguin els diferents actius de la informació. Hem de conscienciar al personal sobre la utilització dels diferents elements.**
- **S'ha de millorar les comunicacions des de l'exterior. No s'estan prenent les mesures suficients.**
- **S'ha de realitzar una gestió documental dels incidents de seguretat per poder actuar en major celeritat quan es produeixin, detectar les causes dels incidents, i reduir l'impacte associat.**

Projectes de millora

Tenint en compte aquests dos anàlisi realitzant es proposaran projectes que abordin els següents punts:

- **Disposar de més personal tècnic especialitzat per fer el manteniment del sistema. Es tracta d'una empresa que està creixent i que no es pot permetre disposar dels sistemes amb un control tan reduït. El control actual comporta que es materialitzin amb major freqüència els errors associats al administrador.**

- **Definir procediments interns per realitzar les diferents tasques. Repercuteix especialment en la disponibilitat de la informació.**

- **Prendre les mesures oportunes per millorar la seguretat de les dades, especialment la confidencialitat de les dades de vigilància de la salut.**

- **Potenciar la protecció de la comunicació entre els equips remots i la central ja que els seus riscos són molt elevats.**

- **Prendre les mesures oportunes per minimitzar els atacs que puguin procedir des de l'exterior.**

Per tant, es presentaran els següents projectes:

- **Organització del sistema de seguretat de la informació**
- **Integració de la gestió de la seguretat dins de la organització. Documentació procediments**
- **Revisió de les relacions contractuals**
- **Implantació d'un sistema de gestió incidental**
- **Configuració d'un firewall i establiment xarxa virtual (VPN) per les connexions exteriors**
- **Instal·lació d'un detector d'intrusions (Ids)**
- **Reestructuració del equip tecnològic**

Projectes de millora

Addicionalment s'han revisat els següents projectes que en la lectura del cas han destacat:

- **Canvi ubicació sala de servidors per reduir el risc associat a inundacions**
- **Millores en el procediment de backup, associades a la seva eficàcia i ubicació actual.**

A més, s'ha fet esment a solucions de Cloud Computing com alternativa a l'allotjament de la informació dins de la pròpia empresa i com a mesura per externalitzar els serveis.

No s'ha arribat a aprofundir suficientment per valorar l'impacte econòmic i els canvis en la maduresa de la organització. De totes formes són alternatives a considerar a mig termini.

Projectes: Organització del sistema de seguretat de la informació

PREVENCIO S.L. definirà la seguretat de la empresa amb el suport que AUDITORIA S.L

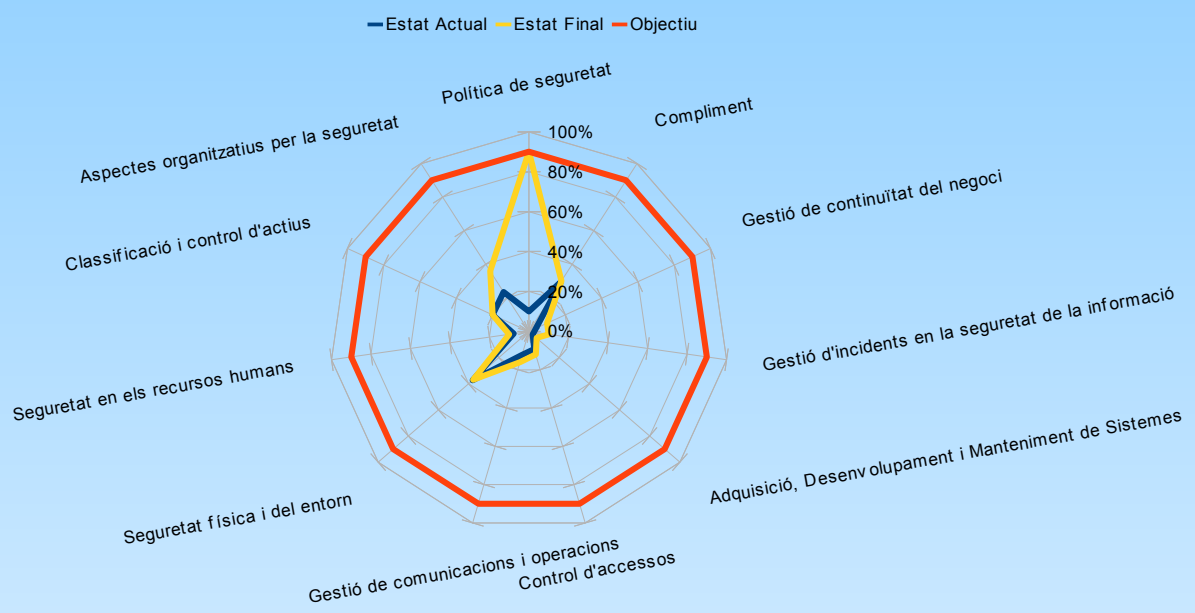
Es definirà els participants del comitè de gestió. És definiran el rols d'aquest grup, principalment:

- **Definir i revisar i aprovar les polítiques de seguretat.**
- **Verificar la eficàcia de la política de seguretat.**
- **Aportar els recursos necessaris per la seguretat de la informació.**
- **Decidir els canvis que es realitzaran en el SGSI.**
- **Assegurar que s'han implantat els controls pactats.**
- **Reunir periòdicament per el control del SGSI**

Aquest grup definirà la política de seguretat, el qual ha de ser accessible i conegut per tot el personal de la organització:

- **Ha de quedar clar què és el que es vol protegir, de qui, de què, i per què**
- **Definir la responsabilitat del personal envers a la seguretat de la informació**
- **Donar les pautes del personal, tant en la seva actuació diària com en possibles problemes que puguin sorgir, i identificar quins són els màxims responsables.**
- **Ha de quedar clara la implicació de la direcció amb les pautes que marca la política.**

Projectes: Organització del sistema de seguretat de la informació



El cost d'implantació de la solució i el retorn de la inversió és el següent:

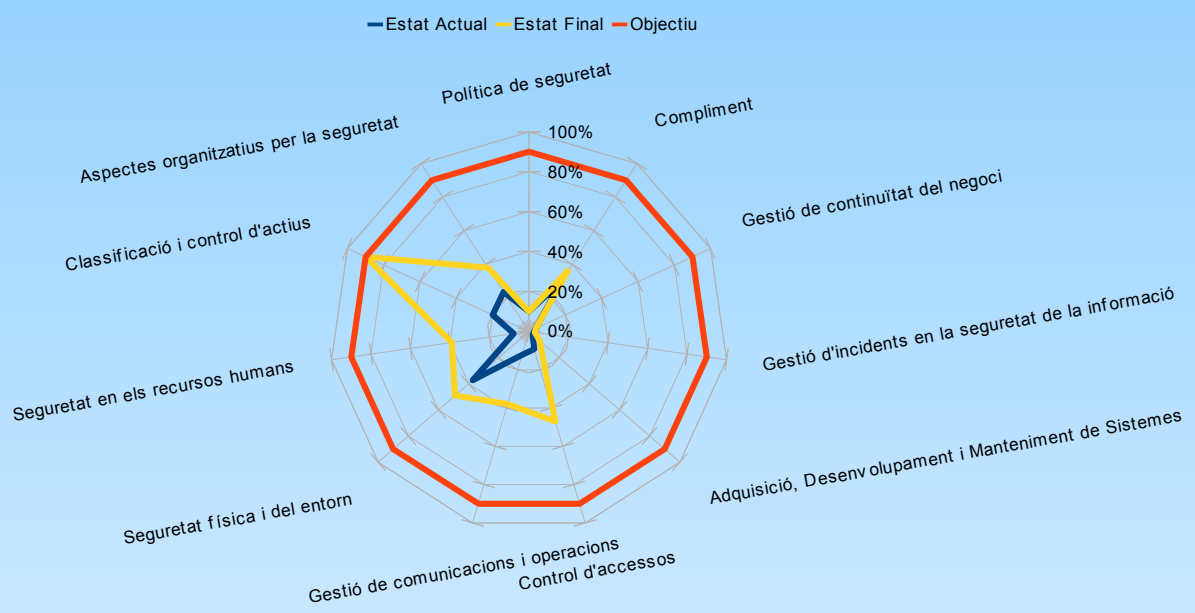
	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	7.000 €	7.000 €	7.000 €	7.000 €	7.000 €
Amortització	5.000 €	5.000 €	5.000 €		
Benefici brut	16.000 €	16.000 €	16.000 €	16.000 €	16.000 €
Benefici net	4.000 €	4.000 €	4.000 €	9.000 €	9.000 €

Projectes: Documentació de procediments interns

PREVENCIÓ S.L. crearà i es definiran els diferents procediments associats al tractament dels actius de la informació, amb la col·laboració de AUDITORIA S.L.

- **S'hauran de revisar i definir els diferents procediments interns. En aquest projecte ens enfocarem més a la part de gestió interna de la organització, envers dels processos dels sistemes informàtics.**
- **S'adaptarà el document de classificació dels actius, incloent dins d'aquests inventari tots els actius de la informació, assignat al seu responsable, format, ubicació, llicència i valor dins del negoci.**
- **S'identificaran tots els processos al que es troben sotmesos la informació des de la seva generació fins a la seva destrucció i es documentarà el seu tractament.**
- **La redacció dels procediments es basaran en la definició de la política de seguretat. Caldrà la col·laboració de diferent personal de la organització, tant en la seva elaboració inicial com en el manteniment periòdic, identificant les variacions en el tractament de la informació.**
- **Per els diferents documents i ens procediments on s'hagin de tenir en compte els diferents aspectes de seguretat, l'Institut Nacional de Tecnologies de la informació (INTECO) disposa de diferents documents formatius que serviran com a referència a PREVENCIÓ S.L.**

Projectes: Documentació de procediments interns



El cost d'implantació de la solució i el retorn de la inversió és el següent:

	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	7.000 €	7.000 €	7.000 €	7.000 €	7.000 €
Amortització	27.667 €	27.667 €	27.667 €		
Benefici brut	138.685 €	138.685 €	138.685 €	138.685 €	138.685 €
Benefici net	104.018 €	104.018 €	104.018 €	131.685 €	131.685 €

Projectes: Revisió de les relacions contractuals

Es revisaran les diferents relacions contractuals amb els diferents actors que interactuen amb PREVENCIÓ S.L. per que s'incloguin mesures de seguretat necessàries.

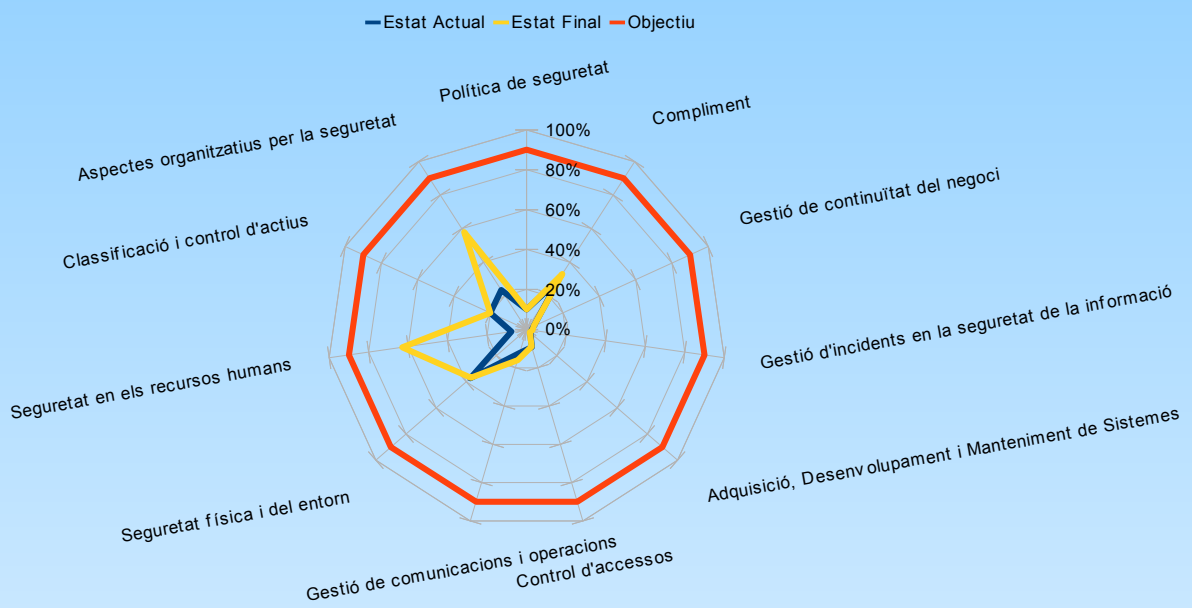
- **Treballadors:** **En la redacció del contracte ha de constar les diferents responsabilitats que té el treballador i les obligacions legals associades al seu lloc de treball. Com a mínim hauria d'haver un model de contracte per cadascuna de les àrees de la empresa.**

- **Proveïdors:** **Dins d'aquesta categoria es trobarien com a proveïdors que interactuen els serveis de prevenció subcontractats, els serveis de missatgeria, els laboratoris clínics, els tècnics informàtics externs, les empreses d'auditoria que revisen la seguretat del sistema, etc... S'haurà de fer constar el nivell de servei desitjat (temps d'entrega, disponibilitat, compromís acordat en cas d'incompliment...), els controls de seguretat física i lògica que estiguin aplicant, la possibilitat d'auditar els serveis oferts i clàusules de confidencialitat.**

- **Clients:** **S'haurien d'incloure un compromís formal respecte a les mesures mínimes per protegir les dades sensibles amb les que tracta PREVENCIÓ S.L. en les instal·lacions del client**

Per la revisió dels diferents models és subcontractarà una assessoria laboral. PREVENCIÓ S.L pot utilitzar com a punt de partida la guia de referència la publicació que realitza INTECO sobre la gestió de contractes en el document guia_avanzada_de_gestion_de_contratos.pdf.

Projectes: Revisió de les relacions contractuals



El cost d'implantació de la solució i el retorn de la inversió és el següent:

	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	1.000 €	1.000 €	1.000 €	1.000 €	1.000 €
Amortització	2.125 €	2.125 €	2.125 €		
Benefici brut	6.375 €	6.375 €	6.375 €	6.375 €	6.375 €
Benefici net	3.250 €	3.250 €	3.250 €	5.375 €	5.375 €

Projectes: Implantació d'un sistema de gestió incidental

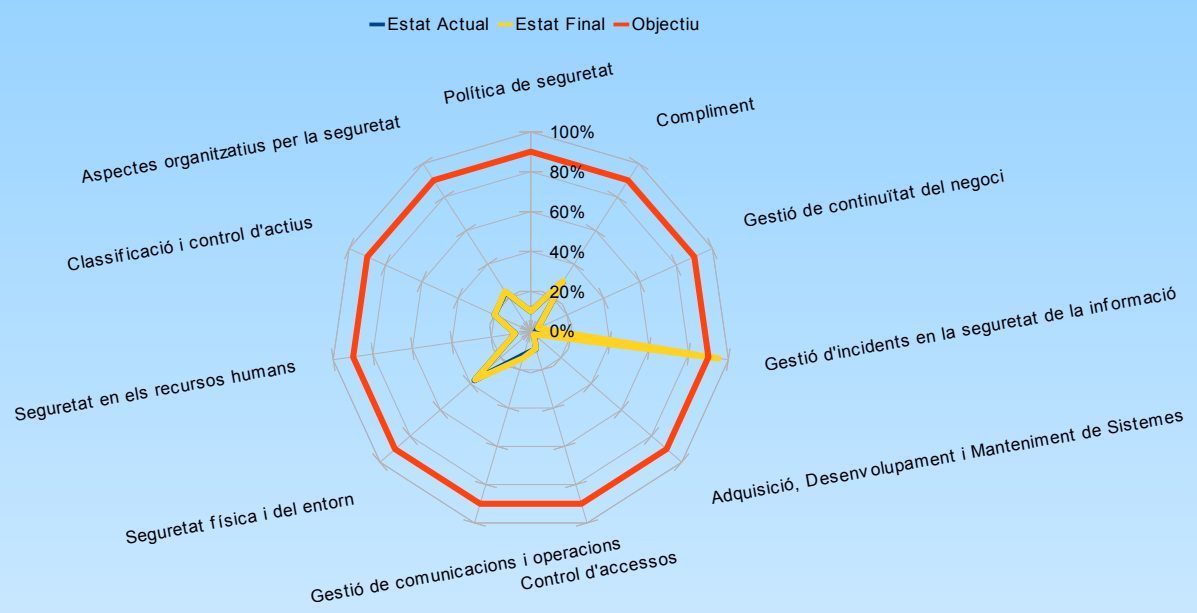
S'implantarà un sistema de gestió incidental per poder avaluar amb una base documental les amenaces que es produeixen en la nostra entitat.

- **S'optarà inicialment per utilitzar una eina que es pot allotjar en el servidor de base de dades de la nostra organització: OTRS, el qual ens permet fer un seguiment de les incidències històriques i de les incidències que actualment es troben en curs.**

- **Aquesta eina en farà us tots els empleats de la organització, per documentar els incidents que s'hagin produït i facilitar el seguiment de la incidència. En aquesta eina s'ha de reportat aspectes com problemes en l'accés al correu, pèrdua d'un portàtil, pèrdua de la connexió al servidor, suport de backup danyat...L'abast del ús de la eina pot anar tant en la resolució d'incidències tècniques com a altres tipus d'operació que decideixi PREVENCIÓ S.L, en base al ús que en faci.**

- **La resolució i documentació final de la incidència anirà a càrrec de la persona que faci la seva resolució o gestió associada. La revisió general anirà a càrrec del responsable de seguretat.**

Projectes: Implantació d'un sistema de gestió incidental



El cost d'implantació de la solució i el retorn de la inversió és el següent:

	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	10.000 €	10.000 €	10.000 €	10.000 €	10.000 €
Amortització	1.667 €	1.667 €	1.667 €		
Benefici brut	25.458 €	25.458 €	25.458 €	25.458 €	25.458 €
Benefici net	13.791 €	13.791 €	13.791 €	15.458 €	15.458 €

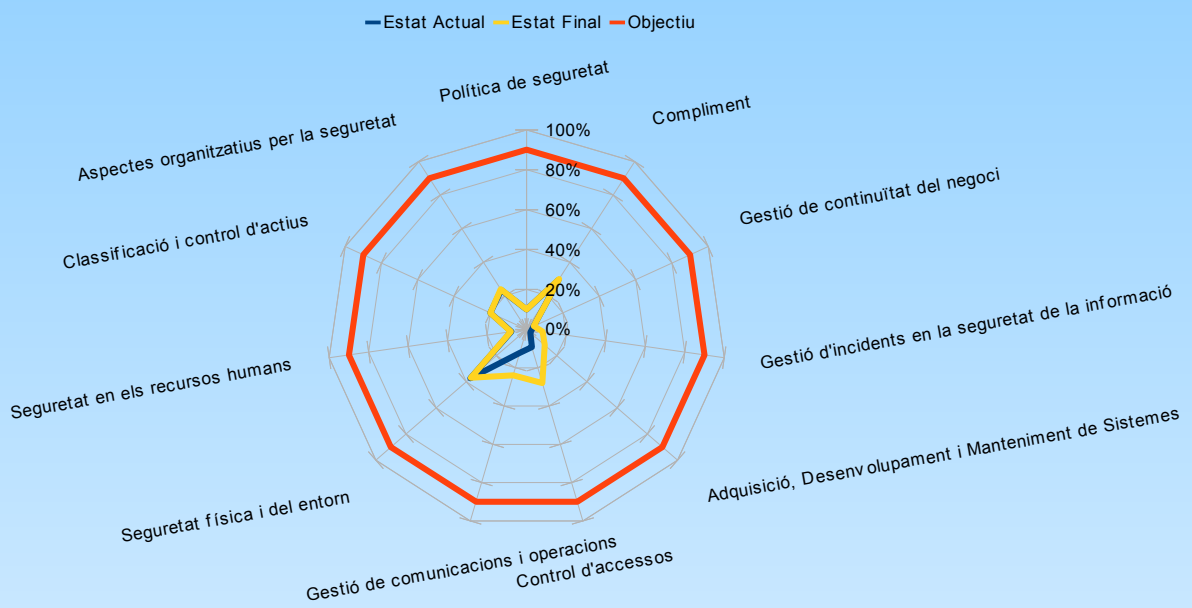
Projectes: Configuració d'un *firewall* i de la xarxa virtual (*VPN*)

S'utilitzarà un servidor Windows 2003 com a firewall i com a servidor VPN. S'escull aquest tipus de solució principalment per els següents motius:

- **Permetrà un major flexibilitat en la solució. En cas de que es requereixi una solució amb més prestacions, es podrà reciclar l'equip per altres serveis.**
- **El volum previst de connexions es limita als tècnics de prevenció, metges i infermeres que treballen fora del edifici de la delegació central, per tant serà un nombre reduït d'usuaris.**
- **Es tracta de la mateixa plataforma de la majoria dels servidors de la organització, facilitant l'ús dels administradors.**
- **S'integra amb el sistema d'autentificació i la gestió de polítiques del sistema operatiu.**
- **S'integrarà les dues funcions per un tema de reducció de costos**

Aquesta solució ens permetrà disposar d'una connexió xifrada per un conjunt de terminals que disposin d'un certificat instal·lat, fent que el canal de comunicació sigui segur i que sigui improbable de que es pugui interceptar la comunicació.

Projectes: Configuració d'un *firewall* i de la xarxa virtual (*VPN*)



El cost d'implantació de la solució i el retorn de la inversió és el següent:

	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	4.000 €	4.000 €	4.000 €	4.000 €	4.000 €
Amortització	2.915 €	2.915 €	2.915 €	2.915 €	2.915 €
Benefici brut	54.974 €	54.974 €	54.974 €	54.974 €	54.974 €
Benefici net	48.059 €	48.059 €	48.059 €	48.059 €	48.059 €

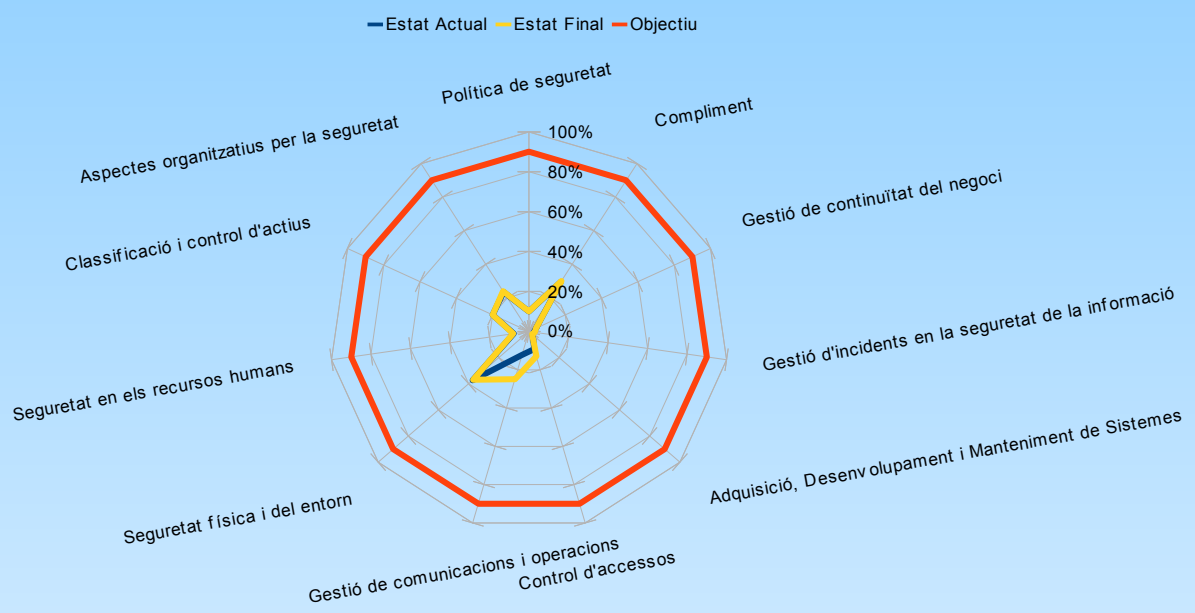
Projectes: Detecció Intrusions. Instal·lació IDS

Un cop muntat el firewall, es segmentarà la xarxa de servidors i s'inclourà un sistema de detecció d'intrusos que farà de passarel·la entre el firewall i el segment de la xarxa de servidors.

Optarem per una solució sense cap cost de llicència de software, que utilitza un dels principals IDs Open Source, Snort. S'ha optat com a referència el conjunt de paquet integrat Security Onion, basat en una distribució Xubuntu, la qual disposa de diferents eines de detecció d'intrusos i de monitorització (Snort, Suricata, Sguil, Squert, Snorby, Bro, NetworkMiner, Xplico).

Per la utilització d'aquestes eines d'anàlisis i de monitorització es requereixen certs coneixements tecnològics, per tant, es considerarà que hi haurà personal dedicat a aquestes revisions

Projectes: Detecció Intrusions. Instal·lació IDS



El cost d'implantació de la solució i el retorn de la inversió és el següent:

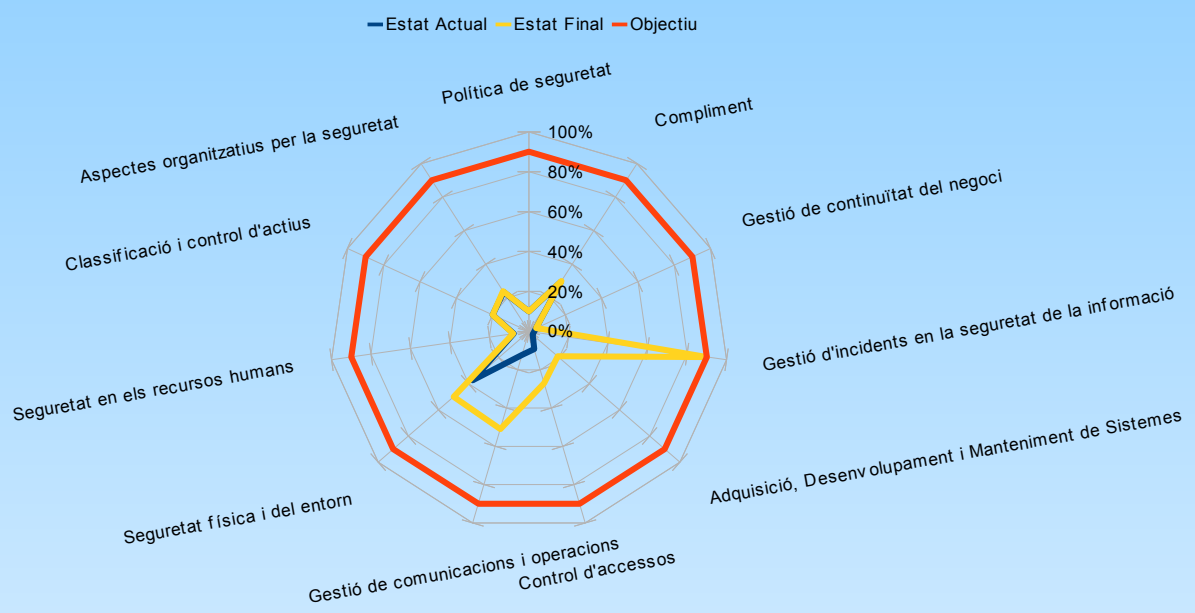
	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	4.000 €	4.000 €	4.000 €	4.000 €	4.000 €
Amortització	1.200 €	1.200 €	1.200 €	1.200 €	1.200 €
Benefici brut	16.121 €	16.121 €	16.121 €	16.121 €	16.121 €
Benefici net	10.921 €	10.921 €	10.921 €	10.921 €	10.921 €

Projectes: Reestructuració equip tecnològic

Es disposa d'un tècnic informàtic un dia a la setmana. Es proposa disposar de personal a jornada completa, per realitzar les tasques de manteniment dels sistemes. El Responsable de Seguretat revisarà la realització de les tasques associades:

- **Revisió diària dels diferents events que es produeixin dins de la plataforma servidora (servidor de correu, servidor de PREVENET, firewall, IDS...).**
- **Resolució incidències tecnològiques**
- **Instal·lació i manteniment de la plataforma per el registre dels diferents incidències que es produeixin en la organització.**
- **Revisió mensual de les versions de software de l'empresa.**
- **Instal·lació dels equips de la organització.**
- **Configuració i distribució de les polítiques de sistema operatiu.**
- **Gestió de les comptes d'usuari segons els perfils definits.**
- **Documentar els diferents procediments tecnològics.**
- **Realització dels backups diaris.**

Projectes: Reestructuració equip tecnològic



El cost d'implantació de la solució i el retorn de la inversió és el següent:

	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	50.000 €	50.000 €	50.000 €	50.000 €	50.000 €
Amortització	0 €	0 €	0 €	0 €	0 €
Benefici brut	259.718 €	259.718 €	259.718 €	259.718 €	259.718 €
Benefici net	209.718 €	209.718 €	209.718 €	209.718 €	209.718 €

Projectes: Canvi en la política de gestió de *backups*

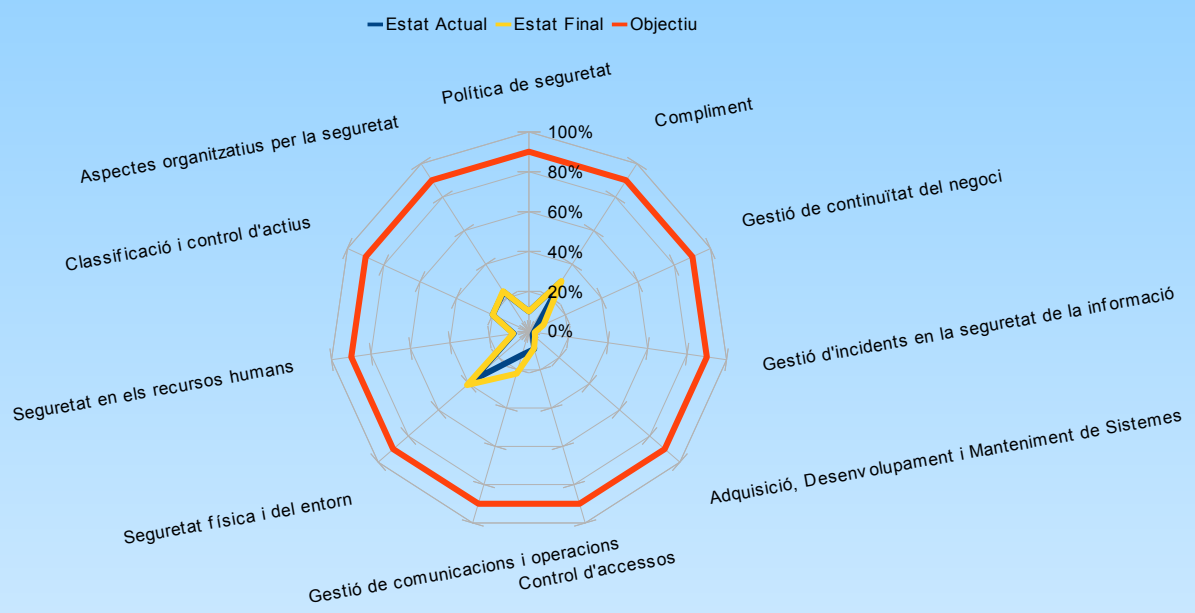
Actualment només s'emmagatzemen dues còpies de backup setmanal en un dels servidors de la organització.

Es proposa emmagatzemar-la en un suport físic diferent. S'enviaran setmanalment còpies a la delegació més propera a la central amb un sistema de transport que ens garanteixi la privacitat de les dades i encriptant les dades del dispositiu associat. De cada backup es guardaran dues còpies en dispositius físics diferents.

Proposarem un procediment que compleixi els següents objectius:

- **Disposar com a mínim de backup del últim mes**
- **Poder recuperar la informació del dia anterior**
- **Garantir pràcticament en el 99,9% dels casos que es pot recuperar informació del dia anterior amb els suports de backup de la central.**
- **En cas de que es danyin tots els suport de backup de la central, encara es pugui garantir en pràcticament un 99 % dels casos que la pèrdua de dades serà com a màxim de la última setmana.**

Projectes: Canvi en la política de gestió de *backups*



El cost d'implantació de la solució i el retorn de la inversió és el següent:

	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	3.500 €	3.500 €	3.500 €	3.500 €	3.500 €
Amortització	667 €	667 €	667 €	0 €	0 €
Benefici brut	9.395 €	9.395 €	9.395 €	9.395 €	9.395 €
Benefici net	5.228 €	5.228 €	5.228 €	5.895 €	5.895 €

Projectes: Inundacions. Canvi de la ubicació de la sala de servidors

La sala de servidors es troba ubicada actualment en la planta baixa, estan exposada a inundacions que es puguin produir en el edifici.

Es proposa la migració actual de les dades en la primera planta del edifici. Aquest canvi requerirà que es realitzin les següents accions:

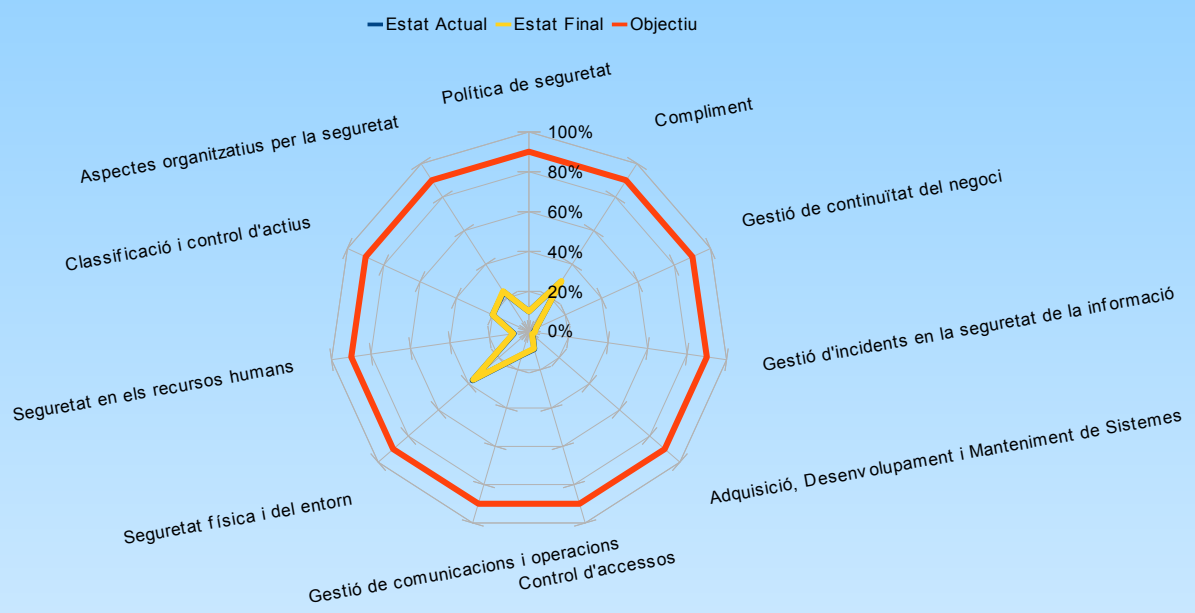
- **Adaptació de la instal·lació elèctrica i de comunicacions del edifici.**
- **Aturada del servei durant el procés de migració.**
- **Trasllat del mobiliari associat. Es contractarà personal extern per realitzar aquest transport.**

No s'aprecien resultats significatius en els dos anàlisis per els següents motius:

- **<u>Maduresa dels controls de seguretat</u>. Aquesta solució només ataca un aspecte de la seguretat física del entorn. No s'ha considerat que varies la maduresa actual del control com per saltar un esglaó de maduresa superior.**

- **<u>Anàlisi de riscos.</u> Les mesures realitzades amb la salvaguardes contra les inundacions afecten bàsicament a les dimensions de disponibilitat i traçabilitat. La majoria dels actius influenciats per la salvaguarda hem prioritzat altres dimensions com la confidencialitat i la integritat. Ens hem basat en la definició de MAGERIT sobre quines dimensions afecten les diferents amenaces.**

Projectes: Inundacions. Canvi de la ubicació de la sala de servidors



El cost d'implantació de la solució i el retorn de la inversió és el següent:

	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	0 €	0 €	0 €	0 €	0 €
Amortització	1.667 €	1.667 €	1.667 €	0 €	0 €
Benefici brut	781 €	781 €	781 €	781 €	781 €
Benefici net	-886 €	-886 €	-886 €	781 €	781 €

Projectes: Solució *Cloud Computing* dels servidors de *PREVENCIÓ S.L.*

Actualment s'està popularitzant la utilització de solucions de Cloud Computing (concretament, la possibilitat d'allotjar els nostres servidors en un proveïdor extern). Aquests tipus de solucions permenten externalitzar part de les mesures de seguretat associades al servidor (electricitat, mesures físiques de seguretat, backup...).

És un tema que requereix analitzar en profunditat aspectes com:

- **Contractes que es realitzessin amb el proveïdor que ofereix el servei, acordant les clàusules de compliment de seguretat dels sistemes en les diferents dimensions de seguretat.**
- **Analitzar a nivell legislatiu el fet que les dades estiguin ubicades físicament en una instal·lació diferent a les de la nostra organització.**

Actualment hi han empreses de reconegut prestigi que ofereixen solucions d'aquest tipus com *IBM* o *Amazon*.

Aquestes solucions es basen en els recursos que necessites:

- **Capacitat de procés**
- **Memòria**
- **Disc**
- **Velocitat de xarxa**
- **Temps que necessites que estiguin disponible els serveis.**

En base a aquests criteris, es realitza la facturació mensual del servei.

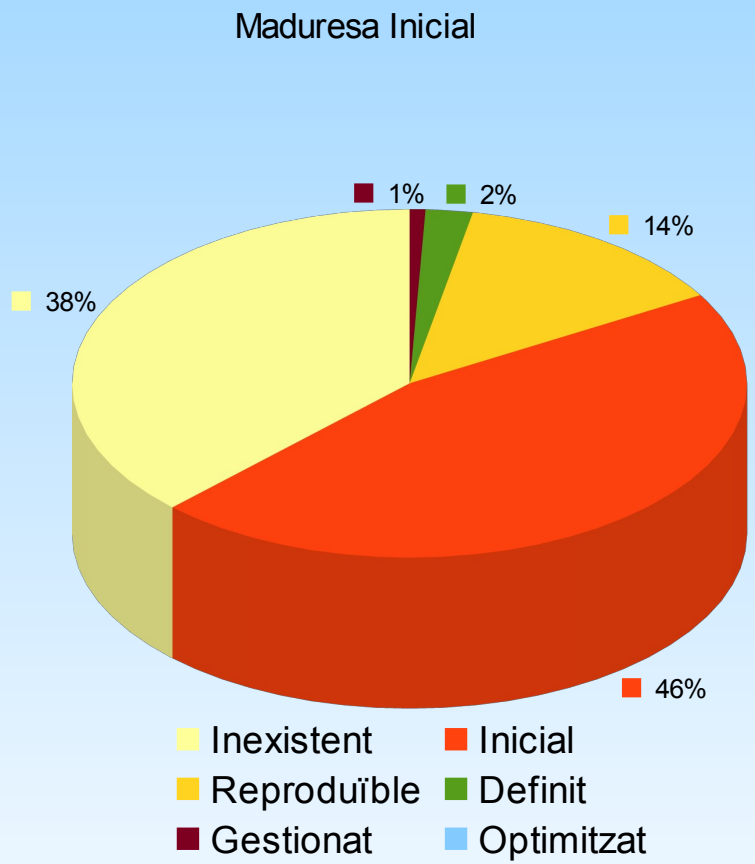
Projectes: Solució *Cloud Computing* dels servidors de *PREVENCIÓ S.L.*

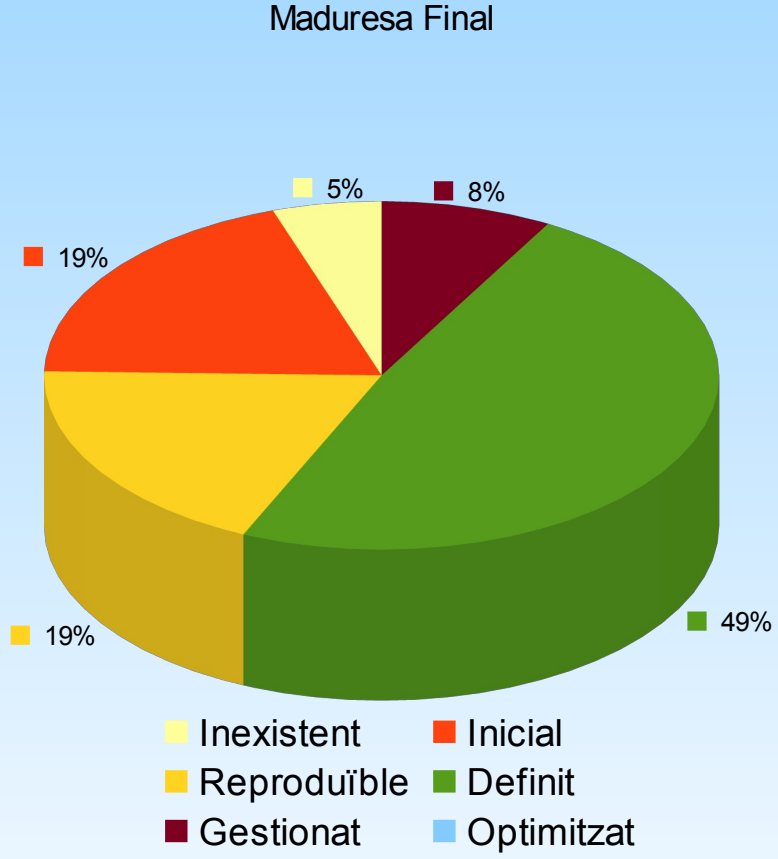
Es tracta d'una solució en fase d'expansió. No disposem del detall de casos similars de PYMES que estiguin treballant amb aquestes alternatives, i no disposem del temps i els coneixements necessaris per fer un anàlisis en profunditat d'aquest tipus de solució.

És una solució que s'hauria de considerar en les futures reunions del comitè, un cop el SGSI hagi assolit la maduresa suficient en mesures de seguretat, com alternativa a propostes de seguretat que es puguin plantejar (solucions de continuïtat del negoci, reduccions de costos...).

Valoració Global: Impacte en la maduresa del sistema

En les següents gràfiques podem observar que gran part dels controls passaran ha estar a un estat definit, que és un dels objectiu que ens havíem marcat amb PREVENCIO S.L. Si ho comparem en l'estat inicial que presenta el sistema abans de la materialització dels projectes, es pot observar fàcilment el canvi en la maduresa dels controls.

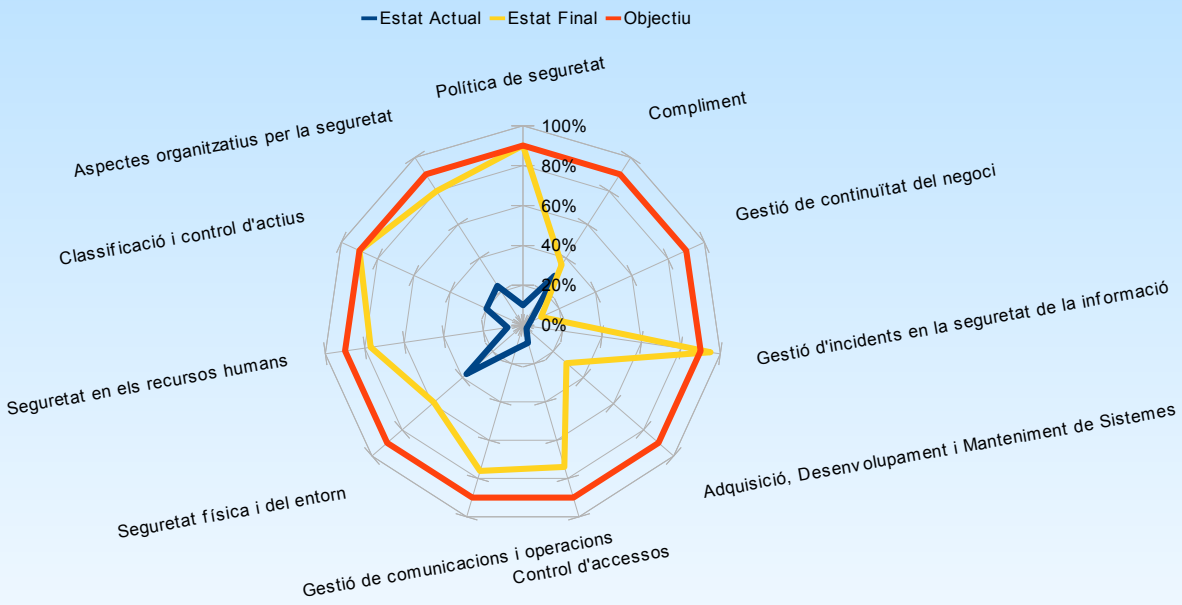




Valoració Global: Impacte en la maduresa del sistema

Es millorarà la maduresa del sistema amb el global dels projectes. Els següents dominis no han tingut una incidència tan significativa:

- **<u>Compliment.</u> Partíem d'un escenari amb una maduresa superior a la resta de dominis. Dins dels projectes proposats no s'ha valorat la realització d'una auditoria externa (només assesorament durant la fase d'implantació), per tant és un projecte que s'ha de proposar en les següents reunions del comitè.**
- **<u>Gestió de la continuïtat del negoci.</u> No és l'aspecte prioritari en aquesta fase inicial d'implantació. S'ha d'abordar un cop la organització disposi de la maduresa suficient, i es puguin assumir els costos.**
- **<u>Adquisició, Desenvolupament i Manteniment del Sistemes.</u> *PREVENCIO S.L* no desenvolupa software, per tant, molts dels controls associats no apliquen. De totes formes, la maduresa de la organització a nivell tecnològic es troba en un estat inicial, i per tant, requeriria d'assessorament extern per la realització dels controls associats.**



Valoració Global: Impacte en el anàlisis de riscos de la organització

Actiu/Amenaces	Valor	Risc Intrínsec	Risc Efectiu	Reducció del risc	%Reducció Risc
Dades	1.410.000 €	76.982 €	34.233 €	42.748 €	55,53%
Aplicacions	2.700.000 €	428.745 €	202.664 €	226.082 €	52,73%
Instal·lacions	750.000 €	17.404 €	13.325 €	4.080 €	23,44%
Equipaments auxiliars	300.000 €	1.315 €	379 €	936 €	71,21%
Hardware	2.250.000 €	174.300 €	94.307 €	79.993 €	45,89%
Xarxes	600.000 €	108.921 €	19.931 €	88.990 €	81,70%
Serveis	650.000 €	42.753 €	19.361 €	23.393 €	54,72%
Personal	1.350.000 €	3.164 €	1.367 €	1.797 €	56,80%
Total	**10.010.000 €**	**853.584 €**	**385.566 €**	**468.018 €**	**54,83%**

A nivell global amb les solucions proposades millorem tant a nivell global com a nivell individual més del 50% del risc que té actualment PREVENCIO S.L.

Són significatives les mesures adoptades en les connexions des de l'exterior, les quals estaven comportant un amenaça considerable en el global de la organització ja que estàvem utilitzant tant xarxes públiques com connexions de xarxes de tercers.

S'han millorat sensiblement els riscos en els actius de dades i aplicacions que són el principal de protecció de la informació, encara que queden uns riscos residuals significatius.
A nivell d'instal·lacions no s'han produït millores destacables ja que no estaven exposant a la organització a un risc tan elevat com a la resta d'actius.

Encara queda bastant marge per millorar la seguretat de la informació. El principal objectiu de la majoria dels projectes presentats és poder valorar l'estat actual de seguretat de PREVENCIO S.L.

Valoració Global: Impacte en el anàlisis de riscos de la organització

A partir d'aquí podrem determinar quines són les accions que s'han de realitzar amb els riscos detectats:

- **Reduir-los o evitar-los. Es la opció ideal i que es troba a l'abast de *PREVENCIÓ S.L***
- **Transferir-los a tercers. En el cas de que siguin costos molt elevats i que es puguin gestionar per terceres organitzacions o bé que es puguin cobrir les despeses mitjançant una assegurança.**
- **Acceptar-los. Aquest risc s'ha de prendre si els costos de la solució no són assumibles per la organització i no ho podem transferir a tercers (tenint en compte les seves conseqüències de que es produeixin), o en el cas que sigui més costosa la solució que el risc assumit.**

El cost global i el retorn de la inversió dels diferents projectes és el següent:

	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	86.500 €	86.500 €	86.500 €	86.500 €	86.500 €
Amortització	42.908 €	42.908 €	42.908 €	4.115 €	4.115 €
Benefici brut	468.018 €	468.018 €	468.018 €	468.018 €	468.018 €
Benefici net	338.610 €	338.610 €	338.610 €	377.403 €	377.403 €

Valoració Global: Planificació

Els projectes més importants per el desenvolupament del *SGSI* són els que posat en primera instància. És necessari que realitzem una reestructuració del equip tecnològic per que es facin càrrec dels projectes tècnics que s'han d'abordar.

No hem ajustat massa el calendari ja que les persones que realitzaran els desplegaments dels diferents projectes no es dediquen en exclusivitat, per tant, s'ha de combinar amb les tasques habituals del personal.

Els projectes amb un menor impacte, com són el de canvi en la política de *backups* i prevenció hem baixat la seva prioritat.

No hem abordat el projecte de *Cloud Computing* (ni tan sols l'hem valorat). No es plantejarà com a mínim fins al desembre del 2013 per desplegar al març del 2014, tal i com s'ha considerat en la planificació actual.

Projectes	setembre 2012	desembre 2012	març 2013	juny 2013	setembre 2013	desembre 2013	març 2014	juny 2014	setembre 2014	desembre 2014	març 2015	juny 2015
Organització del sistema de seguretat de la informació	■											
Documentació procediments		■	■	■	■							
Revisió de les relacions contractuals						■						
Implantació d'un sistema de gestió incidental		■										
Configuració d'un firewall i establiment xarxa virtual (VPN) per les connexions exteriors			■									
Instal·lació d'un detector d'intrusions (Ids)				■								
Canvi en la política de gestió de backups					■							
Prevenció Inundacions						■						
Cloud Computing							■	■	■	■	■	■
Reestructuració del equip tecnològic	■	■	■	■	■	■	■	■	■	■	■	■