ENTREGA FINAL

Treball de Final de Màster:

Elaboració d'un Pla de Seguretat de la Informació

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

Especialitat de Gestió i auditoria de la seguretat informàtica

Autor: Jordi Querol Gómez de Hinojosa

Taula de continguts

0 ENUNCIAT

El projecte planteja l'establiment de les bases per a la realització del Pla Director per a una empresa. Per a això s'abordaran les següents fases:

- *Documentació normativa sobre les millors pràctiques en seguretat de la informació.*
- *Definició clara de la situació actual i dels objectius del Pla Director.*
- *Identificació i valoració dels actius corporatius com a punt departida a una anàlisi de riscos.*
- *Avaluació d'amenaces i classificació de les mateixes.*
- *Avaluació del nivell de compliment de la ISO / IEC 27002:2005 en l'organització.*
- *Propostes de projectes de cara a aconseguir una adequada gestió de la seguretat.*
- *Presentació de resultats.*

Com a entregables del projecte, s'hauran d'obtenir els resultats que s'especifiquen a continuació:

- *Objectius del Pla Director, incloent una presentació a la companyia de les motivacions del pla i la seva necessitat.*
- *Informe de l'estat de la seguretat en l'actualitat, identificant clarament els riscos potencials que afecten els sistemes d'informació.*
- *Avaluació del compliment dels controls de seguretat marcats per la ISO / IEC 27002:2005. Estudi dels diferents dominis a partir de l'estudi detallat dels diferents controls plantejats en la norma.*
- *Proposta de projectes concrets, quantificats econòmica i temporalment, que ajudin a millorar l'estat de la seguretat, alineant l'organització amb els seus objectius plantejats en el Pla Director.*
- *Planificació temporal i econòmica dels mateixos. Detall del impacte sobre els dominis de la norma.*
- *Presentació executiva a la Direcció del resultat del treball.*

1 CONTEXTUALITZACIÓ I DOCUMENTACIÓ

La empresa sobre la que farem el nostre estudi l'anomenarem al llarg del present document com a *PREVENCIÓ S.L.*

1.1 Activitat de negoci

L'activitat del negoci de *PREVENCIÓ S.L* és donar diferents serveis de prevenció de riscos laborals a les empreses que contracten les seves prestacions.

Aquests serveis prestats es basen els requeriments que es troben definits en la *Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales*, els quals són requeriment obligatori per totes les empreses del àmbit espanyol que disposin de treballadors assalariats.

Els seus principals serveis són:

- Analitzar les condicions d'higiene i seguretat, dels diferents tipus de treball que realitza la empresa que els contracta, mitjançant el seu equip de tècnics prevenció de riscos laborals, i poder indicar a l'empresa contractant quins són els canvis que ha de realitzar en els seus protocols de treball.
- Donar suport als tècnics de prevenció propis de les empreses contractants per realitzar anàlisis que requereixin amb material especialitzats, els quals no disposa l'empresa contractant pel seu elevat cost.
- Donar cursos de prevenció per el personal de les empreses contractants.
- Disposar d'un equip d'infermers i metges d'empresa que es troben en jornada parcial o completa en les instal·lacions dels clients per cobrir les necessitats de vigilància de la salut. La disponibilitat del personal sanitari és la que s'acabi acordant amb l'empresa contractant.
- Tenir un equip de suport mèdic específic per els reconeixements mèdics que realitzen les empreses contractants. Aquests equips mèdics disposen del personal i el material necessari per poder realitzar proves específiques per l'empresa contractant, les quals no poden realitzar de manera independent. En base als reconeixements mèdics que es realitzen en funció del lloc de treball, es valorarà si el treballador es apte, no apte, o apte amb restriccions (resultat que comporta que l'empresa contractant hagi de canviar les condicions del lloc de treball per que el treballador pugui desenvolupar la tasca). A més s'encarrega de detectar si existeixen factors que pugin deteriorar la salut dels treballadors.

Actualment l'empresa dona servei a aproximadament unes 1.500 empreses i realitza la vigilància de la salut a aproximadament uns 50.000 treballadors.

1.2 Estructura Organitzativa

L'empresa es troba organitzada en quatre àrees

- Prevenció. És la encarregada de realitzar l'anàlisi dels diferents llocs de treball per avaluar la higiene i seguretat dels diferents equips de treball. També s'encarreguen de realitzar els cursos de formació obligatòria que s'han de realitzar als treballadors que s'incorporen a les empreses. L'equip de treball està format per:
  - El director de prevenció
  - 10 tècnics de prevenció encarregats de fer les diferents revisions a les empreses
  - 20 tècnics desplaçats a les delegacions territorials
  - 20 tècnics desplaçats a diferents empreses.
- Vigilància de la salut. Són els encarregats de determinar les proves mèdiques que s'han de realitzar als treballadors de les empreses contractants segons el tipus de treball realitzat. S'encarreguen d'avaluar si el personal és apte per el lloc ocupat segons el resultat de les proves realitzades. S'introdueixen els resultats de les proves mèdiques realitzades dins del programa de prevenció utilitzat per *PREVENCIÓ S.L.*

  L'equip de treball està composat per:
  - Un director mèdic
  - 2 infermeres d'empresa a la central.
  - 2 administratives que donen suport als equips de vigilància de la salut per concertar les diferents revisions que s'han de realitzar per part de les empreses contractants.
  - Una unitat mòbil de reconeixement amb un mèdic i un infermer
  - 20 infermers i 20 mèdics desplaçats a les diferents delegacions territorials
  - 25 metges i 20 infermeres contractats per *PREVENCIÓ S.L.* els quals treballen en els diferents edificis de les oficines contractants.
- Administrativa/Financera. S'encarrega de la part financera de l'empresa. S'encarrega de la elaboració del contractes laborals, de les gestions amb les administracions i de la compra de material d'oficina i el material necessari per la realització dels diferents controls de prevenció i de vigilància de la salut.

  L'equip de treball es troba composat per:
  - Un director financer
  - 6 administratives
- Comercial/Expansió. Es dedica amb la cerca de nous clients, renovació de contractes amb les empreses i a la absorció de petites empreses de prevenció.

  L'equip de treball està composat per
  - Un director comercial

- Dos comercials
- Una administrativa

La informàtica la gestiona a traves del director comercial, el qual s'encarrega de realitzar les diferents gestions amb proveïdors externs.

S'ha contractat a un tècnic informàtic un dia la setmana per donar suport de manteniment de la infraestructura informàtica de la empresa.

Es tracta d'una empresa d'àmbit nacional que disposa de diferents delegacions a tot l'estat. Cada delegació disposa d'una infermera i un metge d'empresa, els quals s'encarreguen de realitzar els reconeixements mèdics de la seva àrea d'influència. La coordinació dels diferents equips de treball i la comunicació amb els clients es realitza des de la oficina central, ubicada a Barcelona.

1.3 Protocols de treball

El personal de *PREVENCIÓ S.L.* que treballa a jornada parcial/completa en les instal·lacions del client disposen d'un portàtil d'empresa per realitzar el seu treball diari. La connexió a Internet per l'enviament dels diferents informes es realitza generalment a traves de les infraestructura que li facilita el client.

Els equips de *PREVENCIÓ S.L.* que es desplacen puntualment a les instal·lacions de les empreses contractants per la realització de reconeixements mèdic, realitza la pressa de dades en les instal·lacions mitjançant els diferents formularis que disposa en format imprès. Amb posterioritat es desplaça a la seva delegació regional per realitzar la introducció de les dades en el sistema i realitzar l'anàlisi dels resultats. Per aquelles empreses contractants que tenen un petit volum de treballadors, *PREVENCIÓ S.L.* no desplaça cap equip. Són els propis treballadors els que venen a la delegació pertinent a realitzar les proves mèdiques necessàries.

Esta limitat dins del programa *PREVENET* les dades que es poden emmagatzemar en format digital (p.e algunes proves mèdiques i enquestes sobre la salut dels treballadors). Per llei d'aquestes proves s'han de conservar durant un període llarg. Tota la documentació disponible en format imprès s'emmagatzemen a la central en armaris, els quals es tanquen amb clau.

PREVENCIO S.L disposa d'un protocol intern de bones pràctiques en el tractament de la informació. Cal recordar que es gestionen dades sensibles, i per tant, no ha d'estar exposada la documentació a personal aliè a l'empresa.

1.4 Relacions amb proveïdors

PREVENCIÓ S.L subcontracta per la realització les anàlisis d'orina i de sang dels diferents reconeixements mèdics a un únic laboratori. Les diferents mostres s'envien per correu ordinari o missatgeria amb una relació del DNI, nom del treballador edat i detall de l'analítica a realitzar.

Un cop realitzada les analítiques, des de *PREVENCIÓ S.L* disposem d'un usuari/password per accedir a una aplicació del laboratori via *https*. Ens permet descarregar un fitxer de dades amb un format que ens permet incorporar-ho al *PREVENET*.

PREVENCIÓ S.L subcontracta serveis mèdics per realitzar les revisions laborals d'aquelles empreses contractants d'àmbit nacional que disposen de delegacions territorials que no es troben dins de l'àrea d'influència dels equips mèdics propis. Aquests serveis mèdics realitzen les seves revisions amb els seus laboratoris i passen els resultats per correu ordinari o per missatgeria, conservant una còpia de les proves en les seves instàncies.

1.5 Immobiliari

La delegació central de Barcelona es troba allotjada en un edifici de dos plantes. A la part superior es troba l'equip d'administració i els despatxos de direcció i dels tècnics de prevenció.

En la part inferior del edifici es troben els despatxos dels infermers i mèdics que treballen a la central, una sala d'espera i una habitació on es troba allotjat els dos servidors de la empresa i el *SAI*.

La resta de delegacions territorials disposen d'un petit despatx on es realitzen les revisions i on es connecten amb els servidors de la delegació central via ADSL o 3G.

1.6 Infraestructura Informàtica

El sistema informàtic que disposa l'empresa és bastant senzill. La utilització és la següent:

- Correu electrònic. Utilització de firma digital per enviar documentació sensible encriptada. Els directius disposen de *Blackberries* les quals tenen configurat la gestió del correu electrònic a traves del proveïdor de telefonia mòbil
- Eines ofimàtiques (creació de fulls de càlcul, presentacions...)
- Accés a Internet.
- Us d'un programa específic per la prevenció de riscos laborals i vigilància de la salut (*PREVENET*). Aquest *software* disposa d'un sistema propietari per encriptar la informació que s'envia a traves de la xarxa pública.

Per cobrir aquest servei es disposa de la següent infraestructura:

- Un servidor correu *Exchange 2003* . En aquest servidor es disposa d'una unitat de disc on s'emmagatzemen *backups* setmanal amb un historial de dues còpies, tant de la base de dades *SQL,* del correu i dels fitxers.
- Un servidor que fa de controlador de domini, servidor de fitxers, servidor d'impressió i allotja la part servidora del programa *PREVENET,* software que utilitza un *IIS 6.0* i el servidor de base de dades *SQL Server 2000*.
- Un *router* bàsic proporcionat per la empresa proveïdora del *ADSL*. En el *router* tenim connectats els diferents servidors de l'empresa i el *switch utilitzat* per connectar els clients.
- Un *switch* de 24 ports on es troben connectats els diferents equips de la delegació central.
- Un *SAI* per prevenir la aturada dels servidors en cas de fallida elèctrica.

En la central disposa de 20 equips de treball. El *software* instal·lat en aquests equips es:

- *Windows XP*
- *Office 2003* (Instal·lació per defecte).
- La part del client del paquet *PREVENET.*
- *Software* d'antivirus *Symantec Endpoint Protection per Windows XP 5.1*

- Programes específics de comptabilitat
- Connexió amb l'exterior. Aquests equips són utilitzats per el personal d'administració

En cadascuna de les delegacions territorials disposen de dos equips per delegació i una connexió *ADSL/3G* per connectar-se a Internet. Cadascun dels equips disposa d'una versió de *Windows* i *Office* diferent. Generalment els equips són instal·lats des de la central amb la part client per accedir al software *PREVENET.*

Disposa d'una pàgina web externa contractada on es troba allotjada informació de la empresa mitjançant *DotNetNuke.* Aquesta pàgina s'utilitza per oferir informació comercial de l'empresa. Permet omplir un formulari el qual s'envia per correu a les empreses que vulguin sol·licitar informació, pressupostos, etc...

2 OBJECTIU DEL PLA DIRECTOR

2.1 Necessitats inicials de la organització

PREVENCIÓ S.L es troba immersa en una fase de creixement en la empresa. El seu creixement es basa en tres punts: la captació de de nous clients, l'absorció de serveis de prevenció de menor envergadura i la incorporació dels serveis de prevenció que es troben en la plantilla de la pròpia empresa contractant. *PREVENCIÓ S.L.* disposa d'un departament de l'empresa que té com a objectiu principal aquesta expansió de l'empresa.

Aquesta fase de creixement fa que s'hagi de revisar, i en alguns casos definir, els diferents procediments operatius de la empresa. 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. El fet de disposar de diferents equips de treball distribuïts en diferents delegacions territorials fa necessari definir procediments d'operació comuns que faciliti la coordinació dels diferents equips mèdics i de prevenció.

La direcció és conscient de que l'empresa gestiona informació sensible, principalment la associada a l'apartat de vigilància de la salut. La operatòria actual en els processos d'obtenció de les dades, trasllat i emmagatzematge pot comprometre tant la disponibilitat com la integritat de les dades.

Aquesta informació és necessària per realitzar l'avaluació de la aptitud dels treballadors en el seu lloc de treball. L'anàlisi mèdica associada només ha d'estar en coneixement del propi servei de prevenció i del treballador afectat. És obligatori per part del servei de prevenció conservar els resultats mèdics per els processos que es puguin derivar de la prevenció i vigilància de la salut (acomiadaments laborals per no ser apte en el lloc de treball, accidents laborals...) .

La gestió de dades sensibles ha de complir segons la *LOPD* uns requisits de seguretat, per tant, requerirà una adequació amb el tractament actual realitzat amb la informació.

L'empresa vol revisar la seva infraestructura tecnològica i que es tingui en compte dins de la definició dels diferents procediments a revisar. En aquest aspecte ens ha fet saber que la seva intenció es realitzar una despesa moderada, re-aprofitant el material que disposi actualment.

L'empresa vol gestionar el menor nombre de recursos personals dedicats a la infraestructura informàtica. No disposa de personal especialitat dins de la seva plantilla. Aquest aspecte s'haurà de tenir en compte per el desenvolupament de la solució, tenint en compte el volum de negoci, el nombre de treballadors i equips informàtics que disposa l'empresa.

2.2 Objectius finals del Pla Director

Un cop revisades les necessitats de la organització, hem definit conjuntament amb la direcció de *PREVENCIÓ S.L* les línies bàsiques per que es pugui traçar el camí adequat per millorar la seguretat de la informació, actiu valuós dins de l'empresa.

Per tant, s'han de prendre les mesures de seguretat necessàries per tallar i/o minimitzar els danys que pugui representar la materialització de les diferents amenaces a les que es troben exposats aquests actius. Aquests mesures repercutiran en un benefici final per la organització, en contraposició al cost que té la probabilitat de que aquestes amenaces s'acabin materialitzant.

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, de 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 i adequant el pressupost que es pugui destinar anualment a la seguretat. S'ha de realitzar un controls periòdic sobre les mesures de seguretat aplicades per poder disposar d'informació més contrastada a l'hora de realitzar els anàlisis periòdics de seguretat.

S'utilitzarà com a model de bones pràctiques per millorar la seguretat de la informació la normativa *ISO 27002,* estàndard de referència molt estès i valorat en l'anàlisi i gestió de la seguretat de la informació per organitzacions que han volgut implantar un sistema de gestió de seguretat de la informació. El principal avantatge d'aquesta normativa respecte altres models és que es basa en la informació, i no només des de un punt de vista informàtic. Disposa d'un conjunt de controls que són aplicables pràcticament per qualsevol organització.

S'ha acordat amb *PREVENCIÓ S.L* que la principal persona responsable de la seguretat de la informació en la estructura actual de la empresa serà el director comercial i d'expansió ja que en l'actualitat és la persona responsable de la contractació dels serveis informàtics. *AUDITORIA S.L,* com empresa de consultoria de seguretat externa a *PREVENCIÓ S.L* ens encarregarem de col·laborar en la definició del sistema de seguretat de la informació de *PREVENCIÓ S.L*, en la elaboració de propostes per millorar la seguretat de la informació i en la realització de les auditories internes de seguretat de *PREVENCIÓ S.L*. planifiqui periòdicament.

2.3 Comitè de seguretat

El comitè de seguretat estarà format per cadascun dels directors d'àrea de l'empresa (en l'actualitat, el director de prevenció, el director mèdic, el director financer i el director comercial), i per l'empresa que doni els serveis d'assessoria (actualment *AUDITORIA S.L.)*.

Aquest comitè de seguretat es reunirà semestralment per revisar l'estat actual de la seguretat de la organització.

Es revisarà l'estat actual de la organització, en base als controls de seguretat establers i les auditories internes realitzades per avaluar l'estat de seguretat de la organització.

S'exposaran les diferents necessitats, tant a nivell de seguretat com a nivell informàtic que cadascuna de les àrees tingui (per necessitats del negoci, per requeriments legals,...).

S'exposaran les diferents propostes de seguretat que s'hagin acordat entre el responsable de seguretat de *PREVENCIO S.L* i *AUDITORIA S.L* per tal de millorar la seguretat en funció de les necessitats que hagin aparegut en les anteriors reunions del comitè.

Es prioritzaran les propostes de seguretat i es revisarà el pressupost destinat per millorar la seguretat de la informació.

L'empresa que dona els serveis d'assessoria no tindrà un paper de decisió de les mesures de seguretat que es decideixin en el comitè. El seu paper serà d'assessorament, de formació en seguretat i preparació de les propostes que s'acordin realitzar per el comitè de seguretat i les que sol·liciti personalment el responsable de seguretat.

En aquestes reunions del comitè es revisarà el nombre de persones que han de formar-lo, en el cas de que s'hagi realitzat una reestructuració de les àrees que formen l'empresa.

3 ESTAT DEL RISC: IDENTIFICACIÓ I VALORACIÓ DELS ACTIUS I AMENACES

En aquesta fase detallarem els actius que disposa l'empresa per la seva activitat de negoci. Identificarem els actius que s'han introduït com a salvaguardes abans de realitzar aquest anàlisis (p.e antivirus, armaris amb clau, firma digital...), però no els inclourem encara en el inventari d'actius ni el seu impacte en la freqüència i dany de la materialització de les amenaces. Per tant, realitzarem el que s'anomena l'anàlisi de riscos intrínsec, el qual ens permetrà conèixer l'estat inicial de les vulnerabilitats de l'organització.

En posteriors fases del projecte revisarem la eficiència i eficàcia de la inversió que ja s'havia realitzat anteriorment l'empresa, i addicionalment ens permetrà conscienciar de com pot impactar la no utilització per part dels empleats d'aquelles mesures que requereixen una participació activa del personal. L'aplicació de les salvaguardes actuals condicionarà en posteriors fases la priorització dels projectes que es presentaran a *PREVENCIO S.L.* per reduir l'impacte teòric que pugui suposar la materialització de les amenaces.

Es mirarà d'agrupar els diferents actius similars, per evitar introduir major complexitat a l'anàlisi (p.e agruparem els locals llogats en les diferents delegacions, o aquell personal que no comporti uns riscos addicionals als associats a la seva substitució). Aquesta simplificació ens permetrà centrar el nostre anàlisi en els aspectes de seguretat més importants de l'organització. En aquests casos es tindrà en compte per la valoració dels actius i de les amenaces el valor acumulat de les diferents amenaces.

3.1 Inventari d'actius

Agruparem els actius en grups d'acord amb la metodologia *MAGERIT*. Ens centrarem en: instal·lacions, hardware, aplicació, dades, xarxa, serveis, equipament auxiliar i personal.

Els actius que no avaluarem com a salvaguardes en aquesta fase del projecte els marcarem amb un "(*)" per tenir-lo identificats en posterioritat.

3.1.1 Instal·lacions

Les instal·lacions de l'empresa són les següents:

- Edifici central. És l'edifici on es troba ubicades les dades centralitzades de l'empresa i la gran majoria de documents escrits.
- Delegacions Territorials. Esta composat per un conjunt de 20 edificis, els quals disposen dels reconeixements mèdics i els equips portàtils de la delegació.
- Unitat mòbil. A part del material propi per realitzar la revisió, s'emmagatzemen temporalment els formularis i les proves mèdiques dels pacients que s'han tractat abans de que s'enviïn les dades a la central.

3.1.2 Hardware

A nivell de hardware disposem dels següents actius:

- PCs de sobretaula. es tracta d'equips sobre plataforma Windows amb les eines ofimàtiques i de correu instal·lades amb diferents versions, amb un software d'antivirus comú (que s'analitzarà el seu impacte en fases posteriors) i la instal·lació de la part client del programa *PREVENET* (la qual utilitza el seu propi sistema de xifrat de la informació).
- Portàtils. Tenim un conjunt no homogeni de software dels diferents equips. Per simplificar l'anàlisi utilitzarem com a model de referència els equips amb una versió de software més inferior (p.e els de la central) i la connectivitat a través de la xarxa pública dels diferents llocs de treball a través de la xarxa del client. Utilitzarem aquest model ja que és el que presenta uns majors riscos i ens permetrà a posteriori implantar unes mesures de seguretat més generals per tots els equips de la organització.
- Servidor de correu. En aquest equip es troben tant el correu com les còpies de *backup* de les dades informàtiques.
- Servidor aplicació *PREVENET.* En aquest servidor es troben allotjades la resta de dades informàtiques (recurs de fitxers, dades *PREVENET* dins del *SQL*) i el software necessari per poder accedir a aquesta informació).
- *Router* central. Considerarem en l'anàlisi intrínsec que ve amb la configuració de fàbrica i és on es troben connectats actualment els diferents servidors de l'empresa.
- *Switch* central. No es troba configurada cap segmentació de xarxes.
- *Routers* delegacions. Només s'utilitzen per disposar connexió a Internet i accedir a la central.
- *Blackberries*. Es troben configurades per accedir al correu de l'empresa mitjançant *s.* No es gestiona l'accés a la Intranet de l'empresa a través del dispositiu, per tant, només disposen en el dispositiu dades del correu.

3.1.3 Aplicació

Detallem la relació d'aplicacions principals que intervenen actualment en els processos de negoci de la organització.

- *Windows Server.* És el sistema operatiu dels servidors de l'organització
- *Internet Information Service (IIS)*. És el servidor web sobre el que s'executa l'aplicació *PREVENET.*
- *Microsoft SQL Server.* És el motor de base de dades sobre el que s'emmagatzemen les dades introduïdes a traves de l'aplicació *PREVENET.*
- *PREVENET.* És l'aplicació sobre la que es realitzen la introducció i consulta de la informació de les dades de prevenció i de vigilància de la salut.
- *Microsoft Exchange Server.* És tracta del sistema de correu al que accedeixen els usuaris de *PREVENCIO S.L.* Aquest actiu engloba els correus, que encara que podria ser considerat

com a dades, el principal ús de la organització es com a canal de transferència d'informació.

- *Backup Utility* (*). Aplicació utilitzada per realitzada per fer el *backup* de fitxers, correu i les bases de dades de *SQL*.
- *NFS.* Aplicació que proporciona el servei d'accés als fitxers compartits.
- *Windows XP.* Sistema operatiu dels portàtils i *PCs* de la empresa.
- *Symantec End Point* (*). Sistema d'antivirus utilitzat en els equips portàtils i PCs de la empresa.
- *Contasol.* Programa de comptabilitat utilitzat per l'àrea financera. S'emmagatzema la informació en el recurs de dades.
- *Microsoft Office.* Conjunt d'aplicacions ofimàtiques utilitzades per gestionar documents de text, fulles de càlcul, presentacions i accedir al correu de l'organització.

3.1.4 Dades

PREVENCIÓ S.L disposa de la informació associada a la vigilància de la salut dispersa tant en format (imprès i digital) com en la seva localització (aquesta informació es troba part en la central introduïda dins del programa *PREVENET*, i en armaris amb clau en les diferents delegacions i empreses subcontractades). Aquesta tipus d'informació la valorarem com un únic actiu i la seva dispersió es tindrà en consideració en l'anàlisi de les vulnerabilitats del sistema. Tenint en compte aquestes premisses, aplicarem la següent classificació per els actius de dades:

Les dades de de l'empresa s'agruparan en els següents grans blocs:

- Dades de prevenció. Emmagatzemades en el programa *PREVENET* i que s'entrega una informe d'avaluació del risc a les empreses contractants.
- Documentació de formació que s'emmagatzema en el recurs de fitxers.
- Dades de vigilància de la salut. Dins d'aquest grup es troben:
  - Els qüestionaris mèdics en format escrit.
  - Les proves mèdiques realitzades en format imprès.
  - Les dades introduïdes en el programa *PREVENET* associat als reconeixements mèdics realitzats.
  - Les analítiques que es transfereixen entre l'àrea de vigilància de la salut i el laboratori d'anàlisis.
- Procediments interns. Emmagatzemats en el recurs de fitxer de l'àrea associada.
- Dades comptables: Conté els diferents balanços de l'empresa, diferents dades de pagament, contractes empleats...Emmagatzemades en el servidor de fitxers.
- Dades comercials: Tarifes, preus establerts als diferents clients, serveis contractats. Emmagatzemada en el servidor de fitxers.
- Contractes amb clients: Aquesta informació es troba en format imprès i s'emmagatzema en

un dels armaris amb clau.

- Contractes amb proveïdors: Aquesta informació es troba en format imprès i s'emmagatzema en un dels armaris amb clau.

3.1.5 Xarxa

Els principals elements de xarxa detectats són els següents:

- Connexió externa als servidors centrals. Actualment utilitzat exclusivament per per accedir software *PREVENET* i al correu electrònic. S'accedeix a traves de la xarxa pública i en ocasions les dades s'encaminen a través dels elements de comunicació de les empreses contractants.
- Xarxa Local. La connexió es realitza a través del *switch* de l'empresa, dels *routers* de les delegacions i de la xarxa *wifi* associada al *router*. Es connecten els terminals, portàtils i les *blackberries* de l'empresa.

3.1.6 Serveis

Els serveis són els medis utilitzats per accedir a la informació. Inclourem tant els serveis tecnològics com els més tradicionals (p.e emmagatzematge de la informació), ja que disposem de dades, com els reconeixements i els qüestionaris de vigilància que es troben en els dos formats, i per tant, s'han d'avaluar els riscos dels formats.

Els principals serveis que hem pogut identificar en base a la informació proporcionada per la empresa són els següents:

- Accés a la informació impresa. Es conserva en format de paper i són accessibles a traves d'un armari amb clau per el personal del àrea responsable en els edifici on es trobin emmagatzemades les dades, els quals custodien la clau.
- Recursos de fitxers. Es troba la informació compartida per el personal de les diferents àrees. Cadascuna de les àrees de l'empresa disposa d'un recurs de dades on emmagatzemen la informació. Aquests recursos de dades només són accessibles per els treballadors de la central. Les dades del programa de comptabilitat s'emmagatzemen en el recurs del departament financer, conjuntament amb les fulles de càlcul. Hem definit el servei de comptabilitat inclòs dintre de la informació del servei de fitxers ofimàtics del àrea financera ja que la criticitat de la informació és similar i les mesures establertes son pràcticament les mateixes al trobar-se les dades en el mateix repositori.
- Servei de directoris. Cadascun dels empleats de *PREVENCIO S.L* disposa d'un compte personal per accedir a la informació.
- Correu electrònic. Utilitzat per la comunicació interna, i per la comunicació amb clients i proveïdors. És la eina utilitzada per la planificació de reconeixements. Ocasionalment s'utilitza firma digital configurada localment en un conjunt limitat de terminals per enviar informació que requereix un alt grau de confidencialitat.
- Firma digital(*). Mecanisme utilitzat per minimitzar els riscos de seguretat en l'enviament de correus electrònics.

- Consulta i modificació dades de vigilància de la salut. Es realitza a través del software *PREVENET* la informació digital i dels armaris amb la clau la informació impresa.
- Consulta i modificació dades de prevenció. Es realitza a través del software *PREVENET*
- Pàgina *Web* de l'empresa. És un servei que es troba externalitzat, que informa sobre la nostra activitat de negoci i els principals clients als que donem servei i que permet enviar sol·licituds a una compte de correu de la nostra empresa.

3.1.7 Equipaments auxiliars

Els principals equipaments auxiliars són:

- Armaris amb clau(*). Contenen la informació en format imprès. Cada àrea de cadascun dels edificis disposa d'un armari. Els armaris només són accessibles per el personal de la mateixa àrea que treballi en aquest edifici. No tenim certesa de que les empreses que subcontractem tinguin aquest tipus d'equipament auxiliar.
- *S.A.I.*(*) Sistema d'alimentació elèctrica ininterrompuda que es troba connectada als elements *hardware* principals de l'empresa (servidors, *router*, *switch*).
- Sistema elèctric. Cadascuna dels locals té un contracte bàsic amb el proveïdor de la zona.

3.1.8 Personal

En base a les entrevistes realitzades, diferenciarem de la resta de personal de cara a la avaluació de riscos:

- Director Comercial. Disposa dels contactes directes amb altres serveis de prevenció. La seva baixa pot condicionar les subcontractacions realitzades actualment. És soci capitalista de l'empresa.
- Director de Prevenció. Té accés i coneixement sobre l'estat de risc de les diferents empreses contractades. És soci capitalista de l'empresa.
- Comercials. Disposen de cartera de clients pròpia. Un canvi d'empresa pot comportar la baixa d'alguna de les empreses contractades a través del comercial.
- Director Mèdic. Principal persona responsable de l'avaluació en vigilància de la salut. Disposa accés a totes les proves mèdiques i qüestionaris que gestiona *PREVENCIÓ S.L.* És la persona que dona el vist-i-plau definitiu als aptes amb restricció i no-aptes dels reconeixement.
- Infermera central amb experiència. És la persona que porta més temps en el àrea de vigilància de la salut. És la persona que gestiona la planificació dels reconeixements i la que s'encarrega de supervisar l'actuació de les diferents delegacions territorials.
- Director financer. És soci capitalista de l'empresa.
- Equips de prevenció absorbits. Tenen el coneixement i l'accés a la gestió de les empreses a les que antigament els hi contractava.
- Tècnic informàtic. Treballa normalment només 2 hores/setmana. Disposa de les credencials

d'administració per accedir a les dades del sistema. Revisa les incidències i consultes que es puguin formular durant la setmana.

- Resta de personal. Respecte a la resta de personal exposat, la seva substitució no comporta un problema addicional, ja que el que es requereix per realitzar les seves funcions és un perfil més tècnic i no del coneixement de l'empresa.

3.1.9 Taula Resum

En base als criteris detallats, l'inventari d'actius per el risc intrínsec queda de la següent forma (entre parèntesis posarem la nomenclatura que utilitzarem en l'arbre de dependències):

Actiu	Abreviatura
Edifici central. (Inst -E.C)	Inst -E.C
Delegacions Territorials. (Inst -D.T)	Inst -D.T
Unitat mòbil. (Inst-U.M)	Inst-U.M
PCs de sobretaula. (HW-PC)	HW-PC
Portàtils. (HW-PT)	HW-PT
Servidor de correu. (HW-Srv.Cor)	HW-Srv.Cor
Servidor aplicació PREVENET. (HW-SRV.PREV)	HW-Srv.PREV
Router central. (HW-Rou.Cen)	HW-Rou.Cen
Switch Central (HW-SW.Cen)	HW-SW.Cen
Routers delegacions. (HW–Rou.DT)	HW–Rou.DT
Blackberries. (HW-BB)	HW-BB
Windows Server. (Apl-Win.Srv)	Apl-Win.Srv
Windows XP. (Apl-Win.XP)	Apl-Win.XP
Internet Information Service (IIS). (Apl-IIS)	Apl-IIS
Microsoft SQL Server. (Apl-Ms.SQL)	Apl-Ms.SQL
PREVENET. (APL-PREV)	Apl-PREV
Microsoft Exchange Server. (Apl-Ms.Ex.Srv)	Apl-Ms.Ex.Srv
NFS. (Apl-NFS)	Apl-LANMAN
Contasol. (Apl-Conta)	Apl-Conta
Microsoft Office. (APL-MS.OFF)	Apl-MS.OFF
Dades de prevenció. (Data-Prv)	Data-Prv
Documentació de formació. (Data-Form)	Data-Form
Dades de vigilància de la salut. (Data-V.S)	Data-V.S
Procediments interns. (Data-Proc.Int)	Data-Proc.Int
Dades comptables (Data-Conta)	Data-Conta
Dades comercials (Data-Comer)	Data-Comer
Contractes amb clients (Data-Contr.Clie)	Data-Contr.Clie
Contractes amb proveïdors (Data-Contr.Prov)	Data-Contr.Prov
Connexió externa als servidors centrals (X-WAN)	X-WAN
Xarxa local (X.LAN)	Xarxa local (X.LAN)
Accés a la informació impresa. (SRV-IMPRES)	SRV-IMPRES
Recursos de fitxers. (SRV-NFS)	SRV-LANMAN
Servei de directoris.. (SRV-DIR)	SRV-DIR
Correu electrònic. (SRV-MAIL)	SRV-MAIL
Consulta i modificació dades de vigilància de la salut. (SRV-V.S)	SRV-V.S
Consulta i modificació dades de prevenció (SRV-PREV)	SRV-PREV
Pàgina Web de l'empresa. (SRV-WEB)	SRV-WEB
Sistema elèctric (EA-S.Elec)	EA-S.Elec
Director Comercial. (Per-D.Comer)	Per-D.Comer
Director de Prevenció. (Per-D.Prev)	Per-D.Prev
Comercials. (Per-Comer)	Per-Comer
Director Mèdic. (Per-D.V.S)	Per-D.V.S
Infermera central amb experiència. (Per-I.V.S)	Per-I.V.S
Director financer. (Per-D.Fin)	Per-D.Fin
Tècnic informàtic. (Per-Tec.TIC)	Per-Tec.TIC
Resta de personal. (Per-Resta)	Per-Resta

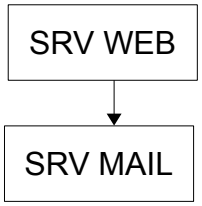
3.2 Valoració dels actius i dependències

3.2.1 Visió global

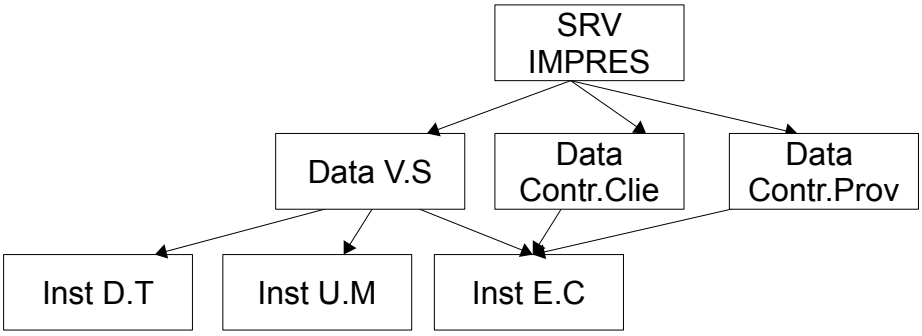
Primer de tot, definirem diferents arbres de dependència. Es a dir, quan es materialitza una amenaça en un actiu inferior, com afecta al actiu superior aquesta materialització. Aquest exercici ens permetrà tenir una primera visió de quins actius són més importants per la organització (en base al conjunt d'actius dels que depèn i les interconnexions) i quins actius poden ser una font de vulnerabilitat més gran (per que intervinguin en moltes de les dependències de les dades i els serveis). Només es posaran les dependències principals per no sobrecarregar l'arbre.

Com a criteri principal per generar l'arbre de dependències ens basarem en els actius que aparentment tenen un major impacte en les tres dimensions principals de seguretat (integritat, confidencialitat i integritat) com són els serveis (actius que té un major impacte la disponibilitat) i les dades (on és més important la confidencialitat i la integritat).

- Pàgina Web de l'empresa. Es tracta d'un actiu de valor baix. El servei es troba externalitzat amb un contracte de servei 24x7. Dona certa visibilitat de la informació de l'empresa en la *web* i permet rebre consultes i sol·licituds a traves del correu. La única dependència associada és el servei de correu, ja que si no es tracten les sol·licituds en menys d'una setmana es perd un client potencial, per tant, la dimensió de seguretat més important per aquest actiu és la disponibilitat.

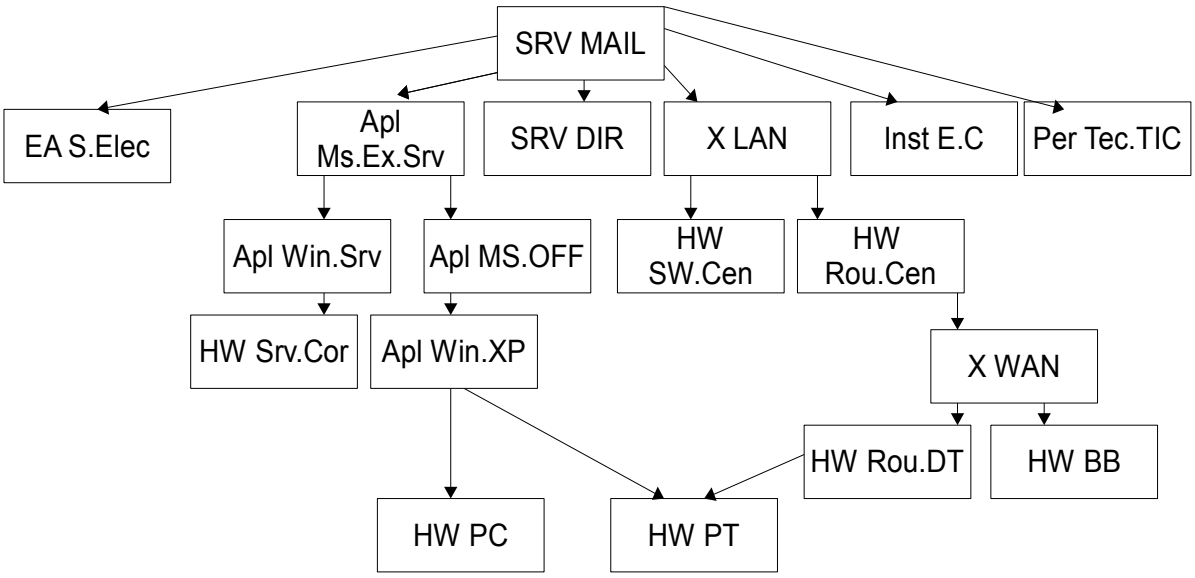


- Accés a la informació impresa. En aquest cas els actius amb major valor son les dades de vigilància de la salut, les quals segons la llei de prevenció de riscos s'han de conservar un determinat període i són dades sensibles al tractar-se de dades mèdiques. Les dades impreses de vigilància de la salut es poden trobar en els diferents edificis de l'empresa i temporalment en la unitat mòbil. La resta de documentació impresa, té un valor mig i s'emmagatzema a l'edifici central. En aquest cas, la dimensió de seguretat més important és la confidencialitat i en menor mesura la resta de dimensions.

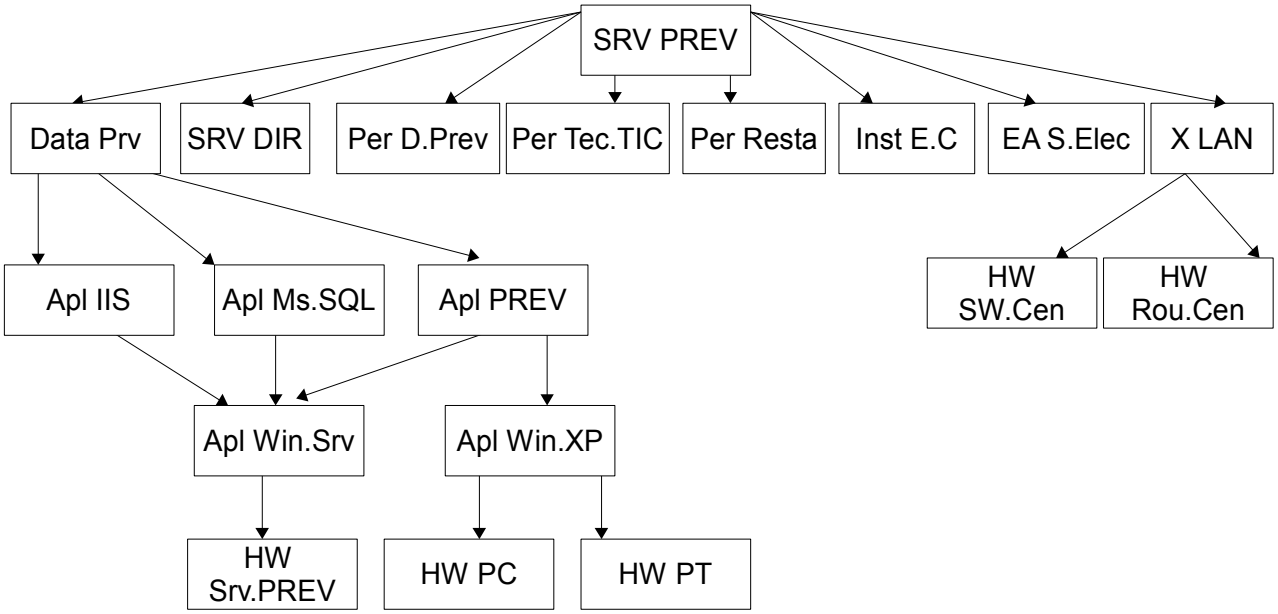


- Servei de correu:

  Es un actiu amb un arbre de dependències molt gran. Requereix que els diferents servidors i les comunicacions de l'empresa estiguin disponibles per que la informació sigui accessible. La confidencialitat de la informació dependrà d'aquestes actius i de la seguretat que es realitzi en els terminals dels usuaris. La integritat de les dades si no s'apliqués cap salvaguarda dependria principalment de que no es danyi la informació dels discos del servidor de correu.

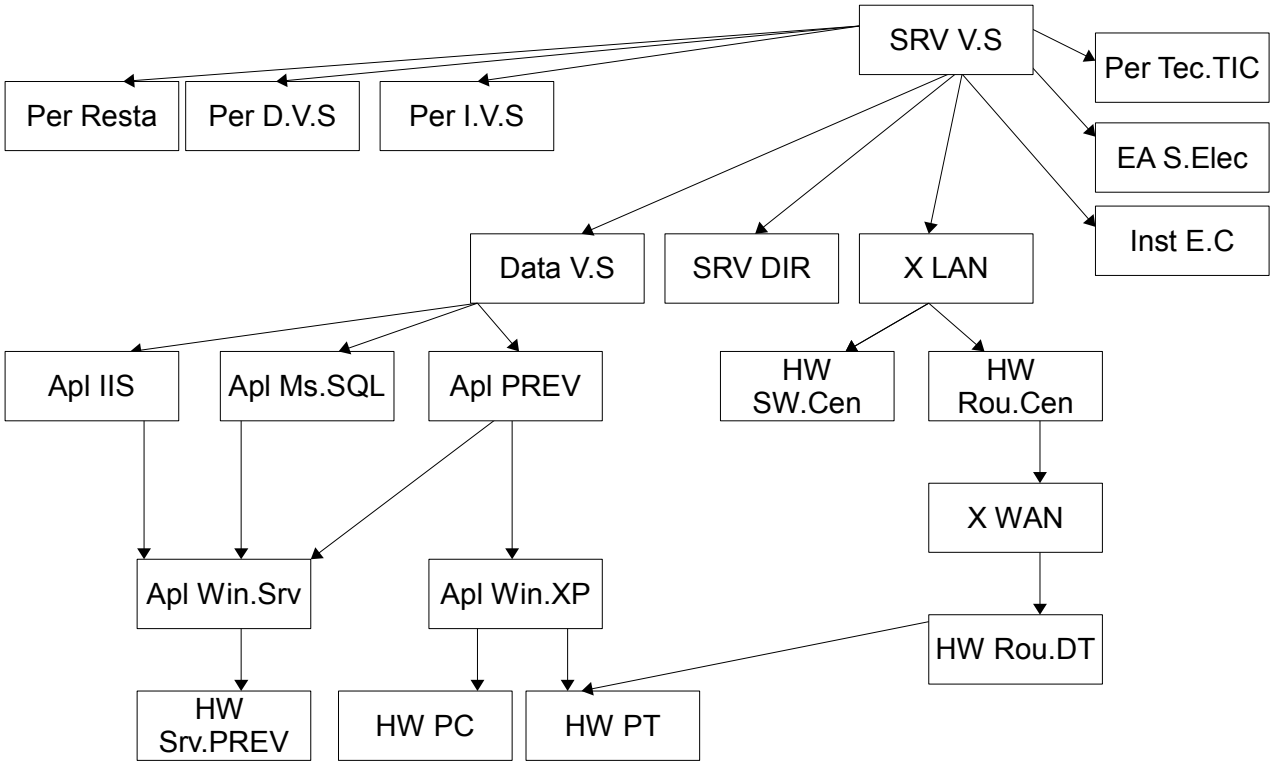


- Servei de prevenció: La principal consideració de seguretat que requereix aquest actiu és que aquesta informació no sigui accessible per tercers. Els informes de prevenció se'ls facilita completament per correu a les empreses contractants, per lo que la disponibilitat no és un criteri de seguretat tant important per aquesta informació.



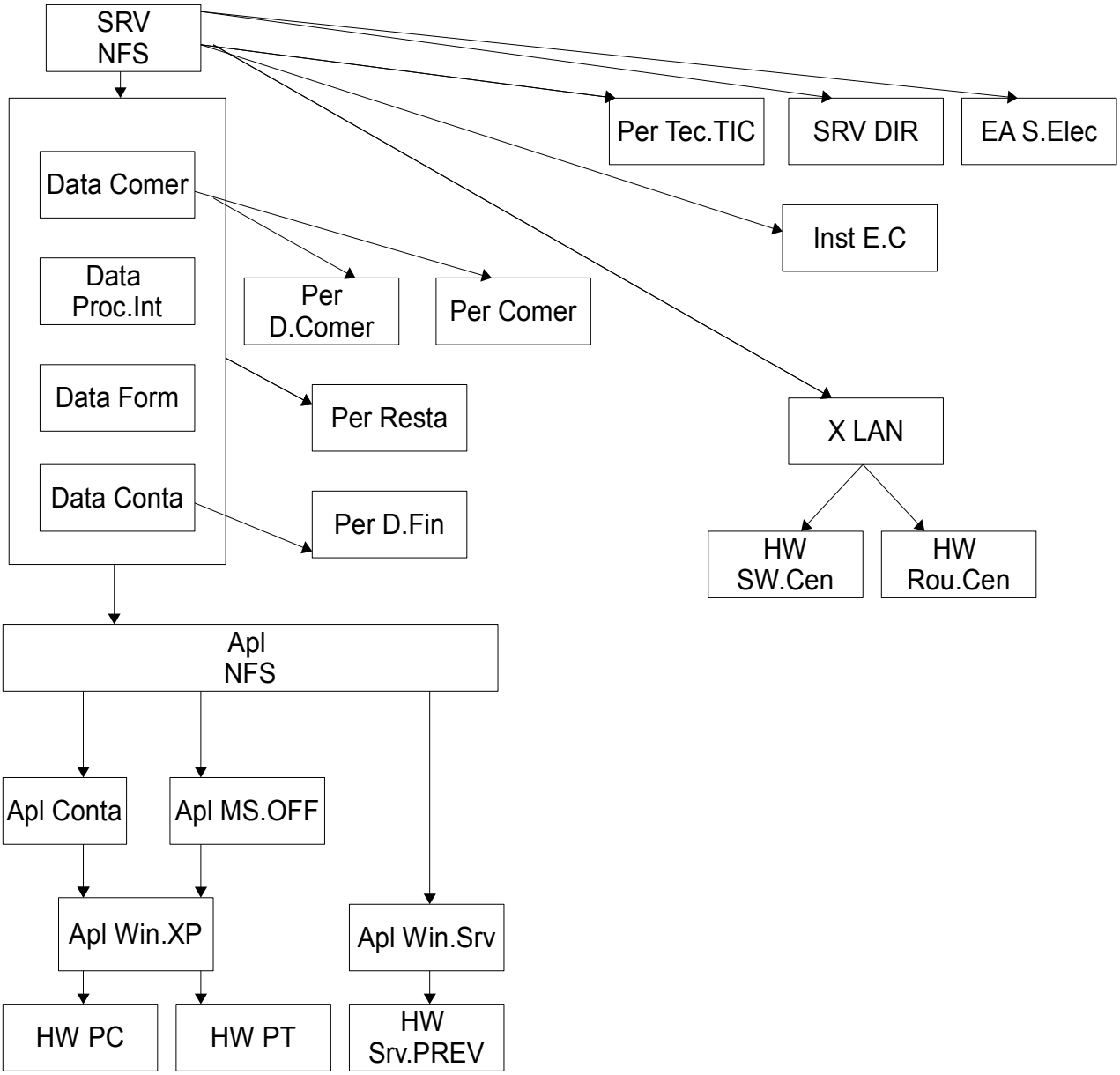
- Servei de vigilància de la salut:

En aquest cas la confidencialitat té un pes major que en altres informacions que disposa l'empresa, ja que es tracten de dades mèdiques que segons la LOPD requereixen mesures de seguretat específiques. A més es tracta d'informació que es pot requerir en judicis per acomiadaments improcedents. La no confidencialitat d'aquesta informació pot suposar un dany a la imatge de *PREVENCIÓ S.L.*



- Servei de recurs de fitxer

  Es tracta de la informació més interna de la organització, només consultable des de els equips de la central. Té un valor mitjà dins de l'organització. Al tractar-se d'un servei que es dona en el mateix servidor que el servidor de *PREVENET*, la seva disponibilitat serà similar.



3.2.2 Valoració global

Un cop realitzat un primera revisió de la dependència dels actius farem una valoració del cost dels actius. Es té en conte varis criteris per realitzar la valoració: El cost de reposició, el cost del lloguer, el temps que es triga en contractar i formar personal nou, l'ús que es fa de l'actiu, la repercussió que pot tenir a nivell legal no disposar del actiu o que sigui accessible per tercers.

Un cop obtinguda la informació per part de l'empresa, farem una abstracció en 5 nivells, tal i com es realitza en l'apartat 2.1 del Llibre II de Magerit (Molt Baix, Baix, Mig, Alt, Molt Alt):

Per fer-ho, utilitzarem la següent escala de valoració dels diferents actius de la organització:

Valoració	**Rang**	**Valor càlcul**
Molt Alta (MA)	Valor >= 200.000 €	300.000 €
Alt (A)	100.000€ < Valor <= 200.000 €	150.000 €
Mitja (M)	50.000 € < Valor <= 100.000 €	75.000 €
Baix (B)	10.000 € < Valor <= 50.000 €	30.000 €
Molt Baix	Valor < = 10.000 €	10.000 €

Seguint aquest criteri, mostrem el resultat de la valoració independent dels actius:

Actiu	Valoració independent	Valoració MAGERIT (5 escalas)	Valoració
Inst -E.C	100.000	150.000	A
Inst -D.T	10.000	30.000	B
Inst-U.M	10.000	30.000	B
HW-PC	10.000	30.000	B
HW-PT	60.000	75.000	M
HW-Srv.Cor	1.000	10.000	MB
HW-Srv.PREV	1.000	10.000	MB
HW-Rou.Cen	200	10.000	MB
HW-SW.Cen	200	10.000	MB
HW–Rou.DT	4.000	10.000	MB
HW-BB	900	10.000	MB
Apl-Win.Srv	1.000	10.000	MB
Apl-Win.XP	16.800	30.000	B
Apl-IIS	100	10.000	MB
Apl-Ms.SQL	3.500	10.000	MB
Apl-PREV	3.000	10.000	MB
Apl-Ms.Ex.Srv	5.000	10.000	MB
Apl-NFS	100	10.000	MB
Apl-Conta	100	10.000	MB
Apl-MS.OFF	36.000	10.000	MB
Data-Prv	1.500.000	300.000	MA
Data-Form	50.000	75.000	M
Data-V.S	3.000.000	300.000	MA
Data-Proc.Int	10.000	10.000	MB
Data-Conta	30.000	30.000	B
Data-Comer	50.000	75.000	M
Data-Contr.Clie	150.000	150.000	A
Data-Contr.Prov	100.000	150.000	A
X-WAN	1.000	10.000	MB
X-LAN	1.000	10.000	MB
SRV-IMPRES	100.000	150.000	MB
SRV-NFS	1.000	10.000	MB
SRV-DIR	1.000	10.000	MB
SRV-MAIL	60.000	75.000	M
SRV-V.S	60.000	75.000	M
SRV-PREV	30.000	30.000	B
SRV-WEB	2.000	10.000	MB
EA-S.Elec	10.000	10.000	MB
Per-D.Comer	30.000	30.000	B
Per-D.Prev	30.000	30.000	B
Per-Comer	10.000	10.000	MB
Per-D.V.S	30.000	30.000	B
Per-I.V.S	5.000	10.000	MB
Per-D.Fin	30.000	30.000	B
Per-Tec.TIC	2.000	10.000	MB

3.2.3 Dependències

Ponderarem el valor dels actius anteriors amb les dependències que suposa l'impacte en un actiu i el seu valor acumulat, mitjançant un anàlisis quantitatiu. Valorarem les dependències directes que hi ha dels diferents actius i ajustarem la valoració associada tenint en compte aquestes dependències dels actius superiors.

Degut al volum d'actius que disposem, és recomanable que aquesta anàlisis de les dependències es realitzés amb eines especifiques com *PILAR,* que és la eina que proposa *MAGERIT* en els llibres en el que es defineix la metodologia d'anàlisis de riscos. En futurs anàlisis que realitzi l'organització es considerarà utilitzar aquestes eines d'anàlisis per realitzar una valoració més eficient com *PILAR.*

	Dependències (%)																																													
Actiu	Inst -E.C	Inst -D.T	Inst-U.M	HW-PC	HW-PT	HW-Srv.Cor	HW-Srv.PREV	HW-Rou.Cen	HW-SW.Cen	HW–Rou.DT	HW-BB	Apl-Win.Srv	Apl-Win.XP	Apl-IIS	Apl-Ms.SQL	Apl-PREV	Apl-Ms.Ex.Srv	Apl-NFS	Apl-Conta	Apl-MS.OFF	Data-Prv	Data-Form	Data-V.S	Data-Proc.Int	Data-Conta	Data-Comer	Data-Contr.Clie	Data-Contr.Prov	X-WAN	X-LAN	SRV-IMPRES	SRV-NFS	SRV-DIR	SRV-MAIL	SRV-V.S	SRV-PREV	SRV-WEB	EA-S.Elec	Per-D.Comer	Per-D.Prev	Per-Comer	Per-D.V.S	Per-I.V.S	Per-D.Fin	Per-Tec.TIC	Per-Resta
Inst -E.C																																														
Inst -D.T																																														
Inst-U.M																																														
HW-PC																																														
HW-PT																																														
HW-Srv.Cor																																														
HW-Srv.PREV																																														
HW-Rou.Cen																													50																	
HW-SW.Cen																																														
HW–Rou.DT					100																																								
HW-BB																																														
Apl-Win.Srv						100	100																																							
Apl-Win.XP				100	100																																									
Apl-IIS							100																																							
Apl-Ms.SQL							100																																							
Apl-PREV							100					100	100																																	
Apl-Ms.Ex.Srv												100								80																											
Apl-NFS												100							25	75																											
Apl-Conta														100																																	
Apl-MS.OFF														100																																	
Data-Prv															100	100	100																													
Data-Form																		100																													10
Data-V.S	80	20	05												60	60	60																													
Data-Proc.Int																		100																													10
Data-Conta																		100																												30	10
Data-Comer																		100																							30						10
Data-Contr.Clie	80																																													
Data-Contr.Prov	80																																													
X-WAN										80	20																																			
X-LAN								100	100																																					
SRV-IMPRES																							60				40	40																		
SRV-NFS	100																					25		25	25	25				100			100					100						30	
SRV-DIR																																														
SRV-MAIL	100																	100												100			100					100						30	
SRV-V.S	100																						100							60			60					60				40	30		30	10
SRV-PREV	100																				100									100			100					100		40					30	10
SRV-WEB																																		30												
EA-S.Elec																																														
Per-D.Comer																																														
Per-D.Prev																																														
Per-Comer																																														
Per-D.V.S																																														
Per-I.V.S																																														
Per-D.Fin																																														

Al realitzar aquesta quantificació valorem la repercussió que pot tenir una incidència d'un actiu sobre els actius que depenen d'ell (degradació del servei , no el seu valor de reposició).

Algunes de les principals consideracions que s'han utilitzat de quantificar les dependències:

- La majoria de les dades de vigilància de la salut poden ser consultades tant en format imprès com en format digital, per tant, la dependència del sistema informàtic es menor
- Te un valor rellevant l'edifici central, més que per el continent, per el contingut de les dades que allotja.
- La xarxa local i els elements que la suporten són bàsics tant per el personal intern com per el personal desplaçat de l'organització.

Finalment, després d'analitzar els següents arbres de dependències, obtenim els següents resultats:

Actiu	**Valoració inicial**	**Valoració acumulada**
Inst -E.C	A	MA
Inst -D.T	B	MA
Inst-U.M	B	A
HW-PC	B	MA
HW-PT	M	MA
HW-Srv.Cor	MB	MA
HW-Srv.PREV	MB	MA
HW-Rou.Cen	MB	MA
HW-SW.Cen	MB	MA
HW–Rou.DT	MB	MA
HW-BB	MB	A
Apl-Win.Srv	MB	MA
Apl-Win.XP	B	MA
Apl-IIS	MB	MA
Apl-Ms.SQL	MB	MA
Apl-PREV	MB	MA
Apl-Ms.Ex.Srv	MB	MA
Apl-NFS	MB	MA
Apl-Conta	MB	MA
Apl-MS.OFF	MB	MA
Data-Prv	MA	MA
Data-Form	M	M
Data-V.S	MA	MA
Data-Proc.Int	MB	B
Data-Conta	B	B
Data-Comer	M	M
Data-Contr.Clie	A	MA
Data-Contr.Prov	A	MA
X-WAN	MB	MA
X-LAN	MB	MA
SRV-IMPRES	MB	A
SRV-NFS	MB	MB
SRV-DIR	MB	MA
SRV-MAIL	M	M
SRV-V.S	M	M
SRV-PREV	B	B
SRV-WEB	MB	MB
EA-S.Elec	MB	MA
Per-D.Comer	B	A
Per-D.Prev	B	M
Per-Comer	MB	A
Per-D.V.S	B	A
Per-I.V.S	MB	A
Per-D.Fin	B	M
Per-Tec.TIC	MB	MA
Per-Resta	MA	MA

Algunes conclusions que ja podem obtenir respecte al valor acumulat resultant són les següents:

- El sistema informàtic, la seva ubicació i el sistema elèctric associats són essencials per garantir la seguretat del sistema.
- La xarxa de comunicacions es requereix per accedir a la informació, tenint en compte la dispersió del personal, comporta una càrrega per el sistema alta.
- El servei de directoris és la via d'accés per qualsevol del accessos a les aplicacions dels servidors, per tant és un servei crític per la disponibilitat de les dades.
- Tot i que el cost i dedicació actual per el personal tècnic que ha de mantenir el sistema no és molt elevat, la repercussió que pot tenir un problema en aquest actiu és d'una magnitud elevada.

3.2.4 Dimensió de seguretat

En aquest punt, i un cop valorat globalment el sistema, estem en disposició de valorar la importància que tenen els diferents actius en funció de les diferents dimensions de seguretat (el que es denomina com una valoració ACIDA). Aquest anàlisis ens permetrà en fases posteriors, poder escollir les salvaguardes prioritzant els aspectes de seguretat que més interessin a la nostra organització.

Les 5 dimensions de seguretat que analitzarem en la taula adjunta són:

- Autenticitat: Garantir que la identitat del origen de les dades.
- Confidencialitat: Garantir que les dades només es troba accessible per les persones autoritzades.
- Integritat: Garantir que la informació és completa i que no es troba alterada
- Disponibilitat: Assegurar que els usuaris tenen accés a la informació quan requereixen accedir-hi.
- Auditoria (Traçabilitat): Assegurar en tot moment qui ha accedit i/o modificat les dades i en quin moment.

Utilitzarem la següent escala per classificació les dimensions de seguretat dels diferents actius:

Valor		Criteri
10	Molt alt	Dany molt greu a la organització
7-9	Alt	Dany greu a la organització
4-6	Mig	Dany important a la organització
1-3	Baix	Dany menor a la organització
0	Despreciable	Irrellevant a efectes pràctics

Actiu	Valoració	Dimensió Seguretat					Observacions
		A	C	I	D	A	
Inst -E.C	MA	4	7	9	7	4	Es troba emmagatzemada la informació. Els danys en aquest actiu pot afectar sensiblement a la majoria de la informació de la organització
Inst -D.T	MA	3	4	6	4	3	Es disposa d'un nombre reduït en format imprès, ja que la majoria de l'informació es troba a la central.
Inst-U.M	A	2	3	3	4	2	Només es disposa temporalment dels últims reconeixements mèdics. Sense aquest servei, es retarda la introducció d'una part dels reconeixements
HW-PC	MA	4	5	3	4	3	Aquests equips es troben a la central i no sempre es troben ocupats. Els usuaris de la central poden accedir a la informació a través d'un altre equip. No es guarden les dades en local
HW-PT	MA	4	6	3	6	3	Son d'us exclusiu per el portador. La no disponibilat dels equips tenen un impacte major per l'accés a la informació. Es troben fora del recinte principal de l'empresa, per tant, es troben més exposats a l'accés per terceres persones
HW-Srv.Cor	MA	3	3	3	7	3	La importancia d'aquest actiu es que es trobi disponible. Les altres dimensions de seguretat de la informació estan condicionades a altres actius (seguretat edifici, vulnerabilitat sistema operatiu...)
HW-Srv.PREV	MA	3	4	4	7	3	La importancia d'aquest actiu es que es trobi disponible. Les altres dimensions de seguretat de la informació estan condicionades a altres actius (seguretat edifici, vulnerabilitat sistema operatiu...). Te un major pes que el servidor de correu ja que es disposen de les dades més especifiques de la organització.
HW-Rou.Cen	MA	4	7	3	7	4	Els principals objectius d'aquest tipus de dispositiu es garantir que només accedeixen els dispositius autoritzats, que tenim un registre de les conexions en cas d'un incident de seguretat i que ens permeti l'accés als servidors tant desde la empresa com desde la resta de seus.
HW-SW.Cen	MA	2	2	2	7	2	Aquest element només es necesita per poder conectar els equips de la central amb els serveis d'informació digital.
HW–Rou.DT	MA	2	2	2	6	2	El principal focus d'activitat d'aquests elements es donar accés als treballadors que es troben en la resta de delegacions
HW-BB	A	2	4	1	4	2	Aquests dispositius ens permeten connectarnos al correu desde qualsevol ubicació. Emmagatzemen correus en local per-lo que poden comprometre l'accés a les dades i ser utilitzats per tercers
Apl-Win.Srv	MA	8	8	8	7	8	El sistema operatiu dels servidors es la porta d'accés a la informació. La seva seguretat local compromet sensiblement en les diferents dimensions de seguretat
Apl-Win.XP	MA	5	5	3	5	5	La seguretat local dels equips compromet l'accés a la informació, principalment en els equips que no es trobin a la central. No disposem d'informació rellevant en local.
Apl-IIS	MA	5	5	3	5	5	La configuració d'aquest servei i el seu manteniment comprometen. Aquest servei es troba en la mateixa màquina que les dades, estan fora de la recomanació del proveidor, per tant, te un impacte major sobre l'accés a la informació. Es registren els accesos externs que es realitzen desde l'exterior.
Apl-Ms.SQL	MA	7	7	7	5	5	Es la porta principal d'accés a la informació de vigilància de la salut i de prevenció. La seva seguretat compromet la confidencialitat, la integritat i la autenticitat de les dades
Apl-PREV	MA	2	5	3	3	2	Es l'aplicació a traves de la qual el personal pot accederi a la informació de prevenció i vigilancia. Disposa d'un mecanisme propi per encriptar la informació. La resta d'aspectes de seguretat recauen sobre els elements de bases de dades y web
Apl-Ms.Ex.Srv	MA	3	3	3	6	3	La seva principal funció recau en la disponibilitat del correu per la planificació.
Apl-NFS	MA	1	2	2	5	1	Es basa en les credencials de sistema operatiu per funcionar. La seva principal funció es que es trobi disponible
Apl-Conta	MA	1	2	2	4	1	La seguretat de l'informació es basa en la gestió de credencials definits a nivell de sistema operatiu i de Directori Actiu.
Apl-MS.OFF	MA	2	3	3	7	2	Es l'eina utilitzada per consultar la majoria de la informació informàtica. Al tractar-se d'un software molt extès, existeixen un ventall de vulnerabilitats associades a versions antigues.
Data-Prv	MA	3	3	4	6	3	Encara que l'informació es facilita a les empreses contractants, pot ser necessàri disposar-le per qualsevol requeriment legal o penal associat.
Data-Form	M	1	2	3	4	1	Informació necessària per realitzar la formació programada amb els diferents clients.
Data-V.S	MA	5	8	8	6	6	Informació sensible que requereix aplicar mesures de seguretat de nivell alt segons la LOPD. Part de la informació es troba distribuida entre les diferents seus i s'ha realitzat un tractament en diferents fases per personal extern i intern.
Data-Proc.Int	B	1	3	3	2	1	El volum de procediments interns definits no és molt alt. La major part d'accions de l'empresa es basa principalment en la experiència dels treballadors.
Data-Conta	B	1	3	3	4	1	Informació que ha d'estar disponible per els cobraments i pagaments que s'han de realitzar
Data-Comer	M	2	3	3	4	2	De la seva disponibilitat dèpen la relació que es pugui tenir amb els clients.
Data-Contr.Clie	MA	4	5	7	7	4	Dins d'aquesta documentació es troben els compromisos que hem d'assolir amb els nostres clients
Data-Contr.Prov	MA	4	5	7	7	4	Aquesta informació ens permet coneixer el compromís dels nostres proveïdors perque poguem assolir els nostres objectius i els que hem formalitzat amb els nostres clients.
X-WAN	MA	4	7	3	7	4	D'aquesta infraestructura depèn la productivat del personal desplaçat fora del edifici central. Es la via d'accés a la nostra informació desde l'exterior.
X-LAN	MA	4	8	3	8	4	Es la xarxa on es troben ubicades les dades. La confidencialitat i la disponibilitat es troben vinculats a aquest actiu.
SRV-IMPRES	A	3	6	6	6	3	L'accés a la informació impresa es troba distribuida en les diferents instal·lacions de la organització. Les dades es troben disponibles en els armaris utilitzats a tal efecte.
SRV-NFS	MB	1	1	1	2	1	La carrèga de seguretat es troba en els actius inferiors.
SRV-DIR	MA	6	8	5	8	5	D'aquest actiu depenen l'accés i els privilegis per accedir a la informació digitalitzada
SRV-MAIL	M	3	4	5	6	3	La perdua del servei de correu dificulta la comunicació interna, amb els proveïdors i amb els clients.
SRV-V.S	M	2	4	4	3	3	El servei s'ha d'enfocar principalment en conservar l'informació i que es compleixin les mesures de seguretat per el tipus d'informació associada.
SRV-PREV	B	1	3	2	4	1	La informació ha d'estar disponible per facilitar-l'hi al client en cas de necessitat.
SRV-WEB	MB	1	1	1	2	1	La principal desavantatge es la qüestió d'imatge que pot suposar la pèrdua del servei associat.
EA-S.Elec	MA	2	3	7	8	4	Una fallada en el sistema elèctric comporta que no es pugui accedir a la major part de la informació. En funció del tipus de falla, pot arribar a comprometre la integritat de la informació.
Per-D.Comer	A	1	6	5	2	1	La cartera de clients contractats pot veure's afectada per una pèrdua d'aquest actiu
Per-D.Prev	M	1	2	3	3	1	La informació que gestiona aquest actiu es necessaria per defensar situacions en les que s'hagi produït un accident o una enfermetat laboral en les empreses contractants. La confidencialitat de la informació que gestiona es menor que la d'altres actius de la organització.
Per-Comer	A	1	6	5	2	1	La cartera de clients contractats pot veure's afectada per una pèrdua d'aquest actiu
Per-D.V.S	A	1	6	5	2	1	Es tracta de personal que gestiona informació que requereix un nivell de seguretat alt segons la legislació vigent
Per-I.V.S	A	1	5	4	2	1	Es tracta de personal que gestiona informació que requereix un nivell de seguretat alt segons la legislació vigent
Per-D.Fin	M	2	4	4	4	2	Les dades que pot comprometre aquest actius són les pròpies de la empresa, no pas la informació compromesa dels clients que es troben en el nostre sistema d'informació.
Per-Tec.TIC	MA	5	7	7	5	5	El seu pes no es troba en el cost associat al personal, si no en els actius que depenen d'aquest actiu. Es tracta d'un actiu amb molts privilegis per accedir a la informació digital.
Per-Resta	MA	5	8	6	5	3	En general, tots els empleats del organització tenen un pes fonamental en la seguretat de la informació. Tenen un major facilitat per accedir a la informació que qualsevol persona aliena a la organització.

3.3 Anàlisis d'amenaces

En aquesta fase estimarem l'impacte i la freqüència de materialització de les amenaces per poder estimar quines pèrdues pot tenir la nostra organització quan aquestes amenaces es materialitzen.

Valorarem la freqüència de les amenaces com el nombre de vegades que es pot materialitzar l'amenaça durant el any i el seu impacte percentual en les diferents dimensions de seguretat.

Les diferents categories d'amenaces que té una organització són bastant comunes. Per tant, utilitzarem un model de referència com és el inventari d'amenaces que disposa el Llibre 2 de la metodologia *MAGERIT*. Això ens permetrà en les següents fases analitzar com impacta en els actius de la nostra organització les diferents amenaces.

Les diferents amenaces estan classificades segons el tipus d'actiu. La freqüència i el impacte de la materialització serà similar per la majoria d'actius si no disposen de salvaguardes. Detallarem quina és la freqüència i impacte general de les diferents amenaces, i indicarem quins actius per les seves característiques específiques les diferenciem de la resta.

Un cop avaluada la freqüència i l'impacte de les diferents amenaces, per facilitar el seu anàlisis posteriors, agruparem els actius i amenaces segons el tipus d'actiu, a excepció d'aquells casos que ja haguem determinat que difereixen de la resta.

Utilitzarem la notació que utilitza *MAGERIT* per identificar les amenaces.

3.3.1 Desastres Naturals

Són aquells successos que es poden produir sense intervenció dels éssers humans de forma directa o indirecta.

3.3.1.1 Foc ([N1])

Es tracta d'una amenaça que es materialitza amb una freqüència baixa. El seu impacte serà alt, en algunes circumstàncies pot comportar el dany total del actiu. Estimarem que la probabilitat de que es produeixi un incendi sigui d'un cop cada deu anys.

L'impacte serà d'un 75% per les instal·lacions, un 10% per els actius de xarxa (afecta a una part de la instal·lació) i d'un 100% per la resta d'actius

3.3.1.2 Danys per aigua ([N2])

Es tracta de les inundacions causades per la pluja. En aquest cas estimem la freqüència cada 5 anys. L'impacte serà d'un 50% per el hardware (en molts casos l'equip quedarà malmès), i per les instal·lacions i xarxes i instal·lacions elèctriques que la estimarem en un 25% (el dany sobre el mateix actiu serà recuperable pràcticament en la seva totalitat, es tracta d'una pèrdua en la seva disponibilitat).

3.3.1.3 Desastres Naturals ([N*])

Abarca la resta de desastres naturals (terratrèmols, llamps). En la zona en la que es troben les nostres instal·lacions és molt poc probable que es materialitzin aquestes amenaces, per tant, hem optat per donar-l'hi el valor teòric de freqüència inexistent.

El seu impacte probablement seria proper al 100% del actiu, però hem estimat que no s'acabaria materialitzant.

3.3.2 De origen Industrial

Són successos que es provoquen de forma incidental per l'activitat humana industrial

3.3.2.1 Foc [I1]

Utilitzarem al mateix criteri que en el cas dels desastres naturals.

3.3.2.2 Aigua [I2]

En aquest cas, també optarem per utilitzar el mateix criteri que en desastres naturals.

3.3.2.3 Desastres industrials [I*]

Es tracten de casuístiques molt especifiques de cadascun dels entorns de treball. Encara que tinguem personal i hardware desplaçats a industries que podrien englobar aquestes amenaces, per les ubicacions habituals en les que es trobaran aquests actius considerarem la probabilitat com a nul·la. El dany probablement acabaria el valor associat del actiu.

3.3.2.4 Contaminació mecànica [I3]

Aquesta amenaça engloba amenaces del tipus vibracions, pols, brutícia en general...

En general serà un tipus de contaminació que no afectarà a la majoria d'actius de la nostra organització. Només ho considerarem per els portàtils que té el nostre personal desplaçat.

En general ho valorarem amb una freqüència improbable i per els portàtils freqüència d'un cop al any. L'impacte mig el definirem del 20%.

3.3.2.5 Contaminació electromagnètica [I4]

Utilitzarem el mateix criteri que l'exposat en contaminació mecànica. Només estaran afectats els terminals del personal desplaçat.

3.3.2.6 Avaria d'origen físic i lògic [I5]

Es tracta de les avaries que es poden produir en els nostres equips, ja sigui per un defecte de fàbrica o com a conseqüència del ús.

Estimarem que la freqüència de la avaria es pot produir un cop cada 5 anys i que l'impacte d'un 50 % (en alguns casos comporta la pèrdua del equip, en altres pot suposar una reparació...)

3.3.2.7 Tall del subministrament elèctric [I6]

En aquest cas estimem que afectarà per igual a tots els actius de la organització. La ocurrència d'aquest tipus d'avaria en la nostra zona la podem estimar amb una freqüència d'un cop al any i

d'una aturada del servei propera al dia de treball, per tant, la repercussió l'hem estimat d'un 10% del valor del actiu a nivell de disponibilitat. La traçabilitat no la considerarem afectada per els actius que disposem (no tenim actius com per exemple, dels que registren l'entrada del personal a les instal·lacions. No hi ha activitat, per tant, no es registra cap accés al sistema informàtic).

3.3.2.8 Condicions inadequades de temperatura i humitat [I7]

Els locals de la nostra organització no tenim condicions de treball inadequades. Considerarem una probabilitat major per els equips del personal desplaçat d'un cop al any. L'impacte el prendrem un valor comú del 20%.

3.3.2.9 Tall en el servei de comunicacions [I8]

Estimarem la probabilitat de que es produeixi una incidència al any i que la seva repercussió sigui d'un 5% (unes hores d'aturada del servei).

3.3.2.10 Interrupció d'altres serveis subministraments essencials [I9]

En el nostre inventari d'actius no hem considerat cap equipament auxiliar que pugui patir aquesta amenaça, per tant la freqüència associada serà 0 i el seu impacte serà nul.

3.3.2.11 Emanacions electromagnètiques [I11]

Aquesta amenaça tracta sobre les emissions electromagnètiques que puguin realitzar els nostres equips, no de les emissions per *WIFI* o *3G*. Considerarem aquesta amenaça com despreciable en el nostre cas.

3.3.3 Errors i Fallides no intencionades

Són errors no intencionats causats per el personal que intervé en els processament de la informació.

3.3.3.1 Errors dels usuaris [E1]

Errors que es manifesten en la utilització dels sistema d'informació. És un error que es produeix amb relativa freqüència i generalment afecten a les dades que s'estaven tractant. Estimaren una ocurrència de 10 cops al any i un impacte del 10%

3.3.3.2 Errors del administrador [E2]

Es tracten d'errors similars al que tenen la resta d'usuaris, però es produeixen en menor freqüència ja que es tracta d'usuaris amb experiència. En canvi el seu impacte és major i més transversal en les diferents dimensions de seguretat ja que disposen d'un privilegi major en l'accés a la informació. Aquesta amenaça no afecta a les dades i els serveis en format imprès. En el cas de les dades de vigilància de la salut al tractar-se d'un format mixt (imprès i digital) hem optat per conservar la ponderació associada al format digital, opció que conservarem en la resta d'amenaces.

3.3.3.3 Errors de monitorització (log) [E3]

Aquest error es produeix quan no es realitza un registre adequat de l'accés a la informació. En la nostra entitat es manifesta freqüentment (uns deu cops al any) ja que no tenim personal especialitzat que es dediqui a revisar aquesta configuració. El seu impacte és alt en la dimensió l'auditoria (traçabilitat). Aquesta amenaça no afecta a les dades i els serveis en format imprès.

3.3.3.4 Errors de configuració [E4]

Ens trobem amb una casuística similar als erros de monitorització. La poca dedicació en personal informàtic repercuteix en la ocurrència d'aquest tipus d'error.

El seu impacte es greu i transversal en les diferents dimensions de seguretat (freqüència d'unes 5 vegades al any i un impacte proper al 50%). Aquesta amenaça tampoc impacte en les dades i els serveis en format imprès.

3.3.3.5 Deficiències en la organització [E7]

Per les característiques de la nostra empresa, el fet d'absorbir personal i que no hi hagin definits procediments escrits per determinar qui ha de fer quines funcions comporta que es produeixin amb més freqüència situacions en la que no es gestionin correctament els actius. Considerem que pot ocórrer amb una freqüència molt alta (unes 100 vegades al any), afectant la disponibilitat dels actius requerits en aquell moment.

3.3.3.6 Difusió de software maliciós [E8]

El parc d'ordinadors que disposem es molt dispers i es troba descentralitzat. El personal no té una consciència sobre l'afectació que pot tenir un mal us dels equips. Aquest tipus d'amenaça es produeix amb una freqüència relativament alta (unes 10 incidències al any) afectant en les diferents dimensions de seguretat (las mes evidents associades a la disponibilitat dels equips i a la confidencialitat de les dades).

3.3.3.7 Errors de re-encaminament [E9]

Es materialitzen aquest tipus d'amenaces en la nostra organització. L'enviament de dades sensibles es pot veure afectada tant en el procés de transport via missatgeria com en l'enviament d'informació sense prendre les degudes mesures de seguretat (utilització de la firma digital)

La freqüència es de uns 10 cops al any i l'impacte es produïra principalment en els actius en els que es realitza l'enviament.

3.3.3.8 Errors de seqüència [E10]

Aquest tipus d'amenaces són merament tècniques i en la actualitzat es produeixen en poca freqüència, per tant, no impactaran en el nostre anàlisis.

3.3.3.9 Fugues d'informació [E14]

De manera accidental arriba una informació compromesa a altres persones. És produeix de forma

esporàdica (1 cop al any) i l'impacte és sobre la confidencialitat de la informació accidentada (1%)

3.3.3.10 Alteració de la informació [E15]

Aquesta modificació accidental de la informació es produeix ocasionalment (10 cops al any) i l'impacte es produeix en la integritat dels actius que s'estan tractant (1%)

3.3.3.11 Introducció d'informació incorrecta [E16]

La probabilitat i l'impacte de que el personal introdueixi les dades erròniament es produeix habitualment (100 cops al any), i el seu impacte es sobre les dades que estan tractant (1%)

3.3.3.12 Degradació de la informació [E17]

La freqüència d'aquesta amenaça és ocasional (10 cops al any) i el seu impacte és mínim (1%)

3.3.3.13 Destrucció de la informació [E18]

La pèrdua de la informació impacta principalment sobre la seva disponibilitat. Freqüència ocasional i impacte mínim.

3.3.3.14 Divulgació de la informació [E19]

Es produeix per manca de discreció. La ocurrència no és alta però el seu impacte en la confidencialitat de la informació es alta (10%).

3.3.3.15 Vulnerabilitats dels programes (software) [E20]

La ocurrència d'errors en el programa durant la seva operació. Per el tipus de software que disposem en la nostra organització (principalment versions antigues), aquest tipus d'ocurrències es produeix de manera freqüentment (100 cops al any), afectant a la informació que s'estava processant en aquell moment (1%).

3.3.3.16 Errors de manteniment /actualització de programes (software) [E21]

En general el software és antic, i al no aplicar les actualitzacions la freqüència d'ocurrència és alta.

3.3.3.17 Erros de manteniment / actualització d'equips (hardware) [E23]

No es realitza una política de renovació d'equips. No es substitueixen fins que no es produeix una avaria irreparable. Calculem la freqüència amb un temps de vida objectiu dels equips (5 anys de vida). El seu impacte repercuteix en l'us del equip per la seva funció assignada (10%).

3.3.3.18 Caiguda del sistema per esgotament de recursos [E24]

Aquest tipus d'amenaces es materialitzen amb major freqüència en aquelles empreses que pateixen un creixement i no es realitza una planificació sobre la capacitat dels recursos.

Aquest tipus d'amenaces es materialitzen un cop al any per a la majoria d'actius amb un impacte a la disponibilitat d'un 10%, i en el cas dels servidors s'està materialitzant 5 cops al any.

3.3.3.19 No disponibilitat del personal [E28]

L'absència del personal es materialitza un cop al any i la mitjana d'absència es de 2 dies (afectant un 1% a la disponibilitat anual)

3.3.4 Atacs intencionats

Són atacs al nostre sistema que es realitzen de forma deliberada. Veurem quina és la freqüència per cadascuna de les següents amenaces, però hem de tenir en compte que el atac intencionat busca realitzar el màxim mal possible, per tant, generalment l'impacte serà mol més gran que les amenaces produïdes per errors no intencionats.

3.3.4.1 Manipulació de la configuració [A4]

És tracta d'un tipus d'atac poc freqüent (l'atacant extern obté les credencials d'administrador), però en el cas de que és materialitzi és molt nociu, ja que pot alterar la informació i el rastre associat.

3.3.4.2 Suplantació de la identitat del usuari [A5]

Un persona interna o externa de la organització utilitza les credencials per fer-se passar per un altre usuari. Aquest tipus d'amenaça afecta en varies dimensions, però principalment en la autenticitat.

La probabilitat és una mica superior a l'atac per manipulació de la informació, ja que l'atacant no te per que tenir un perfil tècnic per accedir al sistema, però l'impacte en la resta de dimensions normalment serà menor.

3.3.4.3 Abús de privilegis d'accés [A6]

Els usuaris del sistema aprofiten els permisos que disposen per fer més accions de les que li pertoquen.

Aquesta amenaça té una freqüència ocasional (10 cops al any) i el seu impacte estaria al voltant del 1%.

3.3.4.4 Us no previst [A7]

Utilitzar els equips personals per un ús no empresarial. Aquesta amenaça afecta principalment a la disponibilitat dels recursos.

Aquest tipus d'amenaça es produeixen amb freqüència (100 cops al any), amb un impacte del 1% en la disponibilitat.

No incloem en aquesta amenaça les instal·lacions elèctriques, ja que no contenen dades

3.3.4.5 Difusió de software maliciós [A8]

La probabilitat de que es doni aquest esdeveniment de forma intencionada és molt baixa

(*PREVENCIÓ S.L.* no és un objectiu principal per ciberdelinqüents) però el seu impacte seria molt gran en qualsevol de les dimensions de seguretat.

3.3.4.6 Re-encaminament de missatges [A9]

Amenaça de baixa probabilitat però que afecta principalment a la confidencialitat de la informació, ja que intencionadament s'està desviant informació i fins i tot no arribar al destí. Si aquest tipus d'anomalia no es detecta el dany que es pugui realitzar a la organització és gran.

3.3.4.7 Alteració de seqüència [A10]

La informació es fragmenta quan s'envia per els sistemes. Una modificació intencionada pot provocar que aquesta informació transmesa es danyi. De baixa probabilitat i d'un impacte moderat.

3.3.4.8 Accés no autoritzat [A11]

L'atacant pot accedir a la informació, aprofitant una errada del sistema en la identificació d'usuari. Aquest tipus de vulnerabilitat és freqüent i el impacte considerable.

No incloem en aquesta amenaça les instal·lacions elèctriques, ja que no contenen dades

3.3.4.9 Anàlisis de tràfic [A12]

En aquest tipus d'amenaces l'atacant es dedica a monitoritzar el tràfic de la organització (origen, destí, volum, freqüència... per extreure conclusions sense tenir que analitzar el contingut associat.

Aquest tipus de amenaces generalment precedeixen a altres tipus d'atacs amb objectius més concrets. Per tant la seva freqüència pot ser molt elevada.

3.3.4.10 Repudi [A13]

En aquest tipus d'amenaces l'emissor o destinatari d'una informació rebutgen haver sigut part de la comunicació o sobre la recepció d'un missatge. Afecta principalment a la traçabilitat de la informació.

De freqüència ocasional. Impacta principalment a la informació transmesa.

3.3.4.11 Intercepció d'informació (escolta) [A14]

L'atacant té accés a la informació sense alterar la informació. De freqüència ocasional (10 cops al any) té un impacte important sobre la confidencialitat dels actius afectats.

3.3.4.12 Modificació de la informació [A15]

En aquesta amenaça l'objectiu és modificar les dades finals per obtenir un benefici especific. És produeix de manera ocasional, però l'impacte pot arribar a ser considerable en la integritat de les dades.

3.3.4.13 Introducció de falsa informació [A16]

Es tracta d'un tipus d'amenaça similar a la modificació de la informació a nivell d'objectiu. La freqüència i l'impacte són similars.

3.3.4.14 Corrupció de la informació [A17]

En aquest cas l'objectiu es que la informació no sigui fiable. De freqüència ocasional, en aquesta ocasió afectaria a la integritat de les dades.

3.3.4.15 Destrucció de la informació [A18]

Aquesta amenaça afecta a la disponibilitat de les dades. De freqüència ocasional, pot arribar a tenir un dany elevat.

3.3.4.16 Divulgació de la informació [A19]

Es tracta d'una amenaça important afectant a la confidencialitat de la nostra informació.

3.3.4.17 Manipulació de programes [A22]

Aquesta amenaça és d'origen merament tècnic, per tant redueix la possibilitat de que l'origen sigui personal amb accés autoritzat. De freqüència baixa però d'impacte elevat.

3.3.4.18 Denegació de servei [A24]

Aquest tipus d'amenaça es materialitza quan no hi ha recursos suficients per accedir a la informació. L'impacte és similar al seu error homòleg. En la nostre organització aquesta amenaça té una freqüència baixa.

3.3.4.19 Robatori [A25]

Considerarem que es tracta d'un fet poc freqüent, però que té un impacte considerable sobre l'actiu afectat, tant en la confidencialitat de la informació que contingui l'actiu com en la seva disponibilitat.

3.3.4.20 Atac destructiu [A26]

Aquest tipus d'atac pot ser perpetrat tant per personal intern o extern. Tant per fer mal objectiu a la organització com per un fet de vandalisme.

També ho considerarem com a poc freqüent però amb un impacte màxim per la nostra organització.

3.3.4.21 Ocupació enemiga [A27]

En aquest cas es tracta d'invasió dels locals de la organització, no disposant de control sobre els medis d'accés a la informació.

Encara que el dany que pogués ocasionar pogués ser molt gran, per la nostra organització, aquest tipus d'amenaça té una probabilitat pràcticament nul·la.

3.3.4.22 No disponibilitat del personal [A28]

Les malalties i altres causes justificades ja s'han analitzat en amenaces no intencionades. En aquest cas es refereix a absentisme laboral, vagues, bloqueig dels accessos per part de tercers.

En aquest cas hem valorat una freqüència d'un cop al any per persona afectada i l'impacte associat respecte a la disponibilitat correspondria a un dia de treball.

3.3.4.23 Extorsió [A29]

Pressió que es pugui tenir per tercers (clients, responsables...) per actuar d'una forma determinada.

Ho establirem cop a mitjana un cop al any per persona i l'impacte moderat.

3.3.4.24 Enginyeria social [A30]

Aquesta amenaça es produeix en aquest cas es tracta de l'abús de la bona fe de les persones utilitzant medis tecnològics.

Ho estimarem de freqüència baixa i d'impacte moderat.

3.3.5 Taula resum

A continuació la taula resum de com afecten les amenaces anteriorment descrites als actius de la nostra organització.

Aquesta valoració ens permetrà veure d'una manera general quines són les amenaces que es poden produir més en la nostra organització.

3.3.5.1 Instal·lacions

Actiu/*Amenaces*	**Freqüència**	**A**	**C**	**I**	**D**	**T**
Inst -E.C		50%	100%	10%	100%	100%
Inst -D.T		50%	100%	10%	100%	100%
Inst -U.M		50%	100%	10%	100%	100%
[N1] - Desastres Naturals - Foc	0,1				75%	75%
[N2] - Desastres Naturals - Inundacions	0,2				25%	25%
[N] - Desastres Naturals - Desastres Naturals*	0				100%	100%
[I1] - Industrials - Foc	0,1				75%	75%
[I2]- Industrials - Inundacions	0,2				25%	25%
[I] - Industrials - Desastres Industrials*	0				100%	100%
[A7] - Atacs Intencionats - Us no previst	100				1%	
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A26] - Atacs Intencionats - Atac Destructiu	0,1				100%	
[A27] - Atacs Intencionats - Ocupació Enemiga	0		100%		100%	

Aquesta taula ens indica que les amenaces que més impacte podent tenir en les instal·lacions són el foc i les inundacions. Tot i que la freqüència és reduïda, el seu impacte és molt gran per aquest tipus d'actiu.

També hem de tenir en compte els accessos no autoritzats, els quals es produeixen amb una freqüència elevada i el seu risc més gran.

3.3.5.2 Hardware

Actiu/*Amenaces*	**Freqüència**	**A**	**C**	**I**	**D**	**T**
HW-PC		100%	100%	20%	100%	100%
HW-Rou.Cen		100%	100%	20%	100%	100%
HW-SW.Cen		100%	100%	20%	100%	100%
HW–Rou.DT		100%	100%	20%	100%	100%
HW-BB		100%	100%	20%	100%	100%
[N1] - Desastres Naturals - Foc	0,1				100%	100%
[N2] - Desastres Naturals - Inundacions	0,2				50%	50%
[N] - Desastres Naturals - Desastres Naturals*	0				100%	100%
[I1] - Industrials - Foc	0,1				100%	100%
[I2]- Industrials - Inundacions	0,2				50%	50%
[I] - Industrials - Desastres Industrials*	0				100%	100%
[I3] - Industrials - Contaminació mecànica	0		20%		20%	20%
[I4] - Industrials - Contaminació electromagnètica	0				20%	20%
[I5] - Industrials - Avaria d'origen físic o lògic	0,2				50%	50%
[I6] - Industrials - Tall del subministrament elèctric	1				10%	0%
[I7] - Industrials - Condicions inadequades de temperatura i humitat	0				20%	20%
[I11] - Industrials - Emanacions electromagnètiques	0		0%			
[E2] - Errors i Fallides no intencionades - Errors del administrador	1	10%	10%	20%	20%	20%
[E4] - Errors i Fallides no intencionades - Errors de configuració	5	50%	10%	10%	50%	50%
[E23] - Errors i Fallides no intencionades - Errors de manteniment/Actualitzacions d'equips (hardware)	0,2				10%	
[E24] - Errors i Fallides no intencionades - Caigudes del sistema per esgotament de recursos	1				10%	
[A4] - Atacs Intencionats - Manipulació de la configuració	0,1	100%	50%	10%	50%	100%
[A6] - Atacs Intencionats - Abús de privilegis d'accés	10		1%	1%		
[A7] - Atacs Intencionats - Us no previst	100				1%	
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	10		50%			
[A24] - Atacs Intencionats - Denegació de Servei	10				50%	
[A25] - Atacs Intencionats - Robatori	0,1		100%		100%	
[A26] - Atacs Intencionats – Atac destructiu	0,1				100%	
[A27] - Atacs Intencionats - Ocupació Enemiga	0		100%		100%	

Actiu/*Amenaces*	Freqüència	A	C	I	D	T
HW-PT		100%	100%	20%	100%	100%
[N1] - Desastres Naturals - Foc	0,1				100%	100%
[N2] - Desastres Naturals - Inundacions	0,2				50%	50%
[N] - Desastres Naturals - Desastres Naturals*	0				100%	100%
[I1] - Industrials - Foc	0,1				100%	100%
[I2]- Industrials - Inundacions	0,2				50%	50%
[I] - Industrials - Desastres Industrials*	0				100%	100%
[I3] - Industrials - Contaminació mecànica	1		20%		20%	20%
[I4] - Industrials - Contaminació electromagnètica	1				20%	20%
[I5] - Industrials - Avaria d'origen físic o lògic	0,2				50%	50%
[I6] - Industrials - Tall del subministrament elèctric	1				10%	0%
[I7] - Industrials - Condicions inadequades de temperatura i humitat	1				20%	20%
[I11] - Industrials - Emanacions electromagnètiques	0		0%			
[E2] - Errors i Fallides no intencionades - Errors del administrador	1	10%	10%	20%	20%	20%
[E4] - Errors i Fallides no intencionades - Errors de configuració	5	50%	10%	10%	50%	50%
[E23] - Errors i Fallides no intencionades - Errors de manteniment/Actualitzacions d'equips (hardware)	0,2				10%	
[E24] - Errors i Fallides no intencionades - Caigudes del sistema per esgotament de recursos	1				10%	
[A4] - Atacs Intencionats - Manipulació de la configuració	0,1	100%	50%	10%	50%	100%
[A6] - Atacs Intencionats - Abús de privilegis d'accés	10		1%	1%		
[A7] - Atacs Intencionats - Us no previst	100				1%	
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	10		50%			
[A24] - Atacs Intencionats - Denegació de Servei	10				50%	
[A25] - Atacs Intencionats - Robatori	0,1		100%		100%	
[A26] - Atacs Intencionats – Atac destructiu	0,1				100%	
[A27] - Atacs Intencionats - Ocupació Enemiga	0		100%		100%	

Actiu/*Amenaces*	Freqüència	A	C	I	D	T
HW-Srv.Cor		100%	100%	20%	100%	100%
HW-Srv.PREV		100%	100%	20%	100%	100%
[N1] - Desastres Naturals - Foc	0,1				100%	100%
[N2] - Desastres Naturals - Inundacions	0,2				50%	50%
[N] - Desastres Naturals - Desastres Naturals*	0				100%	100%
[I1] - Industrials - Foc	0,1				100%	100%
[I2]- Industrials - Inundacions	0,2				50%	50%
[I] - Industrials - Desastres Industrials*	0				100%	100%
[I3] - Industrials - Contaminació mecànica	0		20%		20%	20%
[I4] - Industrials - Contaminació electromagnètica	0				20%	20%
[I5] - Industrials - Avaria d'origen físic o lògic	0,2				50%	50%
[I6] - Industrials - Tall del subministrament elèctric	1				10%	0%
[I7] - Industrials - Condicions inadequades de temperatura i humitat	0				20%	20%
[I11] - Industrials - Emanacions electromagnètiques	0		0%			
[E2] - Errors i Fallides no intencionades - Errors del administrador	1	10%	10%	20%	20%	20%
[E4] - Errors i Fallides no intencionades - Errors de configuració	5	50%	10%	10%	50%	50%
[E23] - Errors i Fallides no intencionades - Errors de manteniment/Actualitzacions d'equips (hardware)	0,2				10%	
[E24] - Errors i Fallides no intencionades - Caigudes del sistema per esgotament de recursos	5				10%	
[A4] - Atacs Intencionats - Manipulació de la configuració	0,1	100%	50%	10%	50%	100%
[A6] - Atacs Intencionats - Abús de privilegis d'accés	10		1%	1%		
[A7] - Atacs Intencionats - Us no previst	100				1%	
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	10		50%			
[A24] - Atacs Intencionats - Denegació de Servei	10				50%	
[A25] - Atacs Intencionats - Robatori	0,1		100%		100%	
[A26] - Atacs Intencionats – Atac destructiu	0,1				100%	
[A27] - Atacs Intencionats - Ocupació Enemiga	0		100%		100%	

Les amenaces que més estan destacant per aquest tipus d'actiu per el seu impacte són també les associades a desastres naturals i industrials, encara que la seva freqüència és reduïda.

La amenaces que es materialitzen amb més freqüència i per tant, són més probables són les associades a atacs no autoritzats, les quals representen un impacte més sensible.

Destaquen també les associades a errors de configuració del administrador. Cal recordar que tenim una persona que només ve un dia a la setmana per tasques de manteniment i revisió.

3.3.5.3 Dades

Actiu/*Amenaces*	**Freqüència**	**A**	**C**	**I**	**D**	**T**
Data-Prv		100%	100%	50%	50%	100%
Data-Form		100%	100%	50%	50%	100%
Data-V.S		100%	100%	50%	50%	100%
Data-Proc.Int		100%	100%	50%	50%	100%
Data-Conta		100%	100%	50%	50%	100%
Data-Comer		100%	100%	50%	50%	100%
[E1] - Errors i Fallides no intencionades - Errors dels usuaris	10			10%	10%	
[E2] - Errors i Fallides no intencionades - Errors del administrador	1	10%	10%	20%	20%	20%
[E3] - Errors i Fallides no intencionades - Errors de monitorització (log)	10		10%	10%	10%	50%
[E4] - Errors i Fallides no intencionades - Errors de configuració	5	50%				50%
[E14] - Errors i Fallides no intencionades - Fugues d'informació	1		1%			
[E15] - Errors i Fallides no intencionades - Alteració de la informació	10			1%		
[E16] - Errors i Fallides no intencionades - Introducció d'informació errònia	100			1%		
[E17] - Errors i Fallides no intencionades - Degradació de la informació	10			1%		
[E18] - Errors i Fallides no intencionades - Destrucció de la informació	10				1%	
[E19] - Errors i Fallides no intencionades - Divulgació de la Informació	1		10%			
[A4] - Atacs Intencionats - Manipulació de la configuració	0,1	100%	50%	10%	50%	100%
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	10		50%			
[A15] - Atacs Intencionats - Modificació de la informació	10			50%		
[A16] - Atacs Intencionats - Introducció d'informació falsa	20			50%		
[A17] - Atacs Intencionats - Corrupció de la informació	10			50%		
[A18] - Atacs Intencionats - Destrucció de la informació	10				50%	
[A19] - Atacs Intencionats - Divulgació de la informació	10		100%			

Actiu/*Amenaces*	**Freqüència**	**A**	**C**	**I**	**D**	**T**
Data-Contr.Clie		100%	100%	50%	50%	100%
Data-Contr.Prov		100%	100%	50%	50%	100%
[E1] - Errors i Fallides no intencionades - Errors dels usuaris	10			10%	10%	
[E2] - Errors i Fallides no intencionades - Errors del administrador	0	10%	10%	20%	20%	20%
[E3] - Errors i Fallides no intencionades - Errors de monitorització (log)	0		10%	10%	10%	50%
[E4] - Errors i Fallides no intencionades - Errors de configuració	0	50%				50%
[E14] - Errors i Fallides no intencionades - Fugues d'informació	1		1%			
[E15] - Errors i Fallides no intencionades - Alteració de la informació	1			1%		
[E16] - Errors i Fallides no intencionades - Introducció d'informació errònia	100			1%		
[E17] - Errors i Fallides no intencionades - Degradació de la informació	10			1%		
[E18] - Errors i Fallides no intencionades - Destrucció de la informació	10				1%	
[E19] - Errors i Fallides no intencionades - Divulgació de la Informació	1		10%			
[A4] - Atacs Intencionats - Manipulació de la configuració	0,1	100%	50%	10%	50%	100%
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	10		50%			
[A15] - Atacs Intencionats - Modificació de la informació	10			50%		
[A16] - Atacs Intencionats - Introducció d'informació falsa	20			50%		
[A17] - Atacs Intencionats - Corrupció de la informació	10			50%		
[A18] - Atacs Intencionats - Destrucció de la informació	10				50%	
[A19] - Atacs Intencionats - Divulgació de la informació	10		100%			

Per els actius de dades els atacs no autoritzats són els que representen una major amenaça independentment del format de les dades.

3.3.5.4 Aplicació

Actiu/*Amenaces*	Freqüència	A	C	I	D	T
Apl-Win.Srv		100%	50%	50%	50%	100%
Apl-Win.XP		100%	50%	50%	50%	100%
Apl-IIS		100%	50%	50%	50%	100%
Apl-Ms.SQL		100%	50%	50%	50%	100%
Apl-PREV		100%	50%	50%	50%	100%
Apl-Ms.Ex.Srv		100%	50%	50%	50%	100%
Apl-NFS		100%	50%	50%	50%	100%
Apl-Conta		100%	50%	50%	50%	100%
Apl-MS.OFF		100%	50%	50%	50%	100%
[I5] - Industrials - Avaria d'origen físic o lògic	0,2				50%	50%
[E1] - Errors i Fallides no intencionades - Errors dels usuaris	10			10%	10%	
[E2] - Errors i Fallides no intencionades - Errors del administrador	1	10%	10%	20%	20%	20%
[E3] - Errors i Fallides no intencionades - Errors de monitorització (log)	10			1%		50%
[E4] - Errors i Fallides no intencionades - Errors de configuració	5	50%	10%	10%	50%	50%
[E8] - Errors i Fallides no intencionades - Difusió de software maliciós	10	1%	2%	2%	2%	1%
[E9] - Errors i Fallides no intencionades - Errors de re-encaminament	10	1%	1%	1%		1%
[E10] - Errors i Fallides no intencionades - Errors de seqüencia	0			1%		
[E14] - Errors i Fallides no intencionades - Fugues d'informació	1		1%			
[E20] - Errors i Fallides no intencionades - Vulnerabilitats dels programes (software)	100		1%	1%	1%	
[E21] - Errors i Fallides no intencionades - Errors de manteniment/Actualitzacions d'equips (software)	100			1%	1%	
[A4] - Atacs Intencionats - Manipulació de la configuració	0,1	100%	50%	10%	50%	100%
[A5] - Atacs Intencionats - Suplantació Identitat	1	100%	20%	1%		
[A6] - Atacs Intencionats - Abús de privilegis d'accés	10		1%	1%		
[A7] - Atacs Intencionats - Us no previst	100				1%	
[A8] - Atacs Intencionats - Difusió de software maliciós	0,2	10%	50%	50%	20%	10%
[A9] - Atacs Intencionats - Re-encaminament de missatges	0,2	10%	50%	20%		20%
[A10] - Atacs Intencionats - Alteració de seqüència	0,2			1%		
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	10		50%			
[A22] - Atacs Intencionats - Manipulació de programes	1	10%	50%	50%		10%

En les aplicacions continuem tenim com a amenaces principals els atacs intencionats i en particular els d'accés autoritzat .

A part dels problemes derivats en l'administració dels sistemes, també destaquen els errors de manteniment i d'actualització del *software*. Disposem d'un conjunt heterogeni de versions de sistema operatiu i eines ofimàtiques, la majoria de les quals tenen més de 8 anys. Per tant es troben més exposades a atacs al portar més temps en el mercat.

3.3.5.5 Xarxa

Actiu/*Amenaces*	Freqüència	A	C	I	D	T
X-WAN		100%	100%	20%	100%	100%
X-LAN		100%	100%	20%	100%	100%
[N1] - Desastres Naturals - Foc	0,1				10%	10%
[N2] - Desastres Naturals - Inundacions	0,2				25%	25%
[N] - Desastres Naturals - Desastres Naturals*	0				100%	100%
[I1] - Industrials - Foc	0,1				10%	10%
[I2]- Industrials - Inundacions	0,2				25%	25%
[I] - Industrials - Desastres Industrials*	0				100%	100%
[I3] - Industrials - Contaminació mecànica	0				20%	20%
[I4] - Industrials - Contaminació electromagnètica	0				20%	20%
[I5] - Industrials - Avaria d'origen físic o lògic	0,2				50%	50%
[I6] - Industrials - Tall del subministrament elèctric	1				10%	0%
[I7] - Industrials - Condicions inadequades de temperatura i humitat	0				20%	20%
[I8] - Industrials - Tall Servei Comunicacions	1				5%	
[I11] - Industrials - Emanacions electromagnètiques	0		0%			
[E2] - Errors i Fallides no intencionades - Errors del administrador	1	10%	10%	20%	20%	20%
[E4] - Errors i Fallides no intencionades - Errors de configuració	5	50%	10%	1%	50%	50%
[E9] - Errors i Fallides no intencionades - Errors de re-encaminament	10	1%	1%	1%		1%
[E10] - Errors i Fallides no intencionades - Errors de seqüencia	0			1%		
[E14] - Errors i Fallides no intencionades - Fugues d'informació	1		1%			
[E24] - Errors i Fallides no intencionades - Caigudes del sistema per esgotament de recursos	1				10%	
[A4] - Atacs Intencionats - Manipulació de la configuració	0,1	100%	50%	10%	50%	100%
[A5] - Atacs Intencionats - Suplantació Identitat	1	100%	20%	1%		
[A6] - Atacs Intencionats - Abús de privilegis d'accés	10		1%	1%		
[A7] - Atacs Intencionats - Us no previst	100				1%	
[A9] - Atacs Intencionats - Re-encaminament de missatges	0,2	10%	50%	20%		20%
[A10] - Atacs Intencionats - Alteració de seqüència	0,2			1%		
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A12] - Atacs Intencionats - Anàlisis de tràfic	100		10%			
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	10		50%			
[A24] - Atacs Intencionats - Denegació de Servei	10				50%	
[A25] - Atacs Intencionats - Robatori	0,1		100%		100%	
[A26] - Atacs Intencionats - Atac Destructiu	0,1				100%	
[A27] - Atacs Intencionats - Ocupació Enemiga	0				100%	

A nivell general continuen destacant la majoria d'amenaces que hem exposat anteriorment, tot i que destaca especialment la probabilitat de que es produeixi una denegació del servei i el seu impacte associat a la disponibilitat del servei.

3.3.5.6 Serveis

Actiu/*Amenaces*	Freqüència	A	C	I	D	T
SRV-NFS		100%	50%	20%	50%	100%
SRV-DIR		100%	50%	20%	50%	100%
SRV-MAIL		100%	50%	20%	50%	100%
SRV-V.S		100%	50%	20%	50%	100%
SRV-PREV		100%	50%	20%	50%	100%
SRV-WEB		100%	50%	20%	50%	100%
[E1] - Errors i Fallides no intencionades - Errors dels usuaris	10			10%	10%	
[E2] - Errors i Fallides no intencionades - Errors del administrador	1	10%	10%	20%	20%	20%
[E3] - Errors i Fallides no intencionades - Errors de monitorització (log)	10					50%
[E4] - Errors i Fallides no intencionades - Errors de configuració	5	50%	10%	10%	50%	50%
[E9] - Errors i Fallides no intencionades - Errors de re-encaminament	10	1%	1%	1%		1%
[E10] - Errors i Fallides no intencionades - Errors de seqüencia	0			1%		
[E24] - Errors i Fallides no intencionades - Caigudes del sistema per esgotament de recursos	1				10%	
[A4] - Atacs Intencionats - Manipulació de la configuració	0,1	100%	50%	10%	50%	100%
[A5] - Atacs Intencionats - Suplantació Identitat	1	100%	20%	1%		
[A6] - Atacs Intencionats - Abús de privilegis d'accés	10		1%	1%		
[A7] - Atacs Intencionats - Us no previst	100				1%	
[A9] - Atacs Intencionats - Re-encaminament de missatges	0,2	10%	50%	20%		20%
[A10] - Atacs Intencionats - Alteració de seqüència	0,2			1%		
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A13] - Atacs Intencionats - Repudi	10					1%
[A24] - Atacs Intencionats - Denegació de Servei	10				50%	

SRV-IMPRES		100%	50%	20%	50%	100%
[E1] - Errors i Fallides no intencionades - Errors dels usuaris	10			10%	10%	
[E2] - Errors i Fallides no intencionades - Errors del administrador	0	10%	10%	20%	20%	20%
[E3] - Errors i Fallides no intencionades - Errors de monitorització (log)	0					50%
[E4] - Errors i Fallides no intencionades - Errors de configuració	0	50%	10%	10%	50%	50%
[E9] - Errors i Fallides no intencionades - Errors de re-encaminament	10	1%	1%	1%		1%
[E10] - Errors i Fallides no intencionades - Errors de seqüencia	0			1%		
[E24] - Errors i Fallides no intencionades - Caigudes del sistema per esgotament de recursos	1				10%	
[A4] - Atacs Intencionats - Manipulació de la configuració	0,1	100%	50%	10%	50%	100%
[A5] - Atacs Intencionats - Suplantació Identitat	1	100%	20%	1%		
[A6] - Atacs Intencionats - Abús de privilegis d'accés	10		1%	1%		
[A7] - Atacs Intencionats - Us no previst	100				1%	
[A9] - Atacs Intencionats - Re-encaminament de missatges	0,2	10%	50%	20%		20%
[A10] - Atacs Intencionats - Alteració de seqüència	0,2			1%		
[A11] - Atacs Intencionats - Accés no autoritzat	100	50%	50%	10%		
[A13] - Atacs Intencionats - Repudi	10					1%
[A24] - Atacs Intencionats - Denegació de Servei	10				50%	

La possibilitat d'accessos no autoritzats en el servei ens plantejarà aplicar mesures preventives per evitar problemes en la disponibilitat del servei.

3.3.5.7 Equipament auxiliar

Actiu/*Amenaces*	Freqüència	A	C	I	D	T
EA-S.Elec		50%	100%	10%	100%	100%
[N1] - Desastres Naturals - Foc	0,1				100%	100%
[N2] - Desastres Naturals - Inundacions	0,2				25%	25%
[N] - Desastres Naturals - Desastres Naturals*	0				100%	100%
[I1] - Industrials - Foc	0,1				100%	100%
[I2]- Industrials - Inundacions	0,2				25%	25%
[I] - Industrials - Desastres Industrials*	0				100%	100%
[I3] - Industrials - Contaminació mecànica	0				20%	20%
[I4] - Industrials - Contaminació electromagnètica	0				20%	20%
[I5] - Industrials - Avaria d'origen físic o lògic	0,2				50%	50%
[I6] - Industrials - Tall del subministrament elèctric	1				10%	0%
[I7] - Industrials - Condicions inadequades de temperatura i humitat	0				20%	20%
[I9] - Industrials - Interrupció d'altres serveis i subministraments essencials	0				0%	
[A7] - Atacs Intencionats - Us no previst	0				1%	
[A11] - Atacs Intencionats - Accés no autoritzat	0	50%	50%	10%		
[A25] - Atacs Intencionats - Robatori	0,1		100%		100%	
[A26] - Atacs Intencionats - Atac Destructiu	0,1				100%	
[A27] - Atacs Intencionats - Ocupació Enemiga	0		100%		100%	

Les amenaces més significatives per aquest actiu son les associades a foc per el seu impacte sobre la disponibilitat del servei i els talls del subministrament elèctric, per la seva freqüència.

3.3.5.8 Personal

Actiu/*Amenaces*		Freqüència	A	C	I	D	T
Per-D.Comer	2		10%	10%	10%	100%	10%
Per-D.Prev	4		10%	10%	10%	100%	10%
Per-Comer	2		10%	10%	10%	100%	10%
Per-D.V.S	2		10%	10%	10%	100%	10%
Per-I.V.S	2		10%	10%	10%	100%	10%
Per-D.Fin	2		10%	10%	10%	100%	10%
Per-Tec.TIC	2		10%	10%	10%	100%	10%
Per-Resta	2		10%	10%	10%	100%	10%
[E7] - Errors i Fallides no intencionades - Deficiències de la organització		100				10%	
[E28] - Errors i Fallides no intencionades - No disponibilitat del personal		1				100%	
[A28] - Atacs Intencionats - No disponibilitat del personal		1				100%	
[A29] - Atacs Intencionats - Extorsió		1	10%	10%	10%		10%
[A30] - Atacs Intencionats - Enginyeria Social		1	10%	10%	10%		10%

A nivell general, destaca les deficiències de la organització a nivell de definició de protocols i responsabilitat en les actuacions, que repercuteixen sobre la disponibilitat del servei.

La resta d'incidències són d'una probabilitat més baixa, i el seu impacte és moderat.

3.3.6 Impacte potencial

Un cop valorades les amenaces, podem quantificar el cost econòmic anual que pot suposar la seva materialització en cadascun dels actius de la organització.

Al tractar-se del primer anàlisis de riscos que es realitza en la nostra organització, no s'han considerat les salvaguardes per poder disposar d'una visió general de la seguretat i la dependència de cadascun dels nostres actius en la seguretat de la informació. En la fase de propostes de nous projectes per millorar la seguretat de *PREVENCIO S.L* analitzarem com d'efectives són les salvaguardes que ja té implantada la organització.

Es ponderarà l'impacte en funció de la dimensió de seguretat que més importància hem donat en la nostre valoració. Optem per calcular només la dimensió més important de cadascun dels actius per no sobrecarregar la valoració del actiu. L'impacte anual és el següent:

Actiu	Valor	Risc Intrínsec
Data-Form	75.000 €	1.510 €
Data-V.S	300.000 €	54.460 €
Data-Proc.Int	30.000 €	2.746 €
Data-Conta	30.000 €	604 €
Data-Comer	75.000 €	1.510 €
Data-Prv	300.000 €	6.041 €
Data-Contr.Clie	300.000 €	5.055 €
Data-Contr.Prov	300.000 €	5.055 €
Apl-Win.Srv	300.000 €	47.638 €
Apl-Win.XP	300.000 €	47.638 €
Apl-IIS	300.000 €	47.638 €
Apl-Ms.SQL	300.000 €	47.638 €
Apl-PREV	300.000 €	47.638 €
Apl-Ms.Ex.Srv	300.000 €	47.638 €
Apl-NFS	300.000 €	47.638 €
Apl-Conta	300.000 €	47.638 €
Apl-MS.OFF	300.000 €	47.638 €
EA-S.Elec	300.000 €	1.315 €
Inst -E.C	300.000 €	8.219 €
Inst -D.T	300.000 €	8.219 €
Inst -U.M	150.000 €	966 €
HW-PC	300.000 €	45.904 €
HW-Rou.Cen	300.000 €	45.904 €
HW-SW.Cen	300.000 €	7.948 €
HW–Rou.DT	300.000 €	7.948 €
HW-BB	150.000 €	3.974 €
HW-PT	300.000 €	46.068 €
HW-Srv.Cor	300.000 €	8.277 €
HW-Srv.PREV	300.000 €	8.277 €
X-WAN	300.000 €	54.460 €
X-LAN	300.000 €	54.460 €
SRV-NFS	10.000 €	270 €
SRV-DIR	300.000 €	8.096 €
SRV-MAIL	75.000 €	2.024 €
SRV-V.S	75.000 €	10.510 €
SRV-PREV	30.000 €	810 €
SRV-WEB	10.000 €	270 €
SRV-IMPRES	150.000 €	20.774 €
Per-D.Comer	150.000 €	82 €
Per-D.Prev	75.000 €	2.466 €
Per-Comer	150.000 €	82 €
Per-D.V.S	150.000 €	82 €
Per-I.V.S	150.000 €	82 €
Per-D.Fin	75.000 €	41 €
Per-Tec.TIC	300.000 €	164 €
Per-Resta	300.000 €	164 €
Total	**10.010.000 €**	**853.584 €**

El resultat obtingut ens permet quantificar quins són els actius que comporten un risc més elevat per la organització pel fet de que es materialitzin les amenaces.

Hi ha que tenir en compte que en aquesta valoració no hem inclòs les salvaguardes que hi ha actualment en la organització. Per tant, un cop incloses en l'anàlisi ens pot reduir l'impacte total.

Segons l'impacte total i la relació respecte al valor del actiu, hem de prioritzar les salvaguardes en:

- Les dades de vigilància de la salut, tant la part informàtica com el servei imprès. Aquestes dades requereixen segons la *LOPD* una protecció especial al tractar-se de dades mèdiques.
- 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.*
- Les aplicacions dels equips client. No disposem d'una infraestructura homogènia i sota un control administratiu.
- Els elements de la comunicació entre els portàtils i el servidors de prevenció. Treballem a través d'una xarxa pública, per tant, la comunicació es pot veure compromesa si no realitzem les mesures de seguretat oportunes.

3.4 Conclusions

Tenint en compte els diferents anàlisis previs que hem realitzat, podem determinar quins aspectes del nostre sistema d'informació destaquen principalment en el nostre anàlisis de riscos

- L'empresa requereix 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. La falta de dedicació comporta que es materialitzin amb major freqüència els errors associats al administrador
- S'ha de definir procediments interns per realitzar les diferents tasques de cadascun. Actualment repercuteix en la eficàcia de disposar la informació.
- S'ha de prendre les mesures oportunes per millorar la seguretat de les dades, especialment la confidencialitat de les dades de vigilància de la salut.
- S'ha d'actualitzar els equips amb les últimes versions de software que permeti minimitzar l'impacte dels atacs de software maliciós.
- S'ha de potenciar la protecció de la comunicació entre els equips remots i la central ja que els seus riscos són molt elevats.
- S'ha de prendre les mesures oportunes per minimitzar els atacs que puguin procedir des de l'exterior.

4 AUDITORIA DE COMPLIMENT DE LA ISO:IEC 27002:2005

En aquest punt analitzarem la maduresa dels diferents controls de seguretat que la normativa ISO 27002 indica que són els que apliquen pràcticament en la majoria de empreses a analitzar la seguretat. Aquest anàlisis ens permetrà conèixer les debilitats de l'empresa i ens permetrà revisar els procediments a aplicar i serà un dels factors a analitzar en la proposta de projectes a presentar per millorar la seguretat de la informació de la empresa.

Avaluarem els diferents controls de seguretat en funció dels següents barems:

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	L0	Inexistent	Manca completa de qualsevol procés recognoscible. 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. Els procediments són inexistents o localitzats en àrees concretes. 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. 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%	L3	Procés definit	L'organització sencera participa en el procés. 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. 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. En base a criteris quantitatius es determinen les desviacions més comuns i s'optimitzen els processos.

4.1 Política de seguretat

La empresa és conscient de que s'ha d'establir un control per determinar les seves actuacions. Es tracta d'una empresa en la qual hi ha una certa rotació del personal, per tant es necessari establir un criteri d'actuació definit en el procés de la informació, especialment en el referent en els apartats de vigilància de la salut, el qual es processa tant per personal intern, i extern de la empresa.

4.1.1 Política de seguretat de la informació

4.1.1.1 Document de política de seguretat

No existeix un document formal en el qual s'estableixi les directrius de seguretat. La direcció de l'empresa és conscient que s'ha d'establir procediments en algunes de les àrees amb les que es tracten dades sensibles i que s'ha de conscienciar al personal sobre les actuacions que comprometen aquesta seguretat.

Considerem que la organització es troba en una fase Inicial en aquest control.

4.1.1.2 Revisió de la política de seguretat

Al no existir un procediment formal, no existeix una revisió de la política de seguretat definida. Els responsables de les diferents àrees de l'empresa són coneixedors dels diferents canvis legislatius que es poden produir i intenten transmetre-ho mitjançant correu electrònic al personal que gestionen.

Considerem que la organització es troba en una fase Inicial en aquest control.

4.2 Organització de la seguretat de la informació

4.2.1 Organització interna

4.2.1.1 Comitè de gestió de seguretat de la informació

S'ha format un comitè de gestió de seguretat de la informació, el qual encara no ha realitzat cap reunió formal ni s'han revisat les accions ni els events que han succeït des de la anterior reunió ni han sorgit propostes sobre la seguretat (no s'ha fet efectiva la gestió dels sistemes de seguretat de la informació). Per tant ens trobem en una fase inicial d'aquest control.

4.2.1.2 Coordinació de la seguretat de la informació

La coordinació de la seguretat de la informació s'ha realitzat fins a data d'avui de manera individual, de manera intuïtiva, sense tenir uns objectius marcats. No existeix un comitè de coordinació de la seguretat. Per tant, ens trobem un altre cope en una fase inicial d'aquest control.

4.2.1.3 Assignació de responsabilitats sobre seguretat de la informació

De manera intuïtiva cadascuna de les persones de l'empresa és coneixedora de quins actius de l'empresa són responsables. En alguns tipus d'actiu, com per exemple, els portàtils o el material mèdic utilitzat per la revisió, se sap a quina persona/delegació s'ha assignat, encara que no es troba

documentat ni informat als treballadors dels procediments de seguretat que s'han de realitzar per aquests actius ni les seves responsabilitats. Per tant, aquest control el considerarem reproduïble, però intuïtiu.

4.2.1.4 Procés d'autorització de recursos per el tractament de la informació

L'adquisició de nous recursos no sempre venen autoritzats per el responsable de seguretat (de fet aquesta figura és una mica difosa en l'organització, ja que l'assumeix el director comercial al ser la persona que s'encarrega de la contractació de personal tècnic, coordinació en la instal·lació de nous programes...).

Alguns dels materials els autoritza directament el director financer al aprovar la sol·licitud de compra, i és el director comercial el que realitza la instal·lació de software addicional (software de *PREVENET*).

Algun altre material ve provinent de l'adquisició de serveis de prevenció, el qual són equips que ja es trobaven en us.

L'únic protocol establert en la utilització de nous equips és la instal·lació d'un antivirus comú per tots els equips de la organització.

Valorarem aquest control en una fase inicial.

4.2.1.5 Acords de confidencialitat

No hi ha establert a nivell contractual cap acord de confidencialitat. La confidencialitat es basa en el codi deontològic que es practica en el sector sanitari.

Considerem que el codi deontològic no es suficient per cobrir totes les necessitats de seguretat de l'empresa, ja que a més no afecta a tot el personal, per tant, considerarem que aquest control és inexistent.

4.2.1.6 Contactes amb autoritats

Es tracta d'una empresa molt dispersa i amb una estructura d'empresa petita. Els únics contactes a nivell d'autoritats són amb l'Agència de Protecció de Dades per validar que es realitzen per el compliment de la *LOPD* de les dades personals que requereixen una seguretat de nivell alt.

Ens trobem amb un nivell inicial de maduresa del control.

4.2.1.7 Contactes amb grups d'interès especial

PREVENCIO S.L s'ha posat en contacte amb la nostra organització per revisar el compliment de seguretat i ens ha assignat un rol d'assessoria per ajudar-los en millorar els procediments i formar un sistema de gestió de seguretat de la informació. Per tant, ens trobem en un estat de maduresa inicial del control.

4.2.1.8 Revisió independent de la seguretat de la informació

AUDITORIA S.L. és la empresa que un cop implantat el sistema de gestió de seguretat de la

informació realitzarà el rol d'assessor Es tracta d'una situació inicial fins que *PREVENCIO S.L* pugui gestionar de manera independent la seguretat de la informació.

Actualment no existeix una relació contractual amb altres empreses per realitzar aquest tipus de revisió, per que pugui analitzar de manera imparcial les decisions que realitzi *PREVENCIO S.L* a nivell de seguretat. Ens consta que hi ha hagut contactes amb altres empreses per la contractació del servei d'assessoria.

Ens trobem en una fase inicial sobre el sistema de gestió de la seguretat. Segons s'ha comentat amb *PREVENCIO S.L* aquest tipus de revisió es realitzaren un cop el sistema de gestió disposi de la maduresa suficient.

Ens trobem també en aquest punt en una fase inicial.

4.2.2 Parts externes

PREVENCIÓ S.L té relació amb varies empreses, les quals de manera directa o indirecta poden tenir o tenen accés a la informació sensible de la organització.

4.2.2.1 Identificació de riscos per el accés a tercers

S'és coneixedor de que la informació de *PREVENCIO S.L* té un riscos en l'accés de tercers. A part de les empreses i personals de serveis que tenen accés a les ubicacions centrals, es té en compte que molt del personal es troba en altres delegacions o inclús treballen en les instal·lacions dels clients

A més, quan es realitzen revisions mèdiques hi han dades que s'envien a traves de missatgeria als laboratoris o inclús els resultats dels informes s'envien a través de missatgeria des de serveis externs contractats cap a la central.

No hi ha documentació on es detalli aquests tipus d'accessos que ha de requerir aquest tipus de personal.

Amb la subcontractació de serveis externs de vigilància de la salut i de prevenció se'ls hi fa saber les necessitats de seguretat de la organització a nivell general i són acceptats a nivell contractual.

En canvi, en els serveis de neteja o el tècnic informàtic no se'ls hi ha fet constar aquest compromís.

Ens trobem en general, en una fase del control reproduïble, però intuïtiu, encara que hi han aspectes de maduresa que s'han de millorar.

4.2.2.2 Requisits de seguretat quan es tracta amb clients

Molt del nostre personal treballa en les instal·lacions del client a on es realitzen revisions mèdiques. Normalment el client facilita una ubicació en la que els metges disposen de la seva clau del despatx associat per garantir la privacitat, encara que no es produeix en tots els casos. No està acordat aquest cel en la contractació del servei

En alguns casos es facilita el resultat de les revisions mèdiques en un paquet postal a una única adreça i és la empresa contractant la que facilita els resultats als treballadors. Aquest procediment pot arribar a comprometre la confidencialitat requerida dels informes mèdics. Es requereix un compromís previ com en el moment de la recepció de que els informes només seran consultables per la persona a la que s'ha realitzat l'informe mèdic. Aquest aspecte tampoc està acordat amb el

client en la majoria de casos. Inclús és el propi client el que sol·licita en alguns casos unes exigències mínimes de seguretat sobre la informació que els hi enviem.

Es tracta d'un control amb una maduresa reproduïble, però en el que clarament es pot observar que requereix una mesures més grans per no comprometre la informació.

4.2.2.3 Requisits de seguretat en contractes amb tercers

Com hem indicat en controls anteriors, es troben identificats els riscos per part de tercers, inclús ens trobem en alguns casos que es fa constar les necessitats de seguretat però no existeix compromisos concrets sobre les mesures de seguretat que han d'adoptar aquests tercers.

S'han de fer constar a nivell contractual aspectes com:

- Nivell de servei desitjats
- Controls de seguretat física i lògica
- Dret d'auditar els serveis oferts

Per tant, aquest control el considerem actualment com inexistent

4.3 Gestió d'actius

4.3.1 Responsabilitat sobre els actius

4.3.1.1 Inventari d'actius

Disposem d'un inventari parcial d'actius físics i a qui estan assignats, però no sobre altres actius com el software, dels serveis, de les dades, ...

Degut a aquestes mancances considerarem que aquest control es troba en una fase inicial.

4.3.1.2 Propietat dels actius

El propietari dels actius es basa en una suposició lògica del personal, en cap cas en un document formal (tot actiu pertany a l'empresa...).

Degut a aquesta indefinició considerarem que aquest control es troba en una fase inicial.

4.3.1.3 Ús adequat dels actius

No hi ha un propietari formal. Per tant, ens trobem en alguns casos en que no realitza una classificació dels actius i una revisió dels actius i del seu ús.

Ens ha fet la organització que el personal disposa d'un document bàsic sobre l'ús del material informàtic (PCs, portàtils...) però no es troba estès a la resta de material d'informació. Ens decantarem en aquest cas per una maduresa inicial del control.

4.3.2 Classificació de la informació

4.3.2.1 Guies de classificació

La informació de vigilància de la salut es troba inventariada, ja sigui la documentació impresa (la qual es troba en armaris amb clau) com la que es gestiona per el programa *PREVENET.*

ET. El propietari "de facto" d'aquesta informació és el director mèdic. Recordem que aquesta informació requereix un nivell de seguretat alt segons la *LOPD.*

No existeix una classificació formal de la documentació en funció dels nivells de seguretat, es gestiona de manera intuïtiva. A nivell informàtic es separà la informació a nivell d'àrees tal i com s'ha exposat en la fase d'inventari d'actius.

Decidim classificar aquest control amb una maduresa reproduïble, ja que es basa en la experiència dels treballadors.

4.3.2.2 Marcat i tractament de la informació

La informació no es troba marcada i els treballadors no són conscients de quin tractament poden realitzar segons la seva classificació.

De fet, ens trobem en casos en els que s'està enviant informació per correu convencional, o no s'han aplicats uns mecanismes efectius per destruir la informació.

Evidentment, no es un comportament estès en tots els casos, per tant indicarem que la maduresa d'aquest control es troba en una fase inicial.

4.4 Seguretat en els recursos humans

En aquest domini ens trobem amb els aspectes formals que s'han de gestionar amb les persones que col·laboren en la nostra organització. La implicació del personal és bàsica per que la seguretat de la informació tingui èxit.

4.4.1 Abans de ser empleat

4.4.1.1 Inclusió de la seguretat en les responsabilitats i funcions laborals

En les relacions contractuals es marquen de manera especifica les funcions especifiques de treball però no es marquen les responsabilitats, ni les obligacions legals.

No es disposa d'una assessoria laboral per la realització d'aquests contractes.

4.4.1.2 Selecció i política de personal

La selecció del personal es realitza a les instal·lacions centrals amb una sala de reunions. No es realitza amb personal especialitzat i les contractacions es basen amb el currículum facilitat i amb una entrevista de treball. El nivell de maduresa d'aquest control és el inicial.

4.4.1.3 Acords de confidencialitat

Com s'ha exposat en anterioritat en altres controls no hi han acords de confidencialitat. En els casos del personal sanitari es basa en el codi deontològic.

Per tant, podem considerar que aquest control només es troba en un estat inicial de maduresa.

4.4.2 Durant la contractació

4.4.2.1 Responsabilitats de la gerència

La gerència no té estructurat com i quan ha d'informar als proveïdors, clients o empleats sobre els requeriments de seguretat. Es va realitzant de manera puntual sense planificació. Per tant, es tracta d'un control que es troba en una fase inicial.

4.4.2.2 Coneixement, educació i entrenament de la seguretat de la informació

No es realitza cap formació especifica als empleats sobre seguretat. La única informació que se'ls hi proporciona en alguns casos és les publicacions que realitza l'estat sobre la *LOPD*. Es tracta d'un control en fase inicial.

4.4.2.3 Procés disciplinari

No hi ha cap document que se'ls hi faciliti els empleats que indiqui sancions disciplinàries en cas d'incompliment de les normatives de seguretat. Per tant, es tracta d'un control inexistent.

4.4.3 Finalitzant o canviat de treball

4.4.3.1 Responsabilitats de finalització

No existeix cap acord de confidencialitat de la informació en els contractes que es realitzen a *PREVENCIO S.L.* en cap de les àrees de la empresa.

Especialment preocupant en l'àrea comercial que pot suposar una pèrdua de la cartera de clients, i en altres àrees que podria comprometre als clients en els defectes detectats en les mesures de prevenció establertes en cadascun dels clients.

Ens trobem en un control inexistent dins de la organització.

4.4.3.2 Retorn d'actius

En la finalització del contracte es consulta l'inventari d'actius per sol·licitar que es retorni el material associat.

El material se'l queda sempre la empresa, no realitzant cap esborrat de la informació que pogués disposar l'usuari en els dispositiu portàtil.

4.4.3.3 Retirada dels drets d'accés

Es facilita les claus del edifici que pugui disposar els usuaris, però no es realitza una baixa immediata ni planificada de les comptes que disposava l'usuari. En alguns casos ens trobem que companys de feina utilitzen la compte de correu per consultar la informació (inclús disposen de la contrasenya per accedir-hi. Es una pràctica habitual.

Per tant, al no ser un procés definit i que es segueixi totalment, considerem que és un control en una fase inicial.

4.5 Seguretat física i ambiental

4.5.1 Àrees segures

4.5.1.1 Perímetre de seguretat física

Les portes d'accés en les instal·lacions de la empresa són úniques. En la central existeix un sistema d'alarma i en la resta de delegacions l'accés és mitjançant un pany.

Un altre cas en les instal·lacions del client. A nivell general els empleats disposen de despatx amb pany, però el client en disposa d'una altra còpia.

Podem considerar, que per tractar-se d'una empresa principalment de serveis amb locals de dimensió reduïda, aquest control es troba en un estat de maduresa reproduïble però intuïtiu.

4.5.1.2 Controls físics d'entrades

L'entrada/sortida de material es troba moderadament controlada. En la central és necessari passar per la entrada en la qual es troba recepció en la qual s'identifica les persones que visiten el centre de treball.

La sortida de material per part dels empleats es controla mitjançant l'inventari d'actius. Si es requereix enviar algun paquet amb material es deixa a recepció per que gestioni amb els serveis de missatgeria la entrega i recepció del material.

Classificarem aquest control com reproduïble però intuïtiu.

4.5.1.3 Seguretat d'oficines, despatxos i recursos

Per les dimensions dels locals no es pot diferenciar els llocs on es realitzen els tractaments de la informació (en pràcticament totes les ubicacions es realitza aquest tipus de tractament).

La ubicació de la sala de servidors no es troba identificada.

Per les dimensions de l'empresa, indicarem que el nivell de seguretat és reproduïble però intuïtiu.

4.5.1.4 Protecció contra amenaces externes i ambientals

Totes les oficines de la entitat es troben en àrees urbanes i els treballadors desplaçats en àrees urbanes o industrials. En els diferents edificis existeix extintors, però no hi ha cap mecanisme per protegir-se contra inundacions o altre tipus de desastres.

No es realitza cap mesura especifica per salvaguardar els mecanismes de recuperació de dades (recordem que el *backup* dels diferents entorns es realitza dins d'un dels equips).

La sala de servidors es troba ubicada en la planta baixa, per tant no es troba suficientment protegida pels casos en els que es produeixin inundacions.

Aquest control es troba en un estat de maduresa inicial.

4.5.1.5 El treball en les àrees segures

No existeixen àrees segures dins dels edificis. Un cop entrat al edifici totes les portes són accessibles. Els despatxos dels directors, encara que tenen pany, es troben sempre oberts durant les hores de treball. La única informació que té una seguretat física addicional és la informació impresa que es troba en armaris amb clau. L'estat d'aquest control es troba en un estat inicial.

4.5.1.6 Accés públic, àrees de càrregues i descàrregues

Es tracta d'una empresa de servei. La única zona de càrrega i descàrrega és la pròpia recepció. Degut a que hi ha poc personal que hi tingui que accedir-hi, no presenta problemes de control. Tota entrada de material es registra. Per el volum d'accessos que es gestiona, podem considerar que aquest control disposa d'un procés definit.

4.5.2 Seguretat del equipament

4.5.2.1 Instal·lació i protecció d'equips

No existeixen molts riscos associats a l'activitat de negoci per les dades de les instal·lacions centrals.

Disposen d'equips d'aire condicionat en totes les habitacions. El despatx té un accés des de l'exterior com a planta baixa i es troba ben il·luminat. No existeix un sistema de detecció de fums. En cas d'incendi s'utilitzen els extintors.

La sala de servidors es troba ubicada en la planta baixa. Seria aconsellable que aquests equips es trobessin ubicats en la primera planta per evitar problemes associats a inundacions, ja siguin les produïdes externament, com les que produeixi per les instal·lacions del propi edifici. Aquest fet marcarà que considerarem que aquest control es troba en una maduresa inicial.

4.5.2.2 Subministrament elèctric

Els equips ubicats en la sala de servidors disposen d'un sistema d'alimentació ininterrompuda, que garanteix que amb un tall en el subministrament elèctric provoqui una aturada del sistema, minimitzant els danys que pugui produir aquesta aturada inesperada. Permet que els serveis es trobin disponibles per les delegacions i per els portàtils de la central que es connecten per wifi

Els PCs no disposen de cap sistema d'abastiment alternatiu, els portàtils disposen de la bateria com a mesura de protecció en cas de tall del subministrament. Podem considerar que aquest control es troba en una maduresa del 90 % (procés definit).

4.5.2.3 Seguretat del cablejat

Les comunicacions de les diferents delegacions va a través de la xarxa pública de comunicacions. El cablejat dels diferents equips es troba sota terra.

Com hem comentat, es tracta d'un edifici no molt gran, per tant no té tantes exigències a l'hora de planificar la seguretat del cablejat.

Val a dir que la xarxa wifi de la xarxa central té una seguretat bàsica que s'hauria de tenir en compte a l'hora d'adoptar mesures de seguretat.

Per tant, considerarem que aquest control es troba en una maduresa inicial pels problemes de seguretat detectats en la xarxa wifi

4.5.2.4 Manteniment dels equips

No s'està realitzant un manteniment dels equips. L'actitud de l'empresa per aquest tipus de control és passiva. Quan apareix els problemes és quan s'arreglen.

Les operatives de manteniment de la plataforma de servidor les realitza el tècnic contractat 2 hores a la setmana, el qual se li paguen les hores addicionals que tingui que realitzar per aquest manteniment.

Les incidències amb els PCs i portàtils les sol revisar el director comercial, i en cas d'avaria, contacta amb un servei tècnic (el que porta amb la garantia del producte o un addicional si es tracta d'un equip sense cap cobriment).

Especialment significatiu és el tema de la plataforma de servidors. Recordem que tots els *backups* s'emmagatzemen en el servidor de correu, per tant, ens podem trobar en un escenari en el que es puguin perdre totes les dades del correu (tant les de les bústies com les del *backup* associat).

En aquest aspecte considerarem que per la gravetat detectada en el incompliment d'aquest control la maduresa és inexistent.

4.5.2.5 Seguretat d'equips fora dels locals de la organització

Per el tipus de treball de la organització, la majoria dels equips es troben fora dels locals de la organització o es desplacen amb certa freqüència.

Per el treball amb equips portàtils l'autorització de la direcció és implícita (no té sentit autoritzar-ho cada vegada)

Manca una política accessible i coneguda per tot el personal de la organització que indiqui les pautes a seguir amb els equips fora de l'organització.

L'organització no disposa de cap assegurança que cobreixi en cas de pèrdua, robatori. La informació no es troba emmagatzemada en local, per tant no suposa un problema de confidencialitat sempre i quan es realitzin les mesures oportunes per el responsable del equip quan abandona momentàniament l'equip de treball (bloqueig del terminal, apagada...).

Respecte a la informació impresa associada als controls mèdics, el personal no deixa el material accessible per els usuaris, si ve es cert que certa informació s'envia a la central o els laboratoris mèdics mitjançant missatgeria. Considerem que aquest control es troba en un estat inicial.

4.5.2.6 Seguretat en la reutilització o eliminació dels equipaments

En la eliminació dels equips no es realitza cap mesura formal d'esborrat de la informació. S'entrega l'equip a personal que farà funcions que al antic propietari del equip. Fins ara el comportament de l'empresa era no dedicar temps en reinstal·lació dels terminals.

Aquesta manca de maduresa del control ha quedat minimitzada per que la informació més rellevant de l'empresa es troba emmagatzemada en els servidors centrals, i la informació que sol haver són en els equips dels tècnics de prevenció còpies de documents de formació a les empreses o esborranys sobre l'estat de compliment de la llei de prevenció de riscos laborals.

Podem considerar que ens troben en un estat inicial de maduresa del control.

4.5.2.7 Retirada de la propietat

Tots els equips amb una titularitat especifica, en cas de que es produeixi alguna avaria, passen per mans del director comercial. En cas de que el equip no es pugui reutilitzar, és el que gestiona la retirada i substitució del equip.

Els equips del personal que es dona de baixa de l'empresa sempre es retorna al director comercial, que és l'encarregat d'indicar-ho en el inventari d'actius.

En aquest cas ens trobem amb un control que té un procés definit.

4.6 Gestió de comunicacions i operacions

4.6.1 Procediments operacionals i responsabilitats

4.6.1.1 Documentació de procediments operatius

Existeix una absència molt gran d'aquest tipus de documentació. Els procediments realitzats per cadascun dels usuaris de la organització es basa en la seva experiència.

Els tècnics de prevenció de la central solen utilitzar com a referència per avaluar nous casos de prevenció o per la formació a empreses els casos utilitzats amb anterioritat, sense que hi hagi una plantilla definida.

Els procediments de seguretat que es realitzen els porta a terme sempre la mateixa persona (per exemple, els processos de *backup* els realitza només el director comercial, i en cas de problemes té l'ajuda del tècnic informàtic).

Hi ha consciència per part de la direcció que s'ha de canviar aquesta manca de documentació i podem observar que en alguns casos s'utilitza com a procediment estudiar els casos realitzats en anterioritat, per tant qualificarem que la maduresa del control es troba en un estat inicial.

4.6.1.2 Gestió de canvis

Hi ha una mancança de procediments definits, per tant la gestió de canvis que pot fer sobre aquests procediments és nul·la. És basa en la experiència del personal en realitzar aquestes modificacions sobre la seva manera de procedir. Per tant, classificarem aquest control com inexistent.

4.6.1.3 Segregació de tasques

La segregació de les tasques depèn del tipus d'activitat. Les merament tècniques dels serveis de vigilància de la salut i de prevenció es troben segregades, ja que cada persona realitza les activitats associades segons el seu criteri.

Les tasques financeres existeix un equip coordinat per el director financer i el personal que té disponible per realitzar les tasques associades amb les relacions contractuals amb els clients i proveïdors.

Els comercials gestionen la seva cartera de clients. Això té una doble lectura, ja que d'un comercial no depengui la seva relació amb la totalitat dels clients, si que ens trobem que aquesta informació no és compartida.

Dels diferents directors d'àrea depèn les tasques més executives. Aquesta funcions són de difícil segregació.

De una de les infermeres de la central depèn la coordinació de les diferents revisions amb les empreses i els problemes que puguin sorgir. En absència d'aquesta infermera aquestes atribucions les ha d'assumir el director de vigilància de la salut i les administratives que disposa aquest àrea. El coneixement sobre la coordinació i les problemàtiques de les empreses es troba habitualment en possessió d'aquesta infermera.

A nivell de seguretat i informàtic les dues figures que hi han són el director comercial, que és el que assumeix la configuració de nous equips i la coordinació dels problemes que puguin aparèixer en el manteniment del equip. Sense aquesta figura, ningú disposa del coneixement associat per configurar els equips, realitzar *backups*, i s'hauria de contactar amb els proveïdors per realitzar la instal·lació dels equips. Respecte el tècnic informàtic és la persona que disposa dels coneixements tècnics per poder realitzar les actuacions en cas d'incidència en els servidors. Ens podem trobar amb una aturada del servei que no es podrà solucionar fins que el tècnic disposi de temps per poder realitzar aquestes accions.

Per les mancances detectades a nivell de tasques d'informàtica i seguretat, considerarem que aquest control es troba en un estat inicial.

4.6.1.4 Separació dels recursos per desenvolupament i per producció

No existeix un entorn de desenvolupament. Tot els software que disposa l'empresa és un software tancat. A part de la realització d'alguna "macro" en *Excel*, no hi ha cap desenvolupament a mida.

Considerarem que aquest control es troba en un estat inexistent, però actualment no és un control en el que sigui necessari realitzar accions per augmentar la maduresa del control.

4.6.2 Gestió de serveis externs

4.6.2.1 Servei d'entrega

La informació associada a la prevenció es facilitat directament al client en una reunió que es realitza amb el client.

Els resultats obtinguts de les proves mèdiques generalment s'entrega al departament de recursos

humans de la empresa contractant, la qual és la encarregada de vetllar per la confidencialitat de les dades del treballador.

Les diferents proves mèdiques, analítiques o resultats obtinguts per serveis de vigilància de la salut subcontractats s'envien generalment a traves de missatgeria.

Les consultes dels resultats del laboratori amb el que es treballa principalment es realitzen a traves d'una aplicació *Web* que disposen a la qual disposem d'un usuari/password. L'accés es realitza a traves d'una connexió *SSL*. El laboratori es compromet en donar-nos els resultats en un període màxim de tres dies

Respecte als equips informàtics no s'estableix cap acord per la reposició dels equips, més enllà del que ens proporciona directament el proveïdor en la seva relació contractual.

Es detecten greus problemes de comunicació en l'enviament de la informació de vigilància de la salut, encara que hi han altres comunicacions de l'empresa que disposen d'una maduresa alta.

En global, considerarem que aquest control es troba en una fase inicial.

4.6.2.2 Monitorització i revisió dels serveis externs

No es realitza cap monitorització especifica sobre el control dels serveis. Les accions es realitzen en base a una reclamació del usuari sobre el servei que oferim. En aquestes casos es revisen els compromisos contractuals que disposem per demanar la responsabilitat al proveïdor.

La monitorització del servei informàtic es realitza un cop per setmana a traves del tècnic contractat per aquesta funció.

Per tant, ens trobem en un control inicial en la nostra organització.

4.6.2.3 Gestionant canvis per els serveis externs

Es troba acordat amb el tècnic informàtic que la activitat que realitza sobre els nostres sistemes en horari laboral no ha d'afectar al servei (correu, *PREVENET...*), encara que les actuacions que realitza són amb el criteri que ell decideixi.

Les accions que s'han de realitzar amb afectació es realitzen fora del horari laboral amb la compensació específica pactada.

Es trobem amb un control en un estat inicial ja que el control realitzat és molt baix però es realitza amb la intenció de no afectar a la disponibilitat del servei per part dels nostres treballadors.

4.6.3 Planificació i acceptació dels sistemes

4.6.3.1 Planificació de la capacitat

Existeix una absència total en la planificació de la capacitat. Es realitza generalment la instal·lació de nous serveis sobre el servidor existent i no es controla el creixement del nombre d'usuaris. Ens ha fet constar *PREVENCIO S.L* que es disposa d'un servidor de correu ja que es van produir problemes de rendiment en el servidor en el qual allotjava totes les aplicacions que van fer penalitzar tots els serveis (a part dels problemes d'accés, es van retornar els correus als clients per

que no es van arribar a entregar).

L'empresa ha optat en el passat per un model reactiu. Només s'han fet accions qual el problema que es produïa era inassumible per accedir a la informació.

En aquest cas ens trobem amb un control inexistent en la organització.

4.6.3.2 Acceptació del sistema

No es realitza cap planificació per la introducció de nous requisits en el nostre sistema, que requereixin una revisió sobre els equips.

No hi ha una planificació en l'actualització del *software*. De fet, s'utilitza el *software* base que venen en els equips, i només s'inclou l'antivirus i la part client del *software PREVENET*.

Aquest control també és inexistent en el nostre sistema.

4.6.4 Protecció contra el software maliciós i codi mòbil

4.6.4.1 Mesures i controls contra software maliciós

La organització és conscient de que s'ha de protegir els equips de *software* maliciós, i de fet, es preocupa d'instal·lar l'antivirus en tots els equips de la organització, on es planifica un escaneig periòdic del equip. No existeix cap procediment en el cas de que es detecti un virus i s'actua sobre la marxa.

Però no es realitzen mesures per controlar la instal·lació de *software* maliciós. Molts dels usuaris de la organització treballen amb els equips amb credencials d'administrador local, permetent la possibilitat d'instal·lar-se *software* d'origen desconegut.

El correu electrònic no disposa de cap sistema de detecció de virus associat. L'us del correu electrònic es basa en el coneixement propi que disposi el personal.

No existeix una política definida per la organització per indicar el bon ús dels equips de la organització i en la que es prohibeixi la utilització de *software* no autoritzat.

Ens trobem en una fase inicial del control.

4.6.4.2 Mesures i controls contra codi mòbil

Tal i com hem comentat en l'apartat anterior, existeix un document bàsic per indicar el bon ús dels equips.

De totes formes no es troba detallat les implicacions que té les operacions realitzades, les quals, poden provocara la execució de codi maliciós quan navega per *Internet* a llocs que no pertanyen al àmbit professional.

No es realitza mesures de prevenció sobre aquest tipus de codi, per tant ens trobem amb un control inicial en la nostra organització.

4.6.5 Còpies de seguretat

4.6.5.1 Recuperació de la informació

Les còpies de *backup* es realitzen amb una freqüència setmanal per part del director comercial. Es realitza de tota la plataforma servidora. La informació s'acaba emmagatzemant en el servidor de correu emmagatzemant les dues últimes còpies.

No es realitzen proves del procediment de restauració. De fet, el director comercial no es troba capacitat per realitzar una restauració del correu o del *SQL*. Realitza aquest *backup* per si es produeix un desastre poder facilitar la informació al tècnic

La freqüència de *backup,* el volum de dades emmagatzemades i la ubicació del *backup* no ens permet cobrir completament les necessitats associades a aquest control. Per tant, considerarem que aquest control es troba en una fase inicial.

4.6.6 Gestió de la seguretat de la xarxa

4.6.6.1 Controls de xarxa

L'accés remot es fa principalment des de els portàtils ubicats en les diferents delegacions i els ubicats en les oficines del client i els terminals *Blackberry.*

No es fa cap seguiment del tràfic extern de la organització. Les revisions que s'han pogut realitzar han sigut a posteriori per un incident de disponibilitat del servei.

Aquest control actualment podríem considerar que és pràcticament inexistent.

4.6.6.2 Seguretat en els serveis de xarxa

L'accés remot es fa principalment des de els portàtils ubicats en les diferents delegacions i els ubicats en les oficines del client.

Des de aquest equips s'accedeix al correu i al programa *PREVENET.* No existeix cap configuració *VPN* per accedir a la informació de la empresa. La seguretat del correu es realitza molt ocasionalment a traves de mecanismes d'encriptació i autentificació. En el cas del software associat a la vigilància de la salut i prevenció disposa d'un mecanisme propi de encriptació de la informació que garanteix la seva comunicació a traves de xarxes públiques.

No es troba configurat i instal·lat cap dispositiu que controli l'accés des de l'exterior (detector d'intrusos firewalls...)

L'accés a la informació del laboratori es realitza mitjançant un usuari/password i un canal *SSL* que es gestiona des de el propi laboratori.

Per els terminals *Blackberries* s'utilitza la configuració per defecte del servei.

Aquest control actualment podríem considerar que és troba en un estat inicial.

4.6.7 Utilització dels medis d'informació

A nivell digital no consten en l'empresa la utilització de medis removibles. Els que s'utilitzen són a nivell particular els empleats, per preparar o presentar cursos de formació.

No existeixen ni a nivell de *backup*, ja que com s'ha exposat en anterioritat, aquestes còpies de seguretat s'emmagatzemen en un dels servidors.

En format imprès existeix diversa documentació. Destaquem principalment les proves mèdiques les quals s'han de conservar durant un temps i en posterioritat s'han de destruir.

4.6.7.1 Gestió de medis removibles

No es disposa de cap procediment per la gestió d'aquest tipus de medi, a excepció dels de vigilància de la salut que es procedeix a la seva destrucció passat el temps legal de conservació de la informació.

No es realitza cap control sobre el material que puguin gestionar els empleats amb els seus dispositius d'emmagatzematge personal.

La informació impresa es guarda en armaris en clau per complir els requisits de protecció que marca la LOPD.

Considerarem que aquest control es troba en una fase inicial per que la gestió no es troba estesa a tota la informació i només hi ha un conjunt limitat de procediments

4.6.7.2 Eliminació de medis

El *backup* es conserven només dues còpies, principalment per un tema d'ocupació del disc. A nivell de documentació impresa es disposa de màquina per la destrucció d'aquest material.

Sobre les còpies que realitza el personal no existeix cap control, per tant, no es pot afirmar que es realitzi una destrucció del material.

Ens trobem que aquests control d'eliminació de medis només es realitza en alguns components del a informació, per tant considerarem que aquest control es troba en una fase inicial.

4.6.7.3 Procediment de manipulació de la informació

No existeix cap procediment definit de manipulació de la informació. No es troba classificada la informació.

Si ve es cert que tant la informació digital com la impresa es troba diferenciat l'accés per les diferents àrees de la empresa.

Considerarem que aquest control es troba en un estat inicial ja que amb la restricció actual ja es pot considerar que l'empresa té una certa consciència en determinar un control sobre l'accés a la informació.

4.6.7.4 Seguretat de la documentació de sistemes

La documentació dels sistemes es bastant reduïda. Aquesta informació només es troba disponible

per el director comercial i el tècnic informàtic. Podem considerar que aquest control es troba en una maduresa intuïtiva ja que es basa en una bona pràctica individual.

4.6.8 Intercanvi d'informació

En aquest objectiu analitzarem com es realitza l'intercanvi d'informació entre les diferents seus de la nostre organització cap a la central, de les empreses externes subcontractades la informació que s'envia als laboratoris clínics i les dades de vigilància de la salut que s'envien a cadascuna de les empreses.

4.6.8.1 Polítiques i procediments per el intercanvi d'informació i software

PREVENCIO S.L. no disposa de cap política sobre la gestió d'aquesta informació i en general no disposa de procediment per el enviament de la informació.

El personal no disposa de cap formació que li permeti conèixer les alternatives que disposa per realitzar l'intercanvi d'informació.

L'únic procediment per l'intercanvi d'informació és l'enviament de les mostres als laboratoris, les quals s'envien associades amb un codi de barres. El laboratori disposa de la relació del codi de barres amb la persona associada, les característiques de les proves a realitzar i altres dades com l'edat, el pes del pacient, antecedents.

En l'enviament que realitza *PREVENCIO S.L* sobre les dades de les revisions mèdiques, s'encarrega d'enviar la informació a recursos humans en sobres tancats, indicant que la informació només haurà de ser accessible per la persona que ha realitzat la revisió.

Considerarem que aquest control es troba en un estat inicial a nivell global, però en molts dels escenaris de treball el control és inexistent.

4.6.8.2 Acords d'intercanvi

Existeix un acord amb el laboratori clínic per que l'enviament de la informació associada als anàlisis clínics estigui dissociada (no identificable el subjecte associat) que s'acaba materialitzant en el procediment utilitzat per l'enviament de les anàlisis clíniques i la obtenció de les dades sigui mitjançant un canal segur.

En canvi, aquest cel no es troba en l'enviament dels informes mèdics, els quals s'està realitzant mitjançant missatgeria.

Per tant considerarem que aquest control es troba en un estat inicial.

4.6.8.3 Medis físics en trànsit

Recordem que l'enviament es realitza mitjançant missatgeria. No s'estan prenent mesures de seguretat per l'enviament de la informació a excepció de les anàlisis clíniques, les quals es garanteix la seguretat mitjançant la dissociació de les dades.

Per tant a nivell general podem considerar que aquest control és inexistent per la majoria de la informació transmesa.

4.6.8.4 Seguretat en la missatgeria electrònica

La comunicació mitjançant correu electrònic es realitza normalment sense utilitzar firma digital. Només s'utilitza enviament amb firma digital en aquells casos en el que el client ho requereix i ens ha facilitat un certificat dels que gestiona la seva entitat.

La majoria del personal no realitza l'enviament de la informació xifrada i no hi ha una conscienciació de que aquesta informació pot arribar a ser accessible per tercers durant el trànsit de la informació. No s'utilitzen aquestes eines quan s'envia, per exemple, pressupostos als clients.

Aquest control es troba en una fase inicial de maduresa.

4.6.8.5 Sistemes d'Informació de Negocis

No existeix cap procediment definit per aquest control. La informació de dades de les diferents àrees es troba restringida per el personal del propi departament.

Qualificarem aquest control en una maduresa reproduïble, però intuïtiva.

4.6.9 Serveis de comerç electrònic

4.6.9.1 Comerç electrònic

No s'utilitza cap mecanisme de comerç electrònic amb els clients.

Amb els proveïdors es realitza algunes operacions, com la compra d'equips, serveis de missatgeria, viatges, hotels.... Sempre es treballa amb proveïdors reconeguts.

No es realitza cap control específic. L'àrea que ha de fer aquestes contractacions ho gestiona com si es tractés d'una comanda impresa. Guarda una còpia impresa de les sol·licituds realitzades.

En el seu àmbit d'utilització considerarem que aquest control es troba en una maduresa reproduïble, però intuïtiva.

4.6.9.2 Transacció en línia

PREVENCIO S.L realitza únicament transaccions electròniques a través del seu banc, el qual proporciona els mecanismes necessaris per minimitzar l'exposició de la informació per utilitzar aquest canal.

Considerarem que aquest control es troba, en base a la seva utilització, en una fase reproduïble, però intuïtiva.

4.6.9.3 Informació pública disponible

No s'han realitzat mesures sobre el servidor *Web PREVENET.* A nivell de seguretat només s'estan realitzant les mesures que disposa el propi producte (d'encriptació de les dades i d'autentificació), però no es realitzen mesures sobre el servidor *Web* (*Internet Information Services*) i sobre el servidor *SQL* el qual es troba allotjat en el mateix equip.

Per tant, aquest control es troba només en un estat inicial.

4.6.10 Monitorització

4.6.10.1 Registre de la auditoria

Els registre que es realitzen en els diferents sistemes són els que venen per defecte. No s'ha realitzat cap configuració especifica.

No hi ha hagut cap seguiment d'aquesta informació per la organització. Per tant podem considerar que aquest control és inexistent.

4.6.10.2 Monitoritzant el us del sistema

No hi ha cap procediment definit. No es realitza cap revisió a no ser que es produeixi un incident i hagi de ser revisat per el tècnic informàtic.

Per tant, aquest control també és inexistent.

4.6.10.3 Protecció de la informació de registre

La protecció dels registres estan protegides en funció del accessos al servei. L'accés als servidors es troba limitada al director comercial i al tècnic informàtic.

No s'ha establert cap política de conservació dels registres. Si els registres comporten un problema d'ocupació, s'eliminen.

Aquests controls només es troben en una fase inicial.

4.6.10.4 Registre d'administradors i operadors

No hi ha cap control sobre els registres de la informació i en concret sobre el registre dels administradors i operadors. Per tant, aquest control també és inexistent.

4.6.10.5 Registre de la avaria

No hi ha un registre formal d'avaries. Aquest control és inexistent.

4.6.10.6 Sincronització del rellotge

Els equips disposen la sincronització per defecte del sistema operatiu. Tots els equips es troben en la mateixa zona horària.
Per tant, encara que de forma accidental, aquest control es troba en una maduresa reproduïble, però intuïtiva.

4.7 Control d'accés

4.7.1 Requisits de negoci per el control d'accés

4.7.1.1 Política de control d'accés

No existeix una política formal de control d'accés. A nivell global cadascun dels empleats coneix quina és la informació sobre la que disposa accés, però no coneixen quin pot ser l'impacte per

l'accés a la seva informació.

Considerarem que aquest control es troba en un estat inicial.

4.7.2 Gestió d'accés d'usuari

4.7.2.1 Registre d'usuaris

No existeix cap procediment definit. L'alta dels usuaris la gestiona el director comercial que proporciona un identificador únic per usuari. No es proporciona per escrit al personal que es dona d'alta al sistema cap informació sobre els seu drets d'accés.

La eliminació dels usuaris que abandone l'organització no es realitza immediatament.

Per tant, ens trobem en un estat inicial del control.

4.7.2.2 Gestió de privilegis

No existeix un procediment formal d'accessos. La gestió dels privilegis la realitza el director comercial, el qual aplica es seu criteri personal per donar aquest tipus d'accessos. Els privilegis es troben segmentats principalment per dos criteris: personal que treballa en les instal·lacions centrals i àrea a la que pertany l'usuari.

Per tant, podem considerar que es un control reproduïble però intuïtiu.

4.7.2.3 Gestió de contrasenyes d'usuaris

No es troba definit cap política associada amb la gestió de contrasenyes. Els usuaris disposen de la contrasenya inicial del sistema i no es troben obligats a canviar-la en el primer ús.

Les contrasenyes no disposen de caducitat. És pràctica habitual compartir la contrasenya entre companys de feina.

La contrasenya és facilitada per el director comercial de forma presencial amb l'usuari final.

Podem considerar que aquest control actualment és inexistent.

4.7.2.4 Revisió dels drets d'accés dels usuaris

La revisió del control no es produeix. Els usuaris disposen dels mateixos accessos durant la seva etapa professional a *PREVENCIO S.L.* Només es revisa els accessos quan apareixen noves necessitats dels sistemes informàtics (p.e utilització d'un *software* que requerís unes credencials específiques.

Per tant, ens tornem a trobar amb un control inexistent.

4.7.3 Responsabilitat dels usuaris

4.7.3.1 Us de contrasenyes

No existeix cap procediment que sigui públic sobre l'us de les contrasenyes. La gestió responsable

de les contrasenyes es basa en la experiència personal de cadascun dels usuaris.

Tal i com hem vist en varis dels controls d'aquest domini, no existeix en general una cultura empresarial de cel sobre l'us i manteniment de les contrasenyes.

Per tant, considerarem que aquest control també és inexistent.

4.7.3.2 Equips informàtics d'usuaris desatesos

No existeix cap procediment formal que sigui d'us comú per tots els usuaris. Només als usuaris que disposen de portàtils se'ls comunica verbalment que tinguin prudència a l'hora d'abandonar temporalment el lloc de treball per bloquejar la sessió i per no deixar a la vista informes que puguin ser de caràcter sensible.

La resta d'usuaris només actuen en funció del seva experiència personal.

Aquest control es troba en una fase inicial, ja que hi ha certa conscienciació quan es treballa en els locals que no són els de la organització

4.7.3.3 Polítiques de pantalles i escriptoris nets

No existeix cap normativa interna a nivell de seguretat sobre pantalles i escriptoris nets, però si sobre en el lloc de treball i d'estalvi energètic. La documentació impresa es troba classificada en el seu armari corresponent, i els equips s'apaguen un cop ha finalitzat la jornada laboral.

Les mancances a nivell de equip informàtic ja s'ha fet esment en anterioritat, i per tant considerarem que aquest control es troba en una fase inicial.

4.7.4 Control d'accés en xarxa

4.7.4.1 Política d'us dels serveis de xarxa

No existeix una política d'accés a la xarxa. Els usuaris disposen d'accés a Internet. L'empresa fa saber al personal que només ha de fer ús dels equips per temes personals de manera excepcional.

A nivell intern no s'ha considerat establir cap tipus de política ja que els privilegis establerts la empresa considera que són els apropiats per les funcions que realitza cadascun dels empleats.

Considerarem que aquest control es troba en una fase inicial, ja que falta una certa conscienciació sobre els perills que pot suposar per la seguretat de la informació uns accessos no controlats.

4.7.4.2 Autentificació d'usuari per connexions externes

La seguretat de l'accés des de xarxes externes es basa en la seguretat que proporciona el programa *PREVENET*, però per l'accés al correu no s'esta realitzant cap mesura.

Per tant, aquest control només es troba en una fase inicial.

4.7.4.3 Identificació d'equips en la xarxa

Aquest control no s'està realitzant. El nombre d'equips que treballen des de el client és important.

No es disposa dels coneixements suficients per autoritzar els accessos puntuals. Només el tècnic informàtic es troba capacitat per realitzar aquest tipus de gestió.

Aquest control actualment és inexistent.

4.7.4.4 Diagnòstic remot i configuració de protecció de ports

No es fa cap control sobre aquest tipus de port. El control actualment és inexistent.

4.7.4.5 Segregació en xarxa

A nivell de *router* només es permeten les connexions iniciades des de l'exterior cap al servidor de prevenció i el de correu.

La segmentació és molt bàsica i exposa a tota la informació digital que té la entitat.

Per tant, considerarem que aquest control és troba en una maduresa inicial.

4.7.4.6 Control de connexió a la xarxa

Es troba configurat el *router* per que les sessions que s'inicien des de l'exterior puguin accedir als ports *HTTP/S* del servidor de prevenció i els ports associats per poder accedir al correu.

Aquest control es troba en una fase inicial.

4.7.4.7 Control d'enrutament en la xarxa

No s'ha establert cap mecanisme de control de connexió de la xarxa. La restricció d'accessos es troba definida a nivell de recursos de xarxa.

La única restricció que li aplicaria a una persona que treballi a la central des de qualsevol punt del exterior és la limitació que hi ha actualment a nivell de ports.

Per tant, aquest control és inexistent.

4.7.5 Control d'accés al sistema operatiu

4.7.5.1 Procediment de connexió de terminals

S'utilitza la opció per defecte del propi sistema operatiu. Es troben configurades les comptes dels usuaris per que es bloquegi la contrasenya al tercer error consecutiu. Recordem que no es fa cap revisió dels events, per tant, tampoc s'està realitzant cap personalització associada als accessos

Aquest control es troba en un estat de maduresa inicial.

4.7.5.2 Identificació i autentificació del usuari

Tots els usuaris disposen del seu identificador únic personal, encara que de manera informal hi

hagin usuaris que comparteixin usuaris (per accedir per exemple al correu si l'altre persona no es troba a la oficina.

No s'ha personalitzat la configuració dels terminals per que registrin la seva configuració personal. Tots venen amb el valor de fàbrica.

Ens trobem, per tant en un control reproduïble, però intuïtiu.

4.7.5.3 Sistema de gestió de contrasenyes

No es fa cap gestió de contrasenyes especial ni per les credencials associades a un treballador ni per les comptes administratives que es creïn per el funcionament de les aplicacions instal·lades.

Tal i com s'ha mencionat en anterioritat, només es realitza la gestió en l'alta inicial, però el sistema no obliga a fer el canvi i no hi ha polítiques restrictives sobre la qualitat de la contrasenya.

Per tant, aquest control és inexistent.

4.7.5.4 Utilització de les facilitats del sistema

No es fa cap tipus de control sobre aquestes funcionalitats disponibles. Recordem que la configuració dels terminals son les que venen de fàbrica.

Per tant, el control és inexistent.

4.7.5.5 Desconnexió automàtica de sessions

A nivell de sistema operatiu, no es fa cap tipus de control sobre aquestes funcionalitats disponibles. Recordem que la configuració dels terminals son les que venen de fàbrica.

A nivell del servidor *Web* es va configurar la limitació de sessió a 30 minuts.

Per tant, el control és pràcticament inexistent.

4.7.5.6 Limitació del temps de connexió

No es fa cap tipus de control addicional que les mencionades en el control de desconnexió automàtica de sessió. Per tant, el control és inexistent.

4.7.6 Control d'accés a les aplicacions

4.7.6.1 Restricció d'accés a la informació

No s'utilitzen mecanismes especials per controlar els accessos a aplicacions. Els nivells d'accessos a les aplicacions es troba generalment limitat a nivell de sistema operatiu, a nivell del *software* instal·lat en els equips (hi han equips que disposen instal·lat el *software* de *PREVENET* i altres equips el *software* de comptabilitat).

Només es proporciona les credencials de *PREVENET* als usuaris que n'han de fer ús.

Podem considerar que aquest control es troba en una maduresa reproduïble, però intuïtiva.

4.7.6.2 Aïllament de sistemes sensibles

No s'està practicant l'aïllament de dades sensibles. A nivell de servidors queda clarament exposat, ja que només s'han separat els serveis per un tema de disponibilitat. No s'ha separat el servei de *SQL* i el servei *Web* tot i que es troba dins de les recomanacions del proveïdor.

El controlador de domini i els recursos interns de la organització es troben en el mateix servidor que el servei *Web* accessible des de l'exterior.

Per tant, aquest control el considerarem com inexistent.

4.7.7 Informàtica mòbil i teletreball

4.7.7.1 Informàtica mòbil i comunicacions

No existeix cap procediment formal sobre l'ús dels equips fora de la organització. Al personal que treballa en les oficines del client se'ls informa de que vagin amb cura amb el material quan abandonen temporalment el lloc de treball.

Com s'ha mencionat anteriorment no es realitza cap assegurança i tampoc es realitzen *backups,* ja que la informació que han de fer ús es troba en els servidors.

Considerarem que aquest control és pràcticament inexistent.

4.7.7.2 Teletreball

No s'ha considerat la opció de realitzar teletreball en l'empresa. Tot accés des de l'exterior es realitza amb els portàtils de la empresa.

Per tant, aquest control és inexistent.

4.8 Adquisició, desenvolupament i manteniment de Sistemes d'Informació

4.8.1 Requisits de seguretat en els sistemes d'informació

4.8.1.1 Anàlisi i especificacions dels requisits de seguretat

No es realitza aquest anàlisi en l'adquisició de *software*. Control inexistent dins de l'organització. Seria convenient que s'analitzés el programari tenint en compte les característiques de la nostra organització, especialment la connexió que es realitza des de l'exterior, la qual utilitza xarxes públiques o de tercers i es deshabilités aquelles característiques que puguin comprometre la seguretat.

4.8.2 Seguretat de les aplicacions del sistema

Conjunt de controls que s'utilitzen per evitar la pèrdua, modificació o mal us de les dades per part dels usuaris.

Actualment dins de la pròpia organització no es realitza cap desenvolupament a mida, per tant es basarà més en un control sobre el comportament de les aplicacions, ja sigui a nivell d'usuari, amb

els controls que disposin les eines adquirides, o amb auditories del sistema. Aquests controls s'haurien de sol·licitar amb els proveïdors per mirar d'implantar-los en el nostre sistema.

Hem de tenir en compte que *PREVENCIO S.L* no disposa de personal qualificat per avaluar aquests controls abans de l'adquisició del *software*, i encara que ho tingués possiblement no podria dedicar el temps suficient en realitzar una validació exhaustiva.

Per la detecció de les diferents anomalies caldrà una col·laboració del personal de la organització d'avisar de les diferents anomalies detectades per tal de poder fer un anàlisis a posteriori.

4.8.2.1 Validació de les dades d'entrada

No es disposa d'aquest tipus de control ja que el *software* que utilitza *PREVENCIO S.L* son paquets tancats. Tampoc disposa de personal especialitzat que pogués realitzar aquesta funció. Els empleats no estan reportant de manera sistemàtica els errors que puguin detectar sobre aquest tipus d'operacions. S'haurà de revisar dins les auditories periòdiques que es planificaran periòdicament.

4.8.2.2 Control del procés intern

En l'actualitat no es realitza cap tipus de control. S'haurà de revisar de configurar el detall que deixen les aplicacions per posteriors revisions. S'haurà de revisar dins les auditories periòdiques que es planificaran periòdicament.

4.8.2.3 Integritat dels missatges

No es realitza aquest tipus de control. S'hauria de revisar si les eines adquirides disposen de processos de verificació integrats de les dades del sistema que ens permetin detectar corrupció de les dades. S'haurien de realitzar comprovacions periòdiques, que ens permetés una detectar-les i es pogués restaurar el sistema amb algunes de les còpies de *backup* disponibles.

4.8.2.4 Validació de les dades de sortida

No es disposa d'aquest tipus de control ja que el *software* que utilitza *PREVENCIO S.L* son paquets tancats. Tampoc disposa de personal especialitzat que pogués realitzar aquesta funció. Els empleats no estan reportant de manera sistemàtica els errors que puguin detectar sobre aquest tipus d'operacions. S'haurà de revisar dins les auditories periòdiques que es planificaran periòdicament.

4.8.3 Controls criptogràfics

Dins de *PREVENCIO S.L* no s'estan adoptant mesures per incorporar controls criptogràfics que permetin principalment assegurar la confidencialitat de la informació quan es treballa fora de la seu central.

Només s'estan utilitzant les que venen per defecte en el sistema, com és la comunicació del *software PREVENET* i les que s'han utilitzat per enviar correus encriptats a petició del client.

4.8.3.1 Política d'ús dels controls criptogràfics

Absència de qualsevol política associada a aquest control. El personal no es troba informat de que

han de realitzar cap mesura per incorporar controls criptogràfics per transmetre la informació, especialment quan treballen fora de la seu central.

4.8.3.2 Gestió de claus

No hi ha establert cap sistema per disposar de claus ni realitzar una distribució als diferents terminals, especialment als portàtils que disposa la organització.

4.8.4 Seguretat en els arxius del sistema

4.8.4.1 Control del software en producció

No es disposa de cap control sobre la instal·lació de *software* en producció. Molts dels usuaris disposen d'accés d'administrador en els seus equips i no s'està implementada cap procés centralitzat que limiti la instal·lació de *software* addicional, ni es realitza una revisió periòdica sobre el *software* instal·lat en els diferents equips.

No es disposa d'un entorn de proves, per tant, els proveïdors i tècnics realitzen els seus canvis directament a producció.

4.8.4.2 Protecció de les dades de prova del sistema

No existeix un entorn de prova per avaluar el comportament dels canvis quan es realitza un canvi a producció. No es disposa de suficient personal tècnic que pugui avaluar aquests canvis. Per tant no s'utilitzen dades reals sobre entorns de proves que puguin comprometre la seguretat de les dades.

Per tant, es tracta d'un control inexistent.

4.8.4.3 Control d'accés als codis de programes font

No existeixen desenvolupaments a mida, per tant no hi ha hagut la necessitat de controlar l'accés d'aquest tipus d'informació per part de tercers.

Es marca com a inexistent aquest tipus de control, ja que si surt la necessitat de desenvolupar programes propis de l'empresa, no es realitzaria cap control.

4.8.5 Seguretat en els processos de desenvolupament i suports

4.8.5.1 Procediments de control de canvis

Els canvis que es realitzen sobre els sistemes aprovats per la organització són els que realitzen el director comercial i el tècnic informàtic.

Els canvis es realitzen amb la aprovació directa del director comercial. Els canvis que el tècnic informàtic considera que tenen un impacte sobre la plataforma servidora es realitzen fora del horari laboral.

No es detalla el procediment que es realitzarà a l'hora de realitzar el canvi. Un cop realitzat, s'informa al director comercial per que gestioni la validació per un usuari que utilitza l'aplicació.

No existeix un procediment formal sobre la gestió de canvis. No es disposa d'un entorn de proves per validar les operacions a realitzar.

Ens trobem en una fase inicial d'aquest control.

4.8.5.2 Revisió tècnica dels canvis en el sistema operatiu

No es realitza cap revisió. El parc tecnològic és molt heterogeni i es el que ve de fàbrica quan es contracta el producte. Els equips es troben configurats amb actualització automàtica del sistema operatiu.

Les úniques proves realitzades són les que es fan en la configuració inicial del equip per que s'integri dins el domini de la organització i s'instal·li el *software* addicional.

Les revisions es realitzen a posteriori si es detecta una anomalia del sistema. Aquest revisions les realitza el tècnic informàtic.

El control es pràcticament inexistent.

4.8.5.3 Restriccions en els canvis als paquets de software

No es disposa de software desenvolupat en la organització. Els canvis en els paquets de *software* es realitzen de manera ocasional. Únicament s'apliquen millores sobre el paquet *PREVENET* quan aporta una nova funcionalitat que representa un benefici per el treball de la organització. Els canvis es validen en els equips del director de vigilància de la salut i el director de prevenció.

Aquest control es troba en un estat inicial, ja que actualment es segueix un criteri restrictiu encara que no es realitzi un control general de tot el *software* de la organització.

4.8.5.4 Fuga d'informació

No es realitza cap monitorització que pugui estar sortint de la organització. No es controla les Ips utilitzades per rebre la informació.

La maduresa d'aquest control actualment és inexistent.

4.8.5.5 Desenvolupament extern del software

Actualment no es realitza cap desenvolupament extern de *software*. Per tant aquest control és inexistent, ja que no ha aparegut cap necessitat d'aplicar-ho.

4.8.6 Gestió de les vulnerabilitats tècniques

4.8.6.1 Control de les vulnerabilitats tècniques

No s'està revisant amb una periodicitat les vulnerabilitats que poden tenir els nostres sistemes. En el tractament d'aquest es realitza de forma reactiva, ja sigui per incidència o per que el proveïdor ens notifiqui aquest tipus de vulnerabilitat.

Actualment no es realitza cap tipus d'auditoria interna (no es disposa de personal per fer-ho) ni externa que permeti detectar aquestes vulnerabilitats a través d'aquest sistema. En la col·laboració

que realitzarà *AUDITORIA S.L.* es planificaran aquest tipus d'auditoria.

4.9 Gestió d'incidents

4.9.1 Comunicació dels incidents i debilitats de seguretat. Reporting de debilitats de seguretat

4.9.1.1 Reporting dels events en la seguretat de la informació

No existeix una eina per reportar els incidents. Quan apareix un incident que es reprodueix de forma repetitiva, es sòl consultar amb un altre company, al tècnic informàtic quan es troba al centre, i si es tracta d'un incident de molta gravetat s'informa al director comercial per que en faci les gestions oportunes (si no pot donar un suport directe, acaba sol·licitant-ho al tècnic informàtic o reportant-ho al proveïdor).

Aquest control es troba en una fase inicial, ja que es basa en l'esforç personal.

4.9.1.2 Reporting de les debilitats en la seguretat de la informació

No es realitza cap documentació formal que permeti a posteriori analitzar els events que es produeixen, la classificació, la freqüència, l'impacte, els sistemes afectats, la hora en que es produeix l'incident i la solució aplicada.

Per tant, aquest control actualment és inexistent.

4.9.2 Gestió d'incidents de seguretat i millores de seguretat

4.9.2.1 Responsabilitats i procediments

Aquest control s'utilitza per analitzar les incidències de seguretat que es produeixen a la organització, en base a la informació que s'ha reportat en els controls anteriorment mencionats. En base als incidents, les solucions aplicades en anterioritat, les causes que han produït l'incident, es determina el procediment que s'ha de aplicar i quins són els actors que han d'actuar i informar si apareix aquest tipus d'incident.

No es troba aquest tipus de control en la organització. La identificació del problemes de seguretat que es produeixen en l'entitat es basen en actuacions menys formals.

4.9.2.2 Aprenent dels incidents en la seguretat de la informació

Aquest control s'utilitza per analitzar a posteriori les incidències de seguretat per que es produeixen a la organització.

En aquests cas s'analitzen les incidències i realitzar alguna mesura addicional per baixar la ocurrència i l'impacte de les mateixes.

No es troba aquest tipus de control en la organització. La identificació del problemes de seguretat que es produeixen en l'entitat es basen en un anàlisis menys formal o a suggerències de tercers.

4.9.2.3 Recol·lecció d'evidències

No s'està realitzant cap procediment per realitzar una recol·lecció de les evidències dels incidents de seguretat que ens permeti capturar la informació per realitzar un anàlisis forense i que serveixen com a proves en un procés legal.

4.10 Gestió de continuïtat de negoci

4.10.1 Aspectes de la continuïtat del negoci

4.10.1.1 Incloent la seguretat de la informació en el procés de gestió de la continuïtat del negoci

Aquest control es troba en una fase inicial. La direcció es conscient de que una interrupció del servei o un dany en els actius d'informació pot paralitzar l'activitat de l'empresa i fins i tot comportar la seva desaparició total.

En l'actual document s'analitza els riscos de seguretat que té l'organització i que ens servirà per mesurar les accions associades al pla de negoci.

No es troba orientada els actius de l'empresa per gestionar els riscos associats.

4.10.1.2 Continuïtat del negoci i avaluació de riscos

Aquest control es troba en un estat inicial, ja que en el present document s'ha realitzat un primer anàlisi dels riscos que poden sofrir els actius d'informació, encara que no es troben analitzats la resta d'actius però no s'han mesurat l'impacte que pot tenir la materialització dels riscos segons els temps d'interrupció del servei o la pèrdua d'informació que es produeixi.

4.10.1.3 Redacció e implantació de plans de continuïtat que incloguin la seguretat de la informació

No existeix cap document ni si s'ha implantat cap pla de continuïtat del negoci que determini els temps de recuperació del servei i la pèrdua de dades que pugui assumir la organització. Per tant, és un control inexistent.

4.10.1.4 Marc de planificació per la continuïtat del negoci

No existeix cap document que determini quan s'ha d'establir un pla de continuïtat del negoci ni els responsables de cadascuna de les etapes del pla, ni el recolzament de proveïdors en l'activació del pla de contingència.

Aquest control actualment és inexistent.

4.10.1.5 Prova, manteniment i re-avaluació dels plans de continuïtat

No hi ha actualment cap pla de contingència, per tant no es poder realitzar proves i avaluar la eficiència de les mesures i procediments establerts en el pla.

4.11 Compliment

4.11.1 Compliment dels requeriments legals

4.11.1.1 Identificació de la legislació aplicable

PREVENCIO S.L. és coneixedora de la legislació aplicable per la seva activitat. Les principals lleis que li afecten en el compliment de la seva activitat són:

- Llei de Prevenció de Riscos Laborals. Determina les dades de salut i el temps que ha de guardar de les revisions mèdiques realitzades.
- LOPD (Llei Orgànica de Protecció de Dades Personals). En aquesta llei es determina l'ús i les mesures de seguretat que ha d'aplicar en la protecció de dades de nivell alt.

Es revisa periòdicament els canvis que puguin sorgir respecte la legislació vigent. Per tant, ens trobem amb un control gestionat i mesurable.

4.11.1.2 Drets de propietat intel·lectual

Tal i com ens informa *PREVENCIO S.L,* tot el *software* que utilitza la organització es troba llicenciat. No s'utilitza cap còpia no legal. El *software* s'obté a traves de proveïdors oficials. Tots els contractes de llicències es troben sota el control del director financer.

Per una altra banda, en l'anàlisi realitzat ens informen que per els cursos de formació és comú utilitzar altres referències documentals, imatges obtingudes de *Internet*, sense plantejar cap acció sobre els drets d'autor que disposin aquests continguts.

En general, podem considerar que és un procés reproduïble, però intuïtiu, amb la excepció del material utilitzat en la formació.

4.11.1.3 Salvaguardes dels registres de la organització

La diferent informació sobre prevenció i vigilància de la salut s'emmagatzema als locals de la organització, ja sigui amb format imprès o electrònic.

La informació es troba classificada en funció del client i del temps que s'ha de conservar la informació. Periòdicament, es revisa la informació emmagatzemada per tal d'eliminar aquella informació que ja ha passat el temps de conservació. La informació només es troba accessible per el personal de la pròpia àrea.

De totes formes i com s'ha avaluat en anteriors controls, existeixen deficiències de seguretat en la utilització d'equips de treball des de fora dels locals de la organització, que ens fa reduir la valoració de la maduresa del control en reproduïble però intuïtiva.

4.11.1.4 Protecció de les dades i de la privacitat de la informació personal

Tal i com hem esmentat, *PREVENCIO S.L* és coneixedora dels requisits que marca la llei espanyola sobre les mesures de seguretat que s'han d'aplicar sobres les dades de caràcter personal. No s'ha

publicat cap procediment escrit d'accés per el personal que gestiona dades sensibles, però es conegut les seves implicacions per la majoria del personal.

Per tant ens trobem amb un control reproduïble, però intuïtiu.

4.11.1.5 Prevenció en el mal ús dels recursos del tractament de la informació

No existeix cap política expressa sobre el ús personal dels equips de la organització. Existeix un document bàsic de bon ús dels equips informàtics. El personal de l'empresa utilitza de manera esporàdica els terminals per activats fora dels objectius propis de la organització.

Per part de la direcció s'ha permès un ús moderat d'aquests recursos, sempre i quant no comporti una pèrdua de temps significativa per el personal. No es troba detallat en el document associat recomanacions sobre quins són els aspectes que haurien de tenir en compte per que no es generin forats de seguretat per accedir al navegador a pàgines de dubtosa reputació.

Per tant ens trobem amb un control reproduïble però intuïtiu ja que hi han mancances significatives en la documentació facilitada als treballadors.

4.11.1.6 Regulació dels controls criptogràfics

L'ús de d'eines de xifratge es limiten bàsicament a la utilització del programa *PREVENET.* Ens trobem amb una empresa que només actua dins del àmbit nacional, per tant no requereix un assessorament sobre la legislació d'altres països.

Podem considerar que no s'està realitzant cap control associat en la actualitat.

4.11.2 Compliment de les polítiques de seguretat i estàndards, i compliment tècnic

PREVENCIO S.L. es troba en una fase inicial d'implantació del sistema de gestió de seguretat de la informació. S'ha format un comitè de seguretat, el qual s'ha compromès a realitzar unes reunions periòdiques en les quals s'avaluarà l'estat actual de seguretat de la informació, les mesures que s'han pres en anterioritat i planificar les futures accions a realitzar.

Per fer aquesta gestió es basen en un anàlisis de riscos mitjançant la metodologia *MAGERIT* i una avaluació de la maduresa de seguretat segons les bones pràctiques definides en la *ISO 27002.*

4.11.2.1 Conformitat amb la política de seguretat i els estàndards

Actualment no hi ha definida una política de seguretat, però la organització s'ha compromès a realitzar una política de seguretat com a base dels diferents procediments de seguretat que s'aplicaran.

Per tant, ens trobem en una fase inicial de maduresa del control.

4.11.2.2 Comprovació de la conformitat tècnica

PREVENCIO S.L ha delegat a AUDITORIA S.L. la gestió de les diferents auditories periòdiques de seguretat per revisar el compliment de les mesures de seguretat implantades.

Per tant ens trobem en fase inicial de maduresa del control.

4.11.2.3 Consideracions sobre les auditories de sistemes

AUDITORIA S.L tindrà que acordar amb la direcció quines són les diferents proves que es realitzaran l'auditoria dels sistemes, minimitzant al màxim l'impacte que pugui tenir per el servei la realització de les mateixes.

Ens trobem en una fase inicial de maduresa del control.

4.11.2.4 Controls d'auditoria de sistemes

AUDITORIA S.L acordarà amb la direcció quin és l'abast de la auditoria i quins són els recursos necessaris per poder realitzar-la. Es registraran tots els accessos que es realitzin en l'auditoria i es presentaran en els resultats obtinguts.

Ens trobem en una fase inicial de maduresa del control.

4.11.2.5 Protecció de les eines d'auditoria de sistemes

Les eines d'auditoria estaran en possessió d' *AUDITORIA S.L.* Un cop realitzada l'auditoria es facilitarà al responsable de seguretat les dades obtingudes en les diferents proves per que en faci custòdia o eliminació, fora de l'abast de qualsevol altre persona.

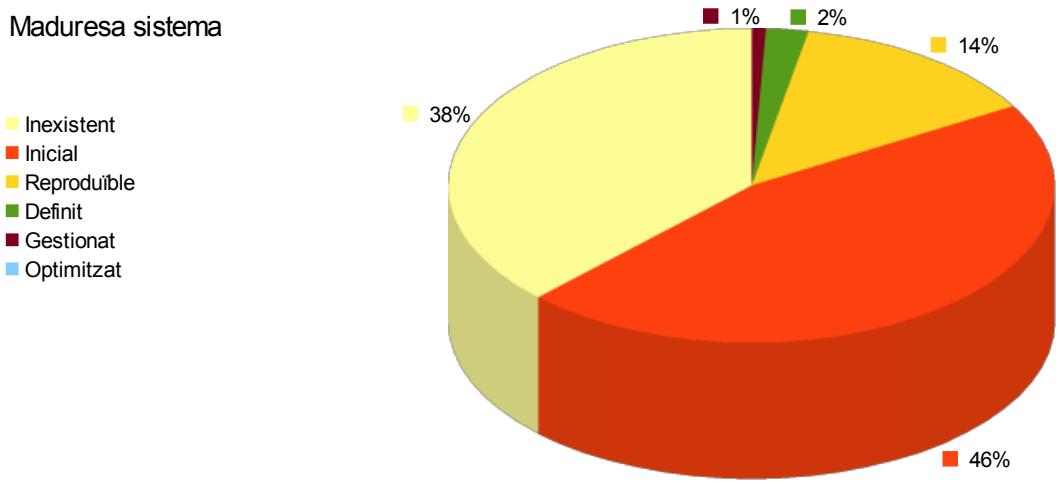
Aquest control també es troba en una fase inicial.

4.12 Presentació global dels resultats i conclusions

Un cop avaluat els diferents controls de seguretat podrem realitzar un conjunt d'interpretació dels resultats:

- Valoració global dels diferents controls. Aquesta avaluació ens donarà una visió de seguretat en conjunt. Utilitzarem
- Valoració dels diferents dominis de seguretat. Aquesta valoració ens permetrà aprofundir en els diferents aspectes de seguretat respecte a l'estat desitjat de seguretat.

4.12.1 Valoració global



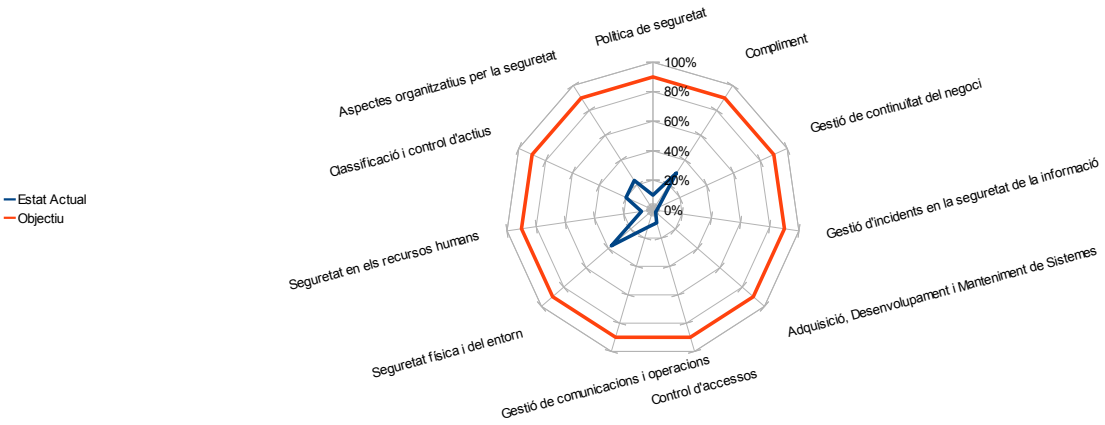
Podem comprovar que l'estat de maduresa general de *PREVENCIO S.L* es troba a nivell general en un nivell Inicial i fins i tot amb un desconeixement alt sobre les mesures de seguretat.

Ens trobem amb una situació habitual en la petita i mitjana empresa que tenen el seu servei d'informació com una eina per desenvolupar el seu negoci i no el valoren com un dels actius principals a protegir.

En empreses amb un baix volum de treballadors és habitual que es basin més en la experiència professional que en la documentació els diferents procediments de negoci, i en particular els referents a la seguretat de la informació.

Podem afirmar en el estudi realitzat que *PREVENCIÓ S.L.* no disposa actualment d'un coneixement suficient per establir les mesures de seguretat requerides per protegir la informació, especialment les de caràcter tècnic. Disposa d'un conjunt reduït de personal amb aquestes funcions, els quals no poden disposar de la disponibilitat requerida per abordar els diferents aspectes de seguretat que s'han de millorar en el sistema actual.

4.12.2 Valoració dels diferents dominis de seguretat



Domini	Estat Actual	Objectiu
Política de seguretat	**10%**	90%
Aspectes organitzatius per la seguretat	**24%**	90%
Classificació i control d'actius	**20%**	90%
Seguretat en els recursos humans	**8%**	90%
Seguretat física i del entorn	**37%**	90%
Gestió de comunicacions i operacions	**12%**	90%
Control d'accessos	**9%**	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	**2%**	90%
Gestió d'incidents en la seguretat de la informació	**3%**	90%
Gestió de continuïtat del negoci	**4%**	90%
Compliment	**30%**	90%

En el gràfic exposat s'ha realitzat s'han ponderat el valor de maduresa dels diferents dominis en el objectiu de seguretat als que pertanyien, i aquests s'han ponderat sobre el seu domini. Com es pot comprovar en el gràfic la situació actual dista bastant de la situació desitjada, en la qual es troben definits els procediments dels diferents aspectes de seguretat i en el que tota la organització sencera intervé en els diferents processos. Aquest objectiu és difícil d'assolir a curt plaç, ja que hi ha un gran volum de controls a revisar i probablement la organització no disposa de tots els recursos humans i econòmics per abordar-los completament, però ha de ser una fita sobre la qual podrem basar la millora del nostre sistema de seguretat.

El conjunt global dels controls es troba en la següent taula:

Control	Eficàcia Inicial
Política de seguretat	**10%**
Política de seguretat de la informació	***10%***
Document de política de seguretat de la informació	10%
Revisió i avaluació	10%
Aspectes organitzatius per la seguretat	**24%**
Organització interna	***14%***
Comitè de gestió de seguretat de la informació	10%
Coordinació de la seguretat de la informació	10%
Assignació de responsabilitats sobre seguretat de la informació	50%
Procés d'autorització de recursos per el tractament de la informació	10%
Acords de confidencialitat	0%
Contactes amb autoritats	10%
Contactes amb grups d'interès especial	10%
Revisió independent de la seguretat de la informació	10%
Seguretat en els accessos de terceres parts	***33%***
Identificació de riscos per el accés a tercers	50%
Requisits de seguretat quan es tracta amb clients	50%
Requisits de seguretat en contractes d'outsourcing	0%
Classificació i control d'actius	**20%**
Responsabilitat sobre els actius	***10%***
Inventari d'actius	10%
Propietat dels actius	10%
Ús adequat dels actius	10%
Classificació de la informació	***30%***
Guies de classificació	50%
Marcat i tractament de la informació	10%
Seguretat en els recursos humans	**8%**
Seguretat abans del treball	***10%***
Inclusió de la seguretat en les responsabilitats i funcions laborals	10%
Selecció i política de personal	10%
Acords de confidencialitat	10%
Durant del treball	***7%***
Responsabilitats de la gerència	10%

Coneixement, educació i entrenament de la seguretat de la informació	10%
Procés disciplinari	0%
Finalització o canvi de treball	***7%***
Responsabilitats de finalització	0%
Retorn d'actius	10%
Retirada dels drets d'accés	10%
Seguretat física i del entorn	**37%**
Àrees segures	***43%***
Perímetre de seguretat física	50%
Controls físics d'entrades	50%
Seguretat d'oficines, despatxos i recursos	50%
Protecció contra amenaces externes i ambientals	10%
El treball en les àrees segures	10%
Accés públic, àrees de càrregues i descàrregues	90%
Seguretat dels equips	***31%***
Instal·lació i protecció d'equips	10%
Subministrament elèctric	90%
Seguretat del cablejat	10%
Manteniment dels equips	0%
Seguretat d'equips fora dels locals de la organització	10%
Seguretat en la reutilització o eliminació dels equipaments	10%
Retirada de la propietat	90%
Gestió de comunicacions i operacions	**12%**
Procediments i responsabilitats d'operacions	***5%***
Documentació de procediments operatius	10%
Gestió de canvis	0%
Segregació de tasques	10%
Separació dels recursos per desenvolupament i per producció	0%
Gestió de serveis externs	***10%***
Servei d'entrega	10%
Monitorització i revisió dels serveis externs	10%
Gestionant canvis per els serveis externs	10%
Planificació i acceptació del sistema	***0%***
Planificació de la capacitat	0%
Acceptació del sistema	0%
Protecció contra software maliciós	***10%***
Mesures i controls contra software maliciós	10%

Mesures i controls contra codi mòbil	10%
Gestió de copies de seguretat i recuperació	***10%***
Recuperació de la informació	10%
Gestió de seguretat en xarxes	***5%***
Controls de xarxa	0%
Seguretat en els serveis de xarxa	10%
Utilització dels medis d'informació	***20%***
Gestió de medis removibles	10%
Eliminació de medis	10%
Procediment de manipulació de la informació	10%
Seguretat de la documentació de sistemes	50%
Intercanvi d'informació	***16%***
Polítiques i procediments per el intercanvi d'informació i software	10%
Acords d'intercanvi	10%
Medis físics en trànsit	0%
Seguretat en la missatgeria electrònica	10%
Sistemes d'Informació de Negocis	50%
Serveis de correu electrònic	***37%***
Comerç electrònic	50%
Transacció en línia	50%
Informació pública disponible	10%
Monitorització	***10%***
Registre de la auditoria	0%
Monitoritzant el us del sistema	0%
Protecció de la informació de registre	10%
Registre d'administradors i operadors	0%
Registre de la avaria	0%
Sincronització del rellotge	50%
Control d'accessos	**9%**
Requisits de negoci per el control d'accés	***10%***
Política de control d'accés	10%
Gestió d'accés d'usuaris	***15%***
Registre d'usuaris	10%
Gestió de privilegis	50%
Gestió de contrasenyes d'usuaris	0%
Revisió dels drets d'accés dels usuaris	0%
Responsabilitats dels usuaris	***7%***

Us de contrasenyes	0%
Equips informàtics d'usuaris desatesos	10%
Polítiques de pantalles i escriptoris nets	10%
Control d'accés a la xarxa	***4%***
Política d'us dels serveis de xarxa	0%
Autentificació d'usuari per connexions externes	10%
Identificació d'equips en la xarxa	0%
Diagnòstic remot i configuració de protecció de ports	0%
Segregació en xarxa	10%
Control de connexió a la xarxa	10%
Control d'enrutament en la xarxa	0%
Control d'accés al sistema operatiu	***3%***
Procediment de connexió de terminals	10%
Identificació i autentificació del usuari	10%
Sistema de gestió de contrasenyes	0%
Utilització de les facilitats del sistema	0%
Desconnexió automàtica de sessions	0%
Limitació del temps de connexió	0%
Control d'accés a les aplicacions i la informació	***25%***
Restricció d'accés a la informació	50%
Aïllament de sistemes sensibles	0%
Informàtica mòbil i teletreball	***0%***
Informàtica mòbil i comunicacions	0%
Teletreball	0%
Adquisició, Desenvolupament i Manteniment de Sistemes	**11%**
Requisits de seguretat dels sistemes	***0%***
Anàlisi i especificacions dels requisits de seguretat	0%
Seguretat de les aplicacions del sistema	***0%***
Validació de les dades d'entrada	0%
Control del procés intern	0%
Integritat dels missatges	0%
Validació de les dades de sortida	0%
Controls criptogràfics	***0%***
Política d'ús dels controls criptogràfics	0%
Gestió de claus	0%
Seguretat dels arxius del sistema	***0%***
Control del software en producció	0%

Protecció de les dades de prova del sistema	0%
Control d'accés als codis de programes font	0%
Seguretat en els processos de desenvolupament i suport	***14%***
Procediments de control de canvis	10%
Revisió tècnica dels canvis en el sistema operatiu	0%
Restriccions en els canvis als paquets de software	10%
Fuga d'informació	50%
Desenvolupament extern del software	0%
Gestió de la vulnerabilitat tècnica	***50%***
Control de les vulnerabilitats tècniques	50%
Gestió d'incidents en la seguretat de la informació	**8%**
Reportant events i debilitats de la seguretat de la informació	***10%***
Reportant els events en la seguretat de la informació	10%
Reportant debilitats en la seguretat de la informació	10%
Gestió de les millores i incidents en la seguretat de la informació	***7%***
Responsabilitats i procediments	0%
Aprenent dels incidents en la seguretat de la informació	10%
Recol·lecció d'evidències	10%
Gestió de continuïtat del negoci	**4%**
Aspectes de la gestió de continuïtat del negoci	***4%***
Incloent la seguretat de la informació en el procés de gestió de la continuïtat del negoci	10%
Continuïtat del negoci i avaluació de riscos	10%
Redacció e implantació de plans de continuïtat que incloguin la seguretat de la informació	0%
Marc de planificació per la continuïtat del negoci	0%
Prova, manteniment i avaluació dels plans de continuïtat	0%
Compliment	**30%**
Compliment dels requisits legals	***49%***
Identificació de la legislació aplicable	95%
Drets de propietat intel·lectual	50%
Salvaguardes dels registres de la organització	50%
Protecció de les dades i de la privacitat de la informació personal	50%
Prevenció en el mal us dels recursos del tractament de la informació	50%
Regulació dels controls criptogràfics	0%
Revisió de la política de seguretat i de la conformitat tècnica	***10%***
Conformitat amb la política de seguretat i els estàndards	10%
Comprovació de la conformitat tècnica	10%

Consideracions sobre la auditoria de sistemes	***10%***
Controls d'auditoria de sistemes	10%
Protecció de les eines d'auditoria de sistemes	10%

Avaluant els diferents resultats, podem valorar els següents aspectes:

- Hem de definir una política de seguretat. Permetrà a *PREVENET* establir les bases sobre el seu sistema de gestió de la informació. Serà un dels pilars per que el personal de la organització prengui consciència sobre el seu rol dins de la seguretat de la informació i ens servirà per prioritzar els diferents aspectes de seguretat que vagin sorgint.
- S'ha començat a posar les bases per gestionar la seguretat de la informació. S'ha establert un comitè de seguretat que serà l'encarregat d'exposar les noves necessitats i d'avaluar i aprovar les noves mesures que es produeixen per reduir els riscos de la organització.
- Tenim inventariats els diferents actius de la organització, però s'ha d'implicar al personal com a principal responsable sobre el material que li han cedit l'us.
- S'ha de millorar la gestió dels recursos humans. Es requereix un assessorament sobre els diferents aspectes relacionats en la contractació i s'ha de conscienciar al personal sobre la confidencialitat que ha de tenir el personal amb els actius d'informació de la organització
- Per el tipus d'activitat de negoci i els actius que gestionem requerim una menor mesura de protecció sobre els actius d'informació dins els locals de la organització, però hem de conscienciar al personal sobre els actius d'informació quan treballen en el client, ja que ens trobem en ubicacions en les que no es disposen de totes les mesures de seguretat i les condicions de treball són diferents.
- S'ha de millorar especialment el control de les comunicacions des de l'exterior. No s'estan prenent les mesures suficients per protegir la informació que es gestiona des de l'exterior. S'han de prendre mesures importants sobre aquest tipus de control. A nivell d'operació recauen la majoria de les obligacions sobre personal no especialitzat. A més es genera una dependència excessiva sobre aquest personal. No existeixen procediments definits per conscienciar al personal sobre la implicació en la seguretat dels processos de negoci. No s'està controlant l'activitat del sistema i per tant, no coneixem l'impacte actual dels diferents agents sobre la seguretat del sistema.
- No s'esta desenvolupant *software* per la nostra organització, i per tant no s'estan aplicant les mesures associades per aquest tipus de control. Encara que actualment no es requereixi una millora excessiva sobre aquests controls s'ha de tenir en compte la inexistència dels controls per si canvia l'escenari actual.
- S'ha de realitzar un control més formal sobre els incidents de seguretat per poder actuar en major celeritat quan es produeixin, poder detectar les causes dels incidents per evitar o reduir l'impacte associat.
- No disposem d'un pla de continuïtat del negoci. És un aspecte que s'hauria de plantejar *PREVENCIO S.L.* tenint en compte que els costos no tenen per que ser tant elevats com en altres organitzacions, ja que els aspectes més prioritaris son la confidencialitat i la integritat

de les dades respecte a la disponibilitat.

- Els empleats de *PREVENCIÓ S.L* disposa d'un alt coneixement legislatiu sobre els requisits legals. S'ha de tenir en compte que la seva activitat de negoci és que els seus clients puguin realitzar les obligacions legals sobre prevenció de riscos laborals. Respecte al compliment de les polítiques de seguretat estem en la fase inicial d'implantació d'un sistema de seguretat de la informació, per tant és a partir d'ara quan començarem a millorar sobre els aspectes relacionats a aquest objectiu.

5 PROPOSTES DE PROJECTES

En base a la avaluació de riscos realitzada i la revisió dels diferents controls de seguretat detallats en la normativa *ISO 27002*, a priori destacaríem els següents aspectes de seguretat a millorar.

A nivell de gestió de la seguretat abordaríem de manera prioritària:

- La implantació d'un sistema de gestió de seguretat que ens permeti detectar els problemes de seguretat de l'organització, valorar els impactes en la organització i el retorn de la inversió de les mesures de seguretat adoptades, i coordinar les mesures de seguretat que es vulguin implantar en la nostra organització.
- La implicació del personal en la materialització de les mesures de seguretat. En aquest punt es requereix que es defineixi una política de seguretat general, que es defineixi una política de seguretat del ús dels equips informàtics i que es defineixin els diferents procediments de la organització tenint sempre en compte la política de seguretat de la informació.
- Adoptar els diferents relacions contractuals que disposa la organització amb els clients, proveïdors i personal per que es defineixin les diferents responsabilitats sobre els actius de seguretat de la informació.
- La implantació d'un sistema per la gestió dels incidents, que ens permetrà registrar els incidents de seguretat que es materialitzen en la nostra organització, tan en freqüència com en impacte que permetrà a *PREVENCIO S.L.* aplicar solucions per reduir l'impacte associat, com tenir una base per poder fer anàlisis posteriors en la gestió del SGSI.

A nivell tècnic s'han d'abordar principalment els següents aspectes:

- La exposició de les nostres dades en el accés al exterior. En aquest punt inclouríem tant els problemes de seguretat dels terminals que es troben fora de les zones sota el control de la nostra organització, com dels elements de seguretat que disposem per controlar l'accés a les nostres dades centralitzades.
- Millores en les infraestructures necessàries per allotjar la informació en la nostra organització. Sobre aquest punt farem menció a solucions d'externalització dels nostres serveis.
- La disposició de personal qualificat per realitzar les tasques de manteniment que requereix el nostre sistema (gestió d'incidències, actualització del sistema, gestió de comptes d'usuari). En aquestes aspectes també es tindrà en compte la externalització dels serveis.

Sobre cadascun dels aspectes que hem destacat es realitzarà un conjunt de propostes de projectes, amb els quals determinarem de manera individual i conjunta com minimitzen l'impacte que puguin sofrir els nostres actius en la materialització d'una amenaça, com afecta a la maduresa dels diferents controls de seguretat de la informació, el cost econòmic de les diferents solucions i el seu retorn de la inversió.

En la fase actual de maduresa de seguretat en la que ens trobem actual considerem que no podem prioritzar només aquells projectes que tinguin una repercussió econòmica a curt termini, si no que s'ha de tenir en compte també assentar unes bases dins de *PREVENCIO S.L.* per que la gestió de la seguretat formi part de la forma de treballar de la organització i faciliti la valoració dels diferents

aspectes de seguretat que s'hagin d'implantar en un futur.

Prèviament realitzarem un anàlisis de riscos amb les diferents salvaguardes que disposa actualment la empresa, i que no es va fer anteriorment, ja que volíem mostrar a l'empresa del impacte que pot suposar per la organització la materialització de les amenaces sobre qualsevol dels seus actius.

Els diferents projectes es valoraran econòmicament de la següent manera:

- Hores dedicades en la implantació del projecte.
- Hores anuals requerides per el manteniment de la solució.
- Cost en Euros en la implantació del projecte.
- Cost en Euros en el manteniment de la solució.

S'utilitzara el mateix criteri per valorar les hores que dediqui el personal intern com el que dediqui les empreses contractades en la implantació de la solució. El cost establert en els diferents projectes presentats serà de 100 €/hora, independentment del personal que hagi de realitzar la funció. Aquests preus s'ajustaran en el desplegament de les diferents solucions.

Els diferents projectes plantejats es basen en una implantació en un temps inferior a un any. Alguns d'ells són projectes que els realitzarà principalment *PREVENCIÓ S.L.,* per tant és l'empresa que marcarà com objectiu realitzar-lo en un any vista o en un temps més espaiat.

Per el càlcul d'amortització dels diferents projectes es repercutirà en els 3 primers anys d'implantació del sistema. Per tant, a partir del 3 any els beneficis que aporti la millora del sistema serà net.

5.1 Avaluació global de les salvaguardes

Com a pas previ a avaluar els diferents projectes en la seguretat de la informació, farem una introducció a com afecten les salvaguardes en els riscos dels diferents actius.

Per un mateix actiu habitualment existeixen vàries tipus de salvaguardes associades:

- Preventives: per disminuir la freqüència d'ocurrència d'una amenaça.
- Detectives: Per manifestar quan es produeix un incident de seguretat.
- Correctives: per recuperar l'actiu al que se li ha materialitzat una amenaça.
- Repressives: que actuen quan s'ha materialitzat una amenaça per reduir els danys que pugui provocar.
- D'avaluació: que ens permeten recollir evidències per un anàlisis de per que s'ha produït l'amenaça i quines actuacions es van realitzar.

Per el càlcul del risc, la influència de les salvaguardes es realitza només sobre la freqüència d'ocurrència i sobre la reducció del impacte, per tant, es mirarà de classificar les diferents salvaguardes com a preventives i/o correctives.

La inclusió d'una salvaguarda eficient no té per que ser suficient per la recuperació d'una amenaça concreta. Per exemple, podem disposar d'un sistema de *backup* que ens permeti recuperar un actiu en el instant anterior a la materialització d'una amenaça, però si no es gestionen els mecanismes per detectar quan es produeix l'amenaça o si no es prenen les mesures per assegurar que la còpia està danyada, ens podem trobar que aquest sistema de *backup* pot no ser eficient.

No es pot garantir al 100% impedir la materialització de les diferents amenaces però si podem gestionar les accions reduir la probabilitat d'ocurrència de la amenaça o el impacte associat.

En base a aquests criteris i tenint com a referència la classificació general que realitza *MAGERIT* sobre les salvaguardes, hem escollit les salvaguardes que hem considerat més significatives del nostre escenari, les hem agrupat com a preventives i/o correctives, hem ponderat la eficiència màxima de les salvaguardes dels dos grups sobre una escala de 100, tenint en compte que amb una gestió eficaç de les diferents salvaguardes no es garanteix el 100% del risc (hem estimat un 95% d'eficàcia màxima tant en salvaguardes preventives com correctives)

Posarem com exemple el *backup*, que podem posar com a criteri de correcció del risc en un màxim del 35% (segons la taula adjunta), en el cas de que que ens permeti recuperar en qualsevol instant del temps previ a la materialització d'una amenaça. Si apliquem els pertinents mecanismes de registre, detecció i recuperació podem incrementar la eficiència de la salvaguarda fins a un 10%.

Aquesta identificació i valoració de les salvaguardes és tracta d'una primera aproximació. Per cadascun dels actius es valorarà fins a quin punt és aplicable aquest criteri inicial.

En base a la maduresa del nostre sistema de gestió de seguretat de la informació s'anirà ajustant el nombre de salvaguardes i la seva eficàcia en funció dels registres, dels canvis en la organització, de les noves vulnerabilitats, de les solucions que vagin apareixent en el mercat i dels diferents anàlisis que es vagin realitzant a *PREVENCIO S.L*

En base als criteris exposats es realitzarà aquesta primera aproximació:

- **Salvaguardes preventives:**

Salvaguardes	Instal·lacions	Hardware	Aplicació	Dades	Xarxa	Serveis	Equipaments Auxiliars	Personal
Salvaguardes associades al bon govern de la seguretat (organització seguretat, politica de seguretat, procediments de seguretat...)	20	10	20	20	10	20	30	20
Control d'accés	70	10	30	30	15	50		
Registre d'actuacions		15	20	20	10	20	20	
Pla de continuïtat	5	5	5	5	5	5	5	5
Firma electrònica Gestió de claus (si utilitza xifrat)				10	5			
Xifrat				10	15			
Inventari		15						
Configuració equips (configuració S.O, segmentació de xarxes, firewalls, IPS...)		20			25			
Manteniment		20	20		10		40	
Especificacions del lloc de treball								30
Selecció del personal								10
Condicions contractuals seguretat								30

- **Salvaguardes correctives:**

Salvaguardes	Instal·lacions	Hardware	Aplicació	Dades	Xarxa	Serveis	Equipaments Auxiliars	Personal
Salvaguardes associades al bon govern de la seguretat (organització seguretat, politica de seguretat, procediments de seguretat...)	20	20	20	20	20	50	20	50
Registre d'incidències		5	15	10	5	5		
Còpies de backup				45				
Detecció i recuperació		5	10	10	5	5		
Protecció davant codi maliciós			35					
Configuració equips (configuració S.O, IDS,...)		55			55			
Proteccions físiques instal·lacions	75						65	
SLA (Acuerdos de disponibillidad)		10	15		10	10	10	
NDA (Compromís de secret de la informació)				5				
Assumpció de responsabilitats i penalització per incumpliment				5		25		45

Aquest taula l'utilitzarem com una primera aproximació. El criteri es tindrà en compte segons l'amenaça que pot afectar a varis tipus d'actius de diferents categories.

5.1.1 Avaluació de les salvaguardes instaurades a *PREVENCIÓ S.L.*

En l'apartat d'estudi de les amenaces hem analitzat l'impacte potencial sense tenir en compte les diferents salvaguardes associades a un element "físic" que disposava la organització. Com ja hem comentat això s'ha fet per conscienciar a *PREVENCIÓ S.L.* de la importància que tenen els diferents actius dins de la seguretat de la informació.

A continuació avaluarem les diferents salvaguardes de la organització.

5.1.1.1 Backup

S'emmagatzema en el servidor de correu, per tant en cas de fallida en el servidor o accions que es puguin materialitzar en la mateixa ubicació (inundacions, accés no autoritzat...), no cobreix tota les casuístiques associades.

Aquesta salvaguarda impacta sobre la disponibilitat i la integritat de les dades, per tant, només s'ha tingut en compte en els errors de dades que comprometen a aquestes dimensions de seguretat.

Només guardem 2 còpies de *backup* setmanals. Si l'error detectat és anterior no podrem recuperar la informació, i es poden arribar a perdre fins a cinc dies en modificacions de les dades.

La utilització del *backup* es realitza quan un empleat detecta que ha eliminat informació, detecta que li falta informació o detecta que hi ha informació que no pot accedir per que es troba danyada. No es realitza cap control que ens permeti detectar que hi ha informació danyada en el servidor o que ha sigut manipulada que ens permeti actuar amb la celeritat necessària per aprofitar les còpies disponibles.

No es realitza cap proba per validar que els backups realitzats són eficients (p.e una proba de restauració de bases de dades, de correus...).

Per tant, valorarem la eficàcia de la salvaguarda en només un 30% d'eficàcia (no s'inclouen els merament procedimentals). Aplicant la salvaguarda en les diferents amenaces a les que pugui influenciar, ens trobem amb el següent resultat.

En base al criteri definit, aquest és la influència anual del backup actual en el risc de la organització.

Actiu/*Amenaces*	Salvaguarda preventiva (Percentatge de disminució)	Salvaguarda curativa (Percentatge de disminució)	Freqüència Intrínseca	Freqüencia residual * Percentatge de disminució impacte	Valor	Risc Intrínsec	Risc Efectiu	Reducció del risc
Data-Prv					300.000 €	6.041 €	4.475 €	1.566 €
Data-Form					75.000 €	1.510 €	1.119 €	391 €
Data-V.S					300.000 €	54.460 €	54.423 €	37 €
Data-Proc.Int					30.000 €	2.746 €	2.193 €	553 €
Data-Conta					30.000 €	604 €	448 €	157 €
Data-Comer					75.000 €	1.510 €	1.119 €	391 €
[E1] - Errors i Fallides no intencionades - Errors dels usuaris	100%	70%	10	7				
[E2] - Errors i Fallides no intencionades - Errors del administrador	100%	70%	1	0,7				
[E3] - Errors i Fallides no intencionades - Errors de monitorització (log)	100%	100%	10	10				
[E4] - Errors i Fallides no intencionades - Errors de configuració	100%	70%	5	3,5				
[E14] - Errors i Fallides no intencionades - Fugues d'informació	100%	100%	1	1				
[E15] - Errors i Fallides no intencionades - Alteració de la informació	100%	70%	10	7				
[E16] - Errors i Fallides no intencionades - Introducció d'informació errònia	100%	70%	100	70				
[E17] - Errors i Fallides no intencionades - Degradació de la informació	100%	70%	10	7				
[E18] - Errors i Fallides no intencionades - Destrucció de la informació	100%	70%	10	7				
[E19] - Errors i Fallides no intencionades - Divulgació de la Informació	100%	100%	1	1				
[A4] - Atacs Intencionats - Manipulació de la configuració	100%	70%	0,1	0,07				
[A11] - Atacs Intencionats - Accés no autoritzat	100%	100%	100	100				
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	100%	100%	10	10				
[A15] - Atacs Intencionats - Modificació de la informació	100%	70%	10	7				
[A16] - Atacs Intencionats - Introducció d'informació falsa	100%	70%	20	14				
[A17] - Atacs Intencionats - Corrupció de la informació	100%	70%	10	7				
[A18] - Atacs Intencionats - Destrucció de la informació	100%	70%	10	7				
[A19] - Atacs Intencionats - Divulgació de la informació	100%	100%	10	10				

En la taula adjunta mostrem l'impacte en els actius de dades. Si estenem aquesta mesura a tots els actius de la informació que es trobin afectats per les mateixes amenaces, llavors obtenim el següents resultats:

Segons l'anàlisi de riscos realitzat, la disponibilitat de *backup* només té una reducció del impacte valorat en uns 9.394 €/anuals. Recordem que hem prioritzat per els nostres actius dimensions de seguretat diferents a la integritat de la informació de la informació, per tant no té el pes esperat el *backup* respecte els riscos que requereixen aquest tipus de salvaguarda.

Més endavant veurem com afecta un canvi en el procediment actual de *backup*.

5.1.1.2 Antivirus/AntiSpam

És troba instal·lat en tots els equips d'usuaris. S'actualitza automàticament i es troba inclòs un escaneig periòdic del equip.

No es fa cap anàlisis a posteriori sobre els diferents casos de seguretat que ens permeti fer un anàlisis de perquè es produeixen i com podem reduir-los.

La solució es troba disponible els equips d'usuari, en cap cas en els servidors, per tant determinarem que la efectivitat del control és d'un 90% (aproximadament un 25 % en els actius d'aplicació).

Actiu/*Amenaces*	**Salvaguarda preventiva (Percentatge de disminució)**	**Salvaguarda curativa (Percentatge de disminució)**	**Freqüència Intrínseca**	**Freqüencia residual * Percentatge de disminució impacte**	**Valor**	**Risc Intrínsec**	**Risc Efectiu**	**Reducció del risc**
Apl-Win.Srv					300.000 €	47.638 €	46.973 €	666 €
Apl-Win.XP					300.000 €	47.638 €	46.973 €	666 €
Apl-IIS					300.000 €	47.638 €	46.973 €	666 €
Apl-Ms.SQL					300.000 €	47.638 €	46.973 €	666 €
Apl-PREV					300.000 €	47.638 €	46.973 €	666 €
Apl-Ms.Ex.Srv					300.000 €	47.638 €	46.973 €	666 €
Apl-NFS					300.000 €	47.638 €	46.973 €	666 €
Apl-Conta					300.000 €	47.638 €	46.973 €	666 €
Apl-MS.OFF					300.000 €	47.638 €	46.973 €	666 €
Total					**2.700.000 €**	**428.745 €**	**422.753 €**	**5.992 €**
[I5] - Industrials - Avaria d'origen físic o lògic	100%	100%	0,2	0,2				
[E1] - Errors i Fallides no intencionades - Errors dels usuaris	100%	100%	10	10				
[E2] - Errors i Fallides no intencionades - Errors del administrador	100%	100%	1	1				
[E3] - Errors i Fallides no intencionades - Errors de monitorització (log)	100%	100%	10	10				
[E4] - Errors i Fallides no intencionades - Errors de configuració	100%	100%	5	5				
[E8] - Errors i Fallides no intencionades - Difusió de software maliciós	100%	10%	10	1				
[E9] - Errors i Fallides no intencionades - Errors de re-encaminament	100%	100%	10	10				
[E10] - Errors i Fallides no intencionades - Errors de seqüencia	100%	100%	0	0				
[E14] - Errors i Fallides no intencionades - Fugues d'informació	100%	100%	1	1				
[E20] - Errors i Fallides no intencionades - Vulnerabilitats dels programes (software)	100%	100%	100	100				
[E21] - Errors i Fallides no intencionades - Errors de manteniment/Actualitzacions d'equips (software)	100%	100%	100	100				
[A4] - Atacs Intencionats - Manipulació de la configuració	100%	100%	0,1	0,1				
[A5] - Atacs Intencionats - Suplantació Identitat	100%	100%	1	1				
[A6] - Atacs Intencionats - Abús de privilegis d'accés	100%	100%	10	10				
[A7] - Atacs Intencionats - Us no previst	100%	10%	100	10				
[A8] - Atacs Intencionats - Difusió de software maliciós	100%	10%	0,2	0,02				
[A9] - Atacs Intencionats - Re-encaminament de missatges	100%	10%	0,2	0,02				
[A10] - Atacs Intencionats - Alteració de seqüència	100%	100%	0,2	0,2				
[A11] - Atacs Intencionats - Accés no autoritzat	100%	100%	100	100				
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	100%	100%	10	10				
[A22] - Atacs Intencionats - Manipulació de programes	100%	10%	1	0,1				

Aquesta salvaguarda està suposant una reducció del risc d'uns 5.992 € anuals.

5.1.1.3 Firma Digital

Tal i com hem anat exposat, la firma digital només s'utilitza en casos residuals en la que el client ens ha proporcionat el certificat i per exigència del client, per tant, aquesta eines no s'estan actualitzant de forma generalitzada i no la inclourem en l'anàlisi. És un mecanisme que es podria considerar per la confidencialitat del correu durant el seu transport en contrapartida a una solució *VPN,* a on la protecció no es troba en el missatge, sinó en el canal d'informació.

5.1.1.4 Armaris amb clau (ignífugs)

En aquests armaris es troba inclosa tota la informació ubicada en les diferents delegacions. La clau està assignada a la persona/es responsables de la informació. La integritat i confidencialitat d'aquesta informació només es troba compromesa quan no es troba dins dels equipaments de *PREVENCIO S.L* (empreses subcontractades i clients). Al tractar-se d'un volum d'informació d'informació (menys del 1%) durant un període limitat (un parell de dies) un considerarem com una exposició pràcticament nul·la.

Aquesta salvaguarda protegeix directament les dades impreses. Ho considerarem com un cas particular en el criteri inicial que hem definit de les salvaguardes i ho valorarem directament sobre l'actiu de dades afectat. Aquesta salvaguarda te una efectivitat del 80% sobre els actius de dades en cas de destrucció i per evitar accessos no autoritzats de la informació impresa.

Per les dades de prevenció podem afirmar que la meitat de les dades són impreses i emmagatzemades en els armaris. Considerarem que aquest armaris són eficients en un 20% dels casos de destrucció, fugues d'informació i accés a la informació per les dades mixtes i un 40% per les que són merament digitals.

Per tant, amb els següents criteris, aquesta és els càlculs resultants:

Actiu/*Amenaces*	Salvaguarda preventiva (Percentatge de disminució)	Salvaguarda curativa (Percentatge de disminució)	Freqüència Intrínseca	Freqüencia residual * Percentatge de disminució impacte	Valor	Risc Intrínsec	Risc Efectiu	Reducció del risc
Data-Prv					300.000 €	6.041 €	5.203 €	838 €
[E1] - Errors i Fallides no intencionades - Errors dels usuaris	100%	100%	10	10				
[E2] - Errors i Fallides no intencionades - Errors del administrador	100%	100%	1	1				
[E3] - Errors i Fallides no intencionades - Errors de monitorització (log)	100%	100%	10	10				
[E4] - Errors i Fallides no intencionades - Errors de configuració	100%	100%	5	5				
[E14] - Errors i Fallides no intencionades - Fugues d'informació	100%	80%	1	0,8				
[E15] - Errors i Fallides no intencionades - Alteració de la informació	100%	100%	10	10				
[E16] - Errors i Fallides no intencionades - Introducció d'informació errònia	100%	100%	100	100				
[E17] - Errors i Fallides no intencionades - Degradació de la informació	100%	100%	10	10				
[E18] - Errors i Fallides no intencionades - Destrucció de la informació	100%	80%	10	8				
[E19] - Errors i Fallides no intencionades - Divulgació de la Informació	100%	80%	1	0,8				
[A4] - Atacs Intencionats - Manipulació de la configuració	100%	100%	0,1	0,1				
[A11] - Atacs Intencionats - Accés no autoritzat	100%	80%	100	80				
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	100%	100%	10	10				
[A15] - Atacs Intencionats - Modificació de la informació	100%	100%	10	10				
[A16] - Atacs Intencionats - Introducció d'informació falsa	100%	100%	20	20				
[A17] - Atacs Intencionats - Corrupció de la informació	100%	100%	10	10				
[A18] - Atacs Intencionats - Destrucció de la informació	100%	80%	10	8				
[A19] - Atacs Intencionats - Divulgació de la informació	100%	80%	10	8				

Actiu/*Amenaces*	Salvaguarda preventiva (Percentatge de disminució)	Salvaguarda curativa (Percentatge de disminució)	Freqüència Intrínseca	Freqüencia residual * Percentatge de disminució impacte	Valor	Risc intrínsec	Risc efectiu	Reducció del risc
Data-Contr.Clie					300.000 €	5.055 €	3.378 €	1.677 €
Data-Contr.Prov					300.000 €	5.055 €	3.378 €	1.677 €
[E1] - Errors i Fallides no intencionades - Errors dels usuaris	100%	100%	10	10				
[E2] - Errors i Fallides no intencionades - Errors del administrador	100%	100%	0	0				
[E3] - Errors i Fallides no intencionades - Errors de monitorització (log)	100%	100%	0	0				
[E4] - Errors i Fallides no intencionades - Errors de configuració	100%	100%	0	0				
[E14] - Errors i Fallides no intencionades - Fugues d'informació	100%	60%	1	0,6				
[E15] - Errors i Fallides no intencionades - Alteració de la informació	100%	100%	1	1				
[E16] - Errors i Fallides no intencionades - Introducció d'informació errònia	100%	100%	100	100				
[E17] - Errors i Fallides no intencionades - Degradació de la informació	100%	100%	10	10				
[E18] - Errors i Fallides no intencionades - Destrucció de la informació	100%	60%	10	6				
[E19] - Errors i Fallides no intencionades - Divulgació de la Informació	100%	60%	1	0,6				
[A4] - Atacs Intencionats - Manipulació de la configuració	100%	100%	0,1	0,1				
[A11] - Atacs Intencionats - Accés no autoritzat	100%	60%	100	60				
[A14] - Atacs Intencionats - Intercepció de la informació (escolta)	100%	100%	10	10				
[A15] - Atacs Intencionats - Modificació de la informació	100%	100%	10	10				
[A16] - Atacs Intencionats - Introducció d'informació falsa	100%	100%	20	20				
[A17] - Atacs Intencionats - Corrupció de la informació	100%	100%	10	10				
[A18] - Atacs Intencionats - Destrucció de la informació	100%	60%	10	6				
[A19] - Atacs Intencionats - Divulgació de la informació	100%	60%	10	6				

En global, estem parlant d'una reducció del risc d'uns 4.192 €/anuals.

5.1.1.5 Sistema d'Alimentació elèctrica ininterrompuda (S.A.I)

Aquest equipament es troba a la sala de servidors i ens permet garantir durant dues hores el subministrament elèctric dels equips informàtics i de comunicacions, per tant, tots el portàtils de la organització (tant els de la delegació central com els del personal desplaçat) poden accedir a la informació, tot i que es produeixin talls puntuals en la central. La efectivitat d'aquest control és del 90%.

Actiu/*Amenaces*	Salvaguarda preventiva (Percentatge de disminució)	Salvaguarda curativa (Percentatge de disminució)	Freqüència Intrínseca	Freqüencia residual * Percentatge de disminució impacte	Valor	Risc Intrínsec	Risc Efectiu	Reducció del risc
EA-S.Elec					300.000 €	1.315 €	575 €	740 €
[N1] - Desastres Naturals - Foc	100%	100%	0,1	0,1				
[N2] - Desastres Naturals - Inundacions	100%	100%	0,2	0,2				
[N] - Desastres Naturals - Desastres Naturals*	100%	100%	0	0				
[I1] - Industrials - Foc	100%	100%	0,1	0,1				
[I2]- Industrials - Inundacions	100%	100%	0,2	0,2				
[I] - Industrials - Desastres Industrials*	100%	100%	0	0				
[I3] - Industrials - Contaminació mecànica	100%	100%	0	0				
[I4] - Industrials - Contaminació electromagnètica	100%	100%	0	0				
[I5] - Industrials - Avaria d'origen físic o lògic	100%	100%	0,2	0,2				
[I6] - Industrials - Tall del subministrament elèctric	100%	10%	1	0,1				
[I7] - Industrials - Condicions inadequades de temperatura i humitat	100%	100%	0	0				
[I9] - Industrials - Interrupció d'altres serveis i subministraments essencials	100%	100%	0	0				
[A7] - Atacs Intencionats - Us no previst	100%	100%	0	0				
[A11] - Atacs Intencionats - Accés no autoritzat	100%	100%	0	0				
[A25] - Atacs Intencionats - Robatori	100%	100%	0,1	0,1				
[A26] - Atacs Intencionats - Atac Destructiu	100%	100%	0,1	0,1				
[A27] - Atacs Intencionats - Ocupació Enemiga	100%	100%	0	0				

Aquest element, segons l'anàlisi realitzat, repercuteix en 740 €/anuals en els actius que depenen del subministrament elèctric.

5.1.1.6 Anàlisis de riscos residual

Tenint en compte els diferents criteris indicats, el risc residual de l'organització és el següent:

Actiu/Amenaces	Valor	Risc Intrínsec	Risc Efectiu	Reducció del risc
Data-Form	75.000 €	1.510 €	1.119 €	391 €
Data-V.S	300.000 €	54.460 €	54.423 €	37 €
Data-Proc.Int	30.000 €	2.746 €	2.193 €	553 €
Data-Conta	30.000 €	604 €	448 €	157 €
Data-Comer	75.000 €	1.510 €	1.119 €	391 €
Data-Prv	300.000 €	6.041 €	3.637 €	2.404 €
Data-Contr.Clie	300.000 €	5.055 €	3.378 €	1.677 €
Data-Contr.Prov	300.000 €	5.055 €	3.378 €	1.677 €
Apl-Win.Srv	300.000 €	47.638 €	46.812 €	826 €
Apl-Win.XP	300.000 €	47.638 €	46.812 €	826 €
Apl-IIS	300.000 €	47.638 €	46.812 €	826 €
Apl-Ms.SQL	300.000 €	47.638 €	46.812 €	826 €
Apl-PREV	300.000 €	47.638 €	46.812 €	826 €
Apl-Ms.Ex.Srv	300.000 €	47.638 €	46.812 €	826 €
Apl-NFS	300.000 €	47.638 €	46.812 €	826 €
Apl-Conta	300.000 €	47.638 €	46.812 €	826 €
Apl-MS.OFF	300.000 €	47.638 €	46.812 €	826 €
EA-S.Elec	300.000 €	1.315 €	575 €	740 €
Inst -E.C	300.000 €	8.219 €	8.219 €	0 €
Inst -D.T	300.000 €	8.219 €	8.219 €	0 €
Inst -U.M	150.000 €	966 €	966 €	0 €
HW-PC	300.000 €	45.904 €	45.719 €	185 €
HW-Rou.Cen	300.000 €	45.904 €	45.719 €	185 €
HW-SW.Cen	300.000 €	7.948 €	7.245 €	703 €
HW–Rou.DT	300.000 €	7.948 €	7.245 €	703 €
HW-BB	150.000 €	3.974 €	3.623 €	351 €
HW-PT	300.000 €	46.068 €	46.068 €	0 €
HW-Srv.Cor	300.000 €	8.277 €	7.586 €	690 €
HW-Srv.PREV	300.000 €	8.277 €	7.586 €	690 €
X-WAN	300.000 €	54.460 €	54.460 €	0 €
X-LAN	300.000 €	54.460 €	54.460 €	0 €
SRV-NFS	10.000 €	270 €	239 €	31 €
SRV-DIR	300.000 €	8.096 €	7.171 €	925 €
SRV-MAIL	75.000 €	2.024 €	1.793 €	231 €
SRV-V.S	75.000 €	10.510 €	10.470 €	40 €
SRV-PREV	30.000 €	810 €	717 €	92 €
SRV-WEB	10.000 €	270 €	239 €	31 €
SRV-IMPRES	150.000 €	20.774 €	20.774 €	0 €
Per-D.Comer	150.000 €	82 €	82 €	0 €
Per-D.Prev	75.000 €	2.466 €	2.466 €	0 €
Per-Comer	150.000 €	82 €	82 €	0 €
Per-D.V.S	150.000 €	82 €	82 €	0 €
Per-I.V.S	150.000 €	82 €	82 €	0 €
Per-D.Fin	75.000 €	41 €	41 €	0 €
Per-Tec.TIC	300.000 €	164 €	164 €	0 €
Per-Resta	300.000 €	164 €	164 €	0 €
Total	**10.010.000 €**	**853.584 €**	**833.266 €**	**20.318 €**

5.2 Organització del sistema de seguretat de la informació

En el present projecte *PREVENCIO S.L.* ha de definir la estructura de seguretat de la empresa amb el suport que *AUDITORIA S.L.* li facilitarà com a referencia en implantació de Sistemes de Gestió de Seguretat de la Informació.

Ja s'ha definit els participants del comitè de gestió. Ara s'haurà de definir el rol d'aquest grup, el qual serà 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 en el *SGSI* i assegurar que s'han implantat els controls pactats.

Un cop definit els rols del comitè de seguretat, ha de definir conjuntament una política de seguretat específica de *PREVENCIO S.L* on s'han d'incloure els següents elements:

- Ha de quedar clar què és el que es vol protegir, de qui o 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 dins de la política i que són els primers que en fan seguiment.

El document resultant està dirigit a tot el personal de la organització, i per tant ha de ser accessible i am un llenguatge no molt tècnic, i on es definirà com entén la organització les principals dimensions de seguretat: autenticitat, confidencialitat i integritat.

En el document de la política de seguretat s'han d'incloure els aspectes més importants que s'han detectat durant la fase de anàlisis de riscos. En el nostre cas, principalment la importància de la protecció en l'accés des de l'exterior amb els equips de la organització i la necessitat de documentar els diferents processos de la organització tenint en compte les mesures de seguretat associada.

L'elaboració d'aquest document recau en tot el personal que forma el comitè de seguretat, encara que la seva redacció anirà a càrrec del responsable de seguretat.

S'haurà de formar un comitè de coordinació de la seguretat. Si no es pot assignar més personal del que s'està dedicant al comitè de gestió, llavors s'haurà de formar amb el mateix personal que el comitè de gestió i una de les persones de la empresa que es dediqui al manteniment del sistema informàtic. Aquest comitè haurà d'assegurar que les activitats de seguretat s'estan realitzant d'acord amb la política de seguretat, implantar les mesures de seguretat determinades per el comitè de gestió, aportar informació sobre la implantació i funcionament de les mesures de seguretat i recomanar les mesures de resposta a incidents en base a la monitorització del sistema.

Aquest comitès es reuniran cada sis mesos, tal i com es va definir en el objectiu del pla director.

La implantació del sistema de gestió de seguretat de la informació tindrà un cost inicial durant el primer any i un cost fixe associat a les tasques de coordinació que es realitzaran durant les reunions periòdiques que es realitzaran.

A nivell d'assessorament extern, el suport associat al comitè de seguretat tindrà un cost inicial de 50 hores el primer any i un cost de 20 hores anuals, sense tenir en compte les diferents auditories programades i la presentació i/o execució de nous projectes que s'acordin amb el responsable de seguretat.

A nivell intern estimem que *PREVENCIÓ S.L.* tindrà un cost inicial de 100 hores el primer any en la definició dels diferents comitès i la redacció de la política de seguretat, i un cost anual de 50 hores en la presentació dels incidents de seguretat i la pressa de decisions que es realitzaran en la reunió del comitè.

El cost de la implantació de la solució és el següent:

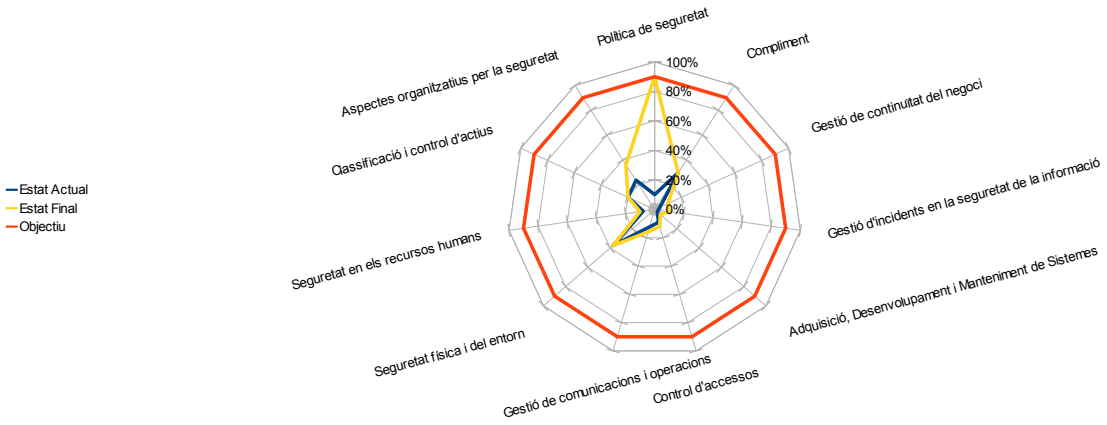
Concepte	**Cost (€)**
Assessorament extern	5.000
Dedicació personal intern	10.000
Total	**15.000**

El cost anual és el següent:

Concepte	**Cost (€/any)**
Assessorament extern	2.000
Dedicació personal intern	5.000
Total	**7.000**

Durant els sis primers mesos es realitzarà la organització del sistema de seguretat i la definició de la política de seguretat. Un cop implantat, la gestió és anual.

5.2.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	90%	90%
Aspectes organitzatius per la seguretat	24%	36%	90%
Classificació i control d'actius	20%	20%	90%
Seguretat en els recursos humans	8%	10%	90%
Seguretat física i del entorn	37%	37%	90%
Gestió de comunicacions i operacions	12%	16%	90%
Control d'accessos	9%	12%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	5%	90%
Gestió d'incidents en la seguretat de la informació	3%	10%	90%
Gestió de continuïtat del negoci	4%	10%	90%
Compliment	30%	30%	90%

Aquest projecte bàsicament marca la direcció en el que es gestionarà i supervisarà el *SGSI*. Marca la política que es definirà a tota la organització. Aquesta definició de la política fa que alguns dels controls siguin com a mínim reconeguts.

5.2.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

Segons les estimacions que hem realitzat en la avaluació de les salvaguardes, la millora en la organització ha de tenir un increment directe en tots el actius de la organització. Es tracta d'una fase inicial i simplement ens permetrà dirigir les mesures sobre els diferents actius, per tant, es tracta d'una millora qualitativa en els controls que s'estan realitzant i en els que s'introduiran.

És difícil de valorar aquesta salvaguarda, ja que es tracta d'un valor intangible, ja que es tracta d'una millora qualitativa. Ho considerarem com un 10 % dins de les diferents mesures que es realitzaran per documentar els procediments, coordinar i valorar les accions de seguretat que es realitzen dins de la organització. Per tant, ho considerarem com un 2 % dins de les salvaguardes preventives.

Amb aquest criteri, en la situació actual de seguretat, representa aproximadament 16.000 €/anuals de reducció del risc general, respecte al cost de dedicació anual, estaríem parlant d'uns beneficis de 9.000 € anuals.

La inversió inicial és de 15.000 € , per tant, si realitzem l'amortització a 3 anys vistes, 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 €

Podem veure que la viabilitat d'aquest projecte és alta, ja que els números de benefici són bastants significatius, i la majoria dels costos es realitzen amb la gestió dels recursos de personal intern.

5.3 Integració de la gestió de la seguretat dins de l'organització. Documentació procediments interns.

La gestió de la seguretat ha de ser un procés de millora continua. Quasi en total seguretat podem afirmar que no podrem cobrir mai el 100% de les amenaces que es puguin materialitzar en la nostra entitat, però amb un sistema madur minimitzarem els riscos, millorarem el temps de resposta i sabrem com actuar en cas de que es produeixen.

PREVENCIO S.L és una organització que dins de la seva activitat de negoci analitza les mesures de seguretat que s'han de prendre per evitar accidents i malalties laborals. Existeix unes normatives *ISO* sobre prevenció de riscos, la família, 14000 i especialment la 14001, que basen la seva metodologia de treball en un cicle de millora continua (*PDCA*). El departament de prevenció pot estar avesat a utilitzar aquest tipus de procediment, encara que no utilitzi actualment aquestes normatives.

Per tant, ens trobem amb uns procediments similars al que pot utilitzar l'àrea de prevenció. Amb l'assessorament tecnològic pertinent els tècnic de prevenció poden participar en aquesta gestió de la seguretat de manera similar a com es realitza per la prevenció de riscos laborals.

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, no en els processos de manteniment dels sistemes informàtics.

Específicament 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, valor dins del negoci.

Es posaran les bases per classificar els diferents actius de la informació i identificar tots els processos al que es troben sotmesos la informació des de la seva generació fins a la seva destrucció (si es que es requereix destruir la informació), tant en la part de recollida, com en el transport de la informació, com en la comunicació a terceres parts.

Aquesta documentació dels procediments s'ha de basar en la definició de la política de seguretat.

En la definició dels diferents procediments, caldrà la col·laboració de diferent personal de la organització, tant en la seva elaboració inicial com en el manteniment periòdic dels procediments, per que s'identifiquin 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*

El cost intern per la elaboració dels diferents procediments de la informació estimem que repercutirà a unes dues persones per àrea de la empresa (8 persones), amb un cost associat del 5% del seu temps de treball (4 hores/quinzena), durant el primer any. Per tant, estem parlant aproximadament d'unes 770 hores.

Un cop definits els diferents procediments de seguretat, el que s'haurà de fer periòdicament és revisar la vigència i/o les modificacions dels diferents procediments. Per aquesta tasca només caldrà una dedicació anual d'unes 15 hores per àrea, per tant, unes 60 hores/anuals

Per el desplegament del primer any, *AUDITORIA S.L.* farà un procés de revisió sobre els procediments definits, tenint en compte principalment si realment van alineats amb la política de

seguretat de l'empresa. En anys posteriors, dins del procés d'auditoria es farà una lectura en un profunditat menor, en base a les entrevistes que és realitzi amb els diferents directors d'àrea en les auditories biennals planificades per el compliment de la *LOPD*.

Estem parlant d'unes 50 hores per el desplegament de la solució i unes 10 hores anuals associades a l'auditoria.

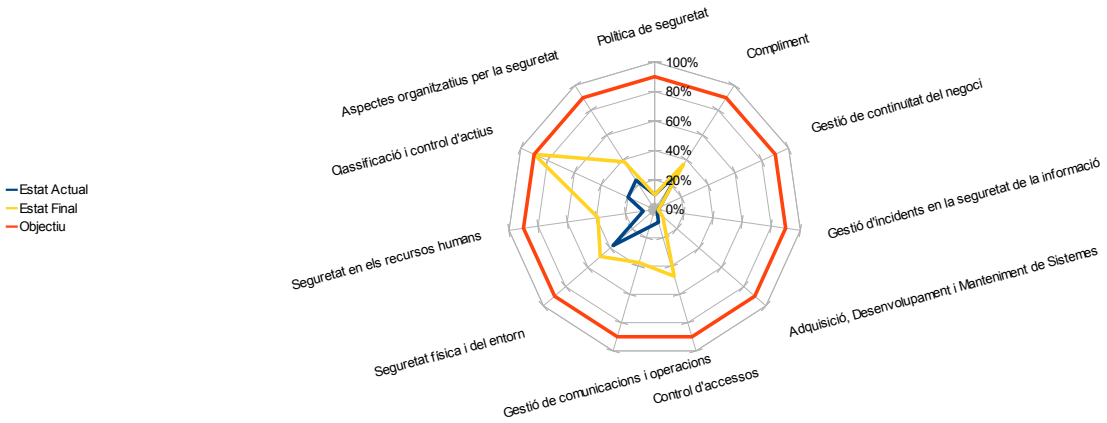
Per tant, el cost de la implantació de la solució és el següent:

Concepte	**Cost (€)**
Assessorament extern	5.000
Dedicació personal intern	77.000
Total	**83.000**

El cost anual és el següent:

Concepte	**Cost (€/any)**
Assessorament extern	1.000
Dedicació personal intern	6.000
Total	**7.000**

5.3.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	10%	90%
Aspectes organitzatius per la seguretat	24%	38%	90%
Classificació i control d'actius	20%	90%	90%
Seguretat en els recursos humans	8%	39%	90%
Seguretat física i del entorn	37%	49%	90%
Gestió de comunicacions i operacions	12%	38%	90%
Control d'accessos	9%	47%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	7%	90%
Gestió d'incidents en la seguretat de la informació	3%	3%	90%
Gestió de continuïtat del negoci	4%	4%	90%
Compliment	30%	36%	90%

En aquest projecte apareixen tres grans fites:

- Classificar els actius per que siguin identificables i disposin d'un responsable associat en cas de que es materialitzi una amenaça.
- Definir els diferents procediments que afecten a la seguretat de la organització. Es per això que aquest projecte impacta en quasi tots els dominis de la organització.
- Disposar d'una política de bon ús del material informàtic, tenint en compte que la majoria treballa fora de les instal·lacions pròpies.

5.3.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

En aquest projecte es defineixen les mesures necessàries per reduir la freqüència d'aparició d'incidents de seguretat i la seva gestió en cas de que es produeixin.

Tal i com hem estimat les salvaguardes del bon govern de la seguretat de la informació, aquest tipus de salvaguarda tenen una incidència significativa en la millora de la seguretat de la informació. A nivell global hem valorat al voltant del 20 % tant les mesures preventives com les organitzatives que es realitzen en aquest aspecte.

El procés de desenvolupament inicial difícilment tindrà la incidència indicada, però ens trobarem en un procés de millora continua en la que podrem anar millorar el diferents procediments associats.

En una fase inicial del projecte, valorarem a nivell la incidència que pugui tenir en les diferents amenaces aproximadament en un 10% sobre el risc dels actius, incidint especialment en la classificació que hem realitzat de les salvaguardes. Aquest percentatge haurà de millorar a mesura que *PREVENCIÓ S.L* tingui un *SGSI* més madur, però aquesta millora no es troba inclosa dins dels càlculs que realitzarem.

Tenint en compte aquest criteri, l'impacte sobre el risc de la organització és de 138.685 € anuals.

Es evident que aquest projecte és molt beneficiós per la organització, veiem el retorn de la inversió, incloent una amortització a 3 anys.

	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 €

De la mateixa manera que en el projecte d'organització del sistema de seguretat, la viabilitat d'aquest projecte és alta, ja que els números de benefici són bastants significatius, i la majoria dels costos es realitzen amb la gestió dels recursos de personal intern.

5.4 Revisió de les relacions contractuals

En els anàlisis realitzats s'han detecta varies deficiències respecte a les diferents relacions contractuals de *PREVENCIÓ* amb els diferents actors que intervenen en els processos de gestió dels actius.

- 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, ja que és el criteri actual per diferenciar la informació.
- 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...

  A nivell general, en els diferents proveïdors contractats que intervinguin directament en el tractament de la informació 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 i la possibilitat d'auditar els serveis oferts.

  Per la resta de proveïdors (p.e serveis de neteja, manteniment instal·lacions), en la mesura del possible, s'ha de fer constar una clàusula de confidencialitat sobre l'accés a les dades de la empresa.
- Clients: El client és el que ens facilita les instal·lacions per el serveis de vigilància de la salut, en les quals s'haurien d'incloure unes mesures mínimes per protegir les dades sensibles amb les que tracta l'empresa. A més moltes vegades és el transmissor de la informació de les revisions mèdiques que es faciliten als treballadors. Per tant ha de constar com és facilitarà aquesta informació i quines mesures es s'adopten per garantir la confidencialitat de la informació.

En aquest cas es revisaran les diferents relacions contractuals amb els diferents actors per que aquestes condicionants quedin incloses en els nous contractes o revisions que s'hagin de realitzar.

Per la revisió dels diferents models és subcontractarà una assessoria laboral. Estem parlant d'uns 10 -15 tipus de contracte, els quals en total comportarien unes 60 hores de treball.

A nivell intern, valoraríem els esforços associats en unes 10 hores, per disposar dels coneixements per aquest tipus de contractes. Anualment, hem dedicarem unes dues hores.

Un cop realitzada aquesta revisió, es probable que requerim la revisió/creació de nous contractes. Estimarem que s'han de revisar/crear uns dos contractes anuals, per tant, ens reservarem unes 8 hores anuals en serveis d'assessoria.

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*, especialment l'apartat *2.2.1 Análisis de Contratos*, el qual marca les consideracions principals que hem de realitzar en la avaluació de qualsevol contracte. També és interessant que es considerés l'apartat *2.8 Gestión de Riesgos* que utilitza una metodologia molt similar a la que hem utilitzat en l'avaluació del estat del risc de seguretat dels actius de la organització.

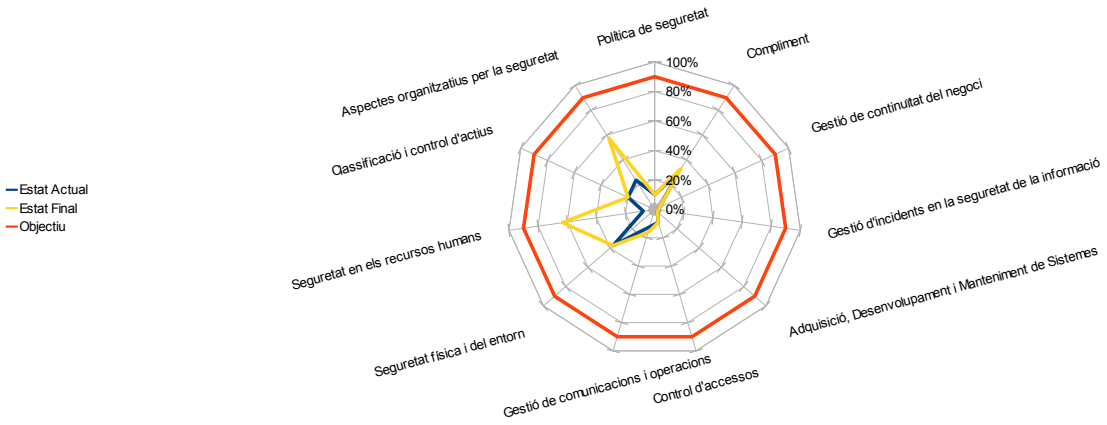
Per tant, el cost de la implantació de la solució és el següent:

Concepte	**Cost (€)**
Assessorament extern	6.000
Dedicació personal intern	1.000
Total	**7.000**

El cost anual és el següent:

Concepte	**Cost (€/any)**
Assessorament extern	800
Dedicació personal intern	200
Total	**1.000**

5.4.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	10%	90%
Aspectes organitzatius per la seguretat	24%	58%	90%
Classificació i control d'actius	20%	20%	90%
Seguretat en els recursos humans	8%	63%	90%
Seguretat física i del entorn	37%	37%	90%
Gestió de comunicacions i operacions	12%	16%	90%
Control d'accessos	9%	9%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	2%	90%
Gestió d'incidents en la seguretat de la informació	3%	3%	90%
Gestió de continuïtat del negoci	4%	4%	90%
Compliment	30%	33%	90%

Aquest projecte també te un impacte en els diferents dominis, ja que es revisen les diferents relacions contractuals. La maduresa real d'aquest projecte s'anirà materialitzant a mesura que es vagin aplicant els nous contractes.

5.4.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

Dins d'aquest projecte s'aborden salvaguardes associades a les condicions contractuals de seguretat, nivells d'acord de servei, nivells d'acords de confidencialitat amb proveïdors, i l'assumpció de responsabilitats per incompliments de contracte.

Amb aquestes mesures introduïdes esperem assolir aproximadament un 75 % sobre l'impacte que hem associat a les salvaguardes associades. Tenint en compte la valoració global de les salvaguardes, ens surt la següent millora respecte el risc associat anual d'uns 6.375 €.

Farem el càlcul d'amortització tenint en compte que s'apliquen els canvis en notes les relacions contractuals en el mateix any. Això en la pràctica no serà així, ja que dependrà de si es poden revisar les relacions contractuals, si es canvia de personal i de clients , etc...

	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 €

5.5 Implantació d'un sistema de gestió incidental

És necessari conèixer els diferents events que es produeixen en la nostra organització, per poder avaluar amb coneixement de causa les amenaces que es produeixen en la nostra entitat.

Per poder registrar les diferents amenaces caldrà disposar d'una plataforma on es registri aquesta informació i que sigui accessible per tots els empleats.

S'implantarà un sistema de gestió incidental, en format *Web*, aprofitant els recursos tecnològics que disposem. Existeixen moltes alternatives en el mercat, moltes d'elles gratuïtes, però hem de buscar la solució que s'adeqüi millor a les necessitats de *PREVENCIO S.L,* que sigui de fàcil ús per tota l'organització i que no comporti una càrrega excessiva en el manteniment tecnològic de la solució.

Optarem 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.

Aquest projecte requerirà de les següents tasques per la seva implantació:

- Instal·lació i configuració del software associat: 20 hores
- Categorització dels diferents tipus d'incidents: 10 hores
- Procediment: Es definirà l'ús d'aquesta eina per els empleats de la organització: 10 hores per els empleats.
- Suport en el ús de l'eina dels empleats: 10 hores

Un cop implantat el sistema és realitzaran les següents tasques en l'us de la eina:

- Reporting d'incidents. Estimarem que es gastaran unes 20 hores/anuals entre tots els empleats en registrar els incidents de seguretat.
- Documentació de la resolució d'incidents. Considerarem que es gasten unes 50 hores/anuals en detallar les accions resolutores de la incidència.
- Anàlisis dels incidents. Aquesta tasca serà proporcional al volum d'incidents que es reportin. Seran la base per ajustar l'anàlisi de riscos i les mesures correctores associades. Ho valorarem en 20 hores/anuals.

Aquesta informació serà accessible per la empresa que es contracti en els serveis d'auditoria, la qual dedicarà unes 20 hores en cadascuna de les auditories biennals que es realitzin.

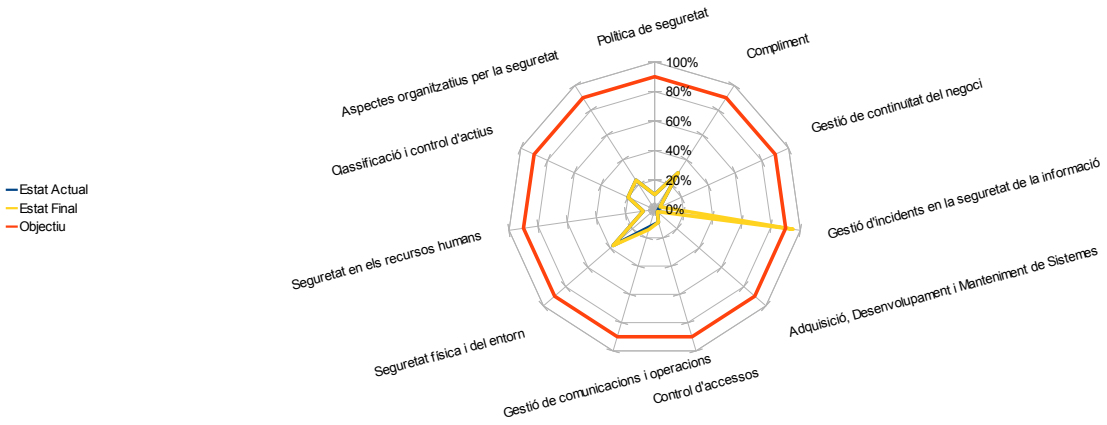
El cost de la implantació de la solució és el següent:

Concepte	**Cost (€)**
Instal·lació i Configuració	2.000
Documentació	2.000
Formació	1.000
Total	**5.000**

El cost anual és el següent:

Concepte	**Cost (€/any)**
Reporting	2.000
Documentació	5.000
Anàlisi	2.000
Auditoria	1.000
Total	**10.000**

5.5.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	10%	90%
Aspectes organitzatius per la seguretat	24%	24%	90%
Classificació i control d'actius	20%	20%	90%
Seguretat en els recursos humans	8%	8%	90%
Seguretat física i del entorn	37%	37%	90%
Gestió de comunicacions i operacions	12%	14%	90%
Control d'accessos	9%	9%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	2%	90%
Gestió d'incidents en la seguretat de la informació	3%	95%	90%
Gestió de continuïtat del negoci	4%	4%	90%
Compliment	30%	30%	90%

L'impacte sobre la maduresa del sistema de gestió es troba clarament marcada en el domini de gestió d'incidents de seguretat, ja que estem dotant de l'eina necessària per realitzar la gestió. Es tracta d'una base de coneixement que ens permetrà millorar la resolució d'incidents i que es requereix per els anàlisis d'auditories posteriors.

5.5.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

Aquesta projecte hem considerat que tindrà un benefici transversal en totes les mesures correctives de seguretat que es realitzin en la organització, ja que permetrà disposar d'un sistema on poder consultar la evolució de la incidència i una base d'experiència per la resolució de noves incidències que es reprodueixen. Millorem a nivell general la gestió del sistema.

La inclusió d'aquest control no comporta directament que es revisin els sistemes, sinó l'eina a traves de la qual es pot registrar i classificar els incidents de seguretat i que és consultable per les diferents persones involucrades en la seguretat de la empresa i auditors externs.

La eficiència inicial d'aquest servei serà d'un 60 % respecte el grau òptim en els primers anys, per tant, el benefici actual sobre el global dels actius afectats estarà al voltat del 3%, segons la valoració global que hem realitzat de les salvaguardes.

Segons aquest criteri, la reducció del risc en la influència en les salvaguardes associades és de 25.458 € anuals.

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 €

5.6 Solucions de seguretat d'accés des de l'exterior

PREVENCIO S.L no disposa de mecanismes de protecció de la informació a banda del xifrat propietari de l'aplicació *PREVENET.*

S'han d'aplicar diferents mesures de seguretat que ens permeti controlar l'accés des de l'exterior amb diferents eines.

Hem de tenir en compte que *PREVENCIO S.L.* vol tenir uns costos reduïts per el desplegament de solucions tecnològiques. Per tant s'haurà de buscar una solució de compromís amb el pressupost assignat i al coneixement tecnològic que disposa la organització.

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

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

PREVENCIÓ S.L. requereix establir un accés segur per la connexió del correu, el qual s'envia a traves del seu client *Outlook*. Existeixen solucions *hardware* per la implantació de *VPN,* però descartarem aquestes alternatives ja que solen requerir un inversió major. S'optarà per utilitzar l'equip també com *firewall* de la organització ja que la seva funció principal serà de canal d'entrada d'usuaris a la xarxa i per reduir costos.

Optarem per la utilització d'un servidor *VPN Windows 2003* 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 no ha de un nombre reduït d'usuaris.
- Es tracta de la mateixa plataforma per tots els servidors de la organització, facilitant l'aprenentatge dels administradors per les mesures de control.
- S'integra amb el sistema d'autentificació i la gestió de polítiques del sistema operatiu.

El cost del software associat estarà al voltant dels 1.000 €. El cost de llicenciament d'un sistema *Windows 2008* estarà al voltant dels 725 €, incloent 5 llicències d'usuari.

El cost de 5 llicencies addicionals costa uns 150 €. Tenint en compte que estimem una concurrència d'uns 100 usuaris, estaríem parlant en total d'uns 2.850 € addicionals.

La instal·lació, configuració i distribució de la configuració, i documentació d'usuaris de la *VPN* estaria sobre les 100 hores.

Anualment es dedicarien 40 hores en el manteniment de la plataforma, on constarien en la revisió de les connexions, manteniment del servidor i incidències d'usuaris associades a les connexions *VPN.*

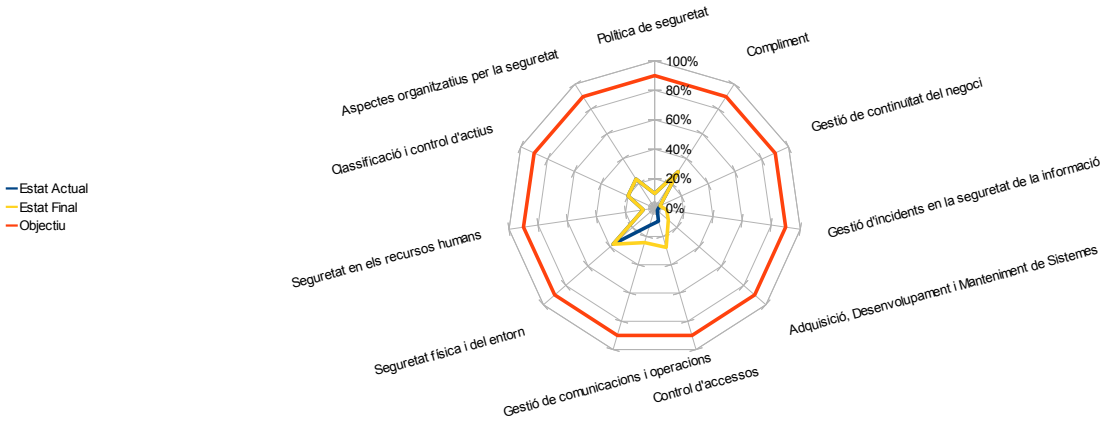
El cost de la implantació de la solució és el següent:

Concepte	**Cost (€)**
Instal·lació, configuració, documentació	10.000
Hardware	1.000
Llicenciament	3.575
Total	**14.575**

El cost anual és el següent:

Concepte	**Cost (€/any)**
Manteniment	4.000
Total	**4.000**

5.6.1.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	10%	90%
Aspectes organitzatius per la seguretat	24%	24%	90%
Classificació i control d'actius	20%	20%	90%
Seguretat en els recursos humans	8%	8%	90%
Seguretat física i del entorn	37%	37%	90%
Gestió de comunicacions i operacions	12%	24%	90%
Control d'accessos	9%	28%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	12%	90%
Gestió d'incidents en la seguretat de la informació	3%	8%	90%
Gestió de continuïtat del negoci	4%	4%	90%
Compliment	30%	30%	90%

Aquest projecte per un costat, introdueix el xifrat dins de les eines que utilitza *PREVENCIO S.L.* i per tant introdueix la gestió de claus que es distribueixen a traves de les polítiques del sistema operatiu, protegint el canal d'informació

Per un altra banda, s'aprofità per no exposar els servidors de la organització a possibles atacs externs i que la informació quedi registrada en un dispositiu de control. Només es pot accedir a la informació a traves dels clients *VPN* que hem definit i limita el control d'accés a la informació.

Al incloure el canal *VPN*, també estem protegint la missatgeria electrònica, factor que incorporem en el control associat.

5.6.1.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

La influència de la connexió *VPN* es una solució de xifrat de la informació en el canal de comunicació des de l'exterior. Es tracta d'una salvaguarda preventiva. Per tant, afecta directament al element de xarxa *X-WAN* i als actius que depenen d'aquesta configuració. Aquesta salvaguarda cobreix el 95% de la prevenció del risc de les amenaces que utilitzen el medi associat per realitzar la escolta i/o modificació de la informació.

La instal·lació del *firewall* i la segmentació de la xarxa també afecta a la part associada a la xarxa local (*X-LAN*), ja que controlarem l'accés als servidors centrals que es troben en aquesta xarxa, i no permetrem l'accés als equips d'usuaris ubicats a la central. Aquesta part del projecte ho inclourem com a salvaguarda correctiva, ja que tracta de minimitzar els atacs que es materialitzin. Aquesta solució cobreix el 50 % d'exposició del actiu en les amenaces associades

Tenint en compte les consideracions indicades, la reducció del risc que comporta aquest projecte és de 54,974 € anuals (32.371 € per les connexions remotes i uns 22.603 € per els accessos des de la xarxa local

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	4.859 €	4.859 €	4.859 €		
Benefici brut	54.974 €	54.974 €	54.974 €	54.974 €	54.974 €
Benefici net	46.115 €	46.115 €	46.115 €	50.974 €	50.974 €

Si incloguéssim la renovació del sistema de seguretat d'accés al exterior en un període de 5 anys, durant els quals es realitza l'amortització de la solució, ens quedaria la següent taula.

	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 €

5.6.2 Detecció Intrusions. Instal·lació *IDS*

L'accés des de l'exterior s'està realitzant a través del *router* que ens proporciona el nostre proveïdor d'Internet.

No s'està realitzant cap mesura de seguretat ni cap control sobre el tràfic de dades que passa a traves d'aquest element *hardware.*

En aquest projecte es considera que s'ha realitzat un muntatge previ d'un *firewall* i s'ha realitzat una segmentació, tal i com s'ha presentat en el projecte de configuració de *VPN*. Per tant, aquest projecte es basa en que ja existeixi aquest muntatge.

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.

En aquest cas optarem per una solució amb sense cap cost de llicència de *software*. Hem 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*). No s'ha optat per una solució basada en *Windows 2003* ja que la solució que utilitza per la detecció d'intrusos és *Microsoft ForeFront,* la qual requereix un llicenciament addicional.

Per la utilització d'aquestes eines d'anàlisis i de monitorització es requereixen certs coneixements tecnològics (independentment de la tecnologia que utilitzem). En la valoració sobre com impacta en mitigar la materialització de les amenaces i en la maduresa dels controls es suposarà que s'estan realitzant les revisions periòdiques pertinents, detectant les intrusions en el sistema i que es realitzen les mesures oportunes.

La instal·lació del equip tindrà un cost associat de 10 hores. L'estudi de les diferents eines i la seva configuració associada tindrà un cost addicional de 40 hores.

Anualment es dedicarà unes 40 hores en la revisió del *logs* associats i en la solució dels incidents de seguretat associats.

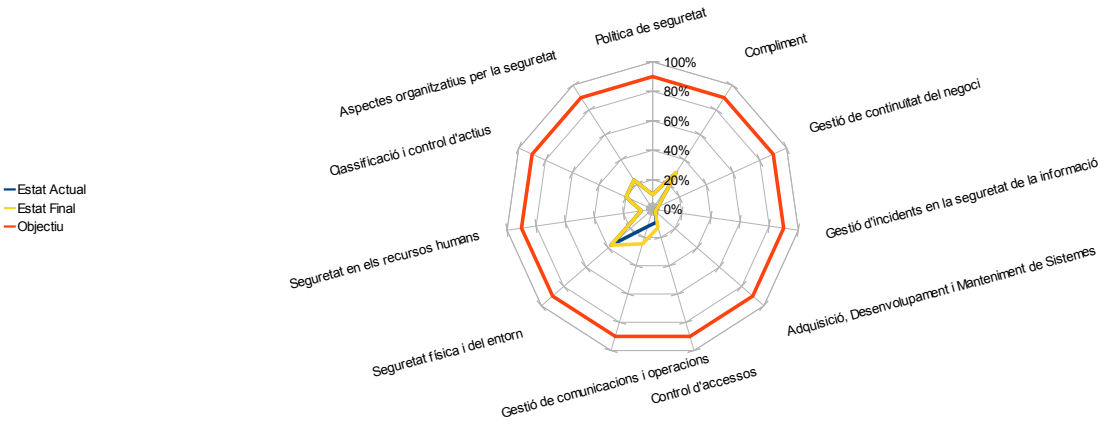
El cost de la implantació de la solució és el següent:

Concepte	**Cost (€)**
Instal·lació, configuració, documentació	5.000
Hardware	1.000
Total	**6.000**

El cost anual és el següent:

Concepte	**Cost (€/any)**
Manteniment	4.000
Total	**4.000**

5.6.2.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	10%	90%
Aspectes organitzatius per la seguretat	24%	24%	90%
Classificació i control d'actius	20%	20%	90%
Seguretat en els recursos humans	8%	8%	90%
Seguretat física i del entorn	37%	37%	90%
Gestió de comunicacions i operacions	12%	25%	90%
Control d'accessos	9%	13%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	2%	90%
Gestió d'incidents en la seguretat de la informació	3%	3%	90%
Gestió de continuïtat del negoci	4%	4%	90%
Compliment	30%	30%	90%

La maduresa que introdueix aquest control és molt especifica. Ens permet identificar amb major precisió quines connexions que es realitzen des de el exterior tenen un comportament anòmal, per tant, podem actuar en conseqüència.

5.6.2.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

La introducció d'un sistema de detecció d'intrusos ens permetrà detectar aquells atacs que es produeixen des de l'exterior i realitzar les mesures correctives associades. Aquest element per si sòl no realitza cap mesura correctiva.

Per tant, podrem controlar amb major precisió quina és la freqüència d'ocurrència de les amenaces des de l'exterior, facilitant els anàlisis posteriors que realitzem de la seguretat a la nostra organització i poder aplicar altres mesures correctives.

La inclusió d'aquesta eina és útil per les mesures correctives que haguem d'aplicar amb una certa celeritat, ja que ens permetrà analitzar d'on provenen els atacs i aplicar mesures, per exemple, en el *firewall* de la organització.

Per tant, en base a la seva utilitat, valorarem l'impacte sobre les amenaces que es puguin realitzar des de l'exterior en un 30% d'eficàcia. Si valorem la possibilitat d'incorporar funcionalitats d'IPS, incrementarà el cost de manteniment i de desplegament, però augmentarà la eficàcia de la solució.

Segons l'anàlisi realitzat, la seva reducció del risc és de 16.121 € anuals.

	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	4.000 €	4.000 €	4.000 €	4.000 €	4.000 €
Amortització	2.000 €	2.000 €	2.000 €		
Benefici brut	16.121 €	16.121 €	16.121 €	16.121 €	16.121 €
Benefici net	10.121 €	10.121 €	10.121 €	12.121 €	12.121 €

Si apliquem la opció de renovació i de revisió de la solució cada 5 anys, tal i com hem fet en el projecte *VPN*, llavors el retorn de la inversió queda de la següent manera:

	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 €

5.7 Millores en les infraestructures

5.7.1 Prevenció 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, ja sigui per una avaria en les instal·lacions o causada per els fenòmens meteorològics.

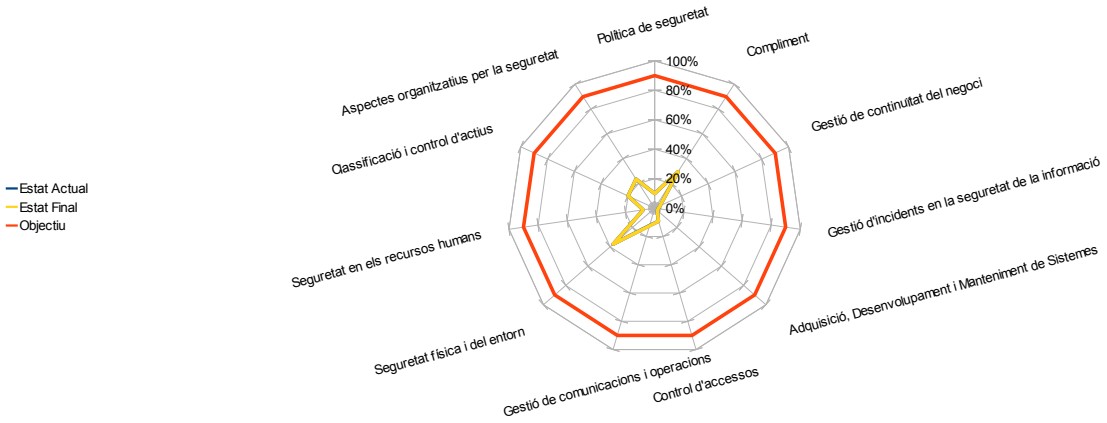
Es proposa la migració actual de les dades en la primera planta del edifici. Aquest canvi requerira que es realitzin les següents modificacions.

- Adaptació de la instal·lació elèctrica i de comunicacions del edifici. Cost estimat: 3.000 €
- Cost del Material associat 500 €
- Aturada del servei durant el procés de migració. Es realitzarà fora del horari laboral per personal tècnic. Entre planificació i trasllat es considera un cost aproximat d'unes 10 hores.
- Trasllat del mobiliari associat. Es contractarà personal extern per realitzar aquest transport, amb un cos associat de 500 €

Aquesta solució no té un cost de manteniment associat. Per tant, el cost de la implantació de la solució és el següent:

Concepte	**Cost (€)**
Material	500
Instal·lació elèctrica	3.000
Migració equips informàtics	1.000
Trasllat mobiliari	500
Total	**5.000**

5.7.1.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	10%	90%
Aspectes organitzatius per la seguretat	24%	24%	90%
Classificació i control d'actius	20%	20%	90%
Seguretat en els recursos humans	8%	8%	90%
Seguretat física i del entorn	37%	37%	90%
Gestió de comunicacions i operacions	12%	12%	90%
Control d'accessos	9%	9%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	2%	90%
Gestió d'incidents en la seguretat de la informació	3%	3%	90%
Gestió de continuïtat del negoci	4%	4%	90%
Compliment	30%	30%	90%

Curiosament, aquesta salvaguarda proposada no canvia la visió global de la maduresa dels controls de seguretat. Aquest escenari es produeix per que només aborda un aspecte de la seguretat física del entorn, i per tant no s'ha considerat que varies la maduresa actual del control com per saltar un esglaó addicional.

5.7.1.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

La salvaguarda que es comenta en el projecte té una incidència molt concreta sobre les amenaces associades. Cobreix gran part dels casos associats a inundacions (no contempla els casos en que es puguin produir goteres, però la incidència ja és més marginal. Per tant, estem parla d'una salvaguarda que es una mesura preventiva que afecta en un 95% del risc associat.

Aquesta salvaguarda afecta a diferents actius (edifici, instal·lació elèctrica, xarxes de comunicació, hardware...)

El resultat obtingut és el d'una reducció del risc anual de 781 €. Segons aquest resultat determinarem que no és prioritària realitzar aquesta inversió.

Segons l'anàlisi de retorn d'inversió, comprovem que durant els primers anys no es recupera la inversió realitzada.

	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 €

Aquest resultat ens porta a les següents reflexions:

- Perquè el benefici associat és tan reduït?

Les mesures realitzades amb la salvaguardes contra les inundacions afecten bàsicament a les dimensions de disponibilitat i traçabilitat. La majoria dels actius afectats hem prioritzat ponderar altres dimensions com la confidencialitat i la integritat. Ens hem basat en la definició de *MAGERIT* sobre quines dimensions afecten aquestes amenaces.

Hem de recordar que l'anàlisi ens dona una aproximació sobre l'impacte dels diferents riscos en el cas de materialització d'una amenaça i ens serveix per prioritzar les mesures de seguretat i realitzar una primera estimació de com repercuteix indirectament en els beneficis de l'empresa.

- Afecta una inundació a la integritat de les dades?

Habitualment no, ja que les còpies de *backup* es troben allotjades en ubicacions físiques diferents. En el cas de *PREVENCIO S.L.* no es compleix actualment aquesta premissa.

- És necessària aquesta inversió?

Tenint en compte la valoració en les diferents dimensions de seguretat que hem realitzat en el nostre anàlisis de riscos previ, existeixen projectes més prioritaris, però pel que hem vist la despesa associada no és molt gran, i un cop pagada l'amortització inicial existeix un benefici net per la empresa, ja que no requereix d'un manteniment associat.

En el cas de que canviessin la valoració en les diferents dimensions de seguretat dels nostres actius, pot canviar la estimació del risc actual.

5.7.2 Solució *Cloud Computing* dels servidors de *PREVENCIÓ S.L*

Farem un esment a aquest tipus de solucions, ja que es una de les alternatives que ens havíem plantejant per millorar les mesures de seguretat al delegar la seguretat física a un proveïdor extern.

Actualment s'està popularitzant la utilització de solucions de *Cloud Computing* (concretament, la possibilitat d'allotjar els nostres servidors en un proveïdor extern), el qual realitza les operacions de manteniment físic del servidor (electricitat, mesures físiques de seguretat, allotjament del *backup*).

És un tema que requereix un anàlisi en profunditat, ja que té un impacte sobre els contractes que es realitzessin amb el proveïdor que ofereix el servei, la validació de que aquest tercer està complint les mesures de seguretat exigides. També s'hauria d'analitzar com impacta 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 a nivell de capacitat de procés memòria, disc, velocitat de xarxa, i el temps que necessites que estiguin disponible els serveis i es solen facturar mensualment.

Es tracta d'una solució en una fase inicial. No tenim el detall de casos similars de *PYMES* que estiguin treballant amb aquestes alternatives, i actualment no disposem del temps i els coneixements necessaris per fer un anàlisis en profunditat que ens permeti valorar amb la necessària exactitud com impactaria en el anàlisis de riscos, els costos, i en els controls de seguretat, però considerem que és un tema a tenir present en les futures reunions del comitè de seguretat com alternativa a propostes de seguretat que es puguin plantejar, un cop la organització hagi assolit la suficient maduresa.

Cal dir que en les solucions d'aquest tipus, el manteniment del sistema operatiu i de les mesures de seguretat associades van a càrrec de la empresa contractant. En l'actualitat no recomanaríem aquest tipus de solució a *PREVENCIO S.L* ja que gran part de la informació més sensible es troba en format imprès i per tant en aquesta fase inicial de gestió de la seguretat són més prioritàries aplicar mesures en la seguretat física.

Només plantejaríem aquest tipus de solució si els costos associats a les mesures de seguretat física no es poguessin assumir, i en canvi si que es poguessin assumir solucions de núvol privat, o en el cas de que *PREVENCIÓ S.L.* es plantegi una solució de continuïtat de negoci, un cop el seu *SGSI* sigui suficientment madur.

5.8 Manteniment del sistema

5.8.1 Canvi en la política de gestió de *backups*

Aquesta mesura és bàsica per que ens puguem plantejar a curt o mig termini un pla de continuïtat del negoci. Hem de tenir en compte que *PREVENCIO S.L.* no pot dedicar molts recursos en els diferents aspectes de seguretat. A més, les dimensions de seguretat més prioritàries sobre les seves dades emmagatzemades són la confidencialitat i la integritat. Per tant, disposant de còpies de *backup* periòdiques en una ubicació diferent a la que es troba l'edifici central es podrà procedir a recuperar la informació.

La informació impresa es troba en armaris ignífugs i en molts casos només té validesa la informació original, per tant, les mesures de seguretat establertes per la informació impresa no es poden millorar substancialment, si no és digitalitza la informació.

Respecte a la informació digital que s'aborda en aquest projecte es proposa emmagatzemar-la en un suport físic diferent. S'enviaran periòdicament còpies a una ubicació física diferent a l'actual amb un sistema de transport que ens garanteixi la privacitat de les dades i encriptant les dades del dispositiu.

No es planteja en aquest projecte mesures en la eficiència del sistema de *backup*, el qual es realitza manualment. Només s'aborden les mesures necessàries per que la probabilitat de recuperar amb èxit una còpia de *backup* estigui al voltant del 99,9 %.

Utilitzarem una de les delegacions de la organització, per no contractar cap edifici addicional i aprofitarem els enviaments que es realitzen periòdicament des de les diferents delegacions cap a la central i viceversa per l'enviament de material utilitzat en els anàlisis de vigilància de la salut.

Definiren el procediment de *backup* per que es realitzi amb dispositius externs. Utilitzarem discos externs connectats via *USB* per utilitzar com a solució econòmica.

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 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 un 99,9 % dels casos que la pèrdua de dades serà com a màxim de la última setmana.

Es realitzarà un còpia total de tots els sistemes setmanalment. Una còpia diferencial diària. S'emmagatzemarà la informació en dispositius externs, els quals s'ubicaran en un armari ubicat en una sala diferent a la sala de servidors.

El mateix dia que es fa la còpia total s'enviarà aquesta còpia a la delegació més propera, la qual ja s'està realitzant en l'actualitat enviament setmanals d'altres tipus d'informació.

El volum de dades a emmagatzemar és inferior als 300 *Gb.* Les còpies incrementals no superen els 100 Gb.

Per realitzar la còpia de *backup* utilitzarem dispositius externs de 1 *Tb*.

Disposarem de 6 dispositius. En dos d'ells s'emmagatzemaran les còpies incrementals, en dos d'ells

s'emmagatzemara les còpies totals. En la resta s'emmagatzemarà les còpies allotjades en la delegació més propera i s'anirà intercanviant setmanalment els dispositius que emmagatzemen les còpies setmanals. Estimarem el temps de vida dels discos externs de sis anys, per tant, s'inclourà anualment el cost de reposició d'un disc

Passat el períodes de conservació de les dades, s'eliminaran les còpies més antigues els dispositius d'emmagatzematge. En el cas de que falli el *backup* per un error en el dispositiu sempre es disposarà d'un dispositiu alternatiu on es conserva la informació.

Els costos associats a la missatgeria no repercutiran en aquest projecte, ja que es realitzava un transport setmanal, i el volum de dades a enviar no variarà sensiblement.

La realització d'aquestes còpies de seguretat tenen un increment d'hores dedicades respecte a les que es feien anteriorment de 2 hores/quinzenals, ja que el canvia principalment és l'emmagatzematge, etiquetatge i gestió del transport de la informació.

Es realitzarà trimestralment una proba de recuperació per validar que els processos definits funcionen correctament. Això requerirà unes deu hores anuals per la realització del procés associat.

La definició del procediment de *backup* té un cost d'unes 10 hores i unes 4 hores en els canvis en la configuració actual.

El cost d'un disc és d'uns 100 €, per tant la inversió inicial en *hardware* és de 600 € i un cost recurrent de 100 € anuals.

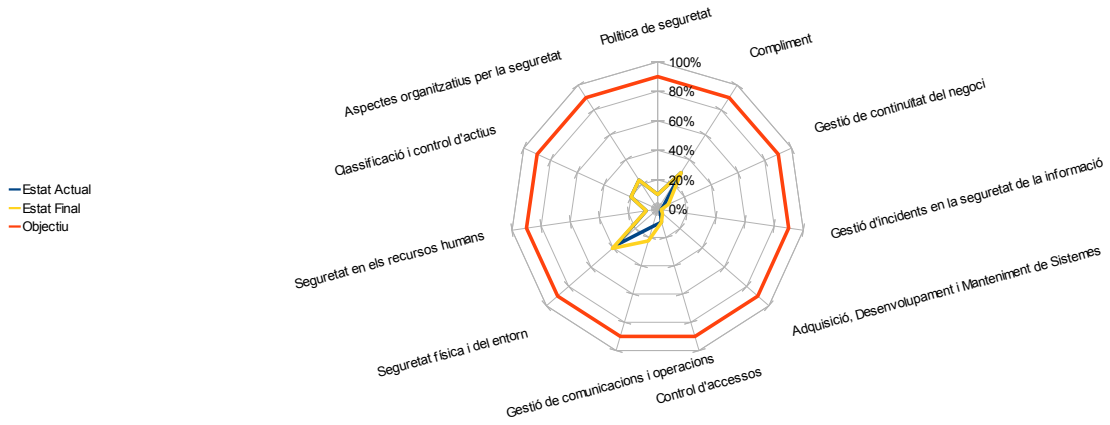
El cost de la implantació de la solució és el següent:

Concepte	**Cost (€)**
Instal·lació, configuració, documentació	1.400
Hardware	600
Total	**2.000**

El cost anual és el següent:

Concepte	**Cost (€/any)**
Manteniment	3.400
Hardware	100
Total	**3.500**

5.8.1.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	10%	90%
Aspectes organitzatius per la seguretat	24%	24%	90%
Classificació i control d'actius	20%	20%	90%
Seguretat en els recursos humans	8%	8%	90%
Seguretat física i del entorn	37%	41%	90%
Gestió de comunicacions i operacions	12%	22%	90%
Control d'accessos	9%	9%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	4%	90%
Gestió d'incidents en la seguretat de la informació	3%	3%	90%
Gestió de continuïtat del negoci	4%	8%	90%
Compliment	30%	30%	90%

Té un impacte relatiu les modificacions que hem realitzat, ja que la organització ja disposava d'un sistema de *backup*. Si ve es cert que les millores en la maduresa que introdueix aquest projecte té a veure a que guardem còpies de *backup* fora del edifici principal, mesura que es podrà tenir en compte en el cas de que *PREVENCIO S.L* es plantegi realitzar un pla de contingència.

El fet de definir un procediment i que emmagatzem més informació i en dispositius externs fa que la maduresa especifica del *backup* sigui un procés definit.

5.8.1.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

Estem aplicant una millora sobre un procés existent en la organització. Estem augmentant la precisió del sistema de *backup* introduït, estem documentant el procés de *backup*, s'estan introduïnt mesures necessàries que apliquen de manera transversal com a solució en un hipotètic futur pla de contingència.

Respecte al *backup* augmentem la eficàcia de la salvaguarda d'un 30 a un 60%, ja que incloem tant la millora en el procés, garanties en la disponibilitat dels dispositius, procediment detallat i proves de recuperació.

Aquesta mesura comporta una reducció del risc de 9.395 € anuals.

Veiem el retorn de la inversió i l'amortització associada:

	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 €

Comprovem que aquests inversió fins i tot es recuperaria en el primer any, tot i no ser la integritat la dimensió de seguretat rellevant del nostre sistema.

5.8.2 Reestructuració equip tecnològic

En l'anàlisi realitzat hem vist com hi han dues figures que s'encarreguen del manteniment dels sistemes informàtics:

- Director Comercial. Persona que no disposa d'una formació associada a l'administració dels sistemes informàtics, el qual s'encarrega de realitzar les tasques de manteniment dels equips d'usuari. La seva activitat principal es troba en el àrea comercial i a més se li ha assignat el rol de responsable de seguretat.
- Tècnic informàtic. Persona que no té una dedicació total a les tasques de manteniment del sistema (només es troba un dia a la setmana) i a la qual se li assignen les tasques de *Help Desk* que hagin pogut sorgir durant la setmana i que no hagi pogut resoldre el Director Comercial.

Actualment no es cobreixen les necessitats de control dels diferents sistemes i s'actua generalment de manera reactiva amb els incidents de seguretat que es manifestin directament (normalment problemes de disponibilitat dels diferents serveis).

En aquest escenari es suggereix que es disposi de personal amb un cert bagatge tècnic amb dedicació completa dins de la jornada laboral de *PREVENCIO S.L.* per tal de descarregar de les tasques de manteniment dels sistemes al Director Comercial, no requerint la contractació de personal extern a jornada parcial, permetent al Director Comercial disposar de temps per poder dedicar-se a la nova funció que ha aparegut amb la introducció d'un Sistema de Gestió de Seguretat de la Informació dins de la organització

Com a mínim es requereix d'una persona que s'encarregui de realitzar el manteniment del sistema.

Les tasques associades que adquirirà aquesta nova figura són:

- Revisió diària dels diferents events que es produeixin dins de la plataforma servidora (servidor de correu, servidor de *PREVENET*, *firewall*, *IDS*).
- Instal·lació i manteniment de la plataforma per el registre dels diferents incidències que es produeixin en la organització. D'aquesta manera es disposarà d'un inventari dels diferents events que s'hagin produït i les actuacions realitzades per poder disposar d'una base en l'actuació dels diferents events.
- 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.
- Realització dels *backups* diaris.

La coordinació i revisió d'aquestes tasques les realitzarà el Director Comercial, com actual responsable de seguretat i com a persona dins de l'empresa que actualment feia la majoria d'aquestes funcions d'una manera més intuïtiva.

El cost associat per la contractació d'una persona que realitzi les funcions indicades s'estima entre uns 40.000 - 50.000 € anuals tenint en compte el salari brut del treballador i els costos de la seguretat social.

El cost anual és el següent:

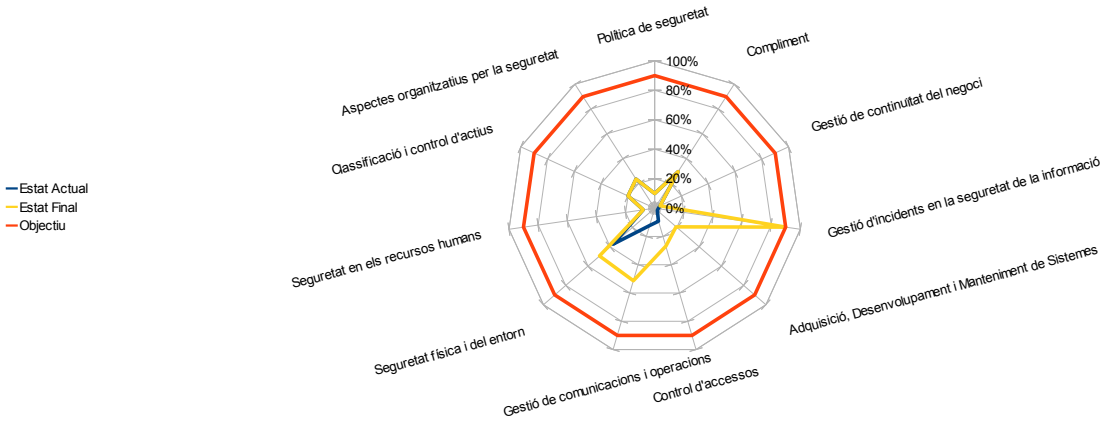
Concepte	**Cost (€/any)**
Administrador de sistemes	50.000
Total	**50.000**

Els costos aquí expressats es poden solapar amb els diferents projectes presentats, ja que es tracta de tasques que pugui estar realitzant l'administrador del sistema (estem parlant aproximadament d'uns 20.000 €/anuals en labors de manteniment pròpiament associables al tècnic informàtic).

Els costos de la implantació de noves solucions, i la càrrega que tindrà el responsable de seguretat en funcions de gestió del sistema de seguretat de la informació són factors que afavoreixen la creació d'aquesta nova figura dins de la organització.

Per simplificar l'anàlisi els càlculs els tractarem com a costos diferenciats, però es tracta d'una funció nova justificada per poder disposar d'un manteniment dels sistemes de la informació eficient amb els factors requerits.

5.8.2.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	10%	90%
Aspectes organitzatius per la seguretat	24%	24%	90%
Classificació i control d'actius	20%	20%	90%
Seguretat en els recursos humans	8%	8%	90%
Seguretat física i del entorn	37%	50%	90%
Gestió de comunicacions i operacions	12%	51%	90%
Control d'accessos	9%	27%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	19%	90%
Gestió d'incidents en la seguretat de la informació	3%	90%	90%
Gestió de continuïtat del negoci	4%	4%	90%
Compliment	30%	30%	90%

Com podem comprovar aquest projecte té un impacte significatiu en la maduresa global de la organització.

El fet de que puguem disposar d'una persona que es dediqui exclusivament a l'administració del sistema i que disposi dels coneixements tecnològics necessaris ens permet abordar diferents aspectes que serien impossibles sense una figura que es dediqués a aquesta funció.

Ens permet disposar d'una resposta més eficient en el cas de que es produeixi un incident de seguretat i que la informació de seguretat dels sistemes estigui documentada i existeixi un procediment associat.

Es poden realitzar accions de manteniment que fins a data d'avui era molt difícil de gestionar.

5.8.2.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

Aquesta nova figura incideix principalment en les següents salvaguardes preventives i correctives que havíem definit al inici d'aquest apartat. Farem una estimació percentual d'influència en les diferents salvaguardes:

Salvaguardes Preventives	**Reducció del risc estimada**
Registre d'actuacions	5,00%
Documentació procediments	2,00%
Manteniment dels sistemes	10,00%
Configuració dels equips (modificacions puntuals)	6,00%

Salvaguardes Correctives	**Reducció del risc estimada**
Registre d'incidències	3,00%
Detecció i recuperació	4,00%
Configuració dels equips (modificacions puntuals)	6,00%

Amb aquestes consideracions, revisem la influència en les diferents salvaguardes, obtenint que aquesta figura, per si sola, té una millora en el risc anual de la organització de 259,718 €.

Es un valor molt significatiu. De totes formes era esperat, ja que per realitzar les diferents accions de manteniment i configuració del sistema tenint en compte el volum actual d'equips, la distribució dels diferents era necessari disposar de personal qualificat amb dedicació completa dins de l'actual plantilla de *PREVENCIÓ S.L.*

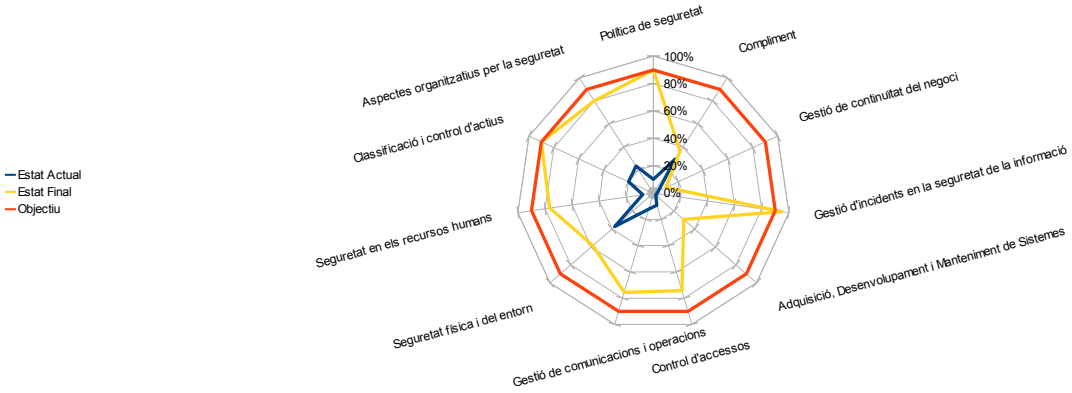
Veiem la taula de retorn de la inversió. En aquest cas es tracta de la diferència entre el cost del personal i el benefici brut:

	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 €

Estimem que només serà necessari una persona per cobrir les tasques de manteniment que actualment realitzava el Director Comercial i les que s'introduiran amb la introducció del sistema de gestió de seguretat de la informació, però es un tema que s'haurà d'analitzar en funció dels anàlisis de riscos de la organització.

5.9 Valoració conjunta dels projectes

5.9.1 Impacte en la maduresa del sistema



Domini	Estat Actual	Estat Final	Objectiu
Política de seguretat	10%	90%	90%
Aspectes organitzatius per la seguretat	24%	80%	90%
Classificació i control d'actius	20%	90%	90%
Seguretat en els recursos humans	8%	77%	90%
Seguretat física i del entorn	37%	59%	90%
Gestió de comunicacions i operacions	12%	76%	90%
Control d'accessos	9%	74%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	2%	29%	90%
Gestió d'incidents en la seguretat de la informació	3%	95%	90%
Gestió de continuïtat del negoci	4%	10%	90%
Compliment	30%	36%	90%

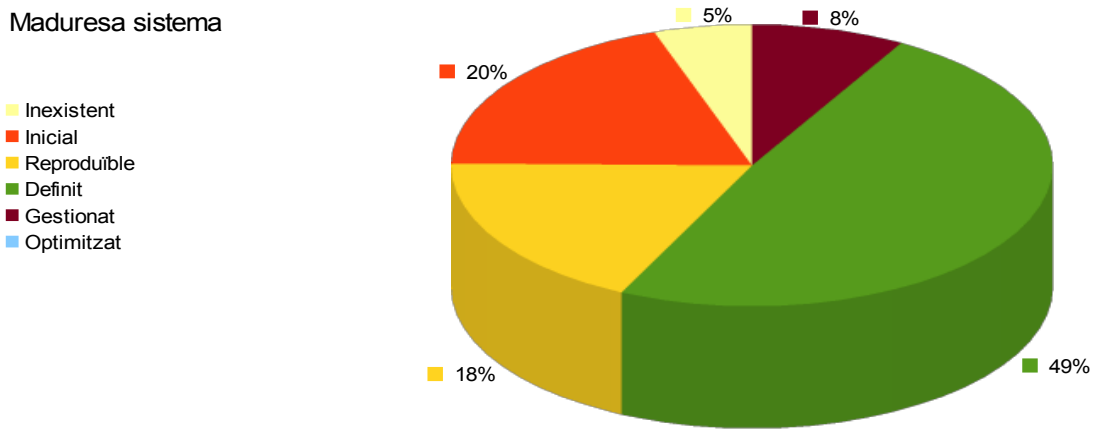
A nivell global es millorarà bastant la maduresa del sistema amb la inclusió dels diferents projectes. En els següents dominis no han tingut una incidència tan significativa:

- Compliment. Partíem d'un escenari amb una maduresa superior a la resta de dominis a nivell legislatiu. El treball que realitza *PREVENCIO S.L* es basa en aspectes legislatius. En futurs projectes s'haurà d'incidir més en els controls associats. Dins dels projectes proposats no s'ha valorat la realització d'una auditoria externa (només assessorament durant la fase

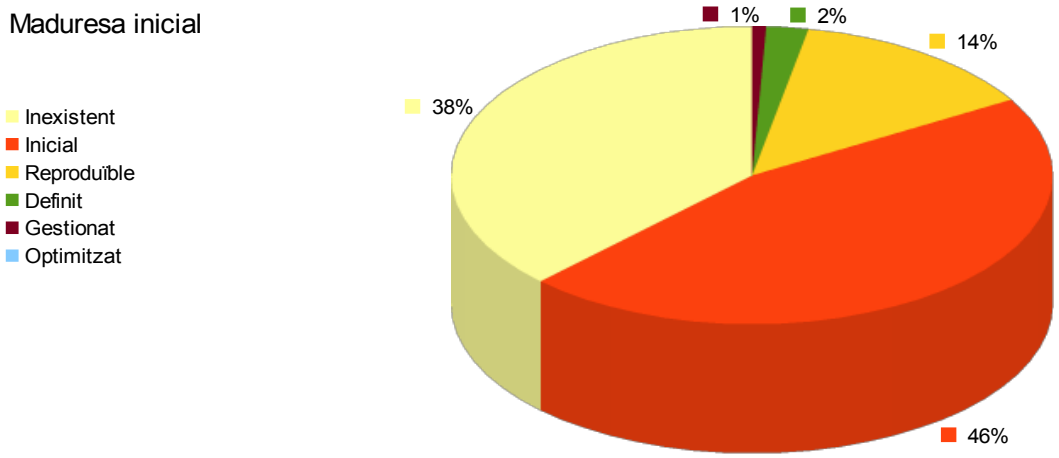
d'implantació), per tant és un projecte que s'ha de proposar en les següents reunions del comitè.

- Gestió de la continuïtat del negoci. No ho considerem un aspecte prioritari en una fase inicial d'implantació d'un sistema de gestió de seguretat de la informació. S'ha d'abordar un cop la organització disposi de la maduresa suficient, sempre i quant pugui assumir els costos associats.
- Adquisició, Desenvolupament i Manteniment del Sistemes. *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.

En la present gràfica podem observar que gran part dels controls han passat ha estar a un estat definit, que és el objectiu que havíem marcat a mig termini d'assolir per *PREVENCIO S.L.*



Si ho comparem en l'estat inicial que presenta el sistema abans de la materialització dels projectes, podem observar visualment el canvi en la maduresa dels controls:



Adjuntem la taula on es detallen els diferents controls de maduresa

Control	Eficàcia Inicial	Eficàcia final
Política de seguretat	**10%**	**90%**
Política de seguretat de la informació	***10%***	***90%***
Document de política de seguretat de la informació	10%	90%
Revisió i avaluació	10%	90%
Aspectes organitzatius per la seguretat	**24%**	**80%**
Organització interna	***14%***	***70%***
Comitè de gestió de seguretat de la informació	10%	90%
Coordinació de la seguretat de la informació	10%	90%
Assignació de responsabilitats sobre seguretat de la informació	50%	90%
Procés d'autorització de recursos per el tractament de la informació	10%	90%
Acords de confidencialitat	0%	90%
Contactes amb autoritats	10%	10%
Contactes amb grups d'interès especial	10%	10%
Revisió independent de la seguretat de la informació	10%	90%
Seguretat en els accessos de terceres parts	***33%***	***90%***
Identificació de riscos per el accés a tercers	50%	90%
Requisits de seguretat quan es tracta amb clients	50%	90%
Requisits de seguretat en contractes d'outsourcing	0%	90%
Classificació i control d'actius	**20%**	**90%**
Responsabilitat sobre els actius	***10%***	***90%***
Inventari d'actius	10%	90%
Propietat dels actius	10%	90%
Ús adequat dels actius	10%	90%
Classificació de la informació	***30%***	***90%***
Guies de classificació	50%	90%
Marcat i tractament de la informació	10%	90%
Seguretat en els recursos humans	**8%**	**77%**
Seguretat abans del treball	***10%***	***63%***
Inclusió de la seguretat en les responsabilitats i funcions laborals	10%	90%
Selecció i política de personal	10%	10%
Acords de confidencialitat	10%	90%
Durant del treball	***7%***	***77%***
Responsabilitats de la gerència	10%	90%
Coneixement, educació i entrenament de la seguretat de la informació	10%	50%

Procés disciplinari	0%	90%
Finalització o canvi de treball	***7%***	***90%***
Responsabilitats de finalització	0%	90%
Retorn d'actius	10%	90%
Retirada dels drets d'accés	10%	90%
Seguretat física i del entorn	**37%**	**59%**
Àrees segures	***43%***	***50%***
Perímetre de seguretat física	50%	50%
Controls físics d'entrades	50%	50%
Seguretat d'oficines, despatxos i recursos	50%	50%
Protecció contra amenaces externes i ambientals	10%	50%
El treball en les àrees segures	10%	10%
Accés públic, àrees de càrregues i descàrregues	90%	90%
Seguretat dels equips	***31%***	***67%***
Instal·lació i protecció d'equips	10%	10%
Subministrament elèctric	90%	90%
Seguretat del cablejat	10%	10%
Manteniment dels equips	0%	90%
Seguretat d'equips fora dels locals de la organització	10%	90%
Seguretat en la reutilització o eliminació dels equipaments	10%	90%
Retirada de la propietat	90%	90%
Gestió de comunicacions i operacions	**12%**	**76%**
Procediments i responsabilitats d'operacions	***5%***	***68%***
Documentació de procediments operatius	10%	90%
Gestió de canvis	0%	90%
Segregació de tasques	10%	90%
Separació dels recursos per desenvolupament i per producció	0%	0%
Gestió de serveis externs	***10%***	***90%***
Servei d'entrega	10%	90%
Monitorització i revisió dels serveis externs	10%	90%
Gestionant canvis per els serveis externs	10%	90%
Planificació i acceptació del sistema	***0%***	***70%***
Planificació de la capacitat	0%	50%
Acceptació del sistema	0%	90%
Protecció contra software maliciós	***10%***	***50%***
Mesures i controls contra software maliciós	10%	50%
Mesures i controls contra codi mòbil	10%	50%

Gestió de copies de seguretat i recuperació	***10%***	***90%***
Recuperació de la informació	10%	90%
Gestió de seguretat en xarxes	***5%***	***95%***
Controls de xarxa	0%	95%
Seguretat en els serveis de xarxa	10%	95%
Utilització dels medis d'informació	***20%***	***90%***
Gestió de medis removibles	10%	90%
Eliminació de medis	10%	90%
Procediment de manipulació de la informació	10%	90%
Seguretat de la documentació de sistemes	50%	90%
Intercanvi d'informació	***16%***	***82%***
Polítiques i procediments per el intercanvi d'informació i software	10%	90%
Acords d'intercanvi	10%	90%
Medis físics en trànsit	0%	90%
Seguretat en la missatgeria electrònica	10%	50%
Sistemes d'Informació de Negocis	50%	90%
Serveis de correu electrònic	***37%***	***63%***
Comerç electrònic	50%	50%
Transacció en línia	50%	50%
Informació pública disponible	10%	90%
Monitorització	***10%***	***58%***
Registre de la auditoria	0%	10%
Monitoritzant el us del sistema	0%	90%
Protecció de la informació de registre	10%	50%
Registre d'administradors i operadors	0%	50%
Registre de la avaria	0%	95%
Sincronització del rellotge	50%	50%
Control d'accessos	**9%**	**74%**
Requisits de negoci per el control d'accés	***10%***	***90%***
Política de control d'accés	10%	90%
Gestió d'accés d'usuaris	***15%***	***70%***
Registre d'usuaris	10%	90%
Gestió de privilegis	50%	90%
Gestió de contrasenyes d'usuaris	0%	90%
Revisió dels drets d'accés dels usuaris	0%	10%
Responsabilitats dels usuaris	***7%***	***90%***
Us de contrasenyes	0%	90%

Equips informàtics d'usuaris desatesos	10%	90%
Polítiques de pantalles i escriptoris nets	10%	90%
Control d'accés a la xarxa	***4%***	***86%***
Política d'us dels serveis de xarxa	0%	90%
Autentificació d'usuari per connexions externes	10%	50%
Identificació d'equips en la xarxa	0%	90%
Diagnòstic remot i configuració de protecció de ports	0%	95%
Segregació en xarxa	10%	90%
Control de connexió a la xarxa	10%	90%
Control d'enrutament en la xarxa	0%	95%
Control d'accés al sistema operatiu	***3%***	***23%***
Procediment de connexió de terminals	10%	50%
Identificació i autentificació del usuari	10%	10%
Sistema de gestió de contrasenyes	0%	10%
Utilització de les facilitats del sistema	0%	10%
Desconnexió automàtica de sessions	0%	10%
Limitació del temps de connexió	0%	50%
Control d'accés a les aplicacions i la informació	***25%***	***70%***
Restricció d'accés a la informació	50%	50%
Aïllament de sistemes sensibles	0%	90%
Informàtica mòbil i teletreball	***0%***	***90%***
Informàtica mòbil i comunicacions	0%	90%
Teletreball	0%	90%
Adquisició, Desenvolupament i Manteniment de Sistemes	**11%**	**29%**
Requisits de seguretat dels sistemes	***0%***	***10%***
Anàlisi i especificacions dels requisits de seguretat	0%	10%
Seguretat de les aplicacions del sistema	***0%***	***15%***
Validació de les dades d'entrada	0%	0%
Control del procés intern	0%	10%
Integritat dels missatges	0%	50%
Validació de les dades de sortida	0%	0%
Controls criptogràfics	***0%***	***10%***
Política d'ús dels controls criptogràfics	0%	10%
Gestió de claus	0%	10%
Seguretat dels arxius del sistema	***0%***	***3%***
Control del software en producció	0%	10%
Protecció de les dades de prova del sistema	0%	0%

Control d'accés als codis de programes font	0%	0%
Seguretat en els processos de desenvolupament i suport	***14%***	***48%***
Procediments de control de canvis	10%	90%
Revisió tècnica dels canvis en el sistema operatiu	0%	50%
Restriccions en els canvis als paquets de software	10%	50%
Fuga d'informació	50%	50%
Desenvolupament extern del software	0%	0%
Gestió de la vulnerabilitat tècnica	***50%***	***90%***
Control de les vulnerabilitats tècniques	50%	90%
Gestió d'incidents en la seguretat de la informació	**8%**	**95%**
Reportant events i debilitats de la seguretat de la informació	***10%***	***95%***
Reportant els events en la seguretat de la informació	10%	95%
Reportant debilitats en la seguretat de la informació	10%	95%
Gestió de les millores i incidents en la seguretat de la informació	***7%***	***95%***
Responsabilitats i procediments	0%	95%
Aprenent dels incidents en la seguretat de la informació	10%	95%
Recol·lecció d'evidències	10%	95%
Gestió de continuïtat del negoci	**4%**	**10%**
Aspectes de la gestió de continuïtat del negoci	***4%***	***10%***
Incloent la seguretat de la informació en el procés de gestió de la continuïtat del negoci	10%	10%
Continuïtat del negoci i avaluació de riscos	10%	10%
Redacció e implantació de plans de continuïtat que incloguin la seguretat de la informació	0%	10%
Marc de planificació per la continuïtat del negoci	0%	10%
Prova, manteniment i avaluació dels plans de continuïtat	0%	10%
Compliment	**30%**	**36%**
Compliment dels requisits legals	***49%***	***63%***
Identificació de la legislació aplicable	95%	95%
Drets de propietat intel·lectual	50%	50%
Salvaguardes dels registres de la organització	50%	50%
Protecció de les dades i de la privacitat de la informació personal	50%	90%
Prevenció en el mal us dels recursos del tractament de la informació	50%	90%
Regulació dels controls criptogràfics	0%	0%
Revisió de la política de seguretat i de la conformitat tècnica	***10%***	***10%***
Conformitat amb la política de seguretat i els estàndards	10%	10%
Comprovació de la conformitat tècnica	10%	10%
Consideracions sobre la auditoria de sistemes	***10%***	***10%***

Controls d'auditoria de sistemes	10%	10%
Protecció de les eines d'auditoria de sistemes	10%	10%

5.9.2 Impacte en el anàlisis de riscos de la organització. Retorn de la inversió

Si analitzem en global els diferents projectes presentats, podem comprovar com es redueix el risc dels diferents actius de la nostra organització.

Actiu	Valor	Risc Intrínsec	Risc Efectiu	Reducció del risc	%Reducció Risc
Data-Form	75.000 €	1.510 €	342 €	1.168 €	77,37%
Data-V.S	300.000 €	54.460 €	25.827 €	28.634 €	52,58%
Data-Proc.Int	30.000 €	2.746 €	910 €	1.836 €	66,85%
Data-Conta	30.000 €	604 €	137 €	467 €	77,37%
Data-Comer	75.000 €	1.510 €	342 €	1.168 €	77,37%
Data-Prv	300.000 €	6.041 €	1.343 €	4.698 €	77,77%
Data-Contr.Clie	300.000 €	5.055 €	2.667 €	2.388 €	47,25%
Data-Contr.Prov	300.000 €	5.055 €	2.667 €	2.388 €	47,25%
Apl-Win.Srv	300.000 €	47.638 €	22.518 €	25.120 €	52,73%
Apl-Win.XP	300.000 €	47.638 €	22.518 €	25.120 €	52,73%
Apl-IIS	300.000 €	47.638 €	22.518 €	25.120 €	52,73%
Apl-Ms.SQL	300.000 €	47.638 €	22.518 €	25.120 €	52,73%
Apl-PREV	300.000 €	47.638 €	22.518 €	25.120 €	52,73%
Apl-Ms.Ex.Srv	300.000 €	47.638 €	22.518 €	25.120 €	52,73%
Apl-NFS	300.000 €	47.638 €	22.518 €	25.120 €	52,73%
Apl-Conta	300.000 €	47.638 €	22.518 €	25.120 €	52,73%
Apl-MS.OFF	300.000 €	47.638 €	22.518 €	25.120 €	52,73%
EA-S.Elec	300.000 €	1.315 €	379 €	936 €	71,21%
Inst -E.C	300.000 €	8.219 €	6.293 €	1.927 €	23,44%
Inst -D.T	300.000 €	8.219 €	6.293 €	1.927 €	23,44%
Inst -U.M	150.000 €	966 €	739 €	226 €	23,44%
HW-PC	300.000 €	45.904 €	25.252 €	20.652 €	44,99%
HW-Rou.Cen	300.000 €	45.904 €	25.252 €	20.652 €	44,99%
HW-SW.Cen	300.000 €	7.948 €	3.981 €	3.967 €	49,92%
HW–Rou.DT	300.000 €	7.948 €	3.981 €	3.967 €	49,92%
HW-BB	150.000 €	3.974 €	1.990 €	1.984 €	49,92%
HW-PT	300.000 €	46.068 €	25.527 €	20.541 €	44,59%
HW-Srv.Cor	300.000 €	8.277 €	4.162 €	4.114 €	49,71%
HW-Srv.PREV	300.000 €	8.277 €	4.162 €	4.114 €	49,71%
X-WAN	300.000 €	54.460 €	5.634 €	48.826 €	89,65%
X-LAN	300.000 €	54.460 €	14.296 €	40.164 €	73,75%
SRV-NFS	10.000 €	270 €	77 €	193 €	71,56%
SRV-DIR	300.000 €	8.096 €	2.303 €	5.793 €	71,56%
SRV-MAIL	75.000 €	2.024 €	576 €	1.448 €	71,56%
SRV-V.S	75.000 €	10.510 €	3.728 €	6.783 €	64,53%
SRV-PREV	30.000 €	810 €	230 €	579 €	71,56%
SRV-WEB	10.000 €	270 €	77 €	193 €	71,56%
SRV-IMPRES	150.000 €	20.774 €	12.371 €	8.403 €	40,45%
Per-D.Comer	150.000 €	82 €	36 €	47 €	56,80%
Per-D.Prev	75.000 €	2.466 €	1.065 €	1.401 €	56,80%
Per-Comer	150.000 €	82 €	36 €	47 €	56,80%
Per-D.V.S	150.000 €	82 €	36 €	47 €	56,80%
Per-I.V.S	150.000 €	82 €	36 €	47 €	56,80%
Per-D.Fin	75.000 €	41 €	18 €	23 €	56,80%
Per-Tec.TIC	300.000 €	164 €	71 €	93 €	56,80%
Per-Resta	300.000 €	164 €	71 €	93 €	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 pràcticament el 50% del risc que té actualment *PREVENCIO S.L.*

Destaca significativament les millores en els actius de dades que és el nostre objectiu principal de protecció de la informació.

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

A nivell d'instal·lacions no s'han produït millores significatives 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.* i poder 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.

La reducció global del risc (468.018 €) És menor que la reducció de totes les propostes realitzades (527.507 €) ja que s'ha produït un solapament de funcions (tal i com hem explicat en el projecte de Reestructuració del equip tecnològic) i per que en cap salvaguarda hem volgut assumir una reducció superior al 95%. Hem aplicat aquest criteri ja es pràcticament impossible de que estiguem coberts de totes les amenaces que es puguin produir, i per tant, aplicar aquesta consideració en cadascun dels anàlisi de riscos que realitzem per la organització.

Veiem en global el retorn de la inversió del conjunt total dels projectes, utilitzant el valor de reducció de riscos menor:

	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 €

Es pot observar clarament que el benefici que aporta les mesures de seguretat proposades tenen un impacte significatiu en el benefici de la pròpia organització. Per tant, en base als resultats obtinguts, recomanem a *PREVENCIÓ S.L* que integri un sistema de gestió de seguretat a la seva organització.

5.9.3 Planificació

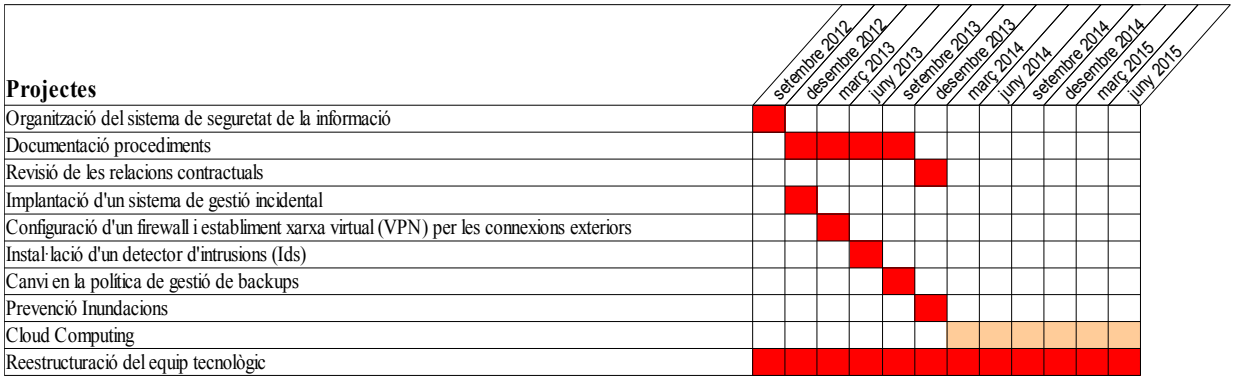
Els projectes més importants per el desenvolupament del *SGSI* són els que posat en primera instància. És necessari que realitzem una reestructuració del equip tecnològic per que es facin càrrec dels projectes tècnics que s'han d'abordar. A més descarregarem de funcions al Responsable de Seguretat que ha de prioritzar les seves noves funcions.

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.

Primer de tot, s'ha de realitzar el pla director per assentar les bases de seguretat. Posteriorment haurem de revisar tots els procediments per adaptar-los a les necessitats de seguretat i que estigui gestionat les accions que s'han de realitzar amb els actius d'informació.

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.



6 RESUM EXECUTIU

En el present projecte s'han presentat les necessitats de *PREVENCIO S.L.* empresa que es dedica a la prevenció dels riscos laborals i de vigilància de la salut.

6.1 Escenari de treball

Aquesta 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.

La empresa tracta amb diferent informació, però destaca principalment la gestió de dades sensibles associades a la salut dels treballadors de les empreses que contracten els seus serveis.

PREVENCIÓ S.L. treballa amb diferents clients i 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 i la incorporació dels serveis de prevenció que es troben en la plantilla de les empreses que contracten el seu servei.

Aquesta fase de creixement fa que s'hagi de revisar, i en alguns casos definir, els diferents procediments operatius de la empresa. 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.

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, de 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 i adequant el pressupost que es pugui destinar anualment a la seguretat.

6.2 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.

  Per l'anàlisi d'amenaces i vulnerabilitats 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 dels diferents actius s'ha utilitzat com a criteri principal la dimensió de seguretat més important de cadascun d'ells (Autenticitat, Confidencialitat, Integritat, Disponibilitat i Traçabilitat).
- 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.

6.3 Resultats obtinguts dels anàlisis realitzats

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.

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 €**

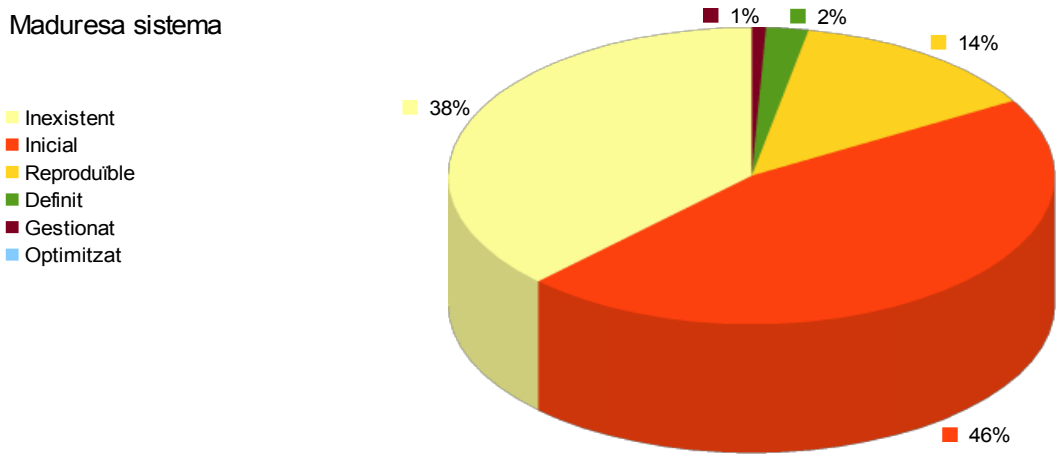
En una primera valoració es pot comprovar que els principals actius als quals recauen un major pes dins de *PREVENCIÓ S.L* són les aplicacions i el hardware. Les dades pròpiament també tenen un valor elevat però les actuacions que s'han de realitzar a nivell de seguretat són menors. També destaca especialment l'impacte que té sobre la seguretat les diferents xarxes.

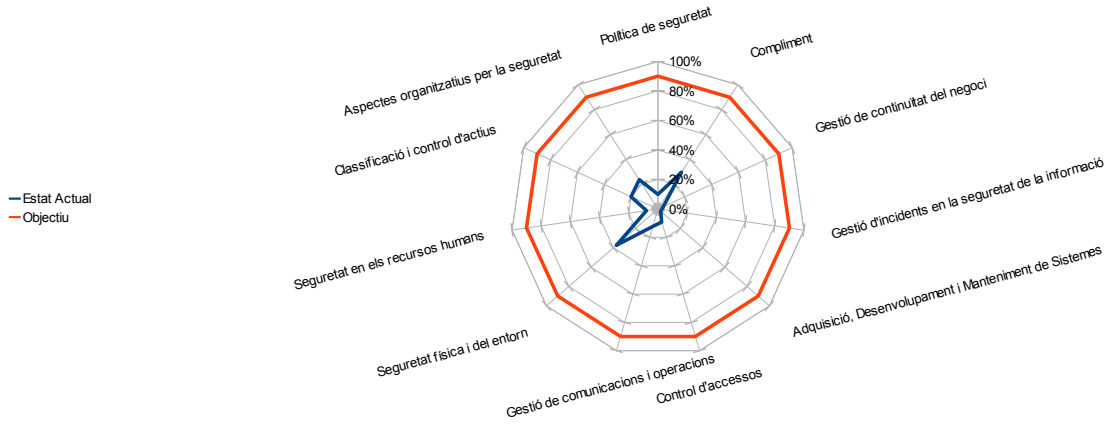
A nivell de serveis la valoració dels actius i dels riscos associats és menor que en altres categories ja que sòl ser l'últim esglaó de dependències (hi han molt pocs actius que depenguin d'un servei i el seu valor es troba repercutit en la resta d'actius de la informació).

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.

Respecte a la maduresa dels diferents controls de seguretat que defineix la norma *ISO 27002*, hem obtingut el següent resultat:





Domini	Estat Actual
Política de seguretat	**10%**
Aspectes organitzatius per la seguretat	**24%**
Classificació i control d'actius	**20%**
Seguretat en els recursos humans	**8%**
Seguretat física i del entorn	**37%**
Gestió de comunicacions i operacions	**12%**
Control d'accessos	**9%**
Adquisició, Desenvolupament i Manteniment de Sistemes	**2%**
Gestió d'incidents en la seguretat de la informació	**3%**
Gestió de continuïtat del negoci	**4%**
Compliment	**30%**

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* (Model de Maduresa de la Capacitat) 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 suficientment com els actius principals a protegir.

6.4 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. Aquestes dades requereixen segons la *LOPD* una protecció especial al tractar-se de dades mèdiques.
- 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.*
- Les aplicacions dels diferents terminals. No disposem d'una infraestructura homogènia i sota un control administratiu necessari.
- Els elements de la comunicació entre els portàtils i el servidors de prevenció. Treballem a través d'una xarxa pública, per tant, la comunicació es pot veure compromesa si no realitzem les mesures de seguretat oportunes.

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. Serà un dels pilars per que el personal de la organització prengui consciència sobre el seu rol dins de la seguretat de la informació i ens servirà per prioritzar a la empresa els diferents aspectes de seguretat que vagin sorgint.
- 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, especialment quan treballen en el client, ja que ens trobem en ubicacions en les que no es disposen de totes les mesures de seguretat i les condicions de treball són diferents.
- S'ha de millorar principalment el control de les comunicacions des de l'exterior. No s'estan prenent les mesures suficients per protegir la informació que es gestiona des de aquestes ubicacions.
- 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.

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

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.

6.4.1 Organització del sistema de seguretat de la informació

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

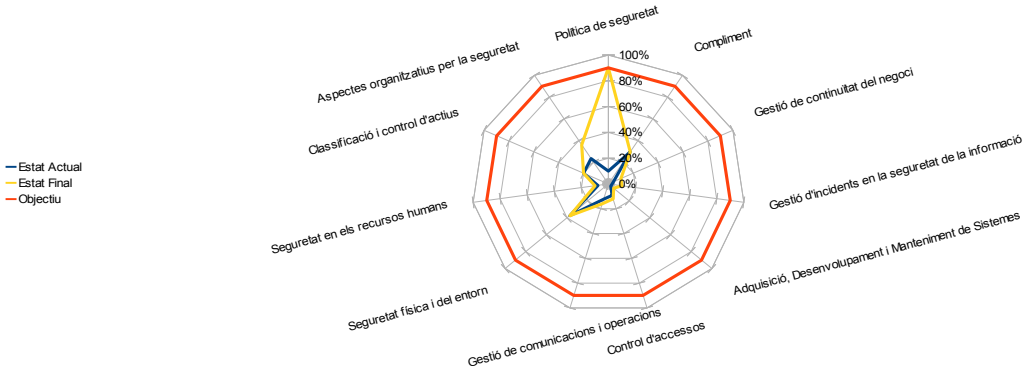
Es definirà els participants del comitè de gestió. És definiran el rols d'aquest grup, principalment:

- 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.
- S'hauran de reunir periòdicament per realitzar les accions associades (s'ha considerat com a mínim cada sis mesos).

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.

L'impacte del projecte en la maduresa del projecte és la següent:



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

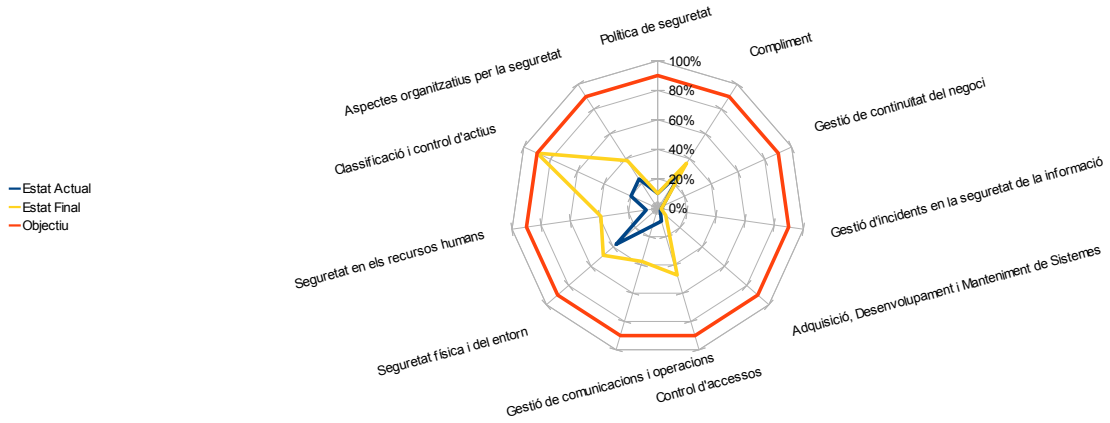
	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	7.000 €	7.000 €	7.000 €	7.000 €	7.000 €
Amortització	5.000 €	5.000 €	5.000 €		
Benefici brut	16.000 €	16.000 €	16.000 €	16.000 €	16.000 €
Benefici net	4.000 €	4.000 €	4.000 €	9.000 €	9.000 €

6.4.2 Integració de la gestió de la seguretat dins de l'organització. Documentació 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.*

L'impacte del projecte en la maduresa del projecte és la següent:



El cost de la 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 €

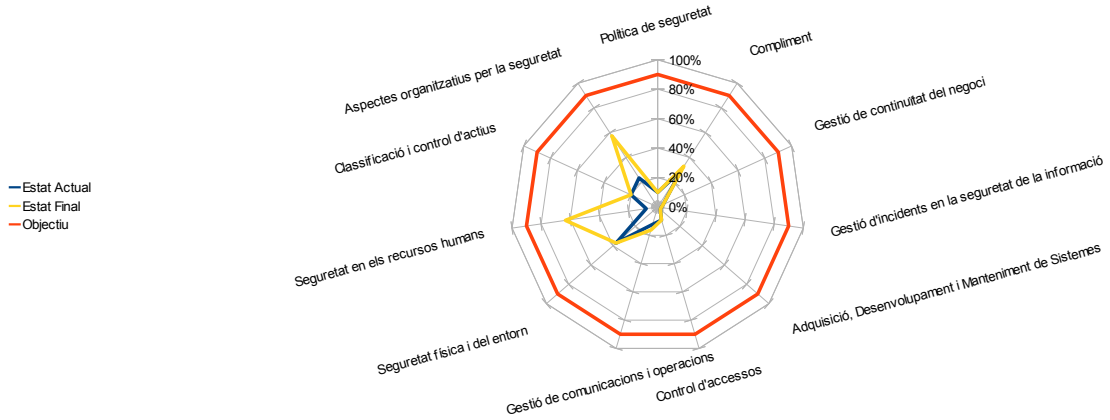
6.4.3 Revisió de les relacions contractuals

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*.

L'impacte del projecte en la maduresa del projecte és la següent:



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

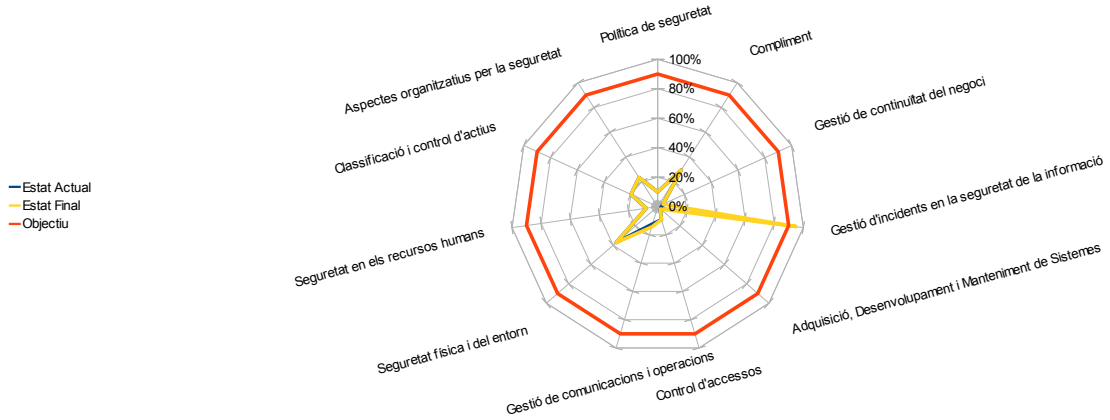
	Anys				
Concepte	1	2	3	4	5
Cost de manteniment	1.000 €	1.000 €	1.000 €	1.000 €	1.000 €
Amortització	2.125 €	2.125 €	2.125 €		
Benefici brut	6.375 €	6.375 €	6.375 €	6.375 €	6.375 €
Benefici net	3.250 €	3.250 €	3.250 €	5.375 €	5.375 €

6.4.4 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.

L'impacte del projecte en la maduresa del projecte és la següent:



El cost de la 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 €

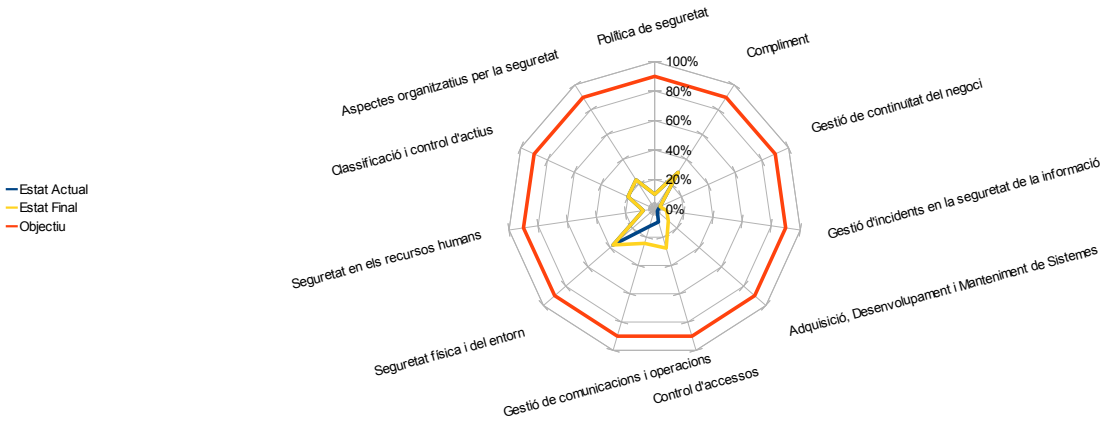
6.4.5 Configuració d'un *firewall* i de la xarxa virtual (*VPN*)

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.

L'impacte del projecte en la maduresa del projecte és la següent:



El cost de la 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 €

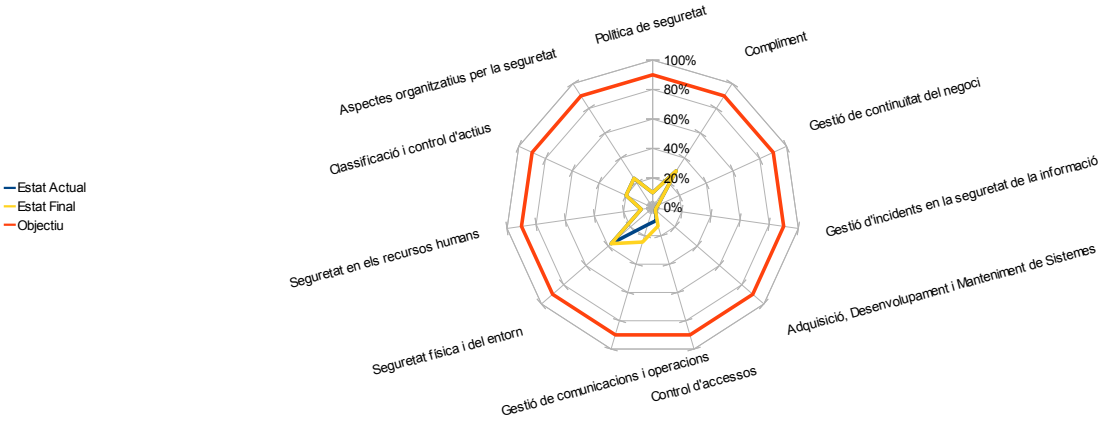
6.4.6 Detecció Intrusions. Instal·lació IDS

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.

L'impacte del projecte en la maduresa del projecte és la següent:



El cost de la 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 €

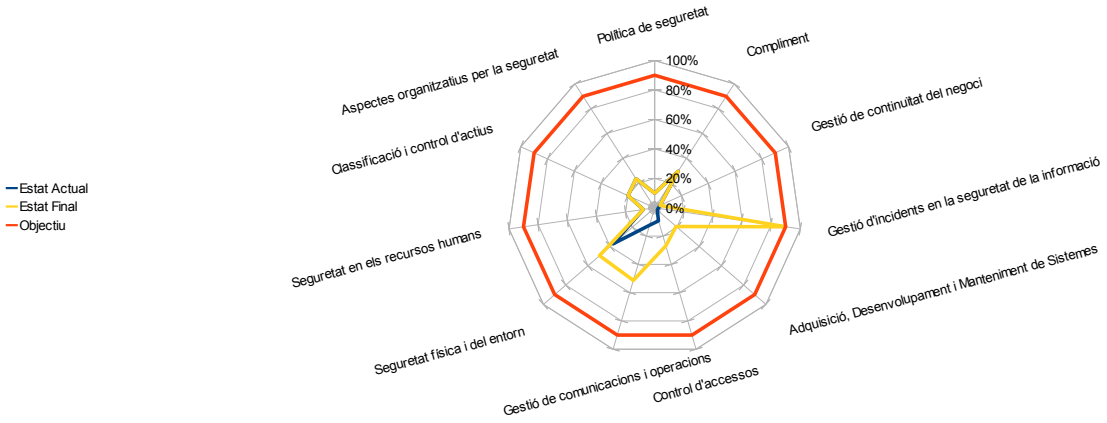
6.4.7 Reestructuració equip tecnològic

Es disposa d'un tècnic informàtic un dia a la setmana. Es suggereix que es disposi de personal amb un cert bagatge tècnic amb dedicació completa per tal de descarregar de les tasques de manteniment dels sistemes al Director Comercial i actual responsable de seguretat. El Responsable de Seguretat serà la persona que revisarà la realització de les tasques associades.

Les tasques inicials que adquirirà aquesta nova figura són:

- 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.

L'impacte del projecte en la maduresa del projecte és la següent:



El cost de la 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 €

6.4.8 Canvi en la política de gestió de *backups*

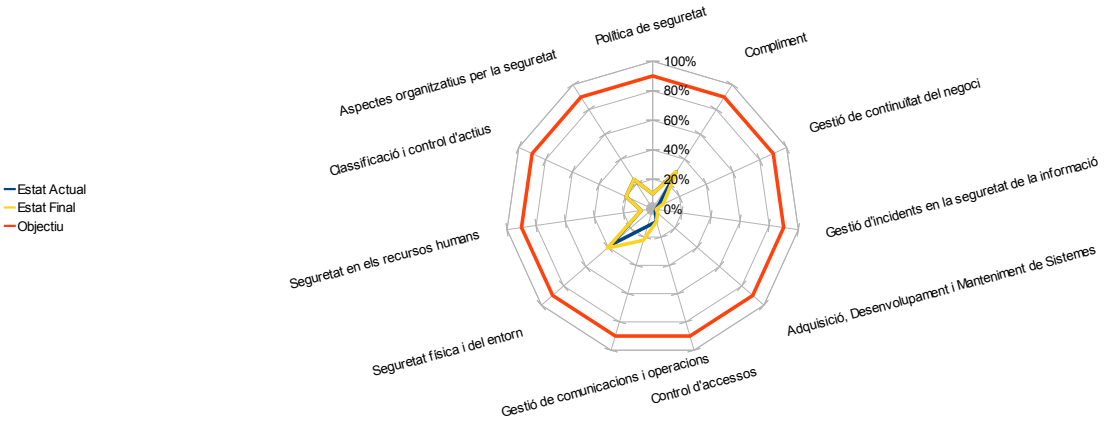
Actualment només s'emmagatzemen dues còpies de *backup* setmanal en un dels servidors de la organització.

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.

L'impacte del projecte en la maduresa del projecte és la següent:



El cost de la 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 €

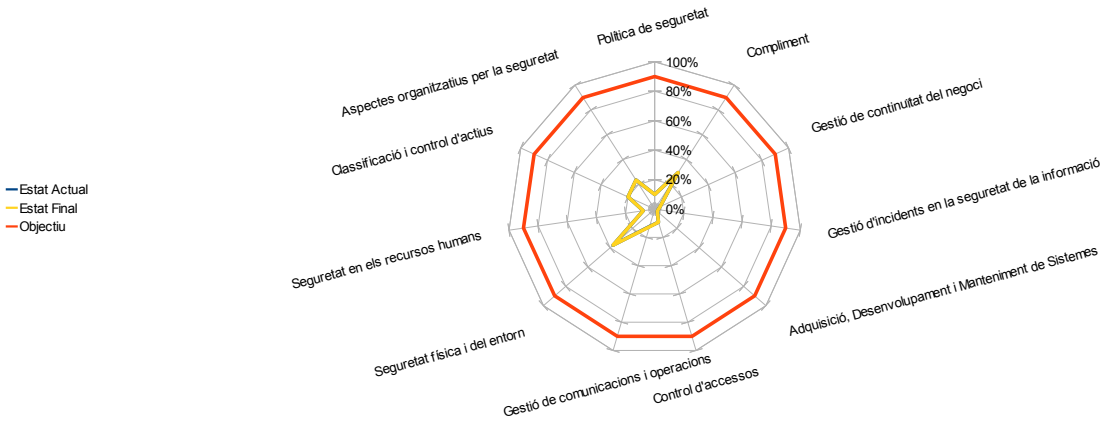
6.4.9 Inundacions. Canvi de la ubicació de la sala de servidors

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.

L'impacte del projecte en la maduresa del projecte és la següent:



El cost de la 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 €

No s'aprecien resultats significatius per els següents motius:

- Maduresa dels controls de seguretat. 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.
- Anàlisi de riscos. 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.

6.4.10 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 permeten externalitzar part de les mesures de seguretat associades al servidor (electricitat, mesures físiques de seguretat, allotjament del *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.

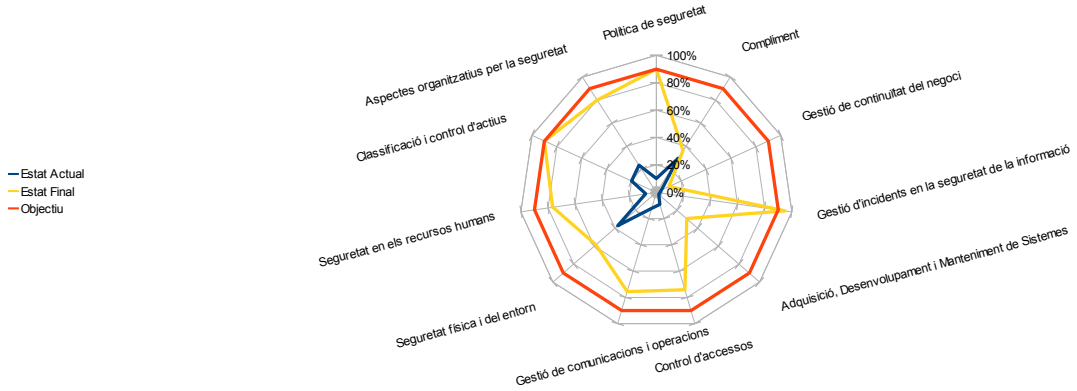
En base a aquests criteris, es realitza la facturació mensual del servei.

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...).

6.5 Valoració global

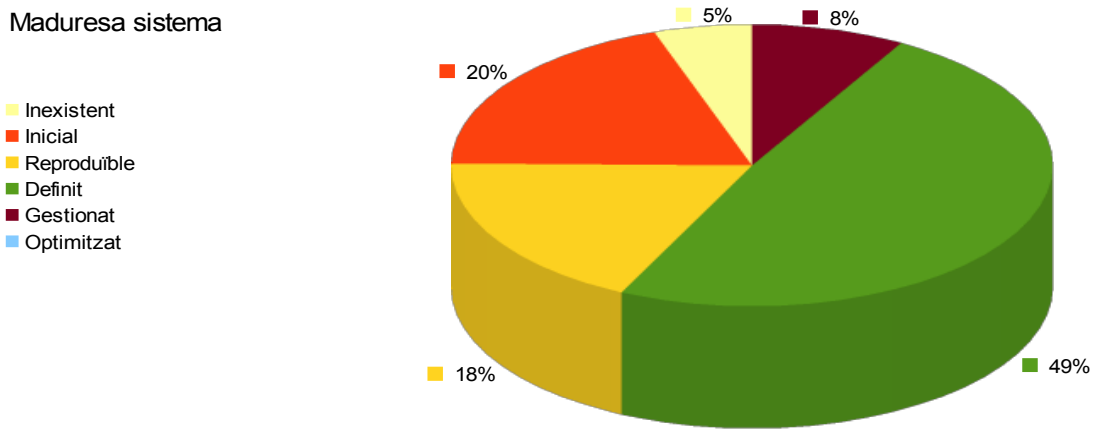
6.5.1 Impacte global en la maduresa del sistema



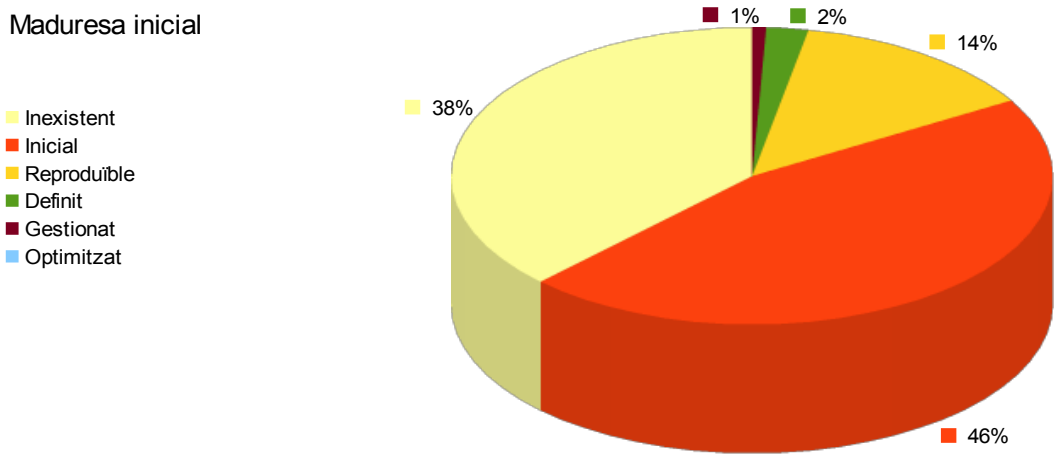
A nivell global es millorarà bastant la maduresa del sistema amb la inclusió dels diferents projectes. En els següents dominis no han tingut una incidència tan significativa:

- Compliment. Partíem d'un escenari amb una maduresa superior a la resta de dominis a nivell legislatiu. El treball que realitza *PREVENCIO S.L* es basa en aspectes legislatius. En futurs projectes s'haurà d'incidir més en els controls associats. Dins dels projectes proposats no s'ha valorat la realització d'una auditoria externa (només assessorament durant la fase d'implantació), per tant és un projecte que s'ha de proposar en les següents reunions del comitè.
- Gestió de la continuïtat del negoci. No ho considerem un aspecte prioritari en una fase inicial d'implantació d'un sistema de gestió de seguretat de la informació. S'ha d'abordar un cop la organització disposi de la maduresa suficient, sempre i quant pugui assumir els costos associats.
- Adquisició, Desenvolupament i Manteniment del Sistemes. *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.

En la present gràfica podem observar que gran part dels controls han passat ha estar a un estat definit, que és el objectiu que havíem marcat a mig termini d'assolir per *PREVENCIO S.L.*



Si ho comparem en l'estat inicial que presenta el sistema abans de la materialització dels projectes, podem observar visualment el canvi en la maduresa dels controls:



6.5.2 Impacte en el anàlisis de riscos de la organització

Valorem el impacte econòmic sobre els diferents actius de la informació:

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.* i poder determinar a mig plaç 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 dels projectes 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 €

6.5.3 Planificació

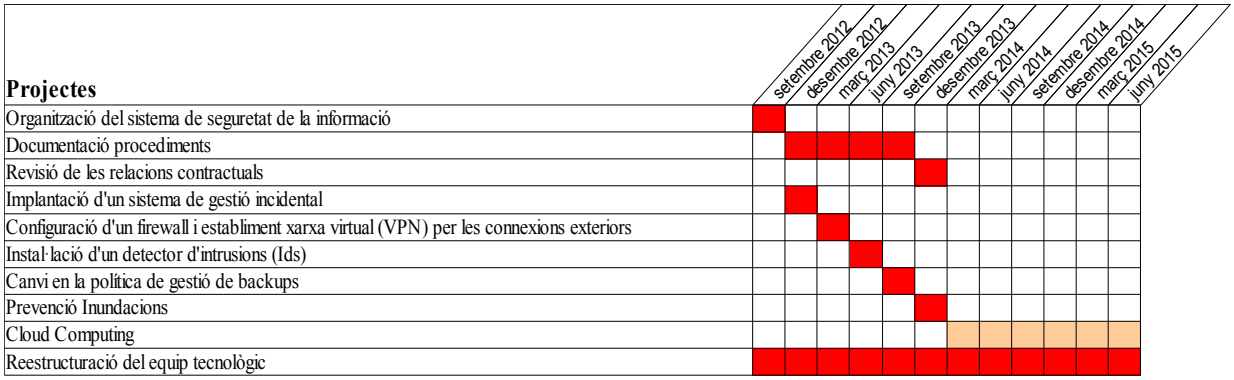
6.5.4 Planificació

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.



7 BIBLIOGRAFIA

PREVENET

http://www.tecnopreven.com/pdf/prevenet.pdf

CONTASOL

http://www.sdelsol.com/es/contasol.php

Llei de Prevenció de Riscos Laborals

http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1995-24292

LOPD

http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

ISO 27002

http://www.17799.com/papers/iso17799scope.pdf

ISO 27002 (traducció al castellà)

http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf

MAGERIT

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

PILAR

https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=187&lang=es

ZOHO WIKI: Wiki amb informació sobre els 133 controls ISO 27002

http://iso27002.wiki.zoho.com/

Portal d'informació sobre la normativa ISO 27000 i dels SGSI en general

http://www.iso27000.es

INTECO Instituto Nacional de Tecnologías de la Información

www.inteco.es

INTECO: Guia avanzada de gestión de contratos

http://www.inteco.es/calidad_TIC/descargas/guias/guia_avanzada_de_gestion_de_contratos

INTECO: Externalización de la seguridad

http://cert.inteco.es/extfrontinteco/icd/pdf/Externalizacion_de_Servicios_de_Seguridad.pdf

INTECO: Catálogo de empresas y de soluciones de seguridad de las TIC

http://cert.inteco.es/icdemoest/Catalogo_STIC/CatalogoAccesible

Definició *Cloud Computing*

http://en.wikipedia.org/wiki/Cloud_computing

Gartner: 7 riscos de seguretat del *Cloud Computing*

http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1

Microsoft: Soluciones de nuve privada

http://www.microsoft.com/es-es/server-cloud/readynow/default.aspx

Comparador de soluciones de nube privada

http://hostarting.es

Guia per empreses seguretat i privacitat Cloud Computing

http://www.inteco.es/file/yBCJI6sIRWy28pdgjxwphw

INTECO. Formació en seguretat en les tecnologies de la informació.

http://cert.inteco.es/Formacion/

Amazon Web Services

http://aws.amazon.com/es/

IBM Cloud Computing

http://www-05.ibm.com/es/cloudcomputing/index4.html

Microsoft: Pymes y autónomos. Guia de Seguridad

http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=227

Norma Técnica Colombiana NTC-ISO 14001

http://intranet.ugc.edu.co/documentos/gestion_calidad/ntc_iso_14001_2004.pdf

Snort

www.snort.org

Security Onion

http://securityonion.blogspot.com.es/

ITIL: Microsoft and Open Source

http://www.microsoft.com/hk/windowsserver/compare/ReportsDetails.mspx?recid=51

Comparativa d'eines help desk Open Source

http://www.dataprix.com/blogs/respinosamilla/aplicaciones-para-gesti-n-incidencias-bugs-productos-opensource

Wikipedia: Comparison of issue-tracking systems

http://en.wikipedia.org/wiki/Comparison_of_ticket-tracking_systems

Introducción técnica a Windows Server 2008

http://www.microsoft.com/latam/technet/windowsserver/longhorn/evaluate/whitepaper.mspx#EWBAC

Redes Privadas Virtuales en Windows 2003

http://technet.microsoft.com/es-es/library/cc759780(WS.10).aspx

Layer 2 Tunneling Protocol

http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol