Escola Politècnica Superior
d'Enginyeria de Vilanova i la Geltrú
UNIVERSITAT POLITÈCNICA DE CATALUNYA

PROJECTE FI DE CARRERA

TÍTOL: Auditoria i execució de pla d'acció per la millora de la seguretat dels sistemes d'informació.

AUTOR: Alexandre Pérez Fernàndez

TITULACIÓ: Enginyeria en Automàtica i Electrònica Industrial

DIRECTOR: Pere Ponsa Asensio

DEPARTAMENT: Enginyeria de Sistemes, Automàtica i informàtica industrial.

DATA: Juliol 2010

TÍTOL: Auditoria i execució de pla d'acció per la millora de la seguretat dels sistemes d'informació.

COGNOMS: Pérez Fernàndez **NOM: Alexandre**

TITULACIÓ: Enginyer en Automàtica i electrònica industrial

ESPECIALITAT: **PLA: 2003**

DIRECTOR: Pere Ponsa Asensio

DEPARTAMENT: Enginyeria de Sistemes, Automàtica i informàtica industrial.

QUALIFICACIÓ DEL PFC

TRIBUNAL

FRANCESC XAVIER ROSET JUAN (PRESIDENT)	MARTA DIAZ BOLADERAS (SECRETARI)	CRISTOBAL RAYA GINER (VOCAL)

DATA DE LECTURA: 12 de Juliol de 2010

Aquest Projecte té en compte aspectes mediambientals: □ Sí □ No

PROJECTE FI DE CARRERA

RESUM (màxim 50 línies)

Comprendre, adaptar i implantar la normativa de seguretat dels sistemes d'informació ISO/IEC 27002:2005 en l'àmbit d'una organització proveïdora de serveis de gestió d'instal·lacions esportives on el sistema d'informació està compost principalment per una part ofimàtica, per l'administració i gestió pròpia del servei, i una part d'automatització industrial, per el manteniment, control i supervisió automatitzada dels equipaments esportius.

A partir del plantejament del problema a resoldre en forma d'auditoria, es vol fer un desplegament que permeti portar a terme un pla d'acció concret, per la millora de la seguretat informàtica, en alguns dels aspectes detectats com vulnerabilitats en els sistemes d'informació del Servei auditat.

Per tal de complir amb aquest objectius, es desenvolupen les següents fases:

La primera correspon a la introducció, on mitjançant diverses reunions amb els responsables del servei i els promotors d'aquest projecte, es defineixen els objectius i es planifiquen les tasques a desenvolupar.

En la segona, s'estudia la norma ISO/IEC 27002:2005 i es desenvolupa el mètode per convertir la mateixa en un qüestionari per l'avaluació de la seguretat dels sistemes d'informació.

La tercera, on s'especifica el funcionament, i es realitza el disseny i desenvolupament de l'eina de suport a l'auditoria basada en el qüestionari d'avaluació creat en la fase precedent.

Finalment, en la quarta fase, s'executen les tasques pròpies de l'avaluació de la seguretat dels sistemes d'informació: Les respostes al qüestionari, l'avaluació, l'estudi dels resultats, l'informe d'auditoria i la confecció d'un pla d'acció per la millora compost principalment per la creació d'un pla de contingència (Pla de continuïtat dels serveis de negoci i pla de represa informàtica dels sistemes sensibles).

Paraules clau (màxim 10):

ISO/IEC 27002:2005	Seguretat	Sistemes Informació	Auditoria
Qüestionari	Avaluació	Continuïtat	Contingència
PHP	AJAX		

Sumari

En suport digital (CD) s'entrega:

- memoria_67248.pdf
- resum_67248.pdf
- poster_67248.pdf
- propostaPFC_67248.pdf
- annex_codi_font_67248.zip
- annex_model_placontingencia_67248.pdf
- annexA_67248.pdf
- annexB_67248.pdf
- annexC_67248.pdf
- annexD_67248.pdf
- annexE_67248.pdf

Inclòs en la memòria format paper:

- Portada.
- Pàgina impresa per la qualificació del PFC.
- Document de proposta original de PFC.
- Breu descripció (Resum i paraules clau).
- Sumari.
- Índex.
- Introducció.
- Cos de la memòria.
- Conclusions.
- Bibliografia.
- Annex A: Qüestionari d'avaluació de la Seguretat dels Sistemes d'informació. basat en la norma ISO/IEC 27002:2005.
- Annex B: Codi font php del Controlador de la lògica de programa del model MVC.
- Annex C: Qüestionari SIS
- Annex D: Enginyeria en Automàtica i Electrònica Industrial.
- Annex E: Article: "Diseño de herramienta de evaluación del grado de cumplimento de normativas en el ámbito de la interacción entre personas y la gestión de los sistemas de información".

Agraïments

L'autor d'aquest projecte agraeix a: David Raya i Rubén Menéndez, del servei STIC (Tecnologies de la Informació i les Comunicacions) de l'EPSEVG (Escola Politècnica Superior de Vilanova i la Geltrú), per la seva participació en la integració de les eines desenvolupades en aquest projecte dins de la infraestructura tècnica de l'escola i pel seu suport continuat. Anton Gomà, Marta Garcia, Andreu Benet, del servei SAF (Servei d'Activitats Físiques) de la UAB (Universitat Autònoma de Barcelona), per la seva participació activa en l'aplicació dels mètodes i eines de suport descrits en aquest treball dins l'organització del seu servei. Ramon Vilanova, del departament de telecomunicació i enginyeria de sistemes (ETSE) de la UAB per la seva participació en la fase de concepció d'aquest projecte i pels seus consells. Molt especialment a Pere Ponsa, director d'aquest projecte, per la seva disponibilitat permanent i per l'aportació dels seus coneixements que m'han servit de guia en el desenvolupament d'aquest projecte. També molt especialment, a la meva companya Roser Jané, i per extensió a la seva i la meva família, pel seu suport constant.

A tots, moltes gràcies per la vostra ajuda, sense la qual aquest projecte no hagués estat possible.

Índex

PART I: INTRODUCCIÓ

PART II: REALITZACIÓ

PART I: INTRODUCCIÓ

Capítol 1: Introducció

1.1 Presentació

Aquest projecte final de carrera (PFC) es va definir a partir d'una proposta de col·laboració entre el departament d'Enginyeria de Sistemes, Automàtica i Informàtica Industrial (ESAII) de l'Escola Politècnica Superior de Vilanova i la Geltrú (EPSEVG), el departament de telecomunicació i enginyeria de sistemes (ETSE) de la Universitat Autònoma de Barcelona (UAB) i el Servei d'Activitats Físiques (SAF) de la Universitat Autònoma de Barcelona (UAB).

El servei SAF s'encarrega de la gestió de les instal·lacions esportives del Campus de la UAB a Bellaterra (Cerdanyola del Vallès). En la seva carta de serveis podem trobar aspectes com: Manteniment i gestió dels sistemes de control i supervisió, gestió d'abonats, control d'accessos, serveis web a usuaris, proveïdor d'aplicacions web per clients específics, etcètera. Com entitat, actua amb el rol de empresa vinculada a la UAB i per tant disposa d'una organització empresarial amb gairebé tots els departaments compresos: Direcció (cap de servei), Administració, Sistemes d'informació, Recursos Humans, etc.

Per la definició dels termes de la col·laboració entre el departament ESAII de l'EPSEVG i el SAF de la UAB, per tal que donés com a resultat el present PFC, es va tenir en compte que el treball de col·laboració apliqués el model definit en el projecte *Role-Playing* [6], model que pretén *escurçar la distància entre el món universitari i el món industrial afavorint l'adquisició de competències principalment pràctiques (aprenentatge de nou coneixement i transferència del mateix, capacitat per resoldre problemes per iniciativa pròpia, capacitat per comprendre les necessitats d'altres grups de treball, etcètera)*, i les necessitats prioritàries dels SAF, expressades pels seus responsables, relacionades amb el programa docent i la experiència professional de l'autor d'aquest projecte. Es va decidir, per tant, que el treball de col·laboració consistiria en una avaluació prèvia de la seguretat dels sistemes d'informació del SAF i execució del pla d'acció resultant per la millora dels aspectes detectats com febles o vulnerables.

Inicialment, es pretenia realitzar una avaluació de la seguretat dels sistemes d'informació amb el suport d'un conjunt de bones pràctiques recollides en la norma ISO/IEC 27002:2005 (estàndard generalment acceptat). No obstant, després d'un estudi preliminar de la norma es va detectar la següent problemàtica:

- Document molt extens: 11 capítols que comprenen 36 objectius de seguretat a complir amb 153 controls a implantar o verificar.
- Difícil interpretació: Llenguatge tècnic que requereix, en moltes ocasions, la participació d'un auditor expert.
- Document genèric: Per excés, al comprendre tots els aspectes relacionats amb la seguretat dels sistemes d'informació, i per defecte, al no recollir les especificitats del SAF.
- Suport en paper: No disposa de cap eina de suport digital que faciliti la recollida de dades i l'estudi posterior de les mateixes.
- No millora continuada: El suport no facilita la represa de l'estudi per tal d'actualitzar-lo i realitzar un treball de millora periòdic.
- Recursos insuficients: L'auditoria prèvia i els posteriors estudis per la millora continuada, suposaven uns requeriments de personal i de recursos molt superior als disponibles en el departament d'Informàtica del SAF.

Per donar solució a aquestes problemàtiques, el PFC desenvolupa, com a part principal del treball, un mètode per adaptar la normativa ISO/IEC 27002:2005 a un qüestionari de seguretat dels sistemes d'informació de forma que l'estudi pugui ser implantant per un responsable informàtic (no expert), i suportat per una eina web que ens dóna, a més, les següents funcionalitats:

- Automatització de la recollida de dades: les respostes del qüestionari de seguretat i els documents adjunts a cada control son recopilades en la base de dades pel seu posterior estudi.
- Definició de perímetre: permet no avaluar controls que no siguin d'aplicació i adjuntar les especificitats del servei auditat.
- Automatització de l'estudi d'Avaluació: avaluació qualitativa, quantitativa i detallada (pla d'acció).
- Millora continuada: Històrics d'evolució i facilitat de represa de l'estudi per auditories periòdiques.

Per aquest PFC, s'ha utilitzat l'eina desenvolupada per realitzar una auditoria de seguretat dels sistemes d'informació del SAF, estudi de l'avaluació detallada, confecció d'un pla d'acció per la millora de la seguretat i un pla de contingència dels sistemes d'informació.

Amb aquest mètode i funcions aconseguim que la gestió de la seguretat dels sistemes d'informació, es a dir, l'auditoria, el pla d'acció i els treballs de millora continuada, pugui ser realitzada en el futur amb els recursos existents en el SAF.

El disseny de l'eina de suport per l'auditoria de la Seguretat dels Sistemes d'Informació permet que aquesta eina pugui ser utilitzada en qualsevol empresa, servei o organització que requereixi autoavaluar-se en el grau de compliment de la normativa ISO/IEC 27002:2005.

1.2 Estat de l'art

Existeixen múltiples estàndards per avaluar la seguretat dels sistemes d'informació. A nivell sectorial, com per exemple la TCSEC (*Trusted Computer Security*), norma d'Estats Units creada en 1985 en el sector militar, o a nivell internacional, com ITSEC (*Information Technology Securtity*), normativa de caire Europeu creada en 1991. En el projecte que ens ocupa, és a dir, l'avaluació de la Seguretat dels Sistemes d'informació en el sí d'una organització empresarial, l'estàndard internacional més estès i comunament acceptat és la norma ISO/IEC 27002:2005.

La norma ISO/IEC 27002:2005 és un codi de bones pràctiques per la gestió de la seguretat en els sistemes d'informació. És aplicable a tota organització independentment de la seva mida o complexitat i les seves recomanacions són flexibles i neutres en quant a la solució tecnològica aplicada. El seu origen el trobem en el 1995, quan el BSI (*British Standard Institute*) publica la norma BS7799, un codi de bones pràctiques per la gestió de la seguretat de la informació. En l'any 2000, la ISO (*International Organization for Standarization*) i la IEC (*International Electrotechnical Comission*) revisen i adopten la norma britànica publicant la ISO/IEC 17799 (*Information technology — Security Techniques — Code of practice for information security management*). Després de ser actualitzada el 2005 en segona edició, l'any 2007 es publica una correcció tècnica (*Technical Corrigendum 1*) per recollir el canvi de codificació implantat per l'organisme internacional per la estandardització, passant a denominar-se ISO/IEC 27002:2005.

En relació a les eines de suport a l'auditoria basada en la norma ISO/IEC 27002:2005, s'ha detectat que les empreses d'auditoria disposen de fulles de càlcul que permeten recollir dades i fer una valoració de cada un dels controls o recomanacions descrites en la norma. Algunes d'aquestes eines tenen un format de qüestionari, d'altres, són un recull dels títols de cada un dels capítols, apartats i sub-apartats de la norma per tal de fer les anotacions i valoracions. En qualsevol dels dos formats, els suports estudiats no preveuen el desenvolupament de l'auditoria sense la participació d'un auditor extern, ja que mantenen el nivell de llenguatge tècnic expert i requereixen disposar del document físic per tal de consultar termes, definicions, descripcions, guies d'implantació, etcètera, de cada un dels

controls. Tampoc s'ha detectat en el mercat una eina web que permeti la automatització de la recopilació de dades "on-line", l'autoavaluació del grau de compliment de la norma, avaluació detallada de suport per la confecció d'un pla d'acció, i el seguiment de l'evolució de la qualitat en la gestió de la seguretat per la millora continuada.

1.3 Objectius

L'objectiu principal és comprendre, adaptar i implantar la normativa de seguretat dels sistemes d'informació ISO 27002:2005 en l'àmbit d'una organització proveïdora de serveis de gestió d'instal·lacions esportives on el sistema d'informació està compost principalment per una part ofimàtica, per l'administració i gestió pròpia del servei, i una part d'automatització industrial, per el manteniment, control i supervisió automatitzada de les instal·lacions esportives.

A partir del plantejament del problema a resoldre en forma d'auditoria, es vol fer un desplegament que permeti portar a terme un pla d'acció concret, per la millora de la seguretat informàtica, en alguns dels aspectes detectats com vulnerabilitats en els sistemes d'informació del Servei d'Activitats Físiques de la UAB.

Els mètodes i eines desenvolupades han de poder ser aplicables a qualsevol altre organització, servei o empresa, independentment de la seva mida o complexitat.

1.4 Planificació de tasques

A partir de la norma ISO 17799-2005 es vol establir un marc de treball que permeti, de forma genèrica, l'aplicació d'una auditoria sobre un servei, organització o empresa, centrant el problema en la seguretat dels sistemes de la informació. Per aplicar aquesta metodologia es desenvoluparà una plataforma en suport digital (Web) que permeti l'automatització de la recollida de dades i informació via telemàtica facilitant així l'accés "on-line" a qualsevol usuari (Auditor o avaluador). Aquesta tasca, suposarà la part més important en quant a temps i recursos emprats.

En el diagrama de la Figura 1 es mostra la primera proposta, que es va fer als responsables del SAF, de distribució temporal de l'execució de les diferents fases en les que es va dividir inicialment aquest projecte.

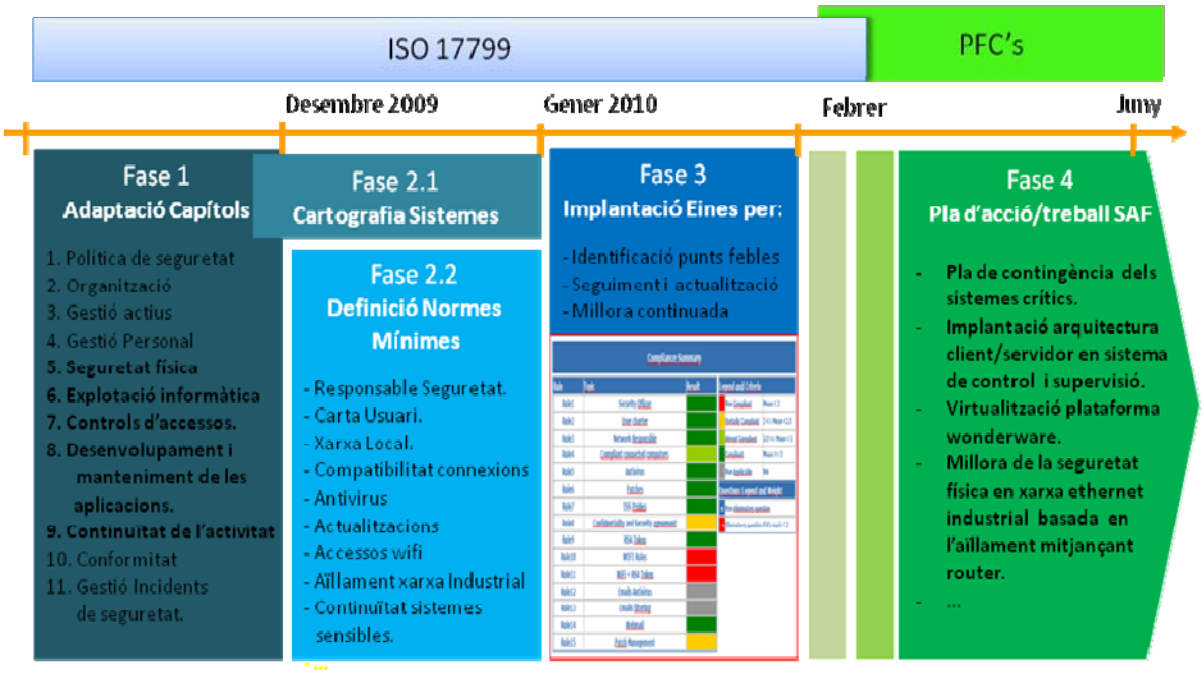


Figura 1:Diagrama temporal desenvolupament tasques

En la fase 1 es pretenia adaptar la norma ISO/IEC 27002:2005 a les especificitats del servei. No obstant, es va decidir convertir la normativa en un qüestionari que ens permetés avaluar el grau de compliment de cada un dels capítols de la norma. Aquest procés ens va portar fins al mes de gener de 2010.

La fase 2, inicialment dividida en dos sub-fases, es pretenia recopilar informacions tècniques en relació als sistemes d'informació: arquitectura de xarxa, nombre i tipus de servidors, aplicacions i serveis, característiques de les sales tècniques, etc. També definir clarament els objectius de seguretat, establint unes normes mínimes a complir. Finalment, es va decidir que les tasques de la fase 2 havien de ser suportades també per l'eina de suport d'auditoria. Per tant, es va avançar el desenvolupament de l'eina de suport, afegint les funcions de recopilació de dades, per tal de tenir una informació complerta dels sistemes d'informació, i de definició de perímetre, per tal de definir els objectius de seguretat pretesos i les especificitats dels servei auditat.

La fase 3, avançada a inicis de desembre de 2009 i allargada fins al febrer de 2010, es va dedicar completament al desenvolupament de l'eina de suport a l'auditoria per l'avaluació del grau de compliment de la norma ISO/IEC 27002:2005.

Entre la fase 3 i la fase 4, hem d'afegir les tasques pròpies de l'auditoria, és a dir, respondre el qüestionari d'avaluació per part del responsable informàtic del servei (març - abril 2010), i estudi i informe de l'avaluació resultant com a part de les tasques desenvolupades en aquest PFC (maig 2010).

Finalment, en la fase 4 (maig - juny de 2010), es va executar el pla d'acció per la millora centrat, principalment, per els motius que es descriuran en l'apartat 4 d'aquesta memòria, en el desenvolupament d'un pla de contingència compost per un pla de continuïtat dels serveis de negoci en mode degradat i un pla de represa informàtica (PRI) dels sistemes sensibles.

1.5 Estructura del PFC

La realització d'aquest projecte es pot dividir en quatre parts diferenciades (figura 2). La primera correspon a la introducció, on mitjançant diverses reunions amb els responsables del SAF i els promotors d'aquest projecte, es defineixen els objectius i es planifiquen les tasques a desenvolupar. En la segona, s'estudia la norma ISO/IEC 27002:2005 i es desenvolupa el mètode per convertir la mateixa en un qüestionari per l'avaluació de la seguretat dels sistemes d'informació. La tercera, on s'especifica el funcionament, i es realitza el disseny i desenvolupament de l'eina per el suport a l'auditoria basada en el qüestionari d'avaluació creat en la part precedent. Finalment, en la quarta part, s'executen les tasques pròpies de l'avaluació de la seguretat dels sistemes d'informació: Les respostes al qüestionari, l'avaluació, l'estudi dels resultats, l'informe d'auditoria i la confecció d'un pla d'acció per la millora compost principalment per la creació d'un pla de contingència (Pla de continuïtat dels serveis de negoci i pla de represa informàtica dels sistemes sensibles).

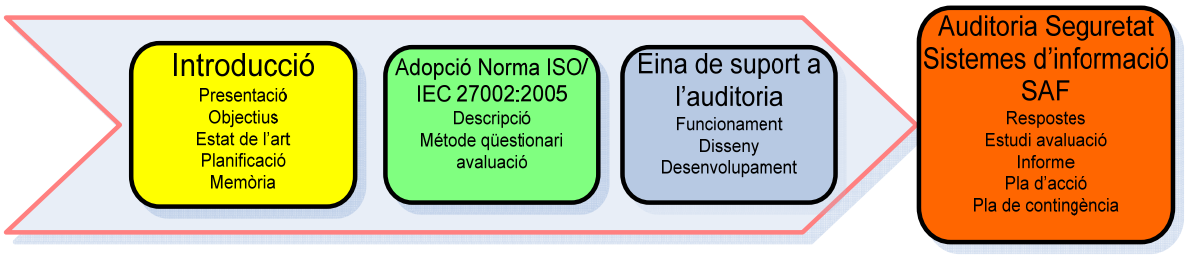


Figura 2: Parts del projecte

1.6 Estructura de la memòria

En la primera part de la memòria, corresponent al capítol 1 es fa la introducció d'aquest projecte: Origen, Definició dels objectius, Estat de l'art, planificació, etc.

Els capítols 2 i 3 corresponen a la part de desenvolupament del projecte, on es creen els mètodes i eines utilitzades en la part d'aplicació.

La part d'aplicació, corresponent al capítol 4, descriu les tasques realitzades per la implantació d'una auditoria de seguretat dels sistemes d'informació basada en la norma ISO/IEC 27002:2005 i suportada per l'eina d'auditoria desenvolupada en la part 2.

L'Annex A, Qüestionari d'avaluació de la Seguretat dels Sistemes d'informació basat en la norma ISO/IEC 27002:2005), correspon al resultat d'aplicació dels mètodes i desenvolupaments descrits en la part 2 d'aquesta memòria. Destacar que es tracta de la part més important del desenvolupament d'aquest projecte en quan a temps i recursos dedicats, així com per la component d'innovació que hi aporta.

L'Annex B, Codi font php del Controlador de la lògica de programa del model MVC, correspon al codi font php íntegre que implementa el Controlador de la lògica de programa. Es tracta de la part principal del codi font des del qual es realitzen les crides a les consultes de bases de dades i a les plantilles de vistes d'usuari.

L'Annex C, Qüestionari SIS, correspon al qüestionari de satisfacció, omplert pel responsable del sistemes d'informació del servei SAF en relació a les tasques del rol avaluador, principalment, respondre el qüestionari i aportació de comentaris, informacions i documents a través de l'eina de suport a l'auditoria.

En L'Annex D, es relaciona els treballs desenvolupats en aquest projecte amb els estudis d'Enginyeria en Automàtica i Electrònica Industrial.

L'Annex E, "Diseño de herramienta de evaluación del grado de cumplimento de normativas en el ámbito de la interacción entre personas y la gestión de los sistemas de información", correspon a un article aprovat per ser defensat en el proper "XI Congreso Internacional de Interacción Persona-Ordenador", Setembre 2010 a Valencia, fruit dels treballs desenvolupats en aquest projecte com es descriurà en el capítol de conclusions.

1.7 Aspectes mediambientals

Fent ús de la guia d'ambientalització [5], publicada per l'Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú, en la qual *s'estableixen les pautes necessàries per tal que els projectes final de carrera realitzats en el campus de l'EPSEVG entrin dins del marc d'actuació del Pla de Medi Ambient de la UPC*, en la realització d'aquest projecte s'han considerats els següents aspectes en les diferents fases:

- **Concepció:**
  - S'han dissenyat programes d'execució ràpida.
- **Construcció:**
  - No s'han utilitzat colors impactants o agressius per a la visió de l'usuari.
  - S'ha utilitzat una dimensió de font suficientment perceptible.
  - S'han implantat funcions per tal d'eliminar els arxius antics.
  - S'han utilitzar fitxers d'extensió mínima: arxius gràfics d'extensió JPG.
- **Explotació:**
  - Infraestructures compartides: El funcionament en producció del resultat d'aquest projecte, implica la utilització dels recursos existents (xarxes informàtiques, servidors, fonts d'alimentació, etc.).
  - Suport digital: Totes les funcions de l'explicatiu desenvolupat es serveixen en format digital (interfase web d'usuari), així com la recopilació de dades i informacions que no requereixen una copia en suport paper.
- **Desmantellament:** L'aplicació no requereix accions de gestió de residus per la posada fora de servei.

PART II: REALITZACIÓ

Capítol 2: Adaptació i aplicació Norma ISO/IEC 27002:2005

2.1 Descripció

La norma ISO/IEC 27002:20005 és un estàndard internacional que recull una sèrie de bones pràctiques i principis generals per tal d'establir la gestió de la seguretat dels sistemes d'informació en el sí d'una organització: inicialitzar, implementar, mantenir i millorar la gestió de la seguretat de la informació.

2.2 Seguretat dels sistemes d'informació

Es considera la informació com un actiu de valor per la organització que requereix, per tant, d'una protecció adequada. Aquesta protecció es fa cada vegada més crítica en la mesura que augmenta l'exposició de la informació, propietat de la nostra empresa, en un entorn d'interconnectivitat creixent.

Internet, xarxes privades, comerç electrònic, serveis web, espais FTP, suports d'emmagatzematge portàtils, correu electrònic, etc. són algunes de les moltes possibilitats on la nostra informació de negoci pot quedar exposada i subjecta a vulnerabilitats o riscos.

L'objectiu de la seguretat de la informació és protegir-la, minimitzant els riscos i eliminant les vulnerabilitats que la nostra informació pugui tenir en un medi determinat, per tal de preservar les següents propietats:

- **Confidencialitat:** que la informació de valor per la organització sigui accessible únicament per les persones autoritzades.
- **Integritat:** assegurar que els mitjans de processament de la informació la mantenen complerta, exacta i verdadera.
- **Disponibilitat:** que la informació sigui accessible, en els instants definits, per els usuaris autoritzats.

Des del punt de vista de les causes que poden posar en perill la preservació de les propietats anteriors, la seguretat dels sistemes d'informació ha d'implantar els procediments i mecanismes adequats per tal d'evitar el frau, l'espionatge, el sabotatge, el vandalisme o la pèrdua de dades o serveis provocades per un incendi o inundació.

La gestió de la seguretat de la informació es realitza implantant un conjunt de controls, politiques, processos i procediments, així com, instaurant una estructura organitzativa i funcions hardware / software adequades, en funció dels riscos i objectius de seguretat fixats per l'empresa. Els controls definits per cada organització han de ser implantats, revisats, actualitzats, millorats i monitoritzats per tal d'assegurar els objectius. Com a punt de partida es poden definir un conjunt de controls considerats essencials, ja sigui perquè són de requeriment legal o de pràctica comuna en la seguretat de la informació. Els punts que poden ser considerats essencials des del punt de vista legislatiu són:

- Protecció i privacitat de les dades personals.
- Protecció dels registres legals de la organització.
- Drets de la propietat intel·lectual.

Els punts considerats de pràctica comuna en la seguretat de la informació són:

- Document de política de seguretat.
- Definició de les responsabilitats en matèria de seguretat dels sistemes d'informació.
- Gestió de les vulnerabilitats tècniques i incidents de seguretat

- Control d'accessos.
- Pla de contingència.
- Etc.

Les dades, processos, sistemes i xarxes informàtiques són un actiu important per l'empresa. Definir, implantar, mantenir i millorar la seguretat en els sistemes d'informació pot ser essencial per tal de mantenir la continuïtat i competitivitat del negoci, minimitzar el danys que un incident pugui provocar a la organització, maximitzar el retorn de les inversions, assegurar la legalitat, aconseguir oportunitats de negoci o mantenir una bona imatge comercial.

2.3 Estructura del document ISO/IEC 27002:2005

L'estàndard conté 11 dominis de control que engloben col·lectivament 36 objectius de control. Seguidament, la llista dels 11 dominis de seguretat amb els seus respectius objectius de control [1]:

a) Política de Seguretat
   i. Política de seguretat dels sistemes d'informació

b) Organització Interna de la seguretat dels Sistemes d'informació
   i. Organització Interna
   ii. Tercers

c) Gestió dels actius
   i. Responsabilitat relatives als actius
   ii. Classificació de les informacions

d) Seguretat lligada als recursos humans (Gestió de Personal)
   i. Abans la presa de funcions
   ii. Durant el contracte
   iii. A la fi o modificació del contracte

e) Seguretat Física
   i. Zones de seguretat
   ii. Seguretat del material

f) Gestió de l'explotació i de les telecomunicacions
   i. Processos i responsabilitats lligades a l'explotació
   ii. Gestió de la prestació de serveis per un tercer
   iii. Planificació i acceptació del sistema
   iv. Protecció contra els codis perjudicial o no desitjat
   v. Copies de seguretat
   vi. Gestió de la seguretat de les xarxes informàtiques
   vii. Manipulació dels suports
   viii. Intercanvi d'informacions
   ix. Serveis de comerç electrònic
   x. Vigilància

g) Control d'accessos
   i. Necessitats en matèria de control d'accessos
   ii. Gestió dels accessos usuaris
   iii. Responsabilitats dels usuaris
   iv. Control d'accés a la xarxa
   v. Control d'accessos als sistemes d'explotació

vi. Control d'accessos a les aplicacions i la informació
vii. Informàtica nòmada o tele-treball

h) Adquisició, desenvolupament i manteniment de les informacions
   i. Necessitat en seguretat dels sistemes d'informació
   ii. Tractament correcte en el si de les aplicacions
   iii. Mitjans criptogràfics
   iv. Seguretat dels fitxers sistema
   v. Seguretat del desenvolupament i gestió del suport
   vi. Gestió de les vulnerabilitats tècniques

i) Gestió dels incidents lligats a la seguretat dels sistemes d'informació
   i. Informe dels incidents i les vulnerabilitats de seguretat en els S.I.
   ii. Gestió dels incidents i millores de la seguretat dels S.I.

j) Gestió del pla de continuïtat de l'activitat
   i. Aspectes de la seguretat dels S.I. en matèria de gestió de la continuïtat de l'activitat

k) Conformitat
   i. Conformitat amb les exigències legals
   ii. Conformitat amb les polítiques i normes de seguretat dels S.I. i conformitat tècnica
   iii. Consideracions per les auditories de seguretat dels S.I.

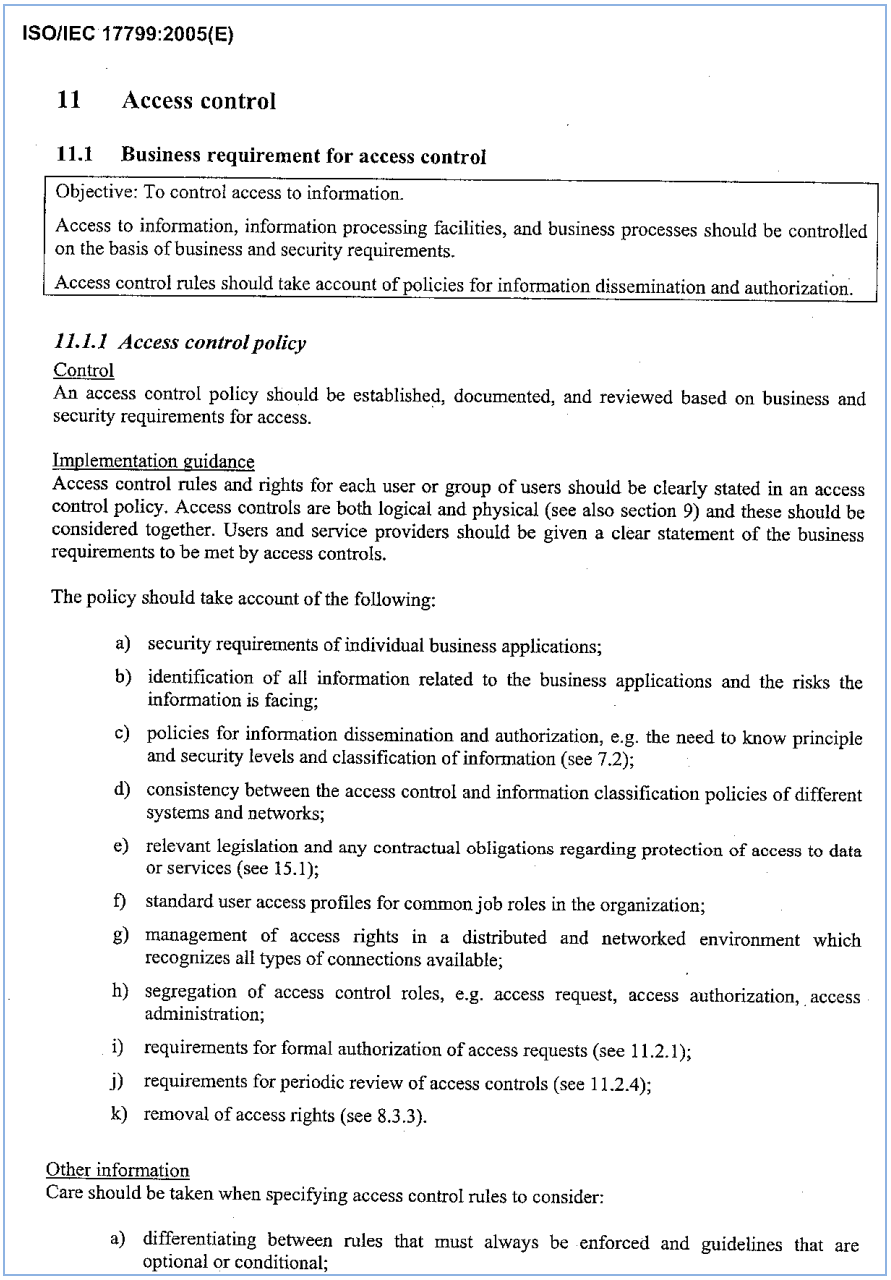
En l'annex Qüestionari es troben les definicions de cada un dels objectius de control (emmarcats amb quadre verd).

L'estàndard no defineix la importància (ponderació) de cada objectiu de control. Depenent de les especificitats del servei o organització avaluada, tots els objectius poden tenir la mateixa importància, no obstant, cada organització ha d' identificar els objectius de control que són d'aplicació en el seus serveis, aplicacions o processos de negoci.

Cada objectiu de control (36 en total) està compost per varis controls a aplicar o implantar per tal de complir amb l'objectiu definit. En total, s'han detectat en aquest estàndard 153 controls. Cada control està estructurat de la següent forma:

- **Control:** Definició del control específic.
- **Guia d'implantació:** Informació detallada de suport a la implantació del control.
- **Informació:** Informació complementaria relacionada amb el control que pot ser considerada, com per exemple, consideracions legals i referències a altres estàndards.

En la figura 3 tenim un exemple de control extret de l'estàndard [1] corresponent al domini "Control d'Accessos" i a l'objectiu de control "Necessitat en seguretat dels sistemes d'informació", amb la seva corresponent guia d'implantació i informació relacionada.



ISO/IEC 17799:2005(E)

11 Access control

11.1 Business requirement for access control

Objective: To control access to information.

Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.

Access control rules should take account of policies for information dissemination and authorization.

11.1.1 Access control policy

Control

An access control policy should be established, documented, and reviewed based on business and security requirements for access.

Implementation guidance

Access control rules and rights for each user or group of users should be clearly stated in an access control policy. Access controls are both logical and physical (see also section 9) and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

a) security requirements of individual business applications;

b) identification of all information related to the business applications and the risks the information is facing;

c) policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information (see 7.2);

d) consistency between the access control and information classification policies of different systems and networks;

e) relevant legislation and any contractual obligations regarding protection of access to data or services (see 15.1);

f) standard user access profiles for common job roles in the organization;

g) management of access rights in a distributed and networked environment which recognizes all types of connections available;

h) segregation of access control roles, e.g. access request, access authorization, access administration;

i) requirements for formal authorization of access requests (see 11.2.1);

j) requirements for periodic review of access controls (see 11.2.4);

k) removal of access rights (see 8.3.3).

Other information

Care should be taken when specifying access control rules to consider:

a) differentiating between rules that must always be enforced and guidelines that are optional or conditional;

Figura 3:Exemple estructura de control

2.4 Mètode d'adaptació a qüestionari d'avaluació

La problemàtica que una empresa pot tenir a l'hora de realitzar una autoavaluació del grau de compliment de la seva organització en relació a una normativa, guia de disseny o estàndard, la trobem en que aquest tipus de documents solen ser extensos i de difícil interpretació i adaptació a les especificitats de l'empresa, sent freqüentment necessària la participació (contractació) d'un expert extern per tal de realitzar l'avaluació.

En el cas particular que ens ocupa, avaluació de la seguretat dels sistemes d'informació basat en la norma ISO/IEC 27002:2005, tal i com hem vist en l'apartat de presentació d'aquesta memòria, es van detectar les següents problemàtiques:

- Document molt extens: 10 capítols que comprenen 36 objectius de seguretat a complir amb 153 controls a implantar o verificar.

- Difícil interpretació: Llenguatge tècnic que requereix, en moltes ocasions, la participació d'un auditor expert.
- Document genèric: Per excés, al comprendre tots els aspectes relacionats amb la seguretat dels sistemes d'informació, i per defecte, al no recollir les especificitats del servei avaluat.
- Suport en paper: No disposa de cap eina de suport digital que faciliti la recollida de dades i l'estudi posterior de les mateixes.
- No millora continuada: El suport no facilita la represa de l'estudi per tal d'actualitzar-lo i realitzar un treball de millora periòdic.
- Recursos insuficients: L'auditoria prèvia i els posteriors estudis per la millora continuada, suposaven uns requeriments de personal i de recursos molt superior als disponibles en el departament d'Informàtica del servei.

Per tal d'habilitar que l'avaluació de la seguretat dels sistemes d'informació, basat en l'estàndard presentat, pugui ser assumida en el sí de l'empresa sense necessitat de recursos externs, es proposa un mètode per transformar la normativa ISO/IEC 27002:2005 a un qüestionari de seguretat dels sistemes d'informació. Aquest qüestionari pot ser respost per un responsable informàtic de l'empresa de forma que, en funció de les respostes recopilades, els dominis i objectius de control puguin ser avaluats.

En la figura 4 es representa la conversió de l'estructura de l'estàndard ISO/IEC 27002:2005 a un qüestionari d'avaluació de la seguretat dels sistemes d'informació.

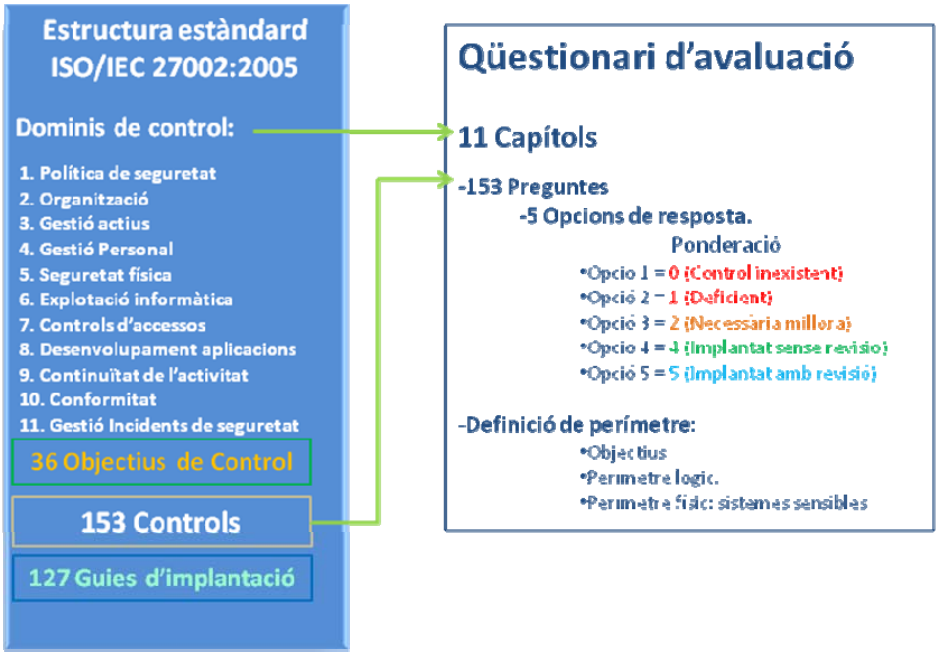


Figura 4:Conversió estructura estàndard a qüestionari d'avaluació

Els dominis de controls corresponen als capítols del qüestionari. Són aquells aspectes de la seguretat de la informació definits en l'estàndard i dels quals requerim una avaluació (avaluació per capítol). Cada capítol està dividit en apartats. Aquest apartats corresponen als objectius de control definits en l'estàndard i dels quals també requerim una avaluació per separat (avaluació detallada). Finalment, cada apartat està compost per una o varies qüestions relatives al control a implantar o revisar per tal de complir amb l'objectiu de control de l'apartat corresponent. Cada qüestió disposa de 5 opcions de resposta ponderades de la següent forma:

- **Opció 1:** valor 0, indica control inexistent.

- **Opció 2:** valor 1, indica control deficient.
- **Opció 3:** valor 2, indica que el control requereix ser millorat.
- **Opció 4:** valor 4, indica control implantat però no disposa de procediments de revisió.
- **Opció 5:** valor 5, indica control implantat amb procediments de verificació i actualització periòdics.

El resultat de l'aplicació d'aquest mètode per l'estàndard ISO/IEC 27002:2005 el podreu comprovar en el qüestionari d'avaluació adjuntat en l'annex A.

En funció de les respostes donades, la ponderació aplicada i el nombre de preguntes, obtenim l'avaluació de cada capítol aplicant la següent fórmula:

$$Avaluació\ Capítol = \frac{\sum_{i=1}^{n} valor\ resposta_i}{n}$$

On *n* es el nombre de preguntes del capítol avaluat.

Aquesta valoració quantitativa ens indicarà si és necessari actuar sobre els objectius de control compresos en el capítol tractat.

En funció del nombre, de la valoració i del pes de cada un dels capítols, obtindrem l'avaluació global del projecte d'implantació de la seguretat dels sistemes d'informació, aplicant la següent fórmula:

$$Av.\ Global = \frac{\sum_{j=1}^{c} p_j \cdot Av.Capítol}{\sum_{j=1}^{c} p_j}$$

On c és el nombre total de capítols i *Pj* el pes o ponderació assignat a cada capítol.

Aquesta valoració quantitativa ens servirà per fer un seguiment continuat de la millora de la seguretat dels sistemes d'informació implantada en l'organització.

Per últim, en funció de les respostes recopilades, obtenim directament l'avaluació detallada: valoració qualitativa i quantitativa de cada control. Es tracta de recopilar les respostes a les qüestions relatives a cada control i indicar quins controls tenen una valoració de menys de 2, ressaltant la necessitat d'aplicar accions de millora o d'implantació per tal de complir amb l'objectiu de control corresponent.

2.5 Mètode d'aplicació

En la figura 5 es representa l'esquema funcional del mètode d'aplicació del qüestionari d'avaluació. En una primera etapa, com hem vist, es tracta d'habilitar l'estàndard a través del qüestionari d'avaluació. La segona fase consisteix en definir els objectius de seguretat o punt de partida (veure part 2) que l'organització es proposa aconseguir amb l'aplicació d'aquest mètode. En aquest punt es definiran també els perímetres (físics o lògics) d'actuació, és a dir, identificar aquells sistemes, processos, serveis, dades, etc, que intervenen en la consecució dels objectius. Una vegada respost el qüestionari en la tercera etapa, s'obté l'avaluació global, per capítol i detallada. En la següent fase, es tracta de realitzar un estudi de l'avaluació obtinguda i realitzar un pla d'acció per tal d'assegurar la confidencialitat, la integritat i disponibilitat d'acord amb els objectius i perímetre definits. Finalment, per dur a terme el pla d'acció, es recorre a les guies d'implantació, incloses en l'estàndard, dels controls que requereixin accions de millora o d'implantació.

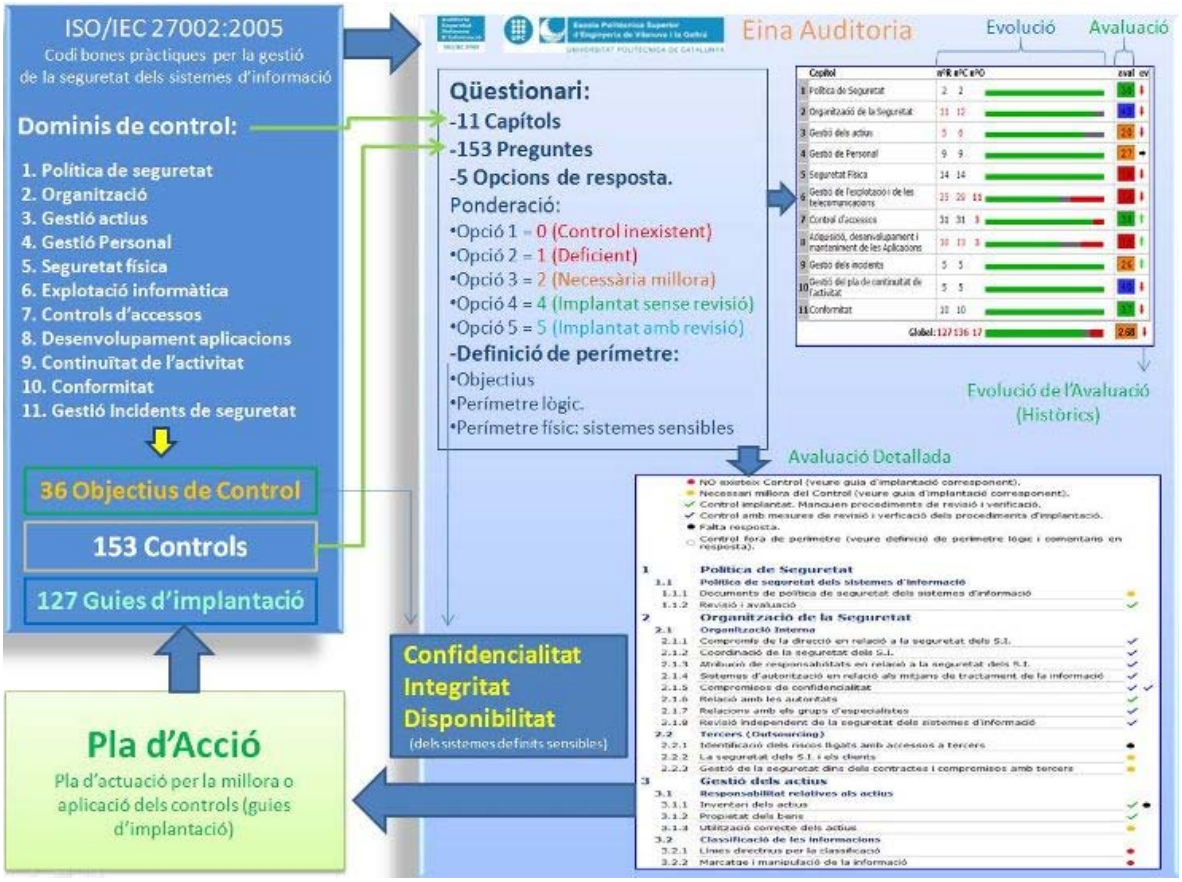


Figura 5: Diagrama mètode d'aplicació qüestionari d'avaluació.

Per tal d'implantar aquest mètode d'aplicació del qüestionari d'avaluació de la seguretat dels sistemes d'informació s'ha desenvolupat (Part 3: Eina de suport a l'auditoria) una eina de suport web que ens dóna, a més, les següents funcionalitats:

- Automatització de la recollida de dades: les respostes del qüestionari de seguretat i els documents adjunts a cada control són recopilades en la base de dades pel seu posterior estudi.
- Definició de perímetre: permet deixar fora de l'avaluació controls que no siguin d'aplicació i adjuntar les especificitats del servei auditat.
- Automatització de l'estudi d'Avaluació: avaluació qualitativa, quantitativa i detallada (pla d'acció).
- Millora continuada: històrics d'evolució i facilitat de represa de l'estudi per auditories periòdiques.

Capítol 3: Eina de suport a l'auditoria

3.1 Descripció funcional de la interfície usuari

3.1.1 Qüestionari

El responsable dels sistemes d'informació té accés al qüestionari d'avaluació iniciant sessió (Figura 6) en el següent espai web: http://qssi.epsevg.upc.edu/

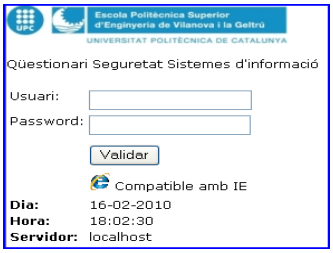


Figura 6: Pantalla inici de sessió

La pàgina per defecte en l'inici de sessió correspon a l'Evolució del qüestionari i seguiment de l'avaluació (veure apartat 3.1.3).

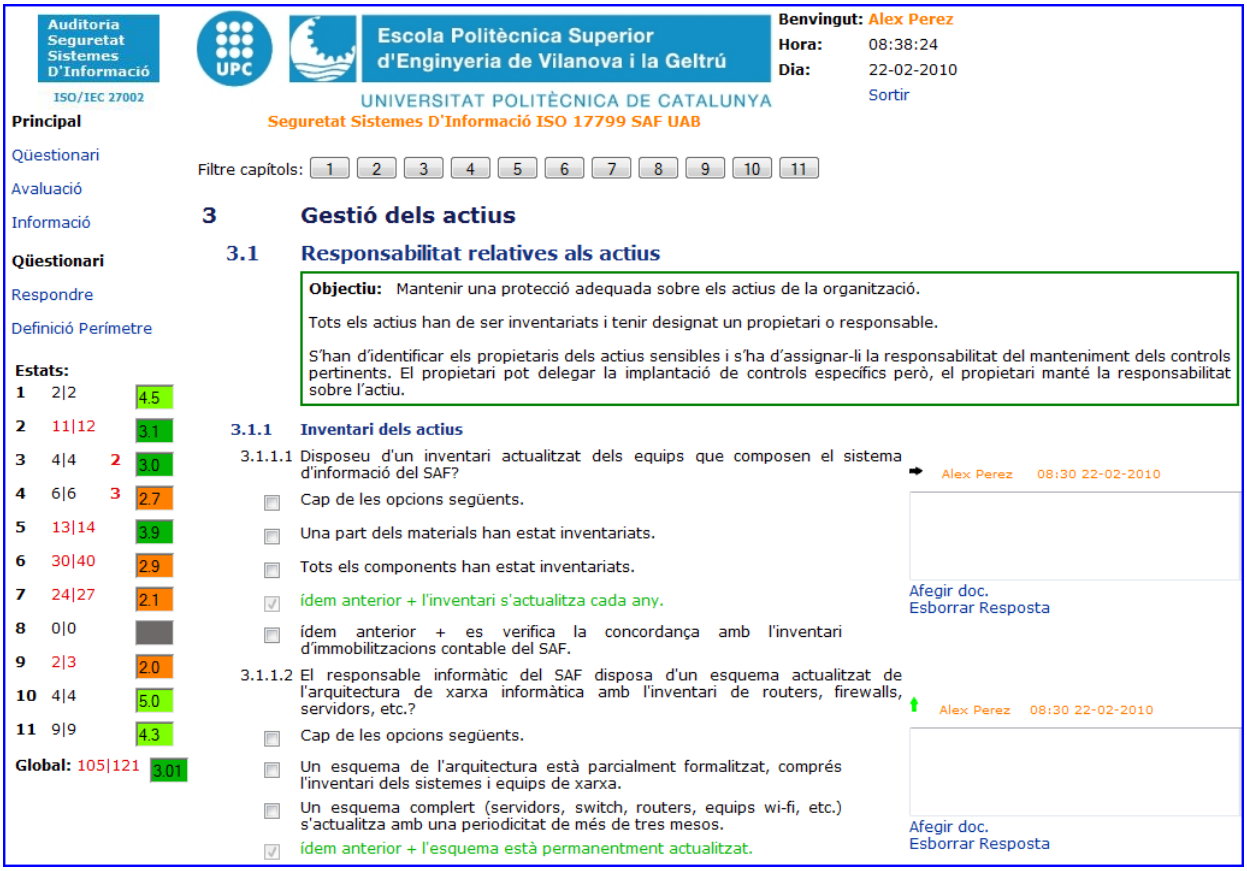


Figura 7: Pantalla funció Respondre

En el menú Principal de la mateixa trobem les següents funcions:

Qüestionari: Opció que ens permetrà accedir a les opcions pròpies del qüestionari.

Avaluació: Opció que ens permetrà accedir a les opcions d'avaluació, històric i avaluació detallada per apartat.

Informació: Opció per accedir a informacions sobre el mètode d'auditoria emprat i les instruccions per complimentar el qüestionari.

Benvingut: Indicador de l'usuari que ha iniciat la sessió, dia i hora.

Sortir: permet finalitzar correctament la sessió d'usuari.

Nom del qüestionari associat a l'usuari: Sota la capçalera, en color taronja.

En la pantalla de la funció respondre (figura 7) tenim:

Estats: Estat actual de l'avaluació de la seguretat per capítol i global.

També l'evolució de complimentació del qüestionari. En números vermells, els capítols on resten preguntes per respondre (nombre de respostes | total de preguntes)

Filtre: Botons per selecció del capítol.

Objectiu: Quadre de text (color verd) on es descriu l'objectiu corresponent a l'apartat de seguretat tractat.

Respondre: Selecció del *checkbox* corresponent. La ponderació de les opcions de resposta va de menor a major (0,1,2,4,5). Passar de l'opció 3 a 4 té un major pes, ja que, correspon a passar de tenir un control no correctament implantat, a tenir-ho correctament.

En el moment de la selecció es produeix l'avaluació instantània i el registre en la base de dades.

Registres: En el moment de respondre, queden també registrats l'usuari auditor, el dia i l'hora. Aquest registre queda indicat al costat de cada qüestió.

Indicadors d'evolució: Símbols que indiquen l'evolució de la resposta per cada pregunta.

➡ Indica, que la qüestió ha estat resposta per primera vegada o que no ha estat modificada.

⬇ Indica que durant l'ultima auditoria, aquesta qüestió ha estat resposta amb una opció de ponderació menor.

⬆ Indica que durant l'ultima auditoria, aquesta qüestió ha estat resposta amb una opció de ponderació major.

Important: Per mantenir la integritat del seguiment de l'evolució de cada control, al finalitzar la primera auditoria, totes les preguntes han de quedar amb l'indicador amb el nom d'auditor, dia i hora. Sí per algun motiu, durant la primera auditoria, es canvia d'opinió o criteri en algunes de les respostes, és convenient utilitzar l'opció d'esborrar resposta. En successives auditories (semestralment, per exemple) serà interessant observar l'evolució de cada control a través d'aquests indicadors.

Esborrar resposta: Permet esborrar la resposta donada, en un canvi de criteri o opinió (important durant la primera auditoria).

Comentari: Quadre de text que ens permet afegir un comentari a cada qüestió. En el moment d'omplir el quadre es produeix el registre en la base de dades.

Afegir Document: Ens permet afegir un document a cada control.
Sota la capçalera ens apareixerà el següent formulari. Ens permet examinar el nostre sistema d'arxius i afegir el document corresponent. El fitxer és carregat en el servidor dins de la carpeta corresponent al vostre qüestionari i al control o pregunta en qüestió. Els documents són accessibles (via http) únicament per part dels usuaris relacionats amb el qüestionari.

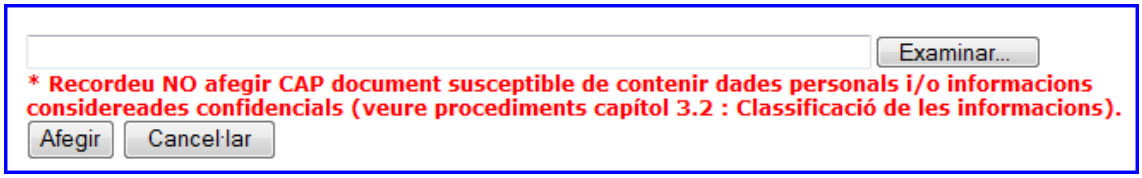


Figura 8: Diàleg Afegir Document

3.1.2 Definició perímetre

Aquesta funció (figura 9), consta dels següents apartats:

Definició d'objectius: De caire informatiu. Es pretén recollir en aquest apartat la definició dels objectius claus que ens ha d'aportar la implantació de la millora en la seguretat dels sistemes d'informació.

Perímetre físic: De caire informatiu. Es pretén acotar el perímetre d'acció de la seguretat dels sistemes d'informació, definit quins sistemes, aplicacions o dades, formen part dels sistemes d'informació crítics o sensibles. Es a dir, aquells que formen part integral de la consecució dels objectius definits prèviament. Totes les respostes del qüestionari haurien només de tenir en compte aquest sistemes definits sensibles i els objectius per assolir.

Perímetre lògic: De caire funcional. Ens permet extreure de l'avaluació de la seguretat aquells apartats que no són d'aplicació en el servei o organització avaluada. Per defecte, tots els controls estan inclosos. En el quadre d'estats, així com en el d'evolució, avaluació i històrics, s'indica en vermell i negreta, els controls que s'han definit fora de perímetre.

Figura 9: Pantalla funció Definició de Perímetre

Les qüestions corresponents als controls definits fora de perímetre apareixen desactivades en el qüestionari i amb la indicació d'apartat definit fora de perímetre.

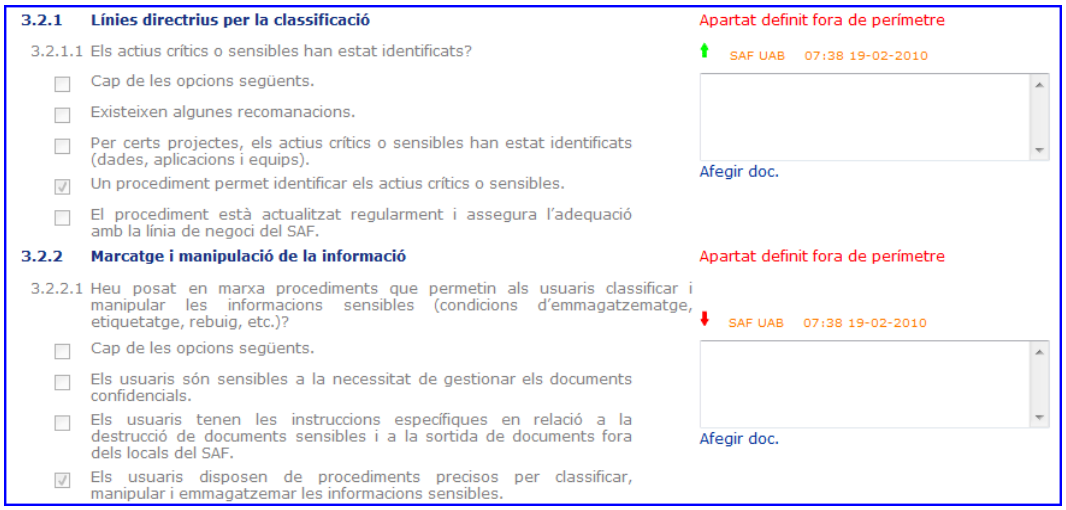


Figura 10:Representació de les qüestions definides fora de perímetre

3.1.3 Evolució

L'evolució (ev) indicada en aquest quadre de seguiment (Figura 11), correspon a l'evolució de l'avaluació respecte l'ultima auditoria enregistrada en l'històric. Això ens permet observar l'evolució qualitativa i quantitativa de la seguretat (veure apartat següent).

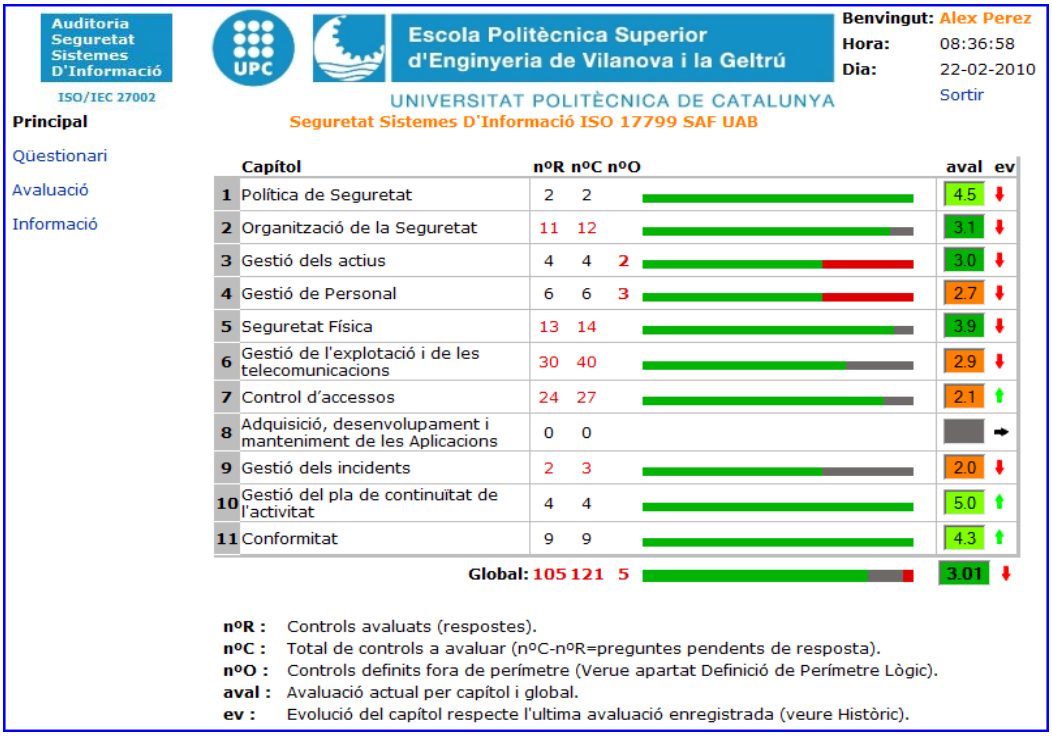


Figura 11: Pantalla funció Evolució

3.1.4 Avaluació

Avaluació actual per capítol i global (qualitativa i quantitativa), seguiment de l'avaluació respecte l'última auditoria enregistrada en l'històric (indicadors) i seguiment d'evolució del qüestionari (Nº respostes, Nº controls, controls fora de perímetre) (Figura 12). També trobem en aquesta pantalla la funció que permet enregistrar l'avaluació actual (auditoria) en la base d'històrics: Botó "Guardar en Històric".

Figura 12: Pantalla funció Avaluació Actual

3.1.5 Avaluació detallada

Avaluació actual per apartat (control) (figura 13). Ens permet detectar de forma visual l'estat actual d'implantació de cada control així com identificar possibles accions correctives.

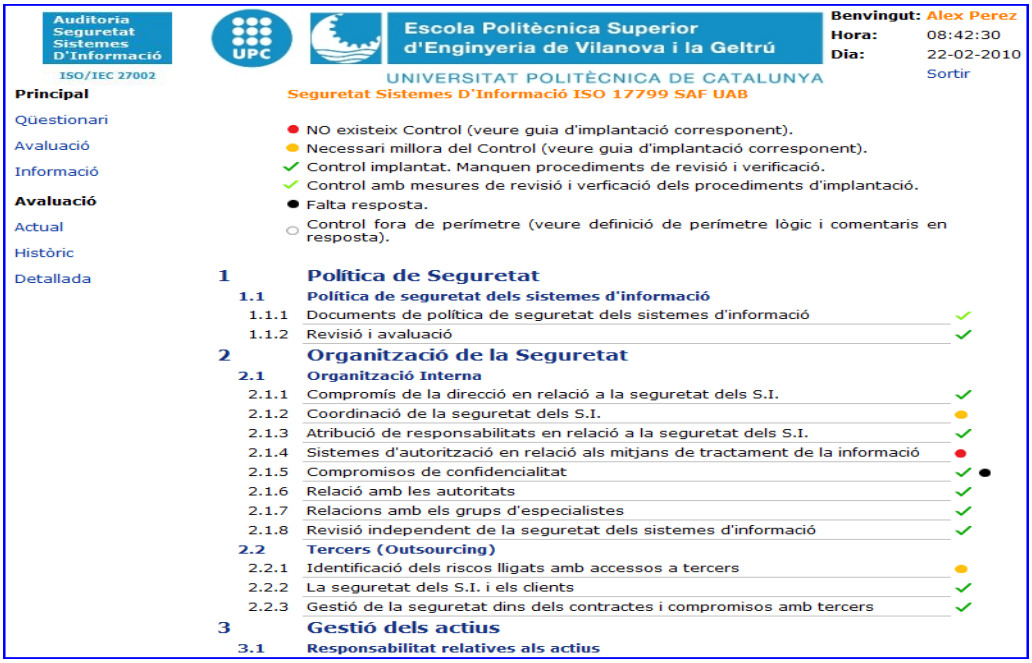


Figura 13: Pantalla Avaluació Detallada

3.1.6 Històrics

Aquesta opció habilita les següents opcions (figura 14):

- Visualitza les cinc últimes auditories enregistrades.
- Ens permet fer un seguiment evolutiu de la seguretat dels sistemes d'informació per capítol i global.
- Indicació de l'usuari que enregistra l'avaluació i la data d'enregistrament.
- Funció d'esborrar l'últim registre d'avaluació.

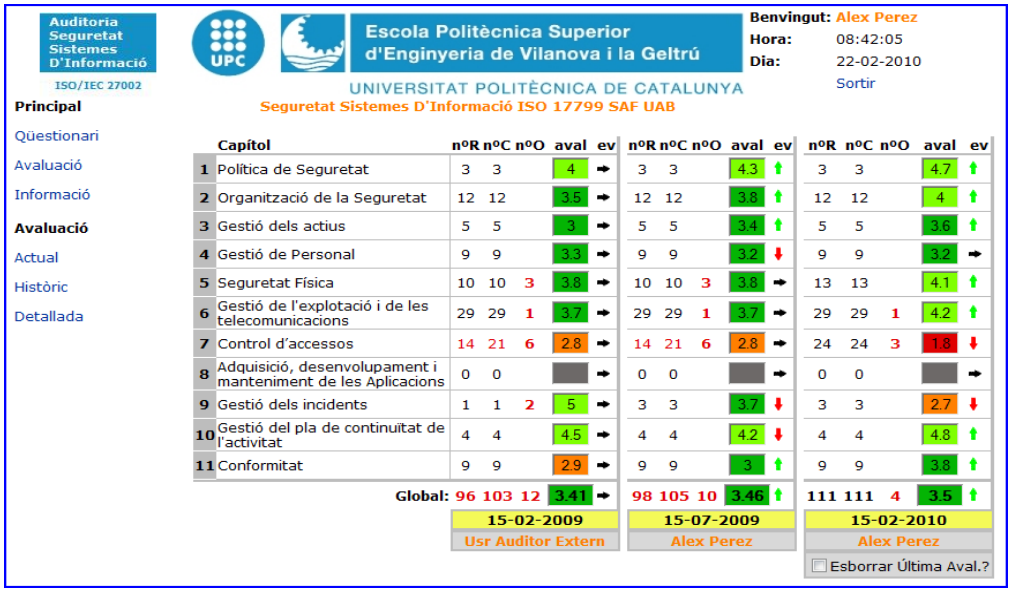


Figura 14: Pantalla d'Històrics

3.1.7 Gestió documental

En la pantalla "Respondre" (figura 7), per cada qüestió (control) tenim la funció "Afegir doc.". Ens permet vincular un document a cada control avaluat per tal de justificar la implantació del control o afegir informació complementaria a la resposta donada. També podrem afegir procediments i polítiques relacionades amb cada un dels controls implantats, disposant així d'una gestió documental (organització per capítols seguint la norma ISO/IEC 27002:2005, actualització, informació de suport, etc.) en relació a la seguretat dels nostres sistemes d'informació.

3.2 Disseny operacional de la interfície usuari

3.2.1 Registres asíncrons

Totes els registres (respostes, vinculació de documents, funcions) proporcionats a través de la interfase de l'eina d'auditoria són enregistrats asíncronament, és a dir, el seu registre en la base de dades o la carrega del fitxer relacionat es produeix en el moment que d'executar la funció sense la necessitat de recarregar la pàgina.

3.2.2 Avaluació instantània

Aprofitant l'operació de registres asíncrons, les funcions d'avaluació es produeixen també de forma instantània, es a dir, quan l'avaluador dóna una nova resposta o modifica una existent, es representa instantàniament el resultat de la nova avaluació en l'apartat *Estats* de la funció *Respondre* o en qualsevol de les funcions d'avaluació sense necessitat d'actualitzar la pàgina.

3.2.3 Seguretat

Els qüestionaris i la informació relacionada són accessibles només per els usuaris habilitats per l'administrador de l'aplicació.

En l'aportació de respostes, comentaris i documents s'indica implícitament que no s'han d'incloure dades personals, informacions confidencials, ni dades tècniques de la infraestructura informàtica que puguin afectar a la seguretat dels sistemes d'informació. Complert aquest requisit, no s'ha considerat necessari la formalització d'un acord de confidencialitat.

3.2.4 Inici de sessió

A través de la pàgina d'inici de sessió, l'usuari és identificat i autentificat per tal de gestionar els drets d'accessos al qüestionari que li correspongui. Els usuaris que tenen accés a un mateix qüestionari poden accedir en el mode Administrador, Editor o Auditor. El rol d'editor i administrador donen dret a la modificació del qüestionari d'avaluació.

3.2.5 Traçabilitat

Per cada resposta del qüestionari, s'enregistra i es mostra per pantalla el nom de l'últim usuari que ha avaluat la qüestió (control) amb la data i l'hora de l'avaluació.

3.3 Desenvolupament

3.3.1 Arquitectura multi – nivell

L'estructura de l'aplicació està dividida en tres capes o nivells:

Capa 1: Nivell de presentació o d'usuari (client). Proporciona la interfase entre l'usuari i el sistema. En aquest nivell es defineix com s'ha de representar la informació, com s'han d'introduir les dades per part de l'usuari i com s'ha d'interactuar amb el client final.

Capa2: Lògica de Procés. En aquest nivell es defineixen les regles de funcionament de l'aplicació. És l'intermediari entre el client i les dades. Com veurem seguidament, aquest nivell el dividirem en tres funcions o unitats diferents.

Capa3: Dades. Gestió i emmagatzematge de les dades.

Aquest disseny de l'arquitectura ens permetrà:

- **Independitzar el desenvolupament**, de forma que, en canvis de requeriments o modificacions de les funcions, permet modificar una capa sense alterar les altres.
- **Escalabilitat**. Qualsevol de les capes pot ser instal·lada en més d'un equip servidor, de forma que es puguin atendre nous requeriments de disponibilitat o rendiment.
- **Independitzar el procés de l'accés a dades**. En cas de canvis en els requeriments del servidor de dades, es podrà modificar l'accés a un altre motor de base de dades sense modificar la lògica de procés i presentació.
- **La possibilitat de crear diferents interfases d'usuari** (capa 1). Nivells de presentació diferents que accedeixen a les mateixes funcions de procés i a les mateixes dades.

La lògica de procés (capa 2), està dividida en tres unitats o funcions diferents:

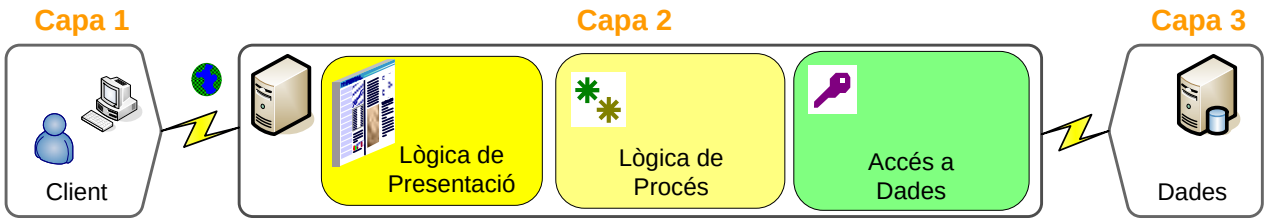


Figura 15: Nivells d'arquitectura i components.

Lògica de presentació: Determina com s'ha de presentar les interfases a l'usuari.

Lògica de procés: Determina les funcionalitats (regles de negoci).

Accés a Dades: Gestiona l'accés a la base de dades i la manipulació de les dades.

3.3.2 Model MVC (model - vista - controlador)

D'acord amb l'arquitectura descrita en l'apartat anterior, per el disseny de l'aplicació s'ha utilitzat el model MVC (model – vista – Controlador) [7].

Aquest patró de disseny, originari dels anys 70 i desenvolupat per Xerox PARC, defineix com a **M**odel la part que administra les dades, com **V**ista la part que gestiona la presentació, i com **C**ontrolador la part que interactua amb l'usuari.

Avui, aquest patró és extensament utilitzat en el desenvolupament d'aplicacions Web.

El model MCV compleix amb l'arquitectura multi-nivell, escollida per aquest projecte, separant la lògica de procés de la presentació. Ho fa possible dividint l'aplicació en tres components:

La vista: És la interfase que visualitza l'usuari a través de la qual interactua introduint o visualitzant les dades. Aquest component no realitza cap tipus de processament de dades i, per aquesta aplicació web, estarà escrit en HTML (*HyperText Markup Language*) [8].

El model: És el component on s'executen les funcionalitats de l'aplicació (lògica de procés).

El controlador: Rep les peticions que l'usuari realitza a través de la interfase i fa les crides pertinents a les funcions del model i a les parts de la vista, per tal de complir amb la petició rebuda.

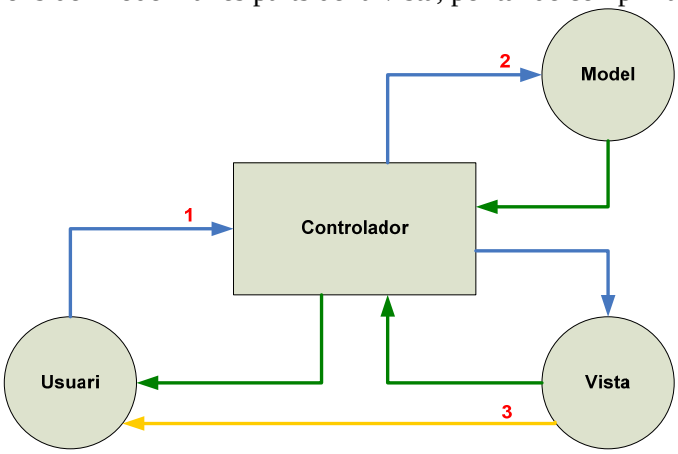


Figura 16: Esquema MVC

L'esquema anterior representa els fluxos d'informació i l'ordre en que es produeixen (números en vermell) durant el tractament d'una petició d'usuari.

En l'instant 1, l'usuari fa una petició a l'aplicació web, per exemple, clic a l'enllaç per accedir al formulari de respondre). En l'instant posterior, el controlador intercepta la petició i la processa per tal de determinar quina funció del model invocar i quina part de la vista representar.

En l'instant 2, el model executa la funció (lògica de procés) i retorna el resultat al controlador. Seguint l'exemple anterior, executarà la funció model que realitza la consulta a la base de dades per tal d'obtenir les qüestions que corresponen al formulari respondre.

En l'instant 3, el controlador determinarà quina vista de les que composen la lògica de presentació és la pertinent per tal de donar format i representar les dades requerides. En l'exemple, invocarà la vista que defineix la pantalla de respondre. Després d'aquesta operació, la vista retorna el control per tal que el controlador enviï el resultat a l'usuari que va realitzar la petició.
Avantatges d'utilitzar aquest model:

- Tenir múltiples formes d'accés a l'aplicació. Dit d'una altra forma, que un sol model sigui servit per diferents vistes. El controlador actua com intermediari entre el model i la vista, per tant, les dades proporcionades per el model poden ser dirigides cap a una vista o una altra, en funció dels requeriments de la interfase usuari. A mode d'exemple, és indiferent si l'usuari utilitza una interfase Flash, HTML, WAP, etc.

- Les dades model no només poden servir a diferents interfases sinó que també poden servir a diferents vistes d'una mateixa interfase. Per exemple, les dades model obtingudes d'un qüestionari, poden servir tant per la vista de respondre com per la vista d'edició del qüestionari.

- Donat que la vista, el model i el controlador funcionen de forma autònoma, és possible fer modificacions, millores o ampliacions dels components de forma menys costosa. Per exemple, si per qualsevol motiu (per exemple, un canvi de proveïdor de base de dades a nivell estratègic d'empresa) es passés d'una base de dades MS SQL Server a una MySQL, llavors, només seria necessari modificar el component model per tal de donar continuïtat a l'aplicació.

3.3.3 Llenguatges i llibreries

En la següent figura es representen els llenguatges, llibreries i aplicacions utilitzats en el desenvolupament d'aquest projecte, dins del model MCV i de l'arquitectura multi-nivell. També s'observa la separació física de cada una de les capes de l'arquitectura, cada una d'elles en un entorn físic diferent, com són, el client web (PC client), el servidor Web i el servidor BD.

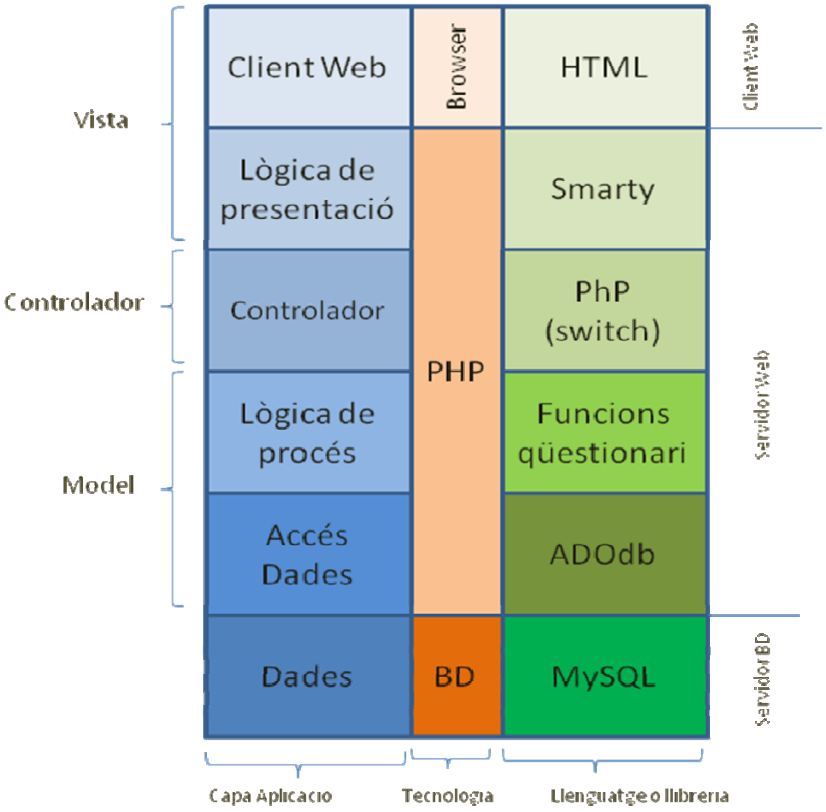


Figura 17: Model MCV - Capes, tecnologies, llenguatges i llibreries.

Destaquem que el model MCV s'ha implementat en llenguatge PHP, utilitzant diferents llibreries , com Smarty, XAJAX o ADOdb per desenvolupar cada un dels components. La base de dades és MySql amb llicencia d'ús general (lliure).
En els següents apartats es defineixen les funcions que aporta cada llibreria dins de l'arquitectura.

i PHP

Amb PHP construïm un **controlador simple** basat en la sentència *switch*. Com hem vist, el controlador gestionarà totes les peticions d'usuari redirigint-les a les funcions de la lògica de procés (normalment consultes a la base de dades) o a la lògica de presentació (pantalles de presentació o vistes).

Aquest controlador simple ens permet desenvolupar un patró de disseny MCV, ja que podem separar la lògica de procés (model) de la lògica de presentació (vistes).

El següent fragment de codi representa l'estructura en PHP del nostre controlador:

```
<php>
Switch ($_REQUEST['accio']){
        case 'login':
        Crida a la lògica de procés (control d'accessos a l'aplicació)
        Crida a la vista d'inici de sessió (formulari de login)
        break;
case 'logout':
        Crida a la lògica de procés (funcions de fi de sessió usuari)
        Crida a la vista de fi de sessió (formulari de logout)
        break;
case 'respondre':
        Crida a la lògica de procés (consulta base de dades)
        Funcions XAJAX per registre asíncron de dades (respostes)
        Crida a la vista (formulari respondre)
        break;
case 'editar':
        Crida a la lògica de procés (consulta base de dades)
        Crida a la lògica de procés (Udate/Inserts base de dades)
        Crida a la vista (formulari editar)
        break;
…

case 'default':
-       Crida a funcions per defecte.
}
</php>
```

El codi font íntegre que implementa el Controlador de la lògica de programa, s'adjunta en l'Annex B.

ii XAJAX

Les funcions de les llibreries XAJAX són una classe extensa de PHP. Ens permeten fer registres a la base de dades i modificacions sobre les vistes de forma asíncrona, és a dir, sense necessitat de recarregar la pàgina o prémer un botó per realitzar el registre o refrescar.

A nivell pràctic i relatiu al nostre desenvolupament, això significa que quan responem una

qüestió en el formulari fent clic en el checkbox que correspongui, aquesta resposta queda enregistrada automàtica i instantàniament en la base de dades. També, el resultat de l'avaluació d'aquesta resposta es visualitza per pantalla de forma instantània sense necessitat de recarregar la pàgina i de refrescar les dades que no s'han modificat.

Aquestes funcions ens aporten una navegació més ergonòmica, al no haver de suportar recàrregues de pàgina html, que en ocasions, comporten temps d'espera en funció de la càrrega de la xarxa. També, les avaluacions són visualitzades dinàmicament, de forma que ens permet fer una presa de decisions amb totes les dades actualitzades.

iii Smarty

Smarty és un motor de plantilles que disposa de diverses funcions específiques per implementar la lògica de presentació. Per exemple, funcions que exploten les dades rebudes des del controlador per tal de representar-les en un format determinat.

Algunes de les funcions que ens aporta Smarty:

Caching: Ens permet habilitar pàgines, part de plantilles o funcions en el sistema de *cach* del servidor web per tal de millorar la disponibilitat i rendiment.

Fitxers de configuració: Ens proporciona funcions per tal de crear fitxers de configuració amb variables compartides per l'aplicació. Ens permeten mantenir valors de variables comuns a l'aplicació en una sola localització i sense que sigui necessària la intervenció del programador per realitzar modificacions o actualitzacions. Les variables de configuració són fàcilment compartides per la lògica de procés i per la lògica de presentació.

Aquestes funcions ens han permès, per exemple, la creació de fitxers de configuració per tal d'habilitar la funció multilingüe de l'aplicació.

Seguretat: Les plantilles no contenen codi PHP, per tant, el dissenyador de la lògica de presentació no té perquè tenir accés a la lògica de procés o de negoci, sovint amb informacions confidencials.

Per aquest projecte no s'han separat els rols dels dissenyadors de la lògica de procés i de la lògica de presentació perquè la manipulació de dades o processos de la lògica de negoci no pot comportar pèrdues d'informacions personals o confidencials. No obstant, es considera una funció important en els projectes que ho requereixin.

Modificadors de variables: El contingut de les variables assignades pot ser fàcilment ajustat, modificat o formatejat amb l'ajut de diverses funcions com *upper-case, html-escaped, formatting dates, truncating*, etc. i sense la intervenció d'un programador.

Altres funcions de plantilles, *debbuging*, millora de la *performance*, o compilació.

iv ADODB

ADODB és el controlador d'accés a la base de dades. Es tracta d'un conjunt de llibreries en PHP que permeten principalment la connexió/desconnexió a la base de dades i l'enregistrament/consulta de dades. En el nostre cas, el *driver* emprat és el corresponent a una base de dades MySQL.

3.3.4 Estructura Base de dades MySQL

L'estructura de la base de dades de l'eina d'auditoria està formada per el conjunt de taules següents:

Qüestionaris: Taula on l'administrador enregistra el qüestionari assignant-li un número d'identificació (*q_id*), nom i títol. D'aquesta forma, l'eina pot treballar simultàniament amb múltiples qüestionaris corresponents a diferents departaments, serveis, o empreses.

Column Name	Datatype
q_id	INTEGER
llengua	VARCHAR(2)
nom	VARCHAR(45)
data_creacio	DATETIME
data_validacio	DATETIME
titol	LONGTEXT

Capítols: Taula on la funció d'edició o el procés d'importació de mySQL enregistra els diferents capítols, sub-capítols i apartats dels quals està format un qüestionari d'avaluació. La dada *id_quest* identifica el qüestionari enregistrat en la taula *Qüestionaris* de forma que cada qüestionari disposa de la seva col·lecció de capítols, sub-capítols i apartats.

Column Name	Datatype
id_cap	INTEGER
num_cap	INTEGER
num_subcap	INTEGER
num_subsubcap	INTEGER
nom_cap	VARCHAR(100)
llengua	VARCHAR(2)
id_quest	INTEGER
id_excl	INTEGER
obj_cap	LONGTEXT

Preguntes: Taula on la funció d'edició enregistra les preguntes i les opcions de resposta de cada qüestionari, identificant el número de capítol, sub-capítol i apartat. Cada pregunta s'identifica amb un número (*num_prg*) per tal d'associar-li la resposta corresponent (veure taula respostes).

Column Name	Datatype
id_prg	INTEGER
id_quest	INTEGER
id_cap	INTEGER
id_subcap	INTEGER
id_subsubcap	INTEGER
num_prg	INTEGER
pregunta	LONGTEXT
opcio0	LONGTEXT
opcio1	LONGTEXT
opcio2	LONGTEXT
opcio3	LONGTEXT
opcio4	LONGTEXT

Respostes: Registre de les respostes per pregunta (*id_preg*). També s'enregistren dades corresponents als comentaris, als fitxers vinculats, a l'usuari que respon per primera vegada o modifica la resposta, la data d'enregistrament i l'evolució de la resposta respecte l'última donada.

Column Name	Datatype
id_preg	INTEGER
id_resp	INTEGER
resposta	INTEGER
comentari	LONGTEXT
file	VARCHAR(99)
usr	VARCHAR(45)
evol	INTEGER
data	VARCHAR(45)

Històric: Taula que dona suport a la funció d'històrics.

Column Name	Datatype
id_his	INTEGER
num_cap	INTEGER
nrxc	INTEGER
npxc	INTEGER
npop	INTEGER
aval	FLOAT
evol	INTEGER
data	VARCHAR(45)
id_quest	INTEGER
id_keyhis	INTEGER
usr	VARCHAR(45)

Cartografia: Taula que suporta la funció de definició de perímetre físic. S'enregistren els components dels sistemes d'informació considerats sensibles identificant el qüestionari al qual pertanyen i el nom i tipus d'element, entre d'altres.

Column Name	Datatype
id_element	INTEGER
id_quest	INTEGER
nom_element	VARCHAR(45)
tipus_element	VARCHAR(45)
coment_elmnt	LONGTEXT
qtat_element	INTEGER
file	VARCHAR(45)
desc_file	LONGTEXT

Objectius: S'enregistra la definició d'objectius mitjançant la funció de definició de perímetre.

Column Name	Datatype
id_obj	INTEGER
id_quest	INTEGER
nom_obj	LONGTEXT
tipus_obj	VARCHAR(45)
coment_obj	LONGTEXT

Usuaris: Taula on l'administrador de l'eina d'auditoria enregistra els usuaris habilitats per els diferents qüestionaris. S'indica, principalment, el qüestionari al qual tenen accés (*id_quest*), el nom d'usuari (*usuari*), la contrasenya (*pass*), i la funció desenvolupada (*rol: Administrador, Editor, Auditor*).

Column Name	Datatype
usr_id	INTEGER
usuari	VARCHAR(45)
pass	VARCHAR(45)
nom	VARCHAR(45)
rol	VARCHAR(45)
id_quest	INTEGER

3.3.5 Proves d'usabilitat

El 22 de febrer de 2010 tres usuaris per separat, van realitzar proves d'usabilitat de la primera versió del prototipus per tal de validar el desenvolupament. Les proves consistien en la utilització de les funcions principals de l'aplicació i se'ls demanava que detectessin problemes en l'ús i en la comprensió de les funcions i les informacions.

Com a resultat d'aquestes proves, es van detectar els següents problemes:

- Funcionament incorrecte de la funció per esborrar criteris de la base de dades (Funció esborrar Resposta).
- Necessari indicar l'evolució de complementació del qüestionari.
- Millorar la comprensió de l'etiqueta "Capítols".
- Ús inadequat del color verd brillant en l'avaluació qualitativa i la funció de resposta. Dificulta la comprensió de les informacions mostrades per incompatibilitat del color amb el contrast de la pantalla de treball.
- Funcions AJAX i de format HTML incompatibles amb navegador Motzilla Firefox©.

Fruit de la detecció d'aquest problemes, es van realitzar les modificacions en el codi necessàries per tal de solucionar-los. Destacar, per la millora qualitativa que representa el fet de que l'aplicació sigui accessible des de tots els navegadors generalment utilitzats, les tasques realitzades per la compatibilitat.

3.3.6 Plataforma de desenvolupament i producció

El Servei de Tecnologies d'Informació i Comunicació de l'EPSEVG, ha posat a disposició, per el desenvolupament i la posada en producció d'aquest projecte, la plataforma descrita en la figura 18. Consta d'un entorn de desenvolupament i un entorn de producció. L'entorn de desenvolupament (kato.epsevg.upc.es) està format per un servidor que proporciona els servei web (servidor php) i la base de dades (mySQL) per tal de realitzar el desenvolupament i les tasques de modificació i millores prèvies a la posada en producció (Aplicació definitiva posada a disposició dels usuaris finals). L'entorn de producció està format per dos servidors, un que proporciona els serveis web (suex) i un altre que proporciona la base de dades de producció (sextam). Aquests entorns estan implantats aprofitant els recursos i infraestructures existents en el servei TIC de l'EPSEVG en matèria de servidors físics, sistemes virtuals, xarxa de comunicacions, serveis de copies de seguretat, etcètera.

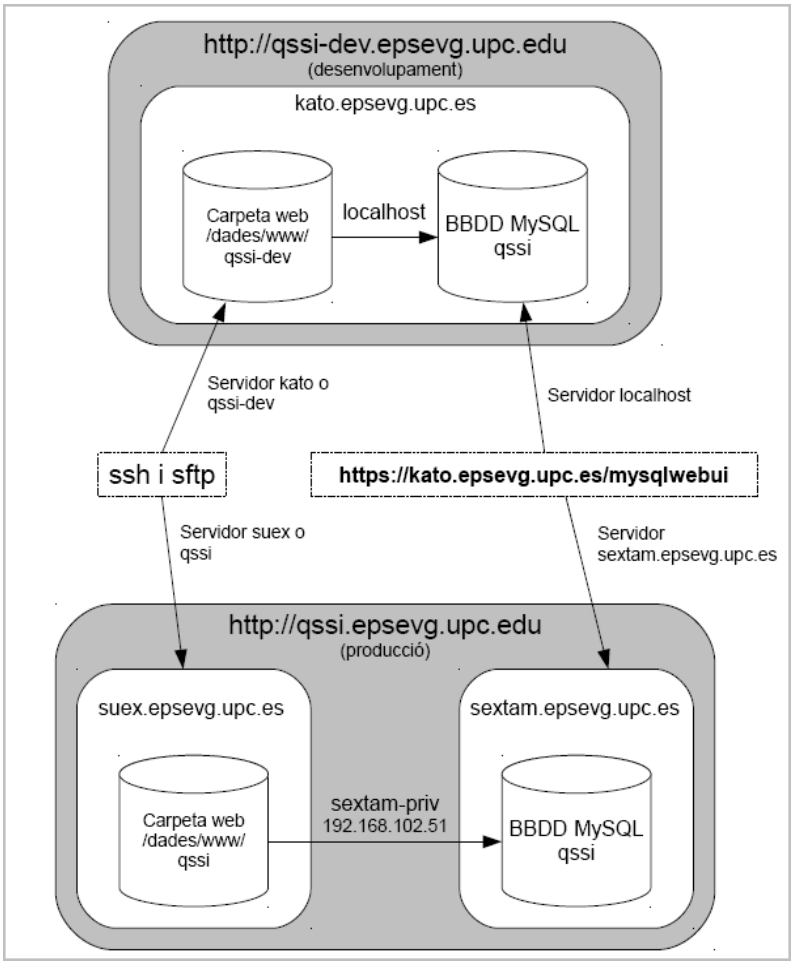


Figura 18:Diagrama de servidors web per desenvolupament i producció (Serveis TIC EPSEVG)

El procés de desenvolupament s'ha produït en diferents fases:

Especificacions: Descripció de les funcions principals de l'aplicació. En aquest projecte, inicialment es tractava de donar accés de forma telemàtica a un qüestionari i l'automatització de la recollida de dades (respostes, comentaris i documents) relatives a cada un dels apartats de l'estàndard de seguretat dels sistemes d'informació. Més endavant, es van afegir les funcions d'edició, avaluació, evolució, històrics, etc.

Construcció del prototipus: El prototipus inicial es construeix en la màquina local del desenvolupador (PC). Aquesta màquina està proveïda dels serveis web, les llibreries PHP i la base de dades mySQL a imatge de com ho estan les màquines de desenvolupament i producció. També d'un editor de textos per tal d'escriure el codi font de l'aplicació.

Validació del prototipus en local: Un cop desenvolupades les funcions principals, el desenvolupador realitza les proves necessàries per tal de verificar el funcionament correcte. Realitzades i validades les correccions necessàries, es fa una versió del paquet de desenvolupament format per una copia del fitxers font emprats i el fitxer corresponent a la copia de seguretat de la base de dades.

Pujada al servidor de desenvolupament: Validat el prototipus, l'usuari desenvolupador carrega via SFTP, en el servidor de desenvolupament i en la carpeta web corresponent, els fitxers creats i les llibreries utilitzades per tal d'executar el prototipus. També es connecta al servidor de base de dades via WEBUI per tal d'importar les taules i dades creades en la realització del prototipus.

Verificació del prototipus en desenvolupament: L'usuari desenvolupador i el director de projecte realitzen les proves necessàries per tal de validar el funcionament correcte de les operacions especificades (o de les modificacions o ampliacions demanades) en l'entorn "on-line". Es a dir, aquest cop es valida també les connexions i protocols de xarxa que intervenen.

Pujada al servidor de producció: Validat el prototipus en el servidor de desenvolupament, l'usuari desenvolupador carrega (copia de fitxers i importació de base de dades) el paquet de desenvolupament verificat.

Verificació del prototipus en producció: L'usuari desenvolupador i el director de projecte realitzen les proves de verificació per validar el funcionament correcte en l'entorn "on-line" de producció.

En aquest punt, i en diferents ocasions, s'ha decidit conjuntament amb el director de projecte i en funció de les necessitats que sorgien durant el desenvolupament, afegir noves funcionalitats o especificacions, com les funcions d'evolució, l'avaluació detallada o els històrics. En aquest casos, es tornava a repetir aquest procés des de la fase de **"Construcció del prototipus".**

Posada en producció: Validat el prototipus final (sense cap més funció a desenvolupar), es dona accés a l'usuari final (avaluador o auditor), comunicant-los les dades d'accés (l'adreça d'accés al servidor de producció i l'usuari i contrasenya individuals), així com les instruccions de funcionament pertinents (veure annex: guies).

Des del punt de vista dels usuaris que participen en el desenvolupament i el funcionament en producció, en la figura 19 es representen els tres servidors que intervenen, les seves adreces http d'accés, les xarxes de comunicacions, els diferents rols d'usuari, així com els diferents tipus d'accés que es produeixen en funció de l'usuari.

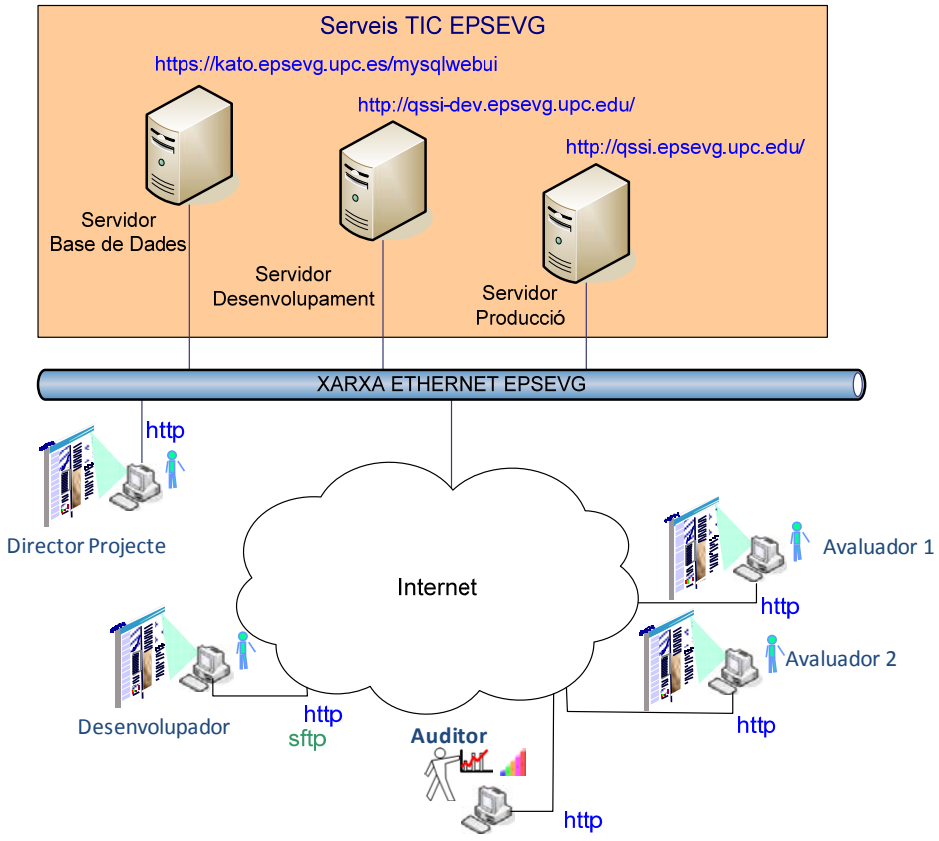


Figura 19: Diagrama de servidors desenvolupament /producció (punt de vista usuaris)

3.4 Millores i evolucions

Implementar funcions d'administració de l'aplicació: Creació d'usuaris, assignació de projectes (Qüestionaris) i drets d'accés (editor, auditor, avaluador).

Millorar el control d'accessos i gestió de contrasenyes: funcions que implementin les recomanacions (controls) definits en el capítol 7 de la norma ISO/IEC 27002:2005 en relació al control d'accessos i gestió de les paraules clau d'accés.

Selecció llengua: Encara que el disseny i el desenvolupament de l'eina està realitzat implementant funcions que permeten el multilingüisme (existeixen fitxers de configuració en català i espanyol), es necessari crear les funcions per tal que l'usuari pugui seleccionar la llengua de treball. Actualment és l'administrador l'encarregat, durant el registre de l'usuari en la base de dades, d'assignar la llengua de treball per cada usuari.

Disseny ergonòmic: Disseny de les funcions i formats adaptats als estàndards de disseny web.

Funcions d'accessibilitat: Implantació de funcions per fer accessible l'aplicació a usuaris amb discapacitat visual o funcional. Nivell Triple-A de conformitat amb les directrius d'accessibilitat per el contingut web 1.0 (W3c WAI AAA).

PART III: APLICACIÓ

Capítol 4: Auditoria Seguretat en els Sistemes d'informació de societat prestadora de serveis (Cas d'estudi: Servei SAF de la UAB).

4.1 Mètode d'auditoria

L'auditoria de seguretat dels sistemes d'informació, basada en la norma ISO/IEC 27002:2005, realitzada sobre els sistemes d'informació del Servei d'Activitats Físiques (SAF) de la Universitat Autònoma de Barcelona (UAB), s'ha dut a terme en les següents fases:

a) Adopció de l'estàndard: Conjuntament amb el responsable dels sistemes d'informació del SAF, s'estudia l'estàndard ISO/IEC 27002:2005 per tal de verificar l'adaptació a les especificitats del servei i validar l'adopció del mateix per ser implantat en el projecte de millora continuada de la seguretat dels sistemes d'informació del servei.

En aquest punt, es decideix també desenvolupar una eina de suport a l'auditoria consistent en un qüestionari realitzat segons els mètodes que es descriuen en la part 2 d'aquesta memòria, amb la finalitat principal d'obtenir una avaluació del grau de compliment de la normativa.

Es defineixen els rols d'usuari que participaran en aquesta auditoria:

Auditor: Autor d'aquest projecte.

Avaluador: Responsable dels sistemes d'informació del SAF

b) Definició del perímetre i objectius de seguretat: L'auditor, l'avaluador i el cap de servei defineixen els objectius de seguretat dels sistemes d'informació i el perímetre a avaluar (infraestructura tècnica, serveis, dades, etc)

c) Resposta del qüestionari de seguretat: Durant un temps definit, segons els recursos disponibles, l'avaluador dona resposta als 153 controls (qüestions) de seguretat aportant respostes, comentaris i documents relacionats, tenint sempre en compte els objectius de seguretat i perímetre definits.

d) Estudi de l'avaluació: L'auditor i l'avaluador realitzen un estudi de l'avaluació per capítol i detallada obtinguda, així com les comentaris i informacions aportades. L'objectiu d'aquest estudi és la detecció de vulnerabilitats per la posterior confecció d'un pla d'acció per la millora de la seguretat dels sistemes d'informació.

e) Pla d'acció: En funció dels objectius definits i de les vulnerabilitats detectades, l'auditor confecciona un pla d'acció per la millora de la seguretat. El responsable dels sistemes d'informació, com a responsable de la seva execució, i amb el suport de l'auditor, validarà i programarà (en el termini d'un semestre) les accions prioritàries a realitzar.

f) Execució pla d'acció: El responsable dels sistemes d'informació del SAF, vetllarà per el compliment de les tasques programades en el pla d'acció.

g) Millora continuada: Executat el pla d'acció, l'avaluador actualitza el qüestionari en funció del resultat de les tasques de millora executades. Finalitzada l'actualització, l'auditor realitza un estudi de l'evolució i de l'avaluació actual per reiniciar amb el procés de millora continuada fase d) "Estudi de l'avaluació".

4.2 Definició de Perímetre i objectius de seguretat

El SAF (Servei d'Activitats Físiques) de la UAB (Universitat Autònoma de Barcelona) gestiona les instal·lacions esportives del campus universitari de la UAB. Aquestes instal·lacions estan a disposició d'unes 40.000 persones entre alumnes, professors i personal interns de la pròpia universitat, així com per individus o col·lectius externs a la universitat.

A nivell d'equipaments, el SAF s'encarrega del manteniment, el control i la supervisió d'instal·lacions tant cobertes com a l'aire lliure: un poliesportiu, camps de tenis i de basquet, camp de gespa, piscina coberta, pistes cobertes poliesportives, edifici central del servei, sales de reunions, vestuaris, sales de fitness i aerobic, etc. Dins d'aquestes instal·lacions el SAF s'encarrega de la gestió, per exemple, del reg, l'aigua calenta sanitària, la il·luminació, terres radiants, la climatització, la depuració, etc. Aquesta gestió la realitza mitjançant una xarxa industrial de dispositius, sensors i autòmats dins d'una plataforma SCADA (*Supervisory Control and Data Acquisition*).

A nivell de proveïdor de serveis, el SAF gestiona l'abonament dels usuaris a les instal·lacions esportives (altes i baixes d'usuaris) així com el control d'accessos als equipaments esportius. També proporciona serveis d'aplicacions web relacionades amb competicions esportives.

En relació al projecte que ens ocupa hem de tenir en compte, per tant, que el SAF gestiona informacions confidencials, dades personals i serveis que es poden considerar crítics en funció de la "pèrdua de negoci" (veure capítol 2) provocada per una pèrdua de dades personals o una aturada parcial o total del servei.

Per l'auditoria de seguretat dels sistemes d'informació del SAF s'han definit els següents objectius:

I) Assegurar la fiabilitat/continuïtat dels Serveis.

- Informàtica gestió.
- Serveis generals instal·lacions.

II) Complir la llei de protecció de dades personals LOPD.

-Assegurar la protecció de les dades personals i la confidencialitat.

III) Garantir la transferibilitat dels sistemes d'informació .

- Assegurar la transferència de coneixements del servei informàtic.

Aquests objectius han quedat definits i descrits en la funció "Definició Perímetre" (veure figura 9).

Per la definició del perímetre físic sobre el qual es realitza l'auditoria de seguretat, es recopila informació dels sistemes, dades, infraestructures, serveis, etc. que intervenen en la consecució dels objectius de seguretat definits. Aquest conjunt de sistemes d'informació els denominarem d'ara en endavant sistemes sensibles. En la figura 20 es representa l'esquema de xarxa corresponent als sistemes sensibles del SAF que es tindran en compte en l'avaluació de la seguretat dels sistemes d'informació.

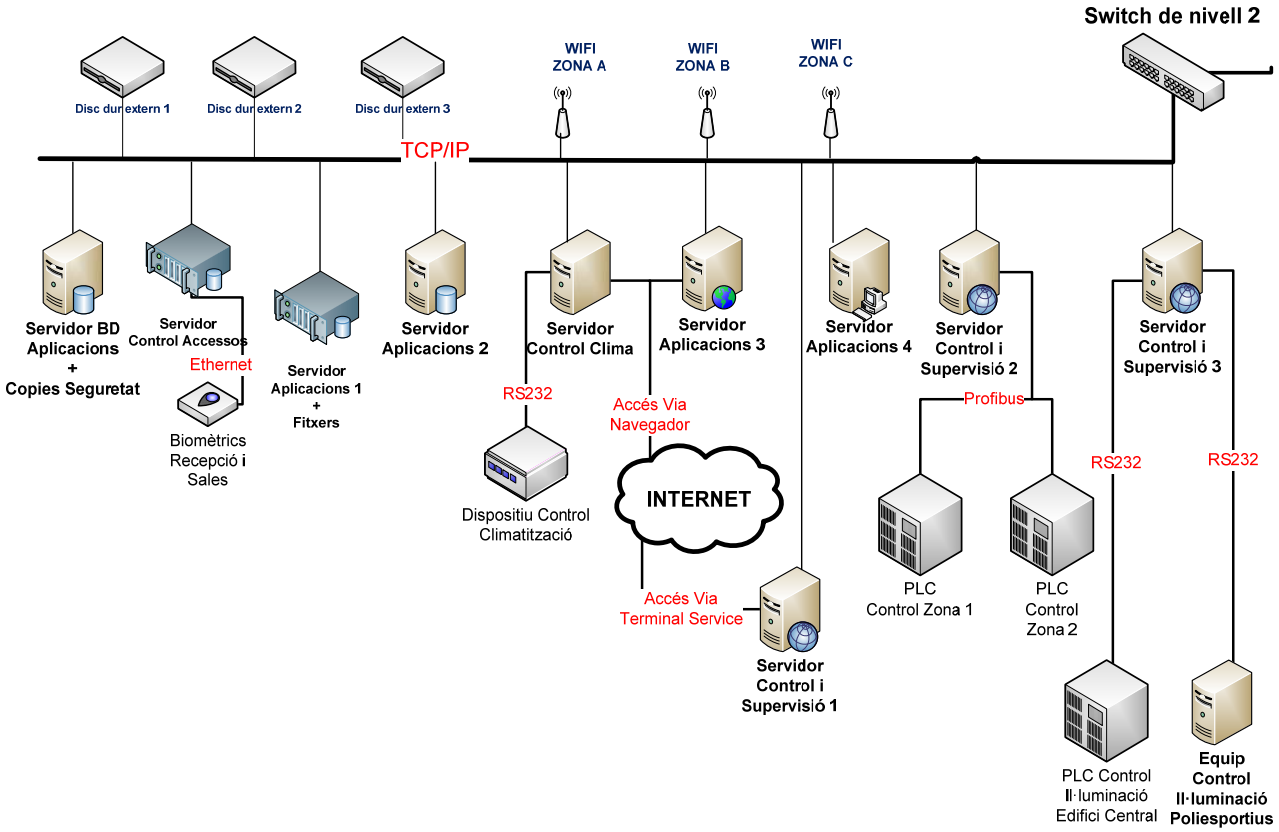


Figura 20:Esquema arquitectura sistemes sensibles SAF

Per motius de seguretat i seguint les recomanacions de l'estàndard implantat, en la memòria d'aquest projecte s'ha obviat qualsevol informació, principalment adreces IP, noms DNS i dades personals que la seva revelació poden suposar una vulnerabilitat per la seguretat dels sistemes d'informació del servei i la no consecució dels objectius plantejats.

4.3 Qüestionari

Durant els dies 3 i 16 de març de 2010 i els dies 21 i 22 d'abril, el responsable dels sistemes d'informació dels sistemes d'informació del servei va donar resposta als 153 controls de seguretat repartits en 11 capítols, aportant comentaris i documents relacionats. El resultat d'aquest treball es pot comprovar en el qüestionari complert adjuntat en l'annex A.

El temps estimat per completar el qüestionari pot variar entre 2.5 i 5 hores en funció de la disponibilitat que l'avaluador tingui de la informació necessària per cada control, del temps dedicat exclusivament per realitzar aquesta tasca, i també de la seva experiència o formació en temes de seguretat dels sistemes d'informació. En el cas que ens ocupa, l'avaluador considera que la tasca de completar el qüestionari ha estat llarga (veure qüestionari SIS de l'Annex C).

4.4 Avaluació

Completat el qüestionari, l'eina de suport a l'auditoria ens dóna la següent avaluació (figura 21) per capítol i global (veure punt 2.4: Mètode adaptació a qüestionari d'avaluació):

1	Política de Seguretat	2	2		3.0
2	Organització de la Seguretat	12	12		1.8
3	Gestió dels actius	6	6		2.2
4	Gestió de Personal	9	9		1.4
5	Seguretat Física	14	14		2.1
6	Gestió de l'explotació i de les telecomunicacions	40	40		2.0
7	Control d'accessos	34	34		2.0
8	Adquisició, desenvolupament i manteniment de les Aplicacions	16	16		1.1
9	Gestió dels incidents	5	5		0.8
10	Gestió del pla de continuïtat de l'activitat	5	5		0.8
11	Conformitat	9	9	1	0.9
	Global: 152	**152**		1	1.76

Figura 21: Avaluació per capítol i global projecte SAF

D'aquesta es desprèn l'avaluació de 0 a 5 i els controls avaluats per cada capítol, el número total de controls avaluats i la nota global del projecte. També, que un control contingut en el capítol 11 ha estat considerat fora de perímetre.

En l'avaluació detallada obtenim l'avaluació qualitativa indicant-nos, per cada control, el seu estat d'implantació segons els següents símbols:

- NO existeix Control (veure guia d'implantació corresponent).
- Necessari millora del Control (veure guia d'implantació corresponent).
- ✓ Control implantat. Manquen procediments de revisió i verificació.
- ✓ Control amb mesures de revisió i verficació dels procediments d'implantació.
- Falta resposta.
- Control fora de perímetre (veure definició de perímetre lògic i comentaris en resposta).

Figura 22: Símbols avaluació qualitativa

Resultat de l'avaluació detallada:

1 Política de Seguretat

1.1 Política de seguretat dels sistemes d'informació

1.1.1 Documents de política de seguretat dels sistemes d'informació ●

1.1.2 Revisió i avaluació ✓

2 Organització de la Seguretat

2.1 Organització Interna

2.1.1	Compromís de la direcció en relació a la seguretat dels S.I.	●
2.1.2	Coordinació de la seguretat dels S.I.	●
2.1.3	Atribució de responsabilitats en relació a la seguretat dels S.I.	●
2.1.4	Sistemes d'autorització en relació als mitjans de tractament de la informació	●
2.1.5	Compromisos de confidencialitat	● ✓
2.1.6	Relació amb les autoritats	✓
2.1.7	Relacions amb els grups d'especialistes	●
2.1.8	Revisió independent de la seguretat dels sistemes d'informació	●

2.2 Tercers (Outsourcing)

2.2.1	Identificació dels riscos lligats amb accessos a tercers	✓
2.2.2	La seguretat dels S.I. i els clients	●
2.2.3	Gestió de la seguretat dins dels contractes i compromisos amb tercers	●

3 Gestió dels actius

3.1 Responsabilitat relatives als actius

3.1.1	Inventari dels actius	● ✓
3.1.2	Propietat dels bens	●
3.1.3	Utilització correcte dels actius	●

3.2 Classificació de les informacions

3.2.1	Línies directrius per la classificació	●
3.2.2	Marcatge i manipulació de la informació	●

4 Gestió de Personal

4.1 Abans la presa de funcions

4.1.1	Rols i responsabilitats	●
4.1.2	Selecció	●
4.1.3	Condicions contractuals	✓

4.2 Durant el contracte

4.2.1	Responsabilitats de la direcció	✓
4.2.2	Sensibilització, qualificació i formació en matèria de la seguretat dels S.I.	●
4.2.3	Processos disciplinaris	●

4.3 A la fi o modificació del contracte

4.3.1	Responsabilitats en la fi del contracte	●
4.3.2	Restitució dels recursos informàtics	●
4.3.3	Supressió dels drets d'accés	●

5 Seguretat Física

5.1 Zones de seguretat

5.1.1	Perímetre de seguretat física	✓
5.1.2	Control d'accessos físics	●
5.1.3	Seguretat de les oficines i sales d'equips tècnics	● ●
5.1.4	Protecció contra les amenaces exteriors i de l'entorn	●
5.1.5	Treball dins de les zones de seguretat	✓
5.1.6	Zones d'accés públic i de lliurement de comandes	✓

5.2 Seguretat del material

5.2.1	Emplaçament i protecció del material	✓
5.2.2	Serveis generals	✓
5.2.3	Seguretat del cablejat	●
5.2.4	Manteniment dels equips	✓
5.2.5	Seguretat del material exterior a les instal•lacions (material en circulació)	●
5.2.6	Rebuig o reciclatge segur del material	●
5.2.7	Sortida d'un actiu	●

6 Gestió de l'explotació i de les telecomunicacions

6.1 Processos i responsabilitats lligades a l'explotació

6.1.1	Procediments d'explotació documentats	🟡
6.1.2	Gestió de les modificacions	🟡
6.1.3	Separació de les tasques	🔴
6.1.4	Separació dels equips de desenvolupament, de test i d'explotació	🔴

6.2 Gestió de la prestació de serveis per un tercer

6.2.1	Prestació de serveis	✓
6.2.2	Vigilància i revisió dels serveis de tercers	🔴
6.2.3	Gestió i evolució dels serveis prestats per un tercer	🔴

6.3 Planificació i acceptació del sistema

6.3.1	Dimensionament	✓
6.3.2	Modificacions del sistema	🟡 ✓

6.4 Protecció contra els codis perjudicials o no desitjats

6.4.1	Mesures contra els codis perjudicials	🟡 ✓ ✓ ✓

6.5 Copies de seguretat

6.5.1	Copies de seguretat de les informacions	🔴 🔴 ✓ ✓

6.6 Gestió de la seguretat de les xarxes informàtiques

6.6.1	Mesures en relació a les xarxes	✓ ✓ ✓
6.6.2	Seguretat dels serveis de xarxa	✓

6.7 Manipulació dels mitjans de tractament informàtic

6.7.1	Gestió dels suports mòbils	🔴
6.7.2	Rebuig de suports	🟡
6.7.3	Procediments de manipulació de les informacions	🔴
6.7.4	Seguretat de la documentació de sistema	🟡

6.8 Intercanvi d'informacions

6.8.1	Política i procediments d'intercanvi de les informacions	✓
6.8.2	Acords d'intercanvi d'informacions	🔴
6.8.3	Suports físics en transit	🔴
6.8.4	Missatgeria electrònica	🟡
6.8.5	Sistema d'informació d'empresa	🔴

6.9 Serveis de comerç electrònic

6.9.1	Comerç electrònic	🔴
6.9.2	Transaccions en línia	🔴
6.9.3	Informacions fetes públiques	🔴

6.10 Vigilància

6.10.1	Informe d'auditoria	🔴
6.10.2	Vigilància de la utilització dels sistemes d'informació	🔴
6.10.3	Protecció de les informacions registrades	🔴
6.10.4	Registre d'administració i registre de les operacions	🔴
6.10.5	Enregistrament dels errors	🟡
6.10.6	Sincronització horària	✓

7 Control d'accessos

7.1 Necessitats de negoci en matèria de control d'accessos

7.1.1	Política de control d'accessos	●

7.2 Gestió dels accessos usuaris

7.2.1	Enregistrament dels usuaris	✓
7.2.2	Gestió dels privilegis	●
7.2.3	Gestió del les claus d'accés d'usuaris	✓
7.2.4	Revisió dels drets d'accés usuaris	● ● ●

7.3 Responsabilitats dels usuaris

7.3.1	Utilització de la clau d'accés	● ✓
7.3.2	Material dels usuaris deixat sense vigilància	●
7.3.3	Política d'oficina neta i escriptori buit	●

7.4 Control d'accés a la xarxa

7.4.1	Política d'utilització dels serveis de xarxa	●
7.4.2	Autentificació de l'usuari per les connexions externes	● ●
7.4.3	Identificació dels equips de xarxa	●
7.4.4	Protecció dels ports de diagnòstic i de configuració a distància	✓
7.4.5	Aïllament de les xarxes	● ✓
7.4.6	Control de les connexions de xarxa	● ● ●
7.4.7	Control de redirecció de xarxa	✓

7.5 Control d'accessos als sistemes d'explotació

7.5.1	Procediments segurs d'obertura de sessió	●
7.5.2	Identificació i autentificació de l'usuari	● ✓
7.5.3	Sistema de gestió de les claus d'accés	✓
7.5.4	Accés a les aplicacions sistema	✓
7.5.5	Desconnexió automàtica de les sessions inactives	✓
7.5.6	Limitació dels horaris de connexió	●

7.6 Control d'accessos a les aplicacions i la informació

7.6.1	Restriccions d'accés a les informacions	●
7.6.2	Aïllament dels sistemes sensibles	●

7.7 Informàtica nòmada o teletreball

7.7.1	Informàtica i comunicacions nòmades	● ✓
7.7.2	Teletreball	●

8 Adquisició, desenvolupament i manteniment de les Aplicacions

8.1 Necessitat en seguretat dels sistemes d'informació

8.1.1	Anàlisis i especificacions de les necessitats en seguretat	●

8.2 Tractament correcte en el si de les aplicacions

8.2.1	Validació de les dades d'entrada	●
8.2.2	Control dels tractaments	●
8.2.3	Validació de les dades de sortida	●

8.3 Mitjans criptogràfics

8.3.1	Política d'utilització dels mitjans criptogràfics	● ●
8.3.2	Gestió de les claus d'accés	●

8.4 Seguretat dels fitxers sistema

8.4.1	Controls de les utilitats d'explotació	●
8.4.2	Protecció de les dades de sistema d'assaig	●
8.4.3	Control d'accés al codi font de les aplicacions	●

8.5	**Seguretat del desenvolupament i gestió del suport**	
8.5.1	Procediment del control de canvis i actualitzacions	🟡
8.5.2	Revisió tècnica de les aplicacions després de les modificacions en el sistema d'explotació	🟡
8.5.3	Restriccions relatives a les modificacions de paquets d'aplicacions d'editors externs.	🟡
8.5.4	Fuita d'informació	🔴
8.5.5	Externalització dels desenvolupament d'aplicacions	🔴
8.6	**Gestió de les vulnerabilitats tècniques**	
8.6.1	Mesures relatives a les vulnerabilitats tècniques	🔴

9 Gestió dels incidents

9.1	**Informe dels incidents i les vulnerabilitats de seguretat en els S.I.**	
9.1.1	Informe dels incidents de seguretat en els S.I.	🟡
9.1.2	Informe de vulnerabilitats de seguretats en els S.I.	🔴
9.2	**Gestió dels incidents i millores de la seguretat dels S.I.**	
9.2.1	Responsabilitats i procediments	🔴
9.2.2	Retorns d'experiència extret dels incidents de seguretat dels S.I.	🔴
9.2.3	Col•lecta de proves	🔴

10 Gestió del pla de continuïtat de l'activitat

10.1	**Aspectes de la seguretat dels S.I. en matèria de gestió de la continuïtat de l'activitat**	
10.1.1	Integració de la seguretat dels S.I. dins del procediment de gestió del pla de continuïtat	🔴
10.1.2	Continuïtat de l'activitat i apreciació dels riscos	🔴
10.1.3	Elaboració i posada en marxa dels plans de continuïtat integrant la seguretat dels S.I.	🟡
10.1.4	Quadre de planificació i de coherència de la continuïtat de l'activitat	🔴
10.1.5	Proves, gestió i apreciació constant dels plans de continuïtat de l'activitat	🔴

11 Conformitat

11.1	**Conformitat amb les exigències legals**	
11.1.1	Identificació de la legislació vigent	🔴
11.1.2	Drets de la propietat intel•lectual	🟡
11.1.3	Protecció dels registres de la societat	🔴
11.1.4	Protecció de les dades i confidencialitat de les informacions relatives a la vida privada	🔴
11.1.5	Prevenció contra la utilització il•lícita dels mitjans del tractament de les informacions	✓
11.1.6	Legislació sobre els mitjans criptogràfics	🔴
11.2	**Revisions de la política de seguretat i de la conformitat tècnica**	
11.2.1	Conformitat amb les polítiques i normes de seguretat	🔴
11.2.2	Verificació de la conformitat tècnica	🔴
11.3	**Consideracions per les auditories de seguretat dels S.I.**	
11.3.1	Mesures de les auditories de seguretat dels S.I.	🔴
11.3.2	Protecció de les eines d'auditoria dels S.I.	○

Els apartats que contenen dos o més símbols corresponen als apartats que estan definits per dos o més controls. Cada símbol indica l'estat d'implantació de cada control individual en l'orde en el que apareixen en el qüestionari.

4.5 Informe

Estudiada l'avaluació per capítols i detallada, i donada la baixa puntuació en alguns dels capítols importants per la consecució dels objectius definits, es proposa realitzar una fase preliminar a la confecció del pla d'acció per tal d'arribar a un punt inicial a partir del qual es pugui desenvolupar un projecte de millora continuada. En concret, els punts que es requereixen millorar, abans de continuar amb la implantació de l'auditoria segons les fases definides en el punt 4.1, són els relacionats amb el control d'accessos (capítol 7 de la norma ISO/IEC 27002:2005) i la gestió del pla de contingència de l'activitat (capítol 10 de la norma ISO/IEC 27002:2005).

Per tal de desenvolupar la fase preliminar (maig - juny 2010) es proposa realitzar les següents tasques (figura 23):

- Identificació sistemes i dades sensibles.
- Identificació connexions habilitades en els sistemes sensibles.
- Anàlisis de riscos (possibilitats de pèrdua de dades/servei o accessos no autoritzats).
- Separació física/lògica entre xarxes de producció i ofimàtiques.
- Aplicació de les recomanacions en relació al Control d'accessos (capítol 7 de la norma ISO/IEC 27002:2005).
- Confecció del pla de contingència: Pla de continuïtat (mode degradat) i Pla de represa informàtica (mode normal).

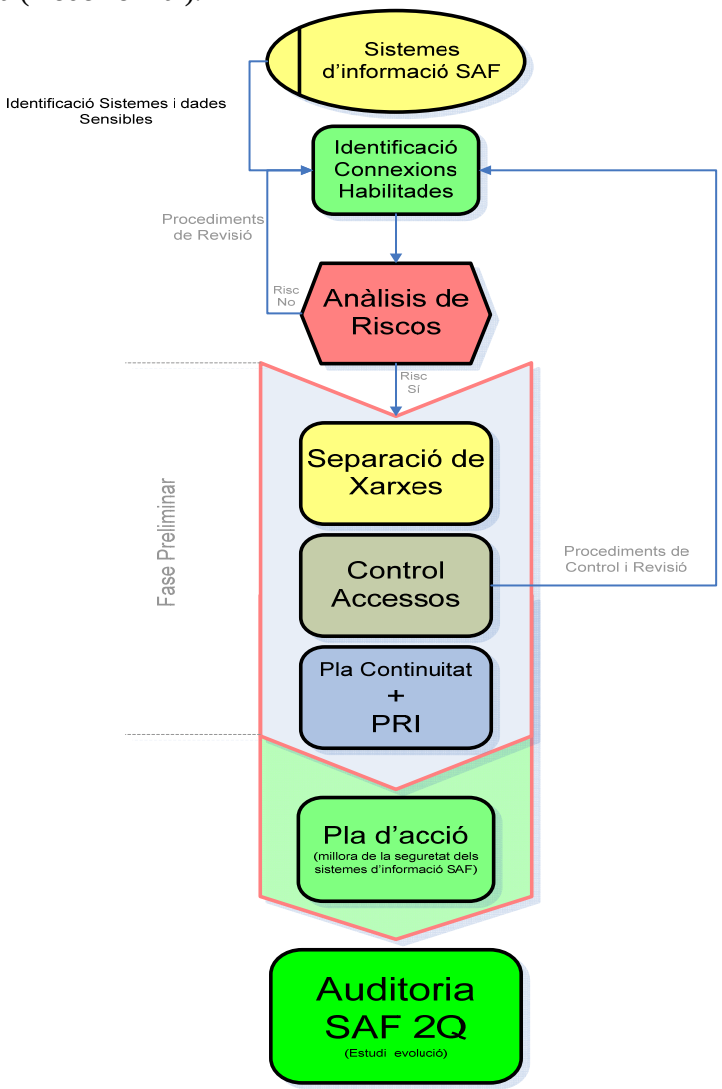


Figura 23: Diagrama desenvolupament fase preliminar

Identificació sistemes i dades sensibles: Identificar i descriure detalladament els Sistemes i dades que

són part fonamental per la consecució dels objectius. Aquestes informacions seran determinants per aplicar les polítiques de control d'accessos i la gestió del pla de continuïtat de l'activitat. Les dades que es requereixen de cada sistema sensible són les següents:

- Nom.
- Descripció (aplicacions, serveis, dades...).
- Ubicació.
- Infraestructura (Hardware / Software).
- Sistemes de copies de Seguretat.
- Subministrament elèctric.
- Connectivitat (esquema de xarxa).
- Administració (accessos autoritzats).
- Seguretat física/lògica implantada.
- Sistema de monitorització.
- Contractes de manteniment i suport.

La recopilació de les informacions de cada sistema sensible es proposa que es realitzi mitjançant el model de fitxa de la figura 24.

Servidor GISAF2						
	**Ubicació**					
	Centre	UAB Cerdanyola del Vallès				
	Edifici	SAF	**Planta**	1ra	**Porta**	
	Departament	Informàtica SAF				
	Nom Ubicació	Rack nom_rack Sala Servidors nom_sala				
Descripció						
Servidor Dades SAF i Gestió d'abonats. Equip de control d'accessos recepció per dades biomètriques dels abonats. Serveis: - DEPORWIN - SQL SERVER: Base de dades principal del SAF IP=158.---.---.88						
Infraestructura	**Servidor:** HP Proliant - GISAF2 **Processador/s:** 2 x Intel Xeon 1,80 GHz. **Memòria:** 6 GB. **Discos:** 2 discos de 72 GB. **Tipus Raid:** Raid1 **Targetes de xarxa:** 3 tipus Gigabit. **Fonts d'alimentació:** 2 **Ventiladors:** 5 ventiladors + 2 opcionals. **Controladora SCSI:** Sí. **Sistema Operatiu:** Windows 2000 Server. **Antiguitat:** maig 2005 **Manteniment:** Reparació i/o substitució peces, 24x24, 4h, vàlid fins maig 2011.					
	Equip Control d'accessos dades biomètriques **Marca:** **Model:** **Manteniment:** Reparació i/o substitució peces, 24x24x365, 4h, vàlid fins maig 2011.					
Sistemes de copies de Seguretat	Tipus suport, Política (diari, 1 mes de vigència),Aplicació					
Subministrament elèctric	- Subministrament serveis generals - SAI (marca, model, potència, manteniment)					
Connectivitat	- LAN Switch de Nivell 2 o Cable: Ethernet Cat.6 100M o Port Switch: - LAN Wi-Fi: Zona piscina, seminaris, sales. - WAN: Router UAB					
Administració	Responsable informàtic.					
Seguretat física/lògica	- Sala Técnica Servei SAF - Router UAB - Firewall UAB					
Sistema de monitorització	Accés remot a visor de successos Windows.					
Contractes manteniment i suport	Els específics dels equips implicats.					

Figura 24: Fitxa identificació sistemes sensibles (fase preliminar)

Identificació connexions habilitades: En la fitxa d'identificació dels sistemes sensibles s'indicà en l'apartat de connectivitat totes les connexions habilitades en el sistema sensible. Aquestes informacions seran importants durant l'anàlisi de riscos i detecció de vulnerabilitats.

Anàlisi de riscos: De cada Sistema sensible, identificació de les situacions de fallida parcial o total que poden provocar una pèrdua de dades o continuïtat de servei.

S'estudiaran les situacions que tenen un grau de probabilitat definit. No s'estudiaran les situacions de fallida total o catàstrofe, ja que es consideren incloses en el pla de contingència global de la UAB .

S'utilitzaran tres nivells per la definició/classificació de la fallida en funció de la seva criticitat:

Nivell 1: Criticitat màxima. Implica fallida greu, amb pèrdua total o parcial de dades o serveis sensibles.
Nivell 2: Criticitat mitja: Implica fallida greu, sense pèrdua de dades o serveis sensibles.
Nivell 3: Criticitat baixa: Implica fallida lleu, sense pèrdua de dades o serveis sensibles.

De cada sistema sensible, s'estudiaran tres àrees diferenciades:

- Instal·lacions (CPD):
  - Fallida subministrament elèctric.
  - Fallida Climatització.
- Connectivitat:
  - Fallida element de xarxa.
  - Fallida connectivitat.
  - Destrucció cablejats, fibres, panells, etc..
- Processament de dades, emmagatzematge i bakcup's:
  - S.O. Total
  - S.O. Parcial
  - Hardware Total
  - Hardware Parcial
    - Disc
    - Ventilador
    - Targeta
    - Font d'alimentació

Per cada sistema sensible i per cada nivell de criticitat s'indicaran els serveis i/o les dades sensibles afectades.

Per cada sistema sensible i per cada situació de fallida, segons les àrees definides anteriorment, s'establirà una taula que relacioni la situació de fallida amb els corresponents plans de contingència (PCL) i de recuperació informàtica (PRI). En la figura 25 es mostra un exemple per un sistema sensible determinat. S'ha considerat la implantació d'un pla de continuïtat del servei afectat (PCL_01) i diversos plans de represa informàtica en funció del tipus de fallida.

Anàlisis de riscos (Situacions de fallida)					
			Nivell	PCL	PRI
Instal·lacions	Subministrament elèctric		1	01	01
	Climatització		2	X	02
Connectivitat	Fallida element de xarxa		1	01	03
	Fallida connectivitat		2	X	04
	Destrucció cablejats		1	01	05
Processament	S.O. Total		1	01	06
	S.O. Parcial		2	X	07
	Hardware Total		1	01	08
	Hardware Parcial	Disc	2	X	09
		Ventilador	3	X	10
		Targeta	2	X	11
		Font d'alimentació	3	X	12
PCL: Pla de continuïtat Local (establiment del servei en mode degradat) PRI: Pla de represa informàtica (restabliment del servei en mode d'operació normal) Nivell 1: Crititat màxima. Implica fallida greu, amb pèrdua total o parcial de dades o serveis sensibles. Nivell 2: Criticitat mitja: Implica fallida greu, sense pèrdua de dades o serveis sensibles. Nivell 3: Criticitat baixa: Implica fallida lleu, sense pèrdua de dades o serveis sensibles.					

Figura 25: Taula anàlisis de riscos i correspondència PCL i PRI

Definició dels Plans de continuïtat (funcionament degradat): Per cada sistema sensible i situació de fallida, es descriuran detalladament els procediments de funcionament en mode degradat que permetin la continuïtat del servei. S'especificarà:

- Temps d'implantació estimat.
- Estimació pèrdua de dades o temps de servei.

Es proposa que els plans de continuïtat es realitzin complimentant el model representat en la figura 26.

PCL_01		
Descripció		
Pla per la continuïtat del servei de gestió de dades i accessos abonats		
Situacions de fallida	- Falta de subministrament elèctric sala servidors. - Element de xarxa fora de servei (Cablejat o Switch). - Fallida total (S.O. o Hardware) servidor GISAF2.	
Responsable implantació	Nom: Telèfon:	
Estimació pèrdua de dades o temps de servei		
Temps implantació		
Accions		
1	Contactar a...	
2	Control presencial accessos.	
3	Procediment per el registre d'accessos manual en recepció..	
4	Procediment per l'enregistrament manual de dades abonats...	
5	...	
6	Redireccioinament temporal de les pàgines DEPORWIN cap a pàgina d'informació	
7	...	
8		
9		

Figura 26: Model fitxa per el Pla de continuïtat local (PCL)

Aquestes accions han d'estar descrites de tal forma que una persona aliena al servei pugui dur a terme amb èxit el procediment de continuïtat del servei interromput.

Definició dels Plans de represa informàtica (funcionament normal): Per cada sistema sensible i situació de fallida, procediments de reinstal·lació, recuperació o reemplaçament del sistema, per tal de redirigir-lo al seu funcionament normal. S'especificarà el temps de resolució estimat (Temps Execució PRI). Es proposa que els plans de represa informàtica es realitzin complimentant el model representat en la figura 27.

Procediments de revisió: Seguint les recomanacions de la norma ISO/IEC 27002:2005, recull de bones pràctiques per la millora la seguretat dels sistemes d'informació, els plans de continuïtat i de represa informàtica hauran de ser revisats, actualitzats i testejats periòdicament.

PRI_01		
Descripció		
Pla de represa subministrament elèctric sala servidors		
Situacions de fallida	- Falta de subministrament elèctric serveis generals. - Fallida quadre elèctric sala servidors. - Curt circuit o sobrecàrrega sala servidors. - SAI fora de servei.	
Responsable execució	Nom: Telèfon:	
Estimació pèrdua de dades o temps de servei		
Temps execució		
Accions		
1	Contactar responsable serveis generals (informació sobre la causa i determinar temps de resolució)...	
2	Verificació del correcte funcionament dels equips SAI's.	
3	En funció del temps de resolució, preparació per la correcta aturada dels sistemes sensibles.	
4	...	
5	...	
6	Preparació equips sala servidors per el moment de la represa del subministrament. Desconnexió física de part dels equips sí es considera necessari (evitar sobrecàrrega).	
7	...	
8	Verificació del correcte funcionament dels equips SAI's.	
9	Verificació de la correcta represa dels servidors i serveis respectius.	

Figura 27: Model fitxa per el Pla de continuïtat local (PCL)

4.6 Pla d'acció

Paral·lelament a la confecció dels plans de continuïtat i de represa informàtica, formant part d'una fase preliminar en el projecte de millora continua de la seguretat dels sistemes d'informació, es proposa com a pla d'acció previ la verificació del compliment de les següents recomanacions, separades per àrees i per cada sistema definit com a sensible:

Hardware

- ✓ Els equips estan clarament identificats.
- ✓ Els equips estan sota contracte de manteniment.
- ✓ La configuració compta amb elements principals redundats: discos, fonts d'alimentació, ventiladors i targetes Ethernet.

Ubicació

- La sala tècnica ha d'estar senyalitzada per la seva localització ràpida en el cas d'emergència sense la presencia del personal IT responsable.
- La sala compta amb una superfície practicable de 8m2 i no disposa de finestres que donin accés des de l'exterior de l'edifici.

Control Ambiental

- La sala disposa d'un equip de climatització de potència en btu's suficient (Una sala de 40m2 requereix una potència de 5000 btu/h).
- No es tracta d'un equip de climatització especial per CPD's, per tant no existeix redundància ni conductes de retorn de ventilació.
- El manteniment del sistema de climatització és realitzat per el personal de manteniment del servei, per tant, no disposa de suport actiu programat i que especifiqui clarament el temps de restabliment del servei de climatització en cas de fallida de l'equip.
- Es necessari que l'equip de climatització porti el control d'humitat de la sala.

Mesures contra incendis i inundacions.

- La sala tècnica disposa d'un sistema de detecció i extinció d'incendis.

Desplegament de la infraestructura

- Els components estan situats en l'interior d'un Rack.
- La sala disposa d'un fals sostre i un terra tècnic per la protecció i facilitació de les interconnexions.
- El cablejat està clarament senyalitzat i protegit dels accessos no autoritzats.

Seguretat física

- El control d'accés físic a la sala és a través d'una porta tancada amb clau. Es necessari un sistema de control d'accessos que permeti l'enregistrament personalitzat dels accessos autoritzats.
- No existeix cap tipus de vigilància activa o passiva dins de la sala tècnica per la detecció d'accessos no autoritzats.

Seguretat lògica

- Política de control d'accessos (capítol 7).
- Es recomanable disposar d'uns sistema de supervisió que avaluï constantment l'estat del sistema i avisi en cas d'una inestabilitat que pugui provocar una pèrdua de servei o dades sensibles.
- Les regles del Firewall han d'inhabilitar els accessos NETBIOS, FTP, IP, RAS, Terminal Services, etc. a totes les màquines connectades a la xarxa Wi-Fi o WAN.
- S'han d'establir regles del FireWall que habilitin els accessos autoritzats des de la xarxa LAN y WAN.

Subministrament elèctric

- La sala tècnica disposa d'una línia elèctrica, de tres fases i exclusiva, provinent del quadre de serveis generals.
- La sala no disposa de grup electrogen d'emergència.
- L'equip disposa d'un equip d'alimentació ininterrompuda SAI propi, amb bateries correctament dimensionades i amb contracte de manteniment en vigor.

Connectivitat

- ✓ Sistema connectat directament al Switch principal del servei (Switch nivell 2).
- ✓ Existència cable redundant.

Les recomanacions senyalades amb un símbol de perill corresponen a aquelles que requereixen executar una acció. El responsable dels sistemes d'informació del servei, ha de verificar les recomanacions, prioritzar les accions i planificar i pressupostat anualment el pla d'acció per la millora de la seguretat dels sistemes d'informació.

4.7 Millora continuada

Realitzats els plans de continuïtat i de represa informàtica i executat el pla d'acció previ, el responsable dels sistemes d'informació del servei, exercint el rol d'avaluador, ha de reprendre el qüestionari d'avaluació actualitzant, modificant i afegint les informacions necessàries en funció dels resultats obtinguts durant l'execució del pla d'acció previ. Actualitzat el qüestionari i obtinguda la nova avaluació, ha de realitzar un nou estudi de l'avaluació i de l'evolució de la qualificació per capítol i detallada amb el suport de les funcions que proporciona l'eina d'auditoria. Finalment, i amb l'ajuda de les guies d'implantació descrites per cada control en el document ISO/IEC 27002:2005, definirà i planificarà el pla d'acció corresponent a l'any o semestre en curs. En la figura 28 es mostra el diagrama del procés de millora continuada.

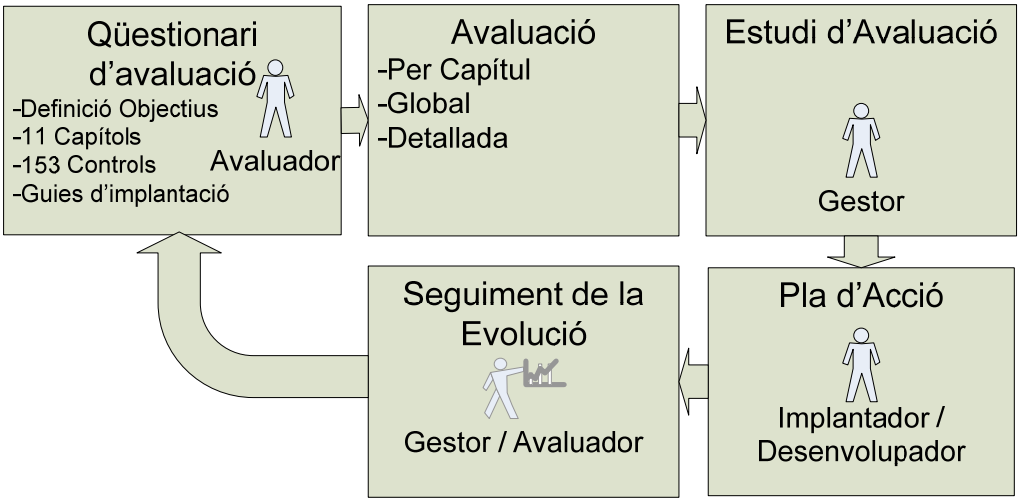


Figura 28: Procés de millora continuada

Es recomana que l'actualització del qüestionari d'avaluació es realitzi cada semestre donant com a resultat la confecció d'un nou pla d'acció per la millora de la seguretat dels sistemes d'informació amb periodicitat anual.

4.8 Valoració resultats i mesura de satisfacció

En el capítol introductori del document ISO/IEC 27002:2005 [1], s'indica quins poden ser els factors rellevants per tal de mesurar l'èxit de la implantació de la seguretat en els sistemes d'informació:

a) La política de seguretat de la informació, els objectius i les activitats són concordants amb els objectius del negoci, empresa o organització.
b) Les eines de suport per la implementació, manteniment, vigilància i millora de la seguretat de la informació estan integrades en la cultura de la organització.
c) Tots els nivells de direcció promouen i donen suport a la implementació de la seguretat de la informació.
d) Bona comprensió dels requeriments de seguretat i de l'anàlisi i gestió dels riscos.
e) Existeixen campanyes d'informació per tal donar a conèixer les informacions de seguretat a tots els managers, empleats, proveïdors, etc.
f) S'ha distribuït a tots els empleats guies i normes de seguretat dels sistemes d'informació.
g) S'ha aprovisionat un pressupost per dur a terme les activitats de gestió de la seguretat dels sistemes d'informació.
h) S'han realitzat entrenaments i formacions en relació a la seguretat de la informació.
i) S'ha establert un sistema de gestió dels incidents de seguretat efectiu.
j) S'ha implantat un sistema d'avaluació i seguiment de l'evolució de la qualitat en la gestió de la seguretat dels sistemes d'informació.

En l'estat actual d'implantació d'aquest projecte no podem mesurar el seu èxit d'implantació, verificant els factors anteriors, fins que no s'executi el pla d'acció previ resultat del primer informe d'avaluació. No obstant, hem demanat als gestors del servei que ens indiquin, mitjançant un qüestionari, quines són les seves previsions/intencions en relació als factors indicats per tal de, primer, donar-los a conèixer aquest indicadors, i segon, per conèixer quina serà la tendència en un futur pròxim en relació a la implantació de la seguretat de la informació en el servei.

PART IV: CONCLUSIONS

Capítol 5: Conclusions i futures línies de treball

El resultat del desenvolupament d'aquest projecte permet que qualsevol organització, servei o empresa, independentment de la seva mida o complexitat, pugui implantar un projecte de qualitat en la gestió de la seguretat dels sistemes d'informació basada en el document ISO/IEC 27002:2005, utilitzant els recursos propis de l'empresa. Dit d'una altra forma, aquest treball posa a disposició, a través d'una eina de suport a l'auditoria, un qüestionari de seguretat dels sistemes d'informació que permet a una organització, a través del seu responsable dels sistemes d'informació, autoavaluar-se en relació a la seguretat de la informació i els sistemes que gestiona sense la participació d'un expert auditor extern. A més, aquesta eina permet també fer un seguiment de qualitat de la gestió de la seguretat i implantar un projecte de millora continuada. En efecte, el resultat d'aquest treball ha estat implantat en dos serveis de dues organitzacions diferents com són, el Servei d'Activitats Físiques de la Universitat Autònoma i el Servei de Tecnologies de la Informació i les Comunicacions de l'Escola Politècnica Superior de Vilanova i la Geltrú.

Per fer-nos una idea del recursos econòmics que una empresa hauria de mobilitzat per tal de fer desenvolupar, per part d'una agent extern, els mètodes i l'eina de suport a l'auditoria resultat d'aquest projecte final de carrera, es proposa la següent taula on s'especifiquen les fases del desenvolupament, el tipus de servei ofert, les hores dedicades per cada tipus de servei en cada fase i un preu/hora informatiu per cada tipus de servei:

Fases desenvolupament/implantació del projecte	Servei	Hores	Preu/hora *	
Disseny conceptual	Analista	5	60	300 €
Especificació	Programador	2	40	80 €
	Analista	5	60	300 €
Desenvolupament eina de suport	Programador	160	40	6.400 €
	Analista	40	60	2.400 €
Confecció Qüestionari	Analista	80	60	4.800 €
Instal·lació	Tècnic informàtic	4	40	160 €
		Total projecte		**14.440 €**

* preu hora aproximat (font internet)

Sí tenim en compte que el preu/hora del servei ofert per un auditor extern, expert en seguretat dels sistemes d'informació, és molt més elevat que el preu/hora dels serveis d'anàlisis i programació, i que les hores dedicades per un auditor extern, que en un principi desconeix els sistemes d'informació a auditar, per completar l'auditoria són moltes més que les d'un responsable dels sistemes d'informació per autoevaluar-se utilitzant les eines proposadades, podem concloure que la quantitat total del projecte indicada en la taula precedent pot ser ràpidament amortitzada. El retorn d'inversió encara seria més favorable sí el producte resultat d'aquest projecte es comercialitzés en format de paquet d'instal·lació en el que totes les empreses compradores participessin del preu de desenvolupament.

Els recursos interns aproximats (en nombre d'hores) emprats per dur a terme la implantació de la gestió de la seguretat dels sistemes d'informació segons es descriu en aquest projecte serien (per cada semestre):

- 2 hores per completar/actualitzar el qüestionari d'avaluació.
- 1h estudi avaluació i evolució.
- 1h confecció actualització del pla d'acció per la millora continuada.

Tal com varem veure en el capítol 2, sent les dades, processos, sistemes i xarxes informàtiques un actiu important per l'empresa, definir, implantar, mantenir i millorar la seguretat en els sistemes d'informació pot ser essencial per tal de mantenir la continuïtat i competitivitat del negoci, minimitzar el danys que un incident pugui provocar a la organització, maximitzar el retorn de les inversions, assegurar la legalitat, aconseguir oportunitats de negoci o mantenir una bona imatge comercial. En aquest sentit, la implantació dels mètodes i eines desenvolupades en aquest projecte poden ser útils i avantatjoses econòmicament per les empreses que requereixin la implantació d'un projecte de gestió de la seguretat dels sistemes d'informació.

Pel que fa a les línies futures de treball, en podem destacar dues:

La primera en el sentit de millorar l'eina de suport a l'auditoria de la seguretat dels sistemes d'informació en els següents aspectes:

- Millores i evolucions proposades en el punt 3.4
- Ampliar / millorar les funcions d'avaluació i representació de resultats.
- Desenvolupar la gestió i confecció del pla d'acció per la millora continuada: Amb el suport de les guies d'implantació presents en el document ISO/IEC i en funció de l'avaluació detallada, es proposés de forma automàtica un pla d'acció per la millora de la seguretat.

La segona línia de treball, ja iniciada, està dirigida en el sentit d'ampliar l'aplicació d'aquests mètodes i eines a l'avaluació del grau d'implantació de guies de disseny, estàndards o normatives. En l'Annex E, *"Diseño de herramienta de evaluación del grado de cumplimento de normativas en el ámbito de la interacción entre personas y la gestión de los sistemas de información"*, es descriu aquesta línia de treball.

Bibliografia

[1] ISO. ISO/IEC 17799. *Information technology- Security Techniques – Code of practices for information security management*. ISO/IEC 2007, 2005.

[2] PHP Group. En URL: http://www.php.net/, Últim accés: 9 abril de 2010

[3] Mysql Enterprise. En URL: http://www.mysql.com/, Últim accés: 9 abril de 2010

[4] XAjax Community. En URL: http://xajaxproject.org/, Últim accés: 9 abril de 2010

[5] Guia d'ambientalització dels projectes de fi de carrera. EPSEVG. Servei d'Informació, Imatge i Publicacions de la UPC, 1998.

[6] Ponsa, P. Vilanova, R. Amante, B., "The use of Role Playing in Engineering Curricula: a Case Study in Human-Automation Systems". Congrés IEEE EDUCON, Madrid, maig 2010.

[7] Modelo Vista Controlador. En URL: http://es.wikipedia.org/wiki/Modelo_Vista_Controlador

[8] HTML (*HyperText Markup Language*). En URL: http://htmlplayground.com/

[9] Davis, G.B. Management Information Systems: conceptual foundations, structure and development. McGraw-Hill, New York. 1974

[10] Carey, J., Galleta, D., Kim, J., Te'eni, D., Wildemuth, B., Zhang, P. The role of human-computer interaction in management information systems curricula: a call to action. Communications of the Association for Information Systems, Vol 13, pp. 357-379, 2004

[11] Zhang, P., Nah, F., Preece, J. HCI studies in Management Information Systems. Behaviour & Information Technology, V 23, Nº 3, pp. 1-13, 2004

[12] Association for Information Systems. En URL: http://www.linknet1.com/sighci/. Última visita: 27/mayo/2010

[13] Ponsa, P., Amante, B., Díaz, M. Ergonomic design applied in a sugar mill interface. Latin American Applied Research Journal, Vol 40, N 1,, pp. 27.34, 2010

[14] ISO. ISO/IEC 25062 Software engineering, software product quality requirements and evaluation (SQuaRE), Common Industry Format (CIF) for usability test reports, 2006

[15] Brooke, J. SUS: A "quick and dirty" usability scale. En Jordan, P.W., Thomas, B.T. y Weerdmeester, B.A. (eds.), Usability Evaluation in Industry. UK: Taylor and Francis, pp. 189-194, 1996

Annex A: Qüestionari d'avaluació de la Seguretat dels Sistemes d'informació. basat en la norma ISO/IEC 27002:2005

1 Política de Seguretat

1.1 Política de seguretat dels sistemes d'informació

Objectiu: Dirigir i donar suport a la gestió de la seguretat dels sistemes d'informació en concordança amb els requeriments del negoci, les lleis i les normes reguladores vigents.

La direcció ha d'establir de forma clara les línies de la política d'actuació i manifestar el seu suport i compromís amb la seguretat de la informació, publicant i mantenint actualitzada, una política de seguretat dins de la seva organització.

1.1.1 Documents de política de seguretat dels sistemes d'informació

1.1.1.1 La Gerència (o el cap de servei) ha aprovat, publicat i comunicat a tots els empleats, un document de política de seguretat dels sistemes d'informació? Anton Goma 11:45 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Sí, en format digital.
- [x] Sí. S'ha fet una publicació de distribució general .
- [ ] Sí. S'ha distribuït de forma individual .
- [ ] Sí. S'ha distribuït de forma individual signada per cada usuari .

Àmbit UAB, aplica igualment al SAF.

Document_unic_definitiu,UAB.pdf X

Esborrar Resposta

1.1.2 Revisió i avaluació

1.1.2.1 La direcció ha designat un responsable de la política de seguretat dels sistemes d'informació encarregat de revisar-la periòdicament amb la finalitat d'assegurar el seu ús continuat, adequació i efectivitat. Anton Goma 11:45 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Hi ha un responsable, però la política es revisa ocasionalment.
- [ ] El responsable de seguretat revisa i actualitza la política de seguretat puntualment, en el moment que es produeixen canvis significatius.
- [x] El responsable de seguretat revisa i actualitza la política de seguretat periòdicament mitjançan un procediment.
- [ ] Ídem anterior + amb el suport d'eines per l'avaluació, revisió i desenvolupament de la política de seguretat.

Àmbit UAB, aplica igualment al SAF.

Afegir doc.

Esborrar Resposta

2 Organització de la Seguretat

2.1 Organització Interna

Objectiu: Gestionar la seguretat de la informació dins de l'organització.

S'ha d'establir una estructura de gestió per iniciar i controlar la implementació de la seguretat de la informació dins de l'organització.

La direcció ha d'aprovar la política de seguretat de la informació, assignar rols de seguretat i coordinar la implantació de la seguretat dins de l'organització.

Si fos necessari, comptar amb les recomanacions de fonts especialitzades com, experts externs, autoritats rellevants, auditors en seguretat, etc. de forma que es coneguin, en intern, les tendències de la industria, l'evolució de les normes i mètodes d'avaluació, així com el tractament de noves incidències en relació a seguretat dels sistemes d'informació.

En aquest punt, s'hauria de promoure una estratègia multidisciplinària de la seguretat dels sistemes d'informació.

2.1.1 Compromís de la direcció en relació a la seguretat dels S.I.

2.1.1.1 La direcció ha nombrat un responsable de la seguretat dels sistemes d'informació?

Anton Goma 11:48 3-03-2010

- [ ] Cap de les opcions següents.
- [x] No, però considera que aquestes responsabilitats formen part de les encarregades al responsable informàtic.
- [ ] Sí, però sense una nominació oficial.
- [ ] Sí, amb una nota oficial de la nominació.
- [ ] Ídem anterior + la persona responsable dedica al menys un 50% del temps de treball a aquesta activitat.

Àmbit SAF

Afegir doc.

Esborrar Resposta

2.1.2 Coordinació de la seguretat dels S.I.

2.1.2.1 La seguretat dels sistemes d'informació és objecte d'un pla d'acció anual?

Anton Goma 11:35 3-03-2010

- [ ] Cap de les opcions següents.
- [x] Les accions de seguretat dels S.I. són realitzades a mesura que apareixen les necessitats.
- [ ] Existeix un pla d'acció anual definit dins el SAF.
- [ ] El pla d'acció del servei, repren el pla d'acció del Servei Informàtic de la UAB .
- [ ] Ídem anterior + accions complementàries dins el SAF.

Àmbit SAF

Afegir doc.

Esborrar Resposta

2.1.3 Atribució de responsabilitats en relació a la seguretat dels S.I.

2.1.3.1 Com són definides les responsabilitats en matèria de la seguretat dels Sistemes d'informació en el SAF?

Anton Goma 11:52 3-03-2010

- [ ] Cap de les opcions següents.
- [x] Les responsabilitats són implícites.
- [ ] Les responsabilitats són indicades als interessats de forma informal.
- [ ] Les responsabilitats son formalitzades en un document, validat per la direcció, i comunicades formalment als interessats.
- [ ] ídem anterior + les responsabilitats són objecte d'una revisió i actualització anual.

Hi ha un document propi del SAF que signen les persones que han de treballar a la Unitat d'Informàtica.

Afegir doc.

Esborrar Resposta

2.1.4 Sistemes d'autorització en relació als mitjans de tractament de la informació

2.1.4.1 S'ha posat en marxa un procediment formal d'acreditació i aprovació dels nous mitjans de tractament informàtic?

Anton Goma 11:50 3-03-2010

- [x] Cap de les opcions següents.
- [ ] Segons el projecte, es segueixen guies i check-lists
- [ ] Es realitza un estudi detallat dels riscos de seguretat que pot comportar el nou sistema de tractament informàtic.
- [ ] Es segueix un procediment formal d'aprovació per els projectes que tenen impacte sobre els sistemes d'informació sempre que el seu pressupost sigui superior a un límit definit per la direcció.
- [ ] Procediment no aplicable en el SAF.

Afegir doc.

Esborrar Resposta

2.1.5 Compromisos de confidencialitat

2.1.5.1 Es demana a les persones, que tenen accés a les informacions sensibles dels sistemes d'informació del SAF, de signar un acord de confidencialitat ("Non Disclosure Agreement")? Anton Goma 11:53 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Sí, a certs empleats.
- [ ] Sí, a certs col•laboradors o proveïdors de serveis.
- [x] Els empleats de les societats proveïdores de serveis que ocupen funcions en els sistemes d'informació i que tenen accés a informacions sensibles, signen un acord de confidencialitat.
- [ ] ídem anterior + es realitza una revisió periòdica.

Afegir doc.
Esborrar Resposta

2.1.5.2 Coneixeu el model d'acord de confidencialitat de Servei Informàtic de la UAB? Anton Goma 11:54 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Es considera suficient les clàusules en els contractes.
- [x] El SAF té el seu propi model d'acord de confidencialitat.
- [ ] S'aplica el model de Servei Informàtic de la UAB i es considera suficient .
- [ ] Amb la base del model de Servei Informàtic de la UAB, s'ha ampliat, conjuntament amb els serveis competents (RH i servei jurídic) per tal realitzar i aplicar un acord de confidencialitat específic a cada situació.

Afegir doc.
Esborrar Resposta

2.1.6 Relació amb les autoritats

2.1.6.1 Existeix en el SAF un procediment d'alerta a les autoritats competents (policia, bombers, protecció civil, etc.) en cas d'incidents (robatori, intrusió, foc, etc.)? Anton Goma 11:56 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Les autoritats competents han estat identificades.
- [ ] Les autoritats competents han estat identificades i les informacions que emeten són tingudes en compte localment en el SAF.
- [ ] ídem anterior + procediment d'alerta en cas d'incident.
- [x] ídem anterior + proves i simulacres puntuals amb les autoritats.

Existeix Pla d'Emergència específic pel SAF

Afegir doc.
Esborrar Resposta

2.1.7 Relacions amb els grups d'especialistes

2.1.7.1 Amb quina freqüència el responsable de seguretat dels sistemes d'informació del SAF participa en els comitès de seguretat de Servei Informàtic de la UAB? Anton Goma 11:56 3-03-2010

- [ ] Cap de les opcions següents.
- [x] Participació puntual i irregular.
- [ ] Cada dos anys.
- [ ] Anualment.
- [ ] El responsable del SAF està integrat en grup de treball de Servei Informàtic de la UAB.

Afegir doc.
Esborrar Resposta

2.1.8 Revisió independent de la seguretat dels sistemes d'informació

2.1.8.1 Es realitzen auditories de seguretat dels S.I. per part d'agents externs al SAF? Anton Goma 11:57 3-03-2010

- [x] Cap de les opcions següents.
- [ ] Es fan auditories internes.
- [ ] Sí, però en un perímetre restringit (per exemple, una aplicació concreta o un servidor determinat).
- [ ] Sí, però en el perímetre definit com a sensible.
- [ ] Sí, regularment, sobre tots els sistemes definits com a sensibles ja estiguin localitzats en el SAF com en les instal•lacions de proveïdors de serveis.

Afegir doc.
Esborrar Resposta

2.2 Tercers (Outsourcing)

Objectiu: Mantenir la seguretat dels sistemes d'informació que són accessibles, processats, comunicats o gestionats per un tercer.

La seguretat en la informació propietat del servei i les instal•lacions de processat de la informació, NO pot ser reduïda per la participació d'un proveïdor, producte o servei extern.

S'ha de controlar els accessos de tercers als dispositius de tractament de la informació de servei.

Quan la necessitat del negoci requereixi l'accés per part d'un tercer als sistemes d'informació, s'ha de realitzar una avaluació de riscos per determinar les implicacions sobre la seguretat i les mesures de control requerides. Aquestes mesures de control s'han de definir i acceptar per contracte amb el tercer.

2.2.1 Identificació dels riscos lligats amb accessos a tercers

2.2.1.1 Teniu actualitzada la llista de contactes de proveïdors de serveis? Anton Goma 12:03 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Només la llista de contactes definits com importants.
- [ ] La llista de la majoria dels contactes.
- [x] La llista de tots els contactes s'actualitza regularment.
- [ ] ídem anterior + està centralitzada i inclou el nom de la persona responsable, la funció i el nom del substitut en cas d'absència. Es realitzen controls regularment.

Afegir doc.
Esborrar Resposta

2.2.2 La seguretat dels S.I. i els clients

2.2.2.1 Quines mesures prèvies es prenen per tal de subministrar als vostres clients o proveïdors un accés als sistemes d'informació del SAF? Anton Goma 12:03 3-03-2010

- [ ] Cap de les opcions següents.
- [x] Es realitza un anàlisi de les necessitats funcionals.
- [ ] Es realitza un anàlisis detallat dels riscos lligats al accés als sistemes d'informació par part del client o proveïdor.
- [ ] ídem anterior + les responsabilitats són clarament identificades i atribuïdes.
- [ ] ídem anterior + es realitzen controls regularment.

Afegir doc.
Esborrar Resposta

2.2.3 Gestió de la seguretat dins dels contractes i compromisos amb tercers

2.2.3.1 Quins són els punts de seguretat inclosos dins els contractes de proveïdors de serveis informàtics? Anton Goma 12:04 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Alguns contractes inclouen, com a mínim, les clàusules de confidencialitat.
- [x] Els contractes considerats crítics inclouen clàusules de confidencialitat i seguretat.
- [ ] Tots els contractes de prestacions de serveis informàtics inclouen el respecte a les normes aplicables de seguretat i les conseqüències eventuals en cas de violació d'aquestes normes par part del proveïdor.
- [ ] ídem anterior + es realitzen controls regularment.

Afegir doc.
Esborrar Resposta

3 Gestió dels actius

3.1 Responsabilitat relatives als actius

Objectiu: Mantenir una protecció adequada sobre els actius de la organització.

Tots els actius han de ser inventariats i tenir designat un propietari o responsable.

S'han d'identificar els propietaris dels actius sensibles i s'ha d'assignar-li la responsabilitat del manteniment dels controls pertinents. El propietari pot delegar la implantació de controls específics però, el propietari manté la responsabilitat sobre l'actiu.

3.1.1 Inventari dels actius

3.1.1.1 Disposeu d'un inventari actualitzat dels equips que composen el sistema d'informació del SAF?

Anton Goma 12:05 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Una part dels materials han estat inventariats.
- [ ] Tots els components han estat inventariats.
- [x] ídem anterior + l'inventari s'actualitza cada any.
- [ ] ídem anterior + es verifica la concordança amb l'inventari d'immobilitzacions contable del SAF.

EQUIPS SAF (02-02-2010).xls X

Esborrar Resposta

3.1.1.2 El responsable informàtic del SAF disposa d'un esquema actualitzat de l'arquitectura de xarxa informàtica amb l'inventari de routers, firewalls, servidors, etc.?

Anton Goma 12:05 3-03-2010

- [ ] Cap de les opcions següents.
- [x] Un esquema de l'arquitectura està parcialment formalitzat, comprés l'inventari dels sistemes i equips de xarxa.
- [ ] Un esquema complert (servidors, switch, routers, equips wi-fi, etc.) s'actualitza amb una periodicitat de més de tres mesos.
- [ ] ídem anterior + l'esquema està permanentment actualitzat.
- [ ] ídem anterior + existeix un procediment per actualitzar l'esquema a cada evolució de l'arquitectura.

PART3.vsd X

Esborrar Resposta

3.1.2 Propietat dels bens

3.1.2.1 Com es té en compte la propietat dels actius dins el SAF?

Anton Goma 12:08 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] La qüestió ha estat posada però no tractada.
- [x] Un propietari ha estat identificat per una part dels sistemes.
- [ ] Un propietari ha estat identificat per tots i cada un dels sistemes, incloent les aplicacions i els equips.
- [ ] ídem anterior + es verifica la concordança amb l'inventari d'immobilitzacions contable SAF.

Afegir doc.

Esborrar Resposta

3.1.3 Utilització correcte dels actius

3.1.3.1 Existeix un document on es recullin les normes d'utilització dels recursos informàtics i de processat de la informació i aquest document és conegut pel conjunt dels usuaris?

Anton Goma 12:11 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Sí, en format digital.
- [x] Sí. S'ha fet una publicació de distribució general.
- [ ] Sí. S'ha distribuït de forma individual.
- [ ] Sí. S'ha distribuït de forma individual signada per cada usuari.

Document_unic_definitiu_nomes_obligacions_pe

Esborrar Resposta

3.2 Classificació de les informacions

Objectiu: Assegurar un nivell de protecció adequat per els actius dels sistemes d'informació.

La informació s'ha de classificar de forma que es detectin necessitats, prioritats i graus de protecció.

La informació té graus variables de sensibilitat i criticitat. Alguns elements dels sistemes d'informació poden requerir un nivell addicional de protecció o un ús especial. S'ha d'utilitzar un sistema de classificació de la informació per definir un conjunt de nivells de protecció i comunicar la necessitat de les mesures d'utilització especial.

3.2.1 Línies directrius per la classificació

3.2.1.1 Els actius crítics o sensibles han estat identificats?

Anton Goma 12:13 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Existeixen algunes recomanacions.
- [x] Per certs projectes, els actius crítics o sensibles han estat identificats (dades, aplicacions i equips).
- [ ] Un procediment permet identificar els actius crítics o sensibles.
- [ ] El procediment està actualitzat regularment i assegura l'adequació amb la línia de negoci del SAF.

Afegir doc.

Esborrar Resposta

3.2.2 Marcatge i manipulació de la informació

3.2.2.1 Heu posat en marxa procediments que permetin als usuaris classificar i manipular les informacions sensibles (condicions d'emmagatzematge, etiquetatge, rebuig, etc.)?

Anton Goma 12:14 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] Els usuaris són sensibles a la necessitat de gestionar els documents confidencials.
- [x] Els usuaris tenen les instruccions específiques en relació a la destrucció de documents sensibles i a la sortida de documents fora dels locals del SAF.
- [ ] Els usuaris disposen de procediments precisos per classificar, manipular i emmagatzemar les informacions sensibles.
- [ ] Els usuaris disposen de procediments de gestió de les informacions en funció del nivell de sensibilitat i dels mitjans per gestionar la confidencialitat (caixes fortes, destructores documents, cables antirobatori, etc.).

Afegir doc.

Esborrar Resposta

4 Gestió de Personal

4.1 Abans la presa de funcions

Objectiu: Assegurar que els empleats, proveïdors i tercers entenen les seves responsabilitats i que aquestes són adequades a les funcions que se'ls ha atribuït, reduint així, el risc de robatori, frau o ús incorrecte de les instal•lacions.

Les responsabilitats en la seguretat dels sistemes d'informació s'han de tractar abans de la presa de funcions, adequant-les a la descripció de les funcions i condicions del treball.

Tots els candidats a un lloc de treball, proveïdors i usuaris tercers, han de ser adequadament seleccionats, especialment per els treballs considerats sensibles.

Empleats, proveïdors i tercers que utilitzin les instal•lacions dels sistemes d'informació, han de firmar un acord de confidencialitat.

4.1.1 Rols i responsabilitats

4.1.1.1 Les persones implicades en la seguretat dels S.I. (responsable de seguretat, administrador sistema, tècnic, suport, usuari, operari, etc.) estan informades del seu rol i responsabilitat en relació a la seguretat dels S.I.?

Anton Goma 12:16 3-03-2010

- ☐ Cap de les opcions següents.
- ☑ Sí, de forma informal.
- ☐ Sí, existeixen clàusules en els contractes de treball i en les fitxes de definició del lloc de treball que nomenen les responsabilitats en la seguretat dels S.I..
- ☐ Els rols i responsabilitats en matèria de seguretat són sistemàticament objecte d'una comunicació individual i formal a cada empleat o col•laborador.
- ☐ Les clàusules específiques de seguretat estan formalitzades en el contractes de treball o en els contractes de prestacions de serveis implicats.

Afegir doc.
☐ Esborrar Resposta

4.1.2 Selecció

4.1.2.1 Quines són les precaucions preses, en conformitat a la llei, envers els candidats a contractar per una funció relacionada amb els sistemes d'informació?

Anton Goma 12:17 3-03-2010

- ☐ Cap de les opcions següents.
- ☑ Entrevista amb el candidat seguint els criteris establerts per el responsable de personal i els experts en la matèria.
- ☐ ídem anterior + es realitzen verificacions de coherència amb els diplomes (estudis) del candidat.
- ☐ ídem anterior + verificacions de coherència del c.v..

Afegir doc.
☐ Esborrar Resposta

4.1.3 Condicions contractuals

4.1.3.1 Quins són els mitjans utilitzats per informar als nous contractats de les regles de seguretat vigents dins el SAF?

Anton Goma 12:25 3-03-2010

- ☐ Cap de les opcions següents.
- ☐ Recomanacions orals.
- ☐ Document de normes de seguretat publicat o penjat en el taulell d'informacions.
- ☑ Tot nou contractat rep el document de normes de seguretat en vigor.
- ☐ Ídem anterior + aquest document és distribuït regularment.

Document_unic_definitiu_nomes_obligacions_pe
☐ Esborrar Resposta

4.2 Durant el contracte

Objectiu: Assegurar que tots els empleats, proveïdors i usuaris tercers són coneixedors de les amenaces i riscos en l'àmbit de la seguretat dels sistemes d'informació, i que estan equipats i preparats per complir la política de seguretat de la organització en el curs normal del seu treball, reduint així el risc d'error humà.

Les responsabilitats de la direcció han de ser definides de forma que s'asseguri que la política de seguretat és complerta per cada un dels empleats individualment.

Un nivell adequat de coneixement, formació i entrenament en els procediments de seguretat i el correcte ús de les instal•lacions dels sistemes d'informació, s'ha de proporcionar a tots els empleats, proveïdors i usuaris tercers, amb la finalitat de minimitzar els possibles riscos de seguretat.

S'ha d'establir un procés disciplinari formal en el cas d'incompliment greu que hagi perjudicat a la seguretat dels sistemes d'informació.

4.2.1 Responsabilitats de la direcció

4.2.1.1 Els responsables jeràrquics posen en marxa mesures per assegurar l'aplicació de les normes de seguretat dels S.I.? Anton Goma 12:26 3-03-2010

- [ ] Cap de les opcions següents.
- [ ] El cap de servei manifesta informalment la necessitat de complir les normes en matèria de seguretat en els S.I..
- [ ] S'emeten notes de servei per recordar les bones pràctiques en matèria de seguretat.
- [x] El cap de servei es preocupa regularment del control d'accés a les aplicacions crítiques, de la verificació de les operacions sensibles i de les copies de seguretat..
- [ ] El cap de servei demana que s'executin regularment controls per tal de verificar que es compleixen les normes de seguretat dels S.I..

Afegir doc.
Esborrar Resposta

4.2.2 Sensibilització, qualificació i formació en matèria de la seguretat dels S.I.

4.2.2.1 Existeix formació/informació per tal de sensibilitzar al personal en relació a la seguretat dels sistemes d'informació? Anton Goma 12:27 3-03-2010

- [ ] Cap de les opcions següents.
- [x] Accions de sensibilització s'organitzen puntualment.
- [ ] Accions de sensibilització destinades al conjunt del personal han tingut lloc recentment.
- [ ] Formacions o informacions de sensibilització (per exemple, via mail) són posades a disposició del personal i col•laboradors.
- [ ] Ídem anterior + es realitzen comunicacions regulars de recordatori.

Àmbit UAB

Afegir doc.
Esborrar Resposta

4.2.3 Processos disciplinaris

4.2.3.1 Està previst un procediment per aplicar eventuals sancions disciplinàries en cas d'incompliment greu que hagi perjudicat a la seguretat dels sistemes d'informació? Anton Goma 12:27 3-03-2010

- [ ] Cap de les opcions següents.
- [x] Es deixa la decisió en mans del cap jeràrquic de la persona infractora i del responsable de Recursos Humans.
- [ ] Sí, en cas de falta greu i en conformitat al codi de treball.
- [ ] Sí, un procediment ha estat elaborat amb la col•laboració dels Recursos Humans i ha estat difós al personal.
- [ ] Sí, un procediment defineix clarament allò que és sancionable o no en cas de perjudici a la seguretat dels sistemes d'informació.

Afegir doc.
Esborrar Resposta

4.3 A la fi o modificació del contracte

Objectiu: Assegurar que els empleats, proveïdors i usuaris tercers que finalitzen les seves funcions, surten de l'organització de forma ordenada.

S'ha de designar un responsable que s'encarregui de gestionar el retorn dels recursos informàtics i de la informació, així com de verificar que la retirada dels drets d'accés ha estat completada.

En relació als drets d'accés als sistemes d'informació, tot canvi de responsabilitats i funcions dins de l'organització, han de ser gestionats com una finalització de contracte, i tota nova funció, responsabilitat o treball ha de ser gestionada seguint les recomanacions del capítol 4.1.

4.3.1 Responsabilitats en la fi del contracte

4.3.1.1 Existeix un procediment per recordar als col•laboradors o empleats en fi de contracte de les seves obligacions contractuals prèvies a deixar el SAF? Anton Goma 12:27 3-03-2010

- [x] Cap de les opcions següents.
- [ ] Aquest punt es deixa a la apreciació del responsable jeràrquic.
- [ ] Existeix una llista de tasques a fer per part dels col•laboradors o empleats abans de deixar el servei .
- [ ] Sí, un nota o mail de recordatori s'envia sistemàticament al responsable jeràrquic abans de la fi de contracte d'un col•laborador o empleat, segons un procediment clarament establert.
- [ ] Sí, es firma document per part del col•laborador o empleat, que li recorda els compromisos post contracte que s'han de complir.

Afegir doc.
Esborrar Resposta

4.3.2 Restitució dels recursos informàtics

4.3.2.1 Existeix un procediment de restitució d'actius o recursos informàtics par part dels col•laboradors o empleats a la fi del seu contracte? Anton Goma 12:27 3-03-2010

- [x] Cap de les opcions següents.
- [ ] Les persones restitueixen, per iniciativa pròpia, els actius o recursos a cada un dels serveis propietaris.
- [ ] Se'ls comunica una llista de serveis interns a consultar abans deixar el SAF.
- [ ] Segons un procediment definit, el responsable jeràrquic es responsabilitza de recuperar els actius o recursos del SAF en possessió de l'empleat o col•laborador abans de la seva partida.
- [ ] Ídem anterior + cada cap de departament informa al responsable RH una vegada les formalitats de sortida han estat realitzades.

Afegir doc.
Esborrar Resposta

4.3.3 Supressió dels drets d'accés

4.3.3.1 Existeix un procediment de supressió dels drets d'accés en el moment que un empleat o col•laborador deixa el SAF per fi de contracte? Anton Goma 14:29 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Es deixa en mans del responsable jeràrquic procurar la retirada progressiva dels drets d'accés de la persona que deixa el departament.
- [ ] Tots els accessos són sistemàticament suprimits en el moment de la sortida.
- [ ] El dia de sortida, els accessos dels usuaris o col•laboradors són automàticament suprimits.
- [ ] En l'anunci d'una finalització de contracte, els drets d'accés de l'empleat o col•laborador són reduïts per evitar tota alteració voluntària o pèrdua de confidencialitat. En el moment de la sortida, els drets d'accés són eliminats.

Afegir doc.
Esborrar Resposta

5 Seguretat Física

5.1 Zones de seguretat

Objectiu: Evitar els accessos no autoritzats, danys i interferències en els sistemes d'informació.

Els recursos per el tractament de la informació crítica o sensible s'han d'ubicar en zones protegides per un perímetre de seguretat definit, amb tanques de seguretat i controls d'accés apropiats.

El nivell de protecció ha de ser proporcional als riscos identificats.

5.1.1 Perímetre de seguretat física

5.1.1.1 Hi ha establert un perímetre de seguretat en els locals informàtics? Anton Goma 14:31 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Certs equips sensibles es troben en sales que no són exclusivament dedicades a l'informàtica.
- [ ] Tots els equips informàtics sensibles es troben en sales tècniques dedicades.
- [x] Tots els equips informàtics, inclosos els de xarxa, es troben en sales tècniques dedicades amb l'accés controlat.
- [ ] Ídem anterior + es fa una revisió anual de la seguretat física en relació a les sales tècniques.

Afegir doc.
Esborrar Resposta

5.1.2 Control d'accessos físics

5.1.2.1 Els accessos als locals informàtics dedicats disposen d'un control d'accés físic mitjançant clau de seguretat, digicode, targeta d'identificació, etc. ? Anton Goma 14:31 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Sí, un sistema de clau de seguretat.
- [ ] Sí, un sistema de codi digital.
- [ ] Sí, per un sistema que permet la identificació individual de les persones habilitades per l'accés (targeta d'identificació nominativa, targeta amb xip, etc.).
- [ ] Ídem anterior + s'efectua una revisió anual dels accessos concedits.

Afegir doc.
Esborrar Resposta

5.1.3 Seguretat de les oficines i sales d'equips tècnics

5.1.3.1 S'han instaurat mesures antirobatori en les sales tècniques dedicades? Anton Goma 14:32 16-03-2010

- [x] Cap de les opcions següents.
- [ ] Si, portes i vidres blindats.
- [ ] Sí, mitjans de vigilància passius (p.e. detectors volumètrics).
- [ ] Sí, mitjans de vigilància actius (p.e. videovigilància 24x7) completen els mitjans passius.
- [ ] Ídem anterior + el perímetre està vigilat per guardes de seguretat o per televigilància i un sistema d'alarma alerta automàticament en cas d'intrusió.

Afegir doc.
Esborrar Resposta

5.1.3.2 Disposeu d'ún sistema de gestió centralitzada d'alarmes en cas d'incendi, inundació i intrusió en els locals informàtics? Anton Goma 14:32 16-03-2010

- [x] Cap de les opcions següents.
- [ ] Sí, però únicament en els locals sensibles.
- [ ] Sí, un sistema parcial en cas d'incendi.
- [ ] Sí, un sistema parcial per l'incendi i la intrusió.
- [ ] Sí, per l'incendi, la inundació i la intrusió.

Afegir doc.
Esborrar Resposta

5.1.4 Protecció contra les amenaces exteriors i de l'entorn

5.1.4.1 Heu tingut en compte les condicions mediambientals de les sales informàtiques? Anton Goma 14:33 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Assegurança contra inundació o incendi.
- [x] Les sales tècniques disposen de proteccions habituals com falsos sostres i falsos terres, detectors d'incendis, extintors visibles de fàcil accés i amb indicacions de domini d'aplicació, alarma anti-intrusió, climatització i detectors d'humitat.
- [ ] S'ha realitzat un anàlisis de riscos mediambientals i s'han instal•lat les proteccions apropiades que de l'anàlisi s'han extret.
- [ ] Ídem anterior + les instal•lacions estan vigilades per un sistema d'alarma automàtic.

Afegir doc.
Esborrar Resposta

5.1.5 Treball dins de les zones de seguretat

5.1.5.1 Heu instaurat mesures de protecció particulars dins les zones sensibles? Anton Goma 14:33 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] No, però les sales sensibles han estat identificades.
- [ ] Les oficines i sales sensibles han estat identificades i tancades amb clau la major part del temps.
- [x] Les oficines i sales sensibles han estat identificades i tancades amb clau sempre que es queden buides de personal.
- [ ] Ídem anterior + revisió anual de l'adequació dels dispositius de vigilància amb el nivell de sensibilitat dels locals.

Afegir doc.
Esborrar Resposta

5.1.6 Zones d'accés públic i de lliurement de comandes

5.1.6.1 S'ha reforçat el control d'accés en aquelles sales tècniques que són accessibles des de zones d'accés al públic per tal d'evitar un accés no autoritzat? Anton Goma 14:34 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Mitjanament controlat. Un accés no autoritzat a una sala sensible és possible.
- [ ] Un empleat vigila les zones de accés públic (normalment, zones de lliurement) pròximes a les sales tècniques sensibles.
- [x] Les zones d'accés públic físicament aïllades. No és possible accedir a les sales informàtiques sensibles des d'una zona d'accés publica.
- [ ] Ídem anterior + una nota de servei està formalitzada per tal de sensibilitzar al personal que es controlin els accessos no autoritzats per part del públic.

Afegir doc.
Esborrar Resposta

5.2 Seguretat del material

Objectiu: Evitar pèrdues, danys o comprometre els actius, així com la interrupció de les activitats del servei.

Els equips han d'estar físicament protegits contra les amenaces externes.

La protecció de l'equip és necessària per reduir els riscos d'accessos no autoritzats a la informació i per evitar pèrdua de dades o danys.

S'han de considerar mesures especials de protecció en els sistemes de copies de seguretat, el cablejat de dades informàtiques i els equips d'alimentació ininterrompuda (SAI) que donen servei als sistemes d'informació sensibles.

5.2.1 Emplaçament i protecció del material

5.2.1.1 L'accés dins les sales tècniques als equipament sensibles d'alimentació elèctrica, climatització, bateries, etc. està restringit al personal tècnic habilitat? Anton Goma 14:35 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Parcialment. L'accés a certs equips sensibles queda accessible al personal del SAF.
- [ ] La major part dels accessos als equips sensibles està restringit al personal tècnic habilitat.
- [x] L'accés a tots els equips sensibles d'alimentació elèctrica, climatització i bateries està restringit per ser accessible només per el personal tècnic habilitat.
- [ ] Ídem anterior + l'accés dins la sala informàtica per part del personal tècnic habilitat es fa acompanyat d'un responsable informàtic.

Afegir doc.
Esborrar Resposta

5.2.2 Serveis generals

5.2.2.1 Els equips estan protegits de les fallides d'aprovisionament elèctric mitjançant fonts permanents com equips ups, generadors de backup, subministrador múltiple, etc?

Anton Goma 14:35 16-03-2010

- [ ] No
- [ ] Parcialment
- [ ] Alguns sistemes crítics
- [x] Tots els sistemes crítics
- [ ] Ídem anterior + revisions i verificacions periòdiques

Afegir doc.
Esborrar Resposta

5.2.3 Seguretat del cablejat

5.2.3.1 L'accés a les vies de cablejat és objecte de mesures de protecció?

Anton Goma 14:36 16-03-2010

- [ ] Cap de les opcions següents.
- [x] La localització dels accessos a les vies de cablejat estan identificades.
- [ ] L'accés a les vies de cablejat més sensibles està protegit per clau o estan dins de locals protegits.
- [ ] Els accessos a totes les vies de cablejat està sota clau o dins d'un local protegit.
- [ ] Tots les vies de cablejat estan en locals protegits.

Afegir doc.
Esborrar Resposta

5.2.4 Manteniment dels equips

5.2.4.1 Els equips estan revisats per el subministrador oficial o per el personal autoritzat, seguint els intervals recomanats i les especificacions ?

Anton Goma 14:36 16-03-2010

- [ ] No
- [ ] Parcialment
- [ ] Puntualment, per els sistemes de producció sensibles.
- [x] Sí, en tots els sistemes de producció sensibles.
- [ ] Ídem anterior + revisions i verificacions periòdiques per tal d'aplicar mesures preventives i/o correctives.

Afegir doc.
Esborrar Resposta

5.2.5 Seguretat del material exterior a les instal•lacions (material en circulació)

5.2.5.1 L'ús de qualsevol equip informàtic del servei en l'exterior de les instal•lacions del propi servei, requereix d'una autorització per part del responsable jeràrquic?

Anton Goma 14:37 16-03-2010

- [x] No.
- [ ] A criteri del responsable jeràrquic.
- [ ] Puntualment es fa un anàlisis de riscos sí l'equip forma part d'un sistema sensible i s'autoritza la sortida.
- [ ] Els sistemes, equips i dades sensibles estan clarament identificats i no està autoritzada la sortida
- [ ] Ídem anterior + accions d'auditoria periòdiques

Afegir doc.
Esborrar Resposta

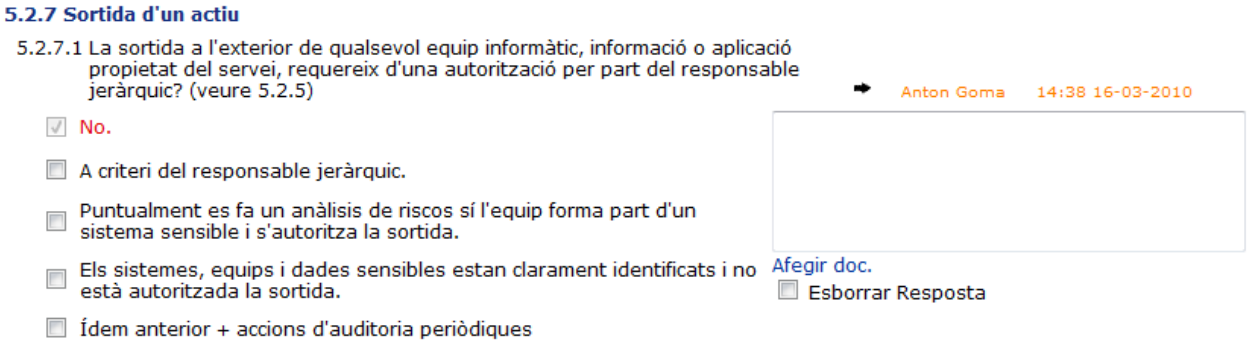
5.2.6 Rebuig o reciclatge segur del material

5.2.6.1 Durant les migracions, rebuig o reciclatge dels equips, existeixen procediments per la reinicialització total dels equips que hagin contingut dades sensibles?

Anton Goma 14:38 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Els discos són esborrats.
- [x] Els discos són esborrats i formatejats.
- [ ] Els discos són esborrats amb una aplicació específica de esborrat segur.
- [ ] Ídem anterior + el procediment és controlat regularment.

Afegir doc.
Esborrar Resposta


5.2.7 Sortida d'un actiu
5.2.7.1 La sortida a l'exterior de qualsevol equip informàtic, informació o aplicació propietat del servei, requereix d'una autorització per part del responsable jeràrquic? (veure 5.2.5)
Anton Goma 14:38 16-03-2010
No.
A criteri del responsable jeràrquic.
Puntualment es fa un anàlisis de riscos sí l'equip forma part d'un sistema sensible i s'autoritza la sortida.
Els sistemes, equips i dades sensibles estan clarament identificats i no està autoritzada la sortida.
Ídem anterior + accions d'auditoria periòdiques
Afegir doc.
Esborrar Resposta

6 Gestió de l'explotació i de les telecomunicacions

6.1 Processos i responsabilitats lligades a l'explotació

Objectiu: Assegurar l'operació correcte i segura dels recursos de tractament de la informació.

S'han d'establir responsabilitats i procediments per la gestió i operació de tots els recursos de tractament de la informació. Això inclou el desenvolupament d'instruccions apropiades d'operació i procediments de resposta a les incidències.

S'ha d'implantar la segregació de tasques, quan sigui pertinent, per reduir el risc d'un mal ús deliberat del sistema o per negligència.

6.1.1 Procediments d'explotació documentats

6.1.1.1 Els procediments d'explotació informàtica són sistemàticament documentats, coneguts, actualitzats, accessibles i aplicats per el personal encarregat? Anton Goma 14:41 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Gran part dels procediments d'explotació existeixen de forma informal (instruccions, notes, mails, etc.).
- [x] Gran part dels procediments d'explotació crítics estan formalment documentats.
- [ ] Tots els procediments d'explotació estan formalment documentats .
- [ ] Tots els procediments d'explotació estan formalment documentats i existeix un procés per l'actualització permanent dels mateixos.

Afegir doc.
Esborrar Resposta

6.1.2 Gestió de les modificacions

6.1.2.1 Totes les aplicacions executades en els sistemes de producció estan estrictament controlades en qualsevol canvi, actualització o modificació?. Es a dir, qualsevol canvi en els sistemes de producció requereix una autorització expressa? Anton Goma 14:42 16-03-2010

- [ ] No.
- [ ] Puntualment.
- [x] Puntualment, per els sistemes de producció sensibles.
- [ ] Sí, en tots els sistemes de producció sensibles.
- [ ] ídem anterior + registre i auditories periòdiques.

Afegir doc.
Esborrar Resposta

6.1.3 Separació de les tasques

6.1.3.1 Hi ha un esforç per limitar els drets d'administració al personal encarregat de l'explotació dels diferents sistemes? Anton Goma 14:42 16-03-2010

- [ ] No.
- [x] Tots els administradors obtenen els drets de control total dels sistemes.
- [ ] En certs sistemes crítics, sempre i quan sigui tècnicament possible, els drets concedits a l'administrador li permeten únicament executar unes tasques determinades.
- [ ] En tots els sistemes crítics, els diferents administradors tenen accés a l'execució de tasques que li són atribuïdes.
- [ ] Ídem anterior + un procediment de control regular dels drets d'accés concedits.

Afegir doc.
Esborrar Resposta

6.1.4 Separació dels equips de desenvolupament, de test i d'explotació

6.1.4.1 Les instal•lacions de test i desenvolupament estan aïllades (router) de les operacionals? Anton Goma 14:42 16-03-2010

- [x] No.
- [ ] No totes les instal·lacions.
- [ ] No totes les instal·lacions sesnsibles.
- [ ] Sí. Totes les instal·lacions sensibles.
- [ ] Ídem anterior + accions d'auditoria periòdiques

Afegir doc.
Esborrar Resposta

6.2 Gestió de la prestació de serveis per un tercer

Objectiu: Implementar i mantenir un nivell apropiat de seguretat i d'entrega de servei en línia amb els acords o contractes amb tercers.

S'ha de verificar la implementació d'acords, vigilar la conformitat i gestionar els canvis per tal d'assegurar que els serveis prestats compleixen els requeriments acordats.

6.2.1 Prestació de serveis

6.2.1.1 Dins el marc de contractes amb els proveïdors de serveis informàtics, es controla que el nivell de servei i les clàusules de seguretat estan definides i aplicades?

Anton Goma 14:48 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Es defineixen els nivells de servei.
- [ ] Es defineixen els nivells de servei, els informes associats i les clàusules de seguretat.
- [x] Ídem anterior + i són aplicades.
- [ ] Ídem anterior + i són auditades regularment.

Afegir doc.
Esborrar Resposta

6.2.2 Vigilància i revisió dels serveis de tercers

6.2.2.1 Es realitzen auditories dels serveis i es controlen els informes i resultats subministrats així com la gestió dels possibles incidents?

Anton Goma 14:48 16-03-2010

- [x] Cap de les opcions següents.
- [ ] Els proveïdors comuniquen alguns elements a petició del SAF.
- [ ] Els proveïdors comuniquen els elements a petició sistemàticament després de produir-se un incident.
- [ ] El proveïdor proporciona mensualment un informe segons els acords contractats. Aquest informe i la forma com els proveïdor ha gestionat els incidents de seguretat són analitzats. Després de cada incident, el proveïdor pren sistemàticament contacte amb el SAF.
- [ ] Una auditoria dels serveis proporcionats per part del proveïdor ha estat realitzada per un tercer a petició del SAF.

Afegir doc.
Esborrar Resposta

6.2.3 Gestió i evolució dels serveis prestats per un tercer

6.2.3.1 Cada evolució o modificació del sistema d'informació dona lloc a una re-estimació dels riscos i procediments (explotació i seguretat) posats en marxa?

Anton Goma 14:49 16-03-2010

- [x] Cap de les opcions següents.
- [ ] L'avaluació del impacte potencial de les modificacions està en principi realitzada, però els procediments no són sistemàticament actualitzats.
- [ ] Es realitza un anàlisi de riscos sistemàtic sobre les operacions crítiques modificades, però no es realitza una actualització dels procediments.
- [ ] Ídem anterior + es produeix actualització dels procediments.
- [ ] Es realitza un anàlisi de riscos previ a la modificació i es proposa un procediment d'aprovació oficial de les modificacions. Els detalls de les modificacions són comunicats a les persones implicades i controls regulars permeten assegurar la correcta implantació de les modificacions .

Afegir doc.
Esborrar Resposta

6.3 Planificació i acceptació del sistema

Objectiu: Minimitzar el risc d'errades del sistema.

És necessària una planificació i preparació per tal d'assegurar la disponibilitat de capacitat i de recursos adequats per els requeriments de rendiment demanats.

S'han de realitzar projeccions de requeriments futurs de capacitat, per tal de reduir el risc de sobrecàrrega del sistema.

S'ha d'establir, documentar i verificar, abans de la seva acceptació, els requeriments operacionals dels sistemes nous.

6.3.1 Dimensionament

6.3.1.1 Es procedeix a estudis de dimensionament dels sistemes i estudis de càrrega provisional amb el propòsit d'assegurar la disponibilitat dels sistemes informàtics en cas de càrrega màxima de les transaccions?

Anton Goma 14:49 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Estudis de dimensionament es realitzen puntualment.
- [ ] Estudis de dimensionament es realitzen sobre els sistemes crítics.
- [x] Els estudis de dimensionament es realitzen sobre tots els sistemes i per cada nou projecte.
- [ ] Ídem anterior + periòdicament a cada augment de volum de les transaccions.

Afegir doc.
Esborrar Resposta

6.3.2 Modificacions del sistema

6.3.2.1 Abans de la posada en producció de cada nova versió, actualització o nou sistema es procedeix a efectuar les proves predefinides durant el desenvolupament per tal d'assegurar la correcta implantació i continuïtat del sistema? Anton Goma 14:50 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Puntualment.
- [x] Per les aplicacions sensibles únicament.
- [ ] Sistemàticament sobre la base de criteris predefinits i de proves realitzades durant el desenvolupament.
- [ ] Sistemàticament i la implantació del nou desenvolupament o actualització reprèn punt per punt els elements definits.

Afegir doc.
Esborrar Resposta

6.3.2.2 En la fase de posada en producció, s'assegura que els equips i sistemes estan actualitzats a nivell de seguretat? Anton Goma 14:53 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Certs equips i sistemes estan actualitzats amb els patch's de seguretat durant la posada en producció.
- [ ] Només els equips i sistemes crítics són sistemàticament actualitzats amb els patch's de seguretat durant la posada en producció.
- [x] Un procediment estipula que els equips i sistemes posats en producció han d'estar actualitzat a nivell de patch's de seguretat.
- [ ] Ídem anterior + existeix un control regular.

Afegir doc.
Esborrar Resposta

6.4 Protecció contra els codis perjudicials o no desitjats

Objectiu: Protegir la integritat de les aplicacions i de la informació.

És necessari prendre precaucions per tal de detectar i evitar la introducció de codis maliciosos, no autoritzats o no desitjats.

Les aplicacions i recursos que composen els sistemes d'informació, son vulnerables a la introducció de software maliciós com virus informàtics. Els usuaris han de conèixer els perills del software maliciós i els administradors de xarxa, han d'introduir controls i mesures específiques per tal de prevenir, detectar i eliminar els virus informàtics.

6.4.1 Mesures contra els codis perjudicials

6.4.1.1 Està instal•lat l'antivirus gestionat per el Servei Informàtic de la UAB en tots els terminals (PC's) de treball i sobre els servidors Windows? Anton Goma 14:53 16-03-2010

- [ ] No.
- [ ] La instal•lació està planificada.
- [ ] La instal•lació està en curs.
- [x] Sí, està instal•lat sobre el conjunt de terminals i servidors Windows.
- [ ] Ídem anterior + i es subministra un informe regular indicant els terminals i servidors no protegits.

Afegir doc.
Esborrar Resposta

6.4.1.2 Utilitzeu el servei de missatgeria corporatiu? Anton Goma 14:53 16-03-2010

- [ ] No.
- [ ] No, i la passarel•la SMTP Internet utilitzada, no respecta les regles Antivirus i de filtratge de fitxers adjunts.
- [ ] No, però la passarel•la SMTP utilitzada respecta les regles antivirus i el filtratge de fitxers adjunts sospitosos.
- [x] Sí, totes les comptes d'usuaris mail són gestionades per el servei Servei Informàtic de la UAB i es beneficien de les proteccions antivirus i filtratge de fitxers adjunts sospitosos.
- [ ] Ídem anterior + es recorda als usuaris dels riscos per la seguretat en la utilització de serveis de missatgeria privats (tipus hotmail, gmail, yahoo) des de qualsevol PC de xarxa del SAF.

Afegir doc.
Esborrar Resposta

6.4.1.3 Existeix un procediment en cas d'alerta per atac virus o per vulnerabilitats crítiques i l'aplicació dels correctius de seguretat sobre la totalitat del parc informàtic té lloc en els terminis indicats en el procediment? Anton Goma 14:57 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] L'aplicació dels correctius de seguretat tenen lloc sobre la totalitat del parc informàtic, però sense objectiu de terminis.
- [ ] L'aplicació dels correctius de seguretat té lloc sobre la part crítica del parc informàtic en el termini indicat en el procediment.
- [ ] L'aplicació dels correctius de seguretat té lloc sobre la totalitat del parc informàtic en un termini de dos setmanes després de la publicació de l'alerta. Les excepcions són identificades i un pla d'acció s'estableix per posar en conformitat el parc crític.
- [x] L'aplicació dels correctius de seguretat té lloc sobre la totalitat del parc informàtic en el termini indicat en el procediment i després d'haver realitzat les proves pertinents sobre un perímetre representatiu.

Afegir doc.
Esborrar Resposta

6.4.1.4 Quins són els mitjans emprats per implantar les actualitzacions de seguretat (actualitzacions automàtiques) en els terminals de sobre taula i en els portàtils? Anton Goma 14:58 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Procediment manual.
- [x] Utilització de Windows Update.
- [ ] Utilització d'aplicació corporativa SMS o WSUS.
- [ ] Ídem anterior + procediments de verificació de implantació correcta de l'actualització.

Afegir doc.
Esborrar Resposta

6.5 Copies de seguretat

Objectiu: Mantenir la integritat i la disponibilitat dels serveis de tractament de la informació i de les comunicacions.

S'ha d'establir una política de copies de seguretat i una estratègia, acceptada per els propietaris del sistema o la informació, que en funció de la seva sensibilitat, minimitzi la pèrdua de dades o discontinuïtat de servei.

És necessari establir procediments rutinaris per tal de verificar (provar) la consistència de les copies de seguretat.

6.5.1 Copies de seguretat de les informacions

6.5.1.1 Existeix un document que estableixi els principis generals de la política de copies de seguretat i aquest ha estat validat per els responsables o propietaris de les aplicacions i sistemes implicats? Anton Goma 14:58 16-03-2010

- [x] Cap de les opcions següents.
- [ ] Sí, els principis generals de les copies de seguretat està documentat.
- [ ] Ídem anterior + el document està validat per alguns dels responsables de les aplicacions i sistemes.
- [ ] Ídem anterior + validat per tots els responsables o propietaris de les aplicacions o sistemes implicats.
- [ ] Ídem anterior + aquesta política és revisada periòdicament.

Afegir doc.
Esborrar Resposta

6.5.1.2 El procediment de copies de seguretat està documentat? Anton Goma 14:58 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] No està formalitzat, però sobre les aplicacions i sistemes crítics es fa una copia de seguretat com a mimin totes les setmanes.
- [ ] Parcialment formalitzat, però sobre les aplicacions i sistemes crítics es fa una copia de seguretat amb una periodicitat definida per els responsables o propietaris dels sistemes.
- [ ] Sí, el procediment de copies de seguretat està formalitzat definint la periodicitat i el tipus de copies realitzades (incremental o completa). El procediment està validat per els responsables de les dades o sistemes.
- [x] Ídem anterior + Es realitzen periòdicament copies de seguretat completes que són emmagatzemades de forma segura a l'exterior del SAF. La durada i condicions de l'emmagatzematge són definides i validades per els responsables.

Afegir doc.
Esborrar Resposta

6.5.1.3 Els suports de les copies de seguretat estan emmagatzemats en sales tècniques específiques? Anton Goma 14:59 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Certs suports de copies de seguretat estan emmagatzemats en una sala tècnica informàtica.
- [ ] Certs suports de copies de seguretat estan emmagatzemats en una caixa de seguretat ignífuga.
- [ ] Els suports de copies de seguretat estan emmagatzemats en una sala de seguretat diferent a la sala informàtica o en una caixa de seguretat ignifuga.
- [x] Els suports de copies de seguretat estan emmagatzemats per un proveïdor de serveis a l'exterior de les instal•lacions del SAF.

Afegir doc.
Esborrar Resposta

6.5.1.4 Es controlen les condicions d'emmagatzematge dels suports de copies de seguretat subministrat per un proveïdor? Anton Goma 15:00 16-03-2010

- [x] Cap de les opcions següents.
- [ ] Les recomanacions són comunicades al proveïdor.
- [ ] Ídem anterior + les condicions de magatzematge dels suport sensibles són ocasionalment controlades.
- [ ] El SAF ha contractualment formalitzat les condicions de com han de ser emmagatzemats els suport de copies de seguretat amb dades o sistemes sensibles.
- [ ] Ídem anterior + les condicions són regularment controlades.

Afegir doc.
Esborrar Resposta

6.6 Gestió de la seguretat de les xarxes informàtiques

Objectiu: Assegurar la protecció de la informació en la xarxa i la protecció de les infraestructures de suport.

La gestió de la seguretat en la xarxa, la qual supera sovint els límits de l'organització, requereix una especial consideració en relació al flux de dades, les implicacions legals, la vigilància i la protecció.

Són necessaris controls addicionals per protegir la informació sensible que pot circular per les xarxes públiques de dades.

6.6.1 Mesures en relació a les xarxes

6.6.1.1 La implementació de les xarxes informàtiques locals són conformes als estàndards del SAF o els indicats per el Servei Informàtic de la UAB? Anton Goma 15:00 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Parcialment.
- [ ] La majoria.
- [x] La implementació de les xarxes locals (arquitectura, direccionament, routing, etc.) i la utilització dels serveis de xarxa estan conformes al estàndards definits pel SAF.
- [ ] Ídem anterior + la implementació de xarxes LAN és periòdicament verificada.

Afegir doc.
Esborrar Resposta

6.6.1.2 Quines són les proteccions implantades per les infraestructures Wi-Fi ofimàtiques que donen accés a la xarxa local? Anton Goma 15:00 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Proteccions que respecten parcialment els estàndards del SAF o els indicats per el Servei Informàtic de la UAB.
- [ ] Certes infraestructures respecten els estàndards.
- [x] Totes les infraestructures Wi-Fi ofimàtiques respecten els estàndards.
- [ ] Ídem anterior + controls regulars.

Afegir doc.
Esborrar Resposta

6.6.1.3 Quines són les proteccions implantades per les infraestructures Wi-Fi industrials que donen accés a la xarxa industrial? Anton Goma 15:01 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] SSID no difosos (broadcast desactivat).
- [ ] Ídem anterior + accés limitat a les adreces MAC autoritzades sobre tots els punts d'accés Wi-Fi.
- [x] Ídem anterior + existeix un filtratge entre els punts d'accés Wi-Fi i la xarxa local per tal de limitar la visibilitat únicament a les aplicacions industrials.
- [ ] Ídem anterior + controls regulars.

Afegir doc.
Esborrar Resposta

6.6.2 Seguretat dels serveis de xarxa

6.6.2.1 Tot nou equip de xarxa (switch, punt d'accés wi-fi, router, etc.) s'instal•la sota control del responsable de la xarxa local del SAF?

Anton Goma 15:02 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Tot nou equip és controlat per el responsable de la xarxa local.
- [ ] Ídem anterior + pels equips considerats sensibles (connexió Internet, firewall, wi-fi, etc.) el responsable de la xarxa controla i supervisa la instal•lació dels mateixos.
- [x] Ídem anterior + a tots els equips se'ls supervisa i controla la instal•lació.
- [ ] Ídem anterior + un informe sobre la instal•lació és confeccionat i registrat en un diari de manteniment.

Afegir doc.
Esborrar Resposta

6.7 Manipulació dels mitjans de tractament informàtic

Objectiu: Prevenir l'accés no autoritzat, modificacions, danys o destrucció dels actius, i la interrupció de les activitats de negoci.

Els mitjans de tractament de dades han de ser controlats i protegits físicament.

S'han d'establir procediments operatius per protegir els documents, mitjans informàtics (Cd's, Dvd's, suports magnètics, etc.), dades i documentació de sistema de possibles accessos no autoritzats, modificacions, robatori i destrucció.

6.7.1 Gestió dels suports mòbils

6.7.1.1 Existeix i s'aplica un procediment per la gestió de la seguretat dels suports mòbils (disc dur extern) utilitzats en l'explotació informàtica?

Anton Goma 15:05 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Cap procediment està formalitzat, però es segueixen algunes pràctiques i normes, per exemple, tots els suports sensibles estan emmagatzemats en un sala de seguretat.
- [ ] Ídem anterior + hi ha una llista de suports sensibles i un procediment per la seva gestió.
- [ ] Ídem anterior + El procediment és permanentment actualitzat i preveu principalment el transport dels suport, les condicions d'emmagatzematge i la posada fora de servei o rebuig dels mateixos. Un inventari és mantingut actualitzat permanentment.
- [ ] Ídem anterior + controls regulars.

Afegir doc.
Esborrar Resposta

6.7.2 Rebuig de suports

6.7.2.1 S'apliquen mesures de seguretat lligades al emmagatzematge i al rebuig dels materials i suports crítics que no són més utilitzats?

Anton Goma 15:05 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] L'emmagatzematge i destrucció dels materials i suports crítics són gestionades per un proveïdor de serveis que s'encarrega d'esborrar el contingut.
- [x] Un procediment de magatzematge i de destrucció dels materials i suports crítics està formalitzat i parcialment aplicat.
- [ ] Els suports crítics són emmagatzemats en caixes de seguretat i posats en rebuig per part del SAF qui s'assegura del esborrat definitiu de les dades i la destrucció del suport.
- [ ] Ídem anterior + aplicada a tots els suports siguin crítics o no.

Afegir doc.
Esborrar Resposta

6.7.3 Procediments de manipulació de les informacions

6.7.3.1 Existeix un procediment per la correcta manipulació i emmagatzematge de la informació per tal de protegir la informació de divulgacions o usos no autoritzats? (veure 6.7.1)

Anton Goma 15:06 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Cap procediment està formalitzat, però es segueixen algunes pràctiques i normes, per exemple, tots els suports sensibles estan emmagatzemats en un sala de seguretat.
- [ ] Ídem anterior + hi ha una llista de suports sensibles i un procediment per la seva gestió.
- [ ] Ídem anterior + El procediment és permanentment actualitzat i preveu principalment el transport dels suport, les condicions d'emmagatzematge i la posada fora de servei o rebuig dels mateixos. Un inventari és mantingut actualitzat permanentment.
- [ ] Ídem anterior + controls regulars.

Afegir doc.
Esborrar Resposta

6.7.4 Seguretat de la documentació de sistema

6.7.4.1 L'accés a la documentació i a les aplicacions de sistemes crítics està restringit només a les persones que en necessiten l'accés per l'exercici de les seves funcions? Anton Goma 15:07 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] La documentació dels sistemes no es considera crítica i l'accés, per tant, no està restringit.
- [x] L'accés a la documentació i a les aplicacions de sistema crítics estan restringides a la informàtica i a certs usuaris amb privilegis d'accés suplementaris.
- [ ] Sí, l'accés a la documentació i les aplicacions crítiques està restringit només al personal informàtic administrador i aquests accessos estan enregistrats.
- [ ] Ídem anterior + controls regulars.

Afegir doc.
Esborrar Resposta

6.8 Intercanvi d'informacions

Objectiu: Evitar la pèrdua, modificació o mal ús de la informació intercanviada entre organitzacions.

S'ha de realitzar els intercanvis sobre la base d'acords formals.

S'ha de controlar que els intercanvis d'informació i software entre organitzacions compleixen els acords, i aquest han de ser compatibles amb la legislació vigent (veure capítol 11).

S'han d'establir procediments i normes per protegir la informació i els suports físics que continguin informació en trànsit.

6.8.1 Política i procediments d'intercanvi de les informacions

6.8.1.1 Disposeu d'una política que formalitzi les regles de seguretat lligades als intercanvis d'informacions electròniques? Anton Goma 15:09 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] No formalment. Recomanacions són regularment enviades per mail.
- [ ] Existeixen bones pràctiques però no estan formalitzades.
- [x] S'ha definit un estàndard i les regles de seguretat estan definides i formalitzades.
- [ ] Una nota ha estat redirigida a l'atenció dels usuaris amb les normes i regles lligades a l'intercanvi d'informacions electròniques. Es realitzen controls i actualitzacions periòdicament.

A nivell UAB

Afegir doc.
Esborrar Resposta

6.8.2 Acords d'intercanvi d'informacions

6.8.2.1 Heu formalitzat les condicions d'intercanvi d'informacions confidencials amb els proveïdors o col•laboradors i les regles a respectar (xifratge)? Anton Goma 15:09 16-03-2010

- [x] Cap de les opcions següents.
- [ ] Existeixen regles tàcites sobre les modalitats d'intercanvi d'informacions confidencials amb les diferents parts.
- [ ] Les modalitats d'intercanvi d'informacions confidencials i les regles a respectar estan formalitzades cas per cas en els contractes.
- [ ] Existeix una política interna en el SAF i en els contractes amb tercers es respecten com a mínim aquesta política.
- [ ] Eines específiques s'utilitzen per l'intercanvi d'informacions confidencials.

Afegir doc.
Esborrar Resposta

6.8.3 Suports físics en transit

6.8.3.1 El suports que contenen informació estan protegits contra els accessos no autoritzats, mal ús o corrupció durant el transport fora de les instal•lacions del servei? Anton Goma 15:10 16-03-2010

- [x] Cap de les opcions següents.
- [ ] Cap procediment està formalitzat, però es fa una advertència al portador per tal que el mitjà sigui transportat amb seguretat.
- [ ] Hi ha una llista de suports sensibles i un procediment per la seva gestió en el transport al exterior.
- [ ] Ídem anterior + El procediment és permanentment actualitzat i preveu principalment el transport dels suports.
- [ ] Ídem anterior + controls regulars.

Afegir doc.
Esborrar Resposta

6.8.4 Missatgeria electrònica

6.8.4.1 Els usuaris són coneixedors dels riscos lligats a un mal ús de la missatgeria? ➡ Anton Goma 15:10 16-03-2010

- ☐ Cap de les opcions següents.
- ☐ La seguretat està assegurada en el nivell de configuració de la missatgeria.
- ☑ Es deixa a criteri de l'usuari.
- ☐ Els usuaris són coneixedors dels riscos lligats a mal ús de la missatgeria.
- ☐ Ídem anterior + els usuaris assisteixen a sessions de formació sobre les bones pràctiques i regles d'utilització de la missatgeria.

Afegir doc.
☐ Esborrar Resposta

6.8.5 Sistema d'informació d'empresa

6.8.5.1 S'han implantat procediments per tal de protegir la informació associada amb la interconnexió dels sistemes d'empresa (per exemple, informacions compartides entre departaments d'administració o comptabilitat)? ➡ Anton Goma 15:15 16-03-2010

- ☑ Cap de les opcions següents.
- ☐ Les informacions compartides per les diferents parts de l'organització NO han estat identificades.
- ☐ Les informacions compartides per les diferents parts de l'organització han estat identificades.
- ☐ Ídem anterior + un procediment ha estat implantat per el correcte tractament de les dades compartides.
- ☐ Ídem anterior + controls regulars.

Afegir doc.
☐ Esborrar Resposta

6.9 Serveis de comerç electrònic

Objectiu: Assegurar la seguretat en els serveis de comerç electrònic.

S'han de considerar les implicacions de seguretat associades amb l'ús de serveis de comerç electrònic, incloses transaccions en línia, i els controls necessaris. S'ha de tenir en compte, la integritat i disponibilitat de la informació publicada electrònicament a través dels mitjans de publicitat.

6.9.1 Comerç electrònic

6.9.1.1 La informació en relació al comerç electrònic que circula per la xarxa pública està protegida contra l'activitat fraudulenta, disputes contractuals i accessos o modificacions no autoritzades? ➡ Anton Goma 15:15 16-03-2010

- ☐ Cap de les opcions següents.
- ☑ A criteri del proveïdor del servei.
- ☐ Es verifica la confidencialitat i integritat de tota transacció, informació de pagament, detalls d'adreces d'entrega i confirmacions de rebut.
- ☐ Es segueix un procediment detallat per tal d'assegurar la protecció les dades de comerç electrònic, seguint les recomanacions de l'estàndard corresponent i la legislació vigent.
- ☐ Ídem anterior + Auditories regulars.

Afegir doc.
☐ Esborrar Resposta

6.9.2 Transaccions en línia

6.9.2.1 La informació implicada en les transaccions en línia està protegida per prevenir la transmissió incomplerta, ruta equivocada, alteració, accés, duplicat o reproducció no autoritzat del missatge? ➡ Anton Goma 15:18 16-03-2010

- ☐ Cap de les opcions següents.
- ☑ Les credencials d'usuari són validades i verificades. Es manté la confidencialitat de la transacció i la privacitat associada a cada una de les parts que intervenen.
- ☐ S'assegura que els detalls de la transacció estan emmagatzemats fora de la zona pública, per exemple en una zona DMZ INTRANET, no sent cap mitjà d'emmagatzematge accessible des de INTERNET.
- ☐ Ídem anterior + S'utilitzen signatures electròniques per cada una de les parts.
- ☐ Ídem anterior + el mitjans de comunicació entre les dues parts està xifrat i els protocols de comunicació són segurs (https, sfttp). Existeixen procediments de verificació i revisió.

Afegir doc.
☐ Esborrar Resposta

6.9.3 Informacions fetes públiques

6.9.3.1 La integritat de la informació, habilitada a través d'un sistema públic, ha estat protegida per prevenir les modificacions no autoritzades? Anton Goma 15:19 16-03-2010

- [ ] Cap de les opcions següents
- [x] Les credencials d'accés als sistema públic que permeten habilitar o modificar la informació (com per exemple, noticies o publicitat en un servidor Web) són validades i verificades.
- [ ] Les aplicacions, dades i tota informació que requereixi un alt nivell d'integritat, i que són accessibles des d'un mitjà públic, estan protegits per mecanismes de signatura digital.
- [ ] Ídem anterior + El sistema d'accés públic ha de ser provat i validat contra febleses o errades abans d' habilitar dita aplicació o informació.
- [ ] Ídem anterior + procediments de verificació i revisió periòdics.

Afegir doc.
Esborrar Resposta

6.10 Vigilància

Objectiu: Detectar les activitats de processament de la informació no autoritzades.

Els sistemes han de ser vigilats i els esdeveniments de seguretat han de ser enregistrats. El registre de les operacions i el registre d'errors ha de ser utilitzat per identificar i prevenir problemes en els sistema d'informació.

El servei ha de complir amb tots els requeriments legals aplicables en la vigilància i registre de les activitats.

La vigilància del sistema ha de ser utilitzada per verificar l'efectivitat dels controls adoptats i per verificar la conformitat del model de política d'accessos.

6.10.1 Informe d'auditoria

6.10.1.1 Existeix un procediment que defineixi la configuració dels informes d'auditoria que enregistren l'activitat dels usuaris, excepcions i esdeveniments de seguretat? Anton Goma 15:19 16-03-2010

- [x] Cap de les opcions següents.
- [ ] Es manté la configuració per defecte dels informes d'auditoria en els sistema i aquest són utilitzats ocasionalment.
- [ ] Es verifica periòdicament els accessos i les excepcions registrades.
- [ ] Implantat un procediment que estableix com han de ser produïts i guardats els informes d'auditoria per un període acordat amb la finalitat que serveixin per el control regular dels accessos, les excepcions de seguretat, així com , per assistir a futures investigacions.
- [ ] Ídem anterior + actualització i verificació del procediment regularment.

Afegir doc.
Esborrar Resposta

6.10.2 Vigilància de la utilització dels sistemes d'informació

6.10.2.1 Apliqueu procediments de vigilància de l'ús de sistemes informàtics crítics? Anton Goma 15:19 16-03-2010

- [x] Cap de les opcions següents.
- [ ] La vigilància s'efectua cas per cas durant esdeveniments específics i els dietaris de registres s'activen únicament a petició.
- [ ] Els dietaris de registres són sistemàticament activats per enregistrar les informacions de base: tentatives d'accés infructuoses, utilització d'operacions privilegiades, tentatives d'us abusives de privilegis. No obstant, aquest dietaris només són consultats en cas d'incident.
- [ ] Ídem anterior + els dietaris són consultats regularment.
- [ ] Ídem anterior + existeix un procediment que precisa quins registres s'han de vigilar i sobre quins sistemes s'ha d'aplicar .

Afegir doc.
Esborrar Resposta

6.10.3 Protecció de les informacions registrades

6.10.3.1 S'ha protegit l'accés a les informacions de registre contra possibles accessos o modificacions no autoritzats? Anton Goma 15:20 16-03-2010

- [x] Cap de les opcions següents.
- [ ] No, però només tenen accés els Administradors de sistemes.
- [ ] Només tenen accés els Administradors de sistemes i les alteracions en l'eliminació o edició dels missatges de registre són enregistrades.
- [ ] Ídem anterior + el fet de superar-se la capacitat d'emmagatzematge dels fitxers de registre no implica que els nous esdeveniments deixin de ser enregistrats o sobreescriguin els anteriors.
- [ ] Ídem anterior + procediments de verificació periòdics per revisar les proteccions i emmagatzemar de forma segura els fitxers de registre.

Afegir doc.
Esborrar Resposta

6.10.4 Registre d'administració i registre de les operacions

6.10.4.1 S'enregistren les activitats administratives del sistema i dels operaris privilegiats per els sistemes crítics del SAF?

Anton Goma 15:21 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Només a certes activitats se'ls registra l'inici de sessió: l'hora de la tentativa de connexió, la compte d'usuari implicada, els resultats de la tentativa, el procediment sol•licitat, etc..
- [ ] Ídem anterior + s'enregistren les adreces IP.
- [ ] Totes les activitats de l'administrador i dels operadors privilegiats són enregistrades sobre tots els sistemes sensibles.
- [ ] Ídem anterior + controls regulars.

Afegir doc.
Esborrar Resposta

6.10.5 Enregistrament dels errors

6.10.5.1 El registre d'errors és analitzat i es prenen accions correctives en conseqüència?

Anton Goma 15:22 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Algunes aplicacions o sistemes tenen habilitats els informes d'errors. Aquest es revisen ocasionalment.
- [x] Tots els sistemes crítics o sensibles tenen habilitat els informes d'errors (sistema, seguretat, aplicació). Els informes són revisats puntualment en produir-se una errada de sistema.
- [ ] Ídem anterior + els informes són revisats periòdicament.
- [ ] Ídem anterior + procediments implantats per tal de verificar que tots els errors enregistrats han estat satisfactòriament resolts i per assegurar que les mesures correctives han estat autoritzades i aquestes no han compromès cap control.

Afegir doc.
Esborrar Resposta

6.10.6 Sincronització horària

6.10.6.1 Els rellotges dels sistemes de processament de la informació dins del domini del servei han estat sincronitzats amb una font acordada i exacta de temps?

Anton Goma 15:22 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Alguns sistemes.
- [x] Tots els sistemes sensibles que requereixen enregistrar operacions en temps real han estat sincronitzats amb una font estàndard UTC (Coordinated Universal Time) de domini o local.
- [ ] Ídem anterior + procediments per detectar i corregir variacions significants.

Afegir doc.
Esborrar Resposta

7 Control d'accessos

7.1 Necessitats de negoci en matèria de control d'accessos

Objectiu: Controlar els accessos a la informació.

S'han de controlar les accessos a la informació i els processos de negoci sobre la base dels requeriments de seguretat i de negoci.

S'han de tenir en compte les polítiques de distribució de la informació i de les autoritzacions.

7.1.1 Política de control d'accessos

7.1.1.1 Quina és la política d'accés als sistemes i aplicacions crítiques? ➡ Anton Goma 15:29 16-03-2010

- ☐ Cap de les opcions següents.
- ☑ Els drets d'accés són atribuïts seguint la petició del responsable jeràrquic.
- ☐ Els drets d'accés són atribuïts seguint una política formal i són revisats ocasionalment.
- ☐ Els drets d'accés són atribuïts seguint una política formal i són revisats regularment.
- ☐ Ídem anterior + els drets d'accés sobre el sistemes crítics són contínuament vigilats amb l'ajuda d'eines administratives.

Afegir doc.
☐ Esborrar Resposta

7.2 Gestió dels accessos usuaris

Objectiu: Assegurar l'accés autoritzat de l'usuari i prevenir els accessos no autoritzats als sistemes d'informació.

S'han d'establir procediments formals per controlar l'assignació dels drets d'accessos als sistemes i serveis.

Els procediments han de cobrir totes les etapes del cicle de vida de l'accés de l'usuari, des del registre inicial del nou usuari fins a la baixa del registre.

Evitar l'assignació de drets d'accés privilegiats que permetin evitar els controls de sistemes.

7.2.1 Enregistrament dels usuaris

7.2.1.1 Existeix un procediment de creació de comptes d'usuari? ➡ Anton Goma 15:29 16-03-2010

- ☐ Cap de les opcions següents.
- ☐ Els drets d'accés són demanats per l'usuari implicat i atribuïts per defecte en el moment de la seva arrivada en el SAF.
- ☐ El compte usuari és demanat per escrit par part del responsable jeràrquic o propietari de l'aplicació.
- ☐ Ídem anterior + en coordinació amb el responsable RH.
- ☑ Ídem anterior + verificació de les incompatibilitats potencials amb els drets d'accés concedits anteriorment (en el cas d'evolució).

Afegir doc.
☐ Esborrar Resposta

7.2.2 Gestió dels privilegis

7.2.2.1 L'atribució de privilegis està restringida i controlada? ➡ Anton Goma 15:30 16-03-2010

- ☐ Cap de les opcions següents.
- ☐ L'atribució de privilegis es fa de forma informal en funció de les necessitats dels usuaris.
- ☑ L'atribució de privilegis es fa de forma informal en funció de les funcions i responsabilitats dels usuaris.
- ☐ L'atribució de privilegis està formalitzada i validada. En un document es detallen el privilegis i les regles d'us adaptades a les responsabilitats del usuaris.
- ☐ Ídem anterior + revisió regular.

Afegir doc.
☐ Esborrar Resposta

7.2.3 Gestió del les claus d'accés d'usuaris

7.2.3.1 Les passwords inicials (usuari) o per defecte (sistema) subministrades són sistemàticament canviades el seu valor per defecte? ➡ Anton Goma 15:34 16-03-2010

- ☐ Cap de les opcions següents.
- ☐ Normalment.
- ☐ El responsable informàtic del SAF demana als nous usuaris canviar la password subministrada inicialment.
- ☑ Totes les passwords (usuaris, sistemes, serveis, aplicacions, equips de xarxa, etc.) són sistemàticament canviades del seu valor per defecte o inicial.
- ☐ Ídem anterior + les corresponents als comptes d'administrador són regularment auditades.

Afegir doc.
☐ Esborrar Resposta

7.2.4 Revisió dels drets d'accés usuaris

7.2.4.1 Heu posat en marxa un procediment de requalificació dels drets d'accés en el moment que un empleat o col•laborador canvia de funció o responsabilitat? ➡ Anton Goma 15:34 16-03-2010

- [ ] Cap de les opcions següents.
- [x] La persona indica, al responsable de la gestió de comptes, el seu canvi de funció.
- [ ] El responsable jeràrquic indica, al responsable de la gestió de comptes, el canvi de funció d'un usuari.
- [ ] Existeix un procediment conjunt amb la gestió de personal i els responsables de departament.
- [ ] Ídem anterior + controls regulars dels drets d'accés concedits.

Afegir doc.
Esborrar Resposta

7.2.4.2 Tot fi de contracte d'un usuari es comunica als responsables de la gestió de comptes usuari per tal de que el compte sigui desactivat immediatament? ➡ Anton Goma 15:35 16-03-2010

- [ ] Cap de les opcions següents.
- [x] De manera informal.
- [ ] El responsable jeràrquic o el responsable de personal, de manera informal.
- [ ] Ídem anterior + procediment formalitzat.
- [ ] Ídem anterior + reconciliació periòdica entre els comptes d'usuaris existents i la llista de personal.

Afegir doc.
Esborrar Resposta

7.2.4.3 Es fa una revisió del comptes inactius bloquejant-los quan l'inactivitat sigui superior a dos mesos? ➡ Anton Goma 15:36 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Sí, ocasionalment. Les comptes no es bloquegen.
- [ ] Sí, ocasionalment. Les comptes es bloquegen i s'informa als responsables jeràrquics de l'usuari.
- [ ] Sí, periòdicament. Les comptes es bloquegen i s'informa als responsables jeràrquics de l'usuari.
- [ ] Ídem anterior + seguint un procediment.

Afegir doc.
Esborrar Resposta

7.3 Responsabilitats dels usuaris

Objectiu: Evitar l'accés a usuaris no autoritzats i no comprometre la integritat de la informació ni de les instal•lacions dels sistemes d'informació.

Per una protecció eficaç, és necessària la cooperació dels usuaris autoritzats.

Els usuaris han de ser conscients de les seves responsabilitats en mantenir l'efectivitat del control d'accessos, particularment pel que fa a l'ús de claus d'accés i a la seguretat del material posat a la seva disposició.

Una política d'escriptori net ha de ser implantada per tal de reduir el risc d'accessos no autoritzats, danys a informacions, suports digitals o les instal•lacions dels sistemes d'informació.

7.3.1 Utilització de la clau d'accés

7.3.1.1 Com es sensibilitza als usuaris a escollir un password adequat? ➡ Anton Goma 15:37 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Alguns usuaris han estat formats.
- [x] S'ha fet una formació al conjunt dels usuaris però aquesta no ha estat renovada o actualitzada.
- [ ] Formació anual per el conjunt dels usuaris per recordar les bones pràctiques a l'hora de construir un password segur.
- [ ] Ídem anterior + els sistemes sensibles disposen de mecanismes per detectar constitucions de passwords no segures.

Afegir doc.
Esborrar Resposta

7.3.1.2 Durant l'inici de sessió, els sistemes sensibles disposen de mecanismes per detectar passwords de menys de sis caràcters, de bloquejar l'usuari després del cinquè intent, de guardar un històric de 10 passwords, de demanar la renovació després dels dos mesos d'antiguitat del password? ➡ Anton Goma 15:43 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Només dos d'aquest criteris s'aplica a les comptes usuaris i administratives.
- [ ] Tres criteris.
- [x] Els quatre criteris.

Són 6 mesos en lloc de 2.

Afegir doc.
Esborrar Resposta

7.3.2 Material dels usuaris deixat sense vigilància

7.3.2.1 Es usuaris bloquegen la sessió en el moment que deixen sol el seu PC i els usuaris amb portàtil l'asseguren a més a més amb un cable antirobatori o el guarden sota clau?

Anton Goma 15:43 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Alguns usuaris.
- [ ] Es realitzen formacions de sensibilització.
- [ ] Ídem anterior + es verifica periòdicament el compliment de les bones pràctiques.
- [ ] Ídem anterior + els sistemes sensibles se'n assegura el compliment. Les sessions es bloquegen automàticament per inactivitat i tots els equips estan en sales de seguretat.

Afegir doc.
Esborrar Resposta

7.3.3 Política d'oficina neta i escriptori buit

7.3.3.1 Les estacions de treball es bloquegen automàticament després d'un període d'inactivitat determinat?

Anton Goma 13:28 27-04-2010

- [x] Cap de les opcions següents.
- [ ] Bloqueig manual per part del usuaris.
- [ ] La majoria d'estacions automàticament.
- [ ] Totes les estacions automàticament.
- [ ] Ídem anterior + controls regulars.

No es bloqueja actualment de cap forma. No hi ha costum de fer bloqueig manual.

Afegir doc.
Esborrar Resposta

7.4 Control d'accés a la xarxa

Objectiu: Evitar els accessos no autoritzats als serveis de xarxa.

Els accessos a les xarxes de dades, tant internes com externes, han de ser controlats.

L'accés d'usuari a les xarxes, no ha de comprometre la seguretat dels serveis de xarxa, utilitzant:

a)Apropiades interfases entre les xarxes de l'organització, les públiques i les privades.

b)Mecanismes d'autentificació per usuaris i equips.

c)Control d'accessos dels usuaris als sistemes d'informació.

7.4.1 Política d'utilització dels serveis de xarxa

7.4.1.1 Existeix un procediment de validació de tota nova petició d'accés distant a la xarxa del SAF per part d'un tercer?

Anton Goma 15:53 16-03-2010

- [ ] No.
- [x] El responsable informàtic o seguretat S.I. concedeix i valida les connexions distants.
- [ ] Ídem anterior + es signa el pertinent acord de confidencialitat i es segueix un check-list per tal de verificar l'adequació de la seguretat dels equips propietat del tercer.
- [ ] Ídem anterior + les connexions transiten per les infraestructures gestionades per el SAF o Servei Informàtic de la UAB i disposen d'una connexió VPN segura.
- [ ] Ídem anterior + revisió regular de les connexions distants habilitades a tercers.

S'autoritzen mitjançant l'obertura específica de ports del router corporatiu UAB a les IPs autoritzades.

Afegir doc.
Esborrar Resposta

7.4.2 Autentificació de l'usuari per les connexions externes

7.4.2.1 Utilitzeu un mecanisme d'autentificació per les connexions distants tipus RAS habilitades per usuaris del SAF?

Anton Goma 15:54 16-03-2010

- [ ] No.
- [x] Sí, mecanisme simple d'usuari i password.
- [ ] Sí, autentificació forta (per exemple Token RSA) per una part de les connexions.
- [ ] Ídem anterior + per totes les connexions.
- [ ] Ídem anterior + controls regulars de l'activitat de les connexions.

Les connexions distants es fan per VPN

Afegir doc.
Esborrar Resposta

7.4.2.2 Utilitzeu un mecanisme d'autentificació per les connexions distants tipus RAS habilitades a proveïdors o col•laboradors externs? Anton Goma 15:54 16-03-2010

- [ ] No.
- [x] Sí, mecanisme simple d'usuari i password.
- [ ] Sí, autentificació forta (per exemple Token RSA) per una part de les connexions.
- [ ] Ídem anterior + per totes les connexions.
- [ ] Ídem anterior + controls regulars de l'activitat de les connexions.

Afegir doc.
Esborrar Resposta

7.4.3 Identificació dels equips de xarxa

7.4.3.1 S'utilitzen mecanismes d'autentificació automàtics per tal de validar les connexions a la xarxa local per part d'equips o de sistemes localitzats específicament? Anton Goma 15:56 16-03-2010

- [x] No.
- [ ] Alguns sistemes disposen de validació automàtica de les connexions quan és necessari permetre la connexió només a equips o localitzacions específiques.
- [ ] Ídem anterior + En tots els sistemes sensibles.
- [ ] Ídem anterior + mitjançant protecció física (router o firewall).
- [ ] Ídem anterior + procediments de verificació i revisió periòdics.

No pels equips de dins la UAB, sí pels equips de fora.

Afegir doc.
Esborrar Resposta

7.4.4 Protecció dels ports de diagnòstic i de configuració a distància

7.4.4.1 L'accés als utilitaris de vigilància i gestió dels firewals, està restringit només als administradors autoritzats? Anton Goma 15:56 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Els tècnics informàtics tenen privilegis de modificar les regles firewall.
- [ ] Només les persones encarregades de la gestió del firewal estan autoritzades.
- [x] Ídem anterior + es verifiquen les adreces IP de les estacions que es connecten al firewall en mode administratiu.
- [ ] Ídem anterior + verificació regular de les regles firewall.

Afegir doc.
Esborrar Resposta

7.4.5 Aïllament de les xarxes

7.4.5.1 Les connexions Internet són sistemàticament assegurades per un equip Firewall i un servidor Proxy? Anton Goma 15:56 16-03-2010

- [ ] No.
- [ ] Només per un firewall.
- [ ] Sí.
- [x] Sí. Aquests equips estan d'acord a les normes relatives indicades per el Servei Informàtic de la UAB.
- [ ] Ídem anterior + un procediment permet controlar i detectar tota connexió Internet diferent a la habilitada.

Afegir doc.
Esborrar Resposta

7.4.5.2 Tot servidor visible des de Internet està situat en una DMZ INTERNET protegida per un Firewall i IDS (Internet Detection System)? Anton Goma 16:01 16-03-2010

- [ ] No. Estan situats en la zona INTRANET sense filtre.
- [ ] Estan situats en la zona INTERNET però sense mecanisme de filtratge.
- [x] Estan situats en la zona INTERNET amb mecanisme de filtratge Firewall.
- [ ] Ídem anterior + IDS.
- [ ] Ídem anterior + es fan regularment auditories de vulnerabilitats.

És possible que els equips en DMZ de la UAB també estiguin darrera un IDS, però no ho sabem ara per ara.

Afegir doc.
Esborrar Resposta

7.4.6 Control de les connexions de xarxa

7.4.6.1 Tota màquina que pertanyi a un tercer (proveïdor o col•laborador extern, consultor o visitant) i que es connecti a la xarxa local, satisfà, abans de la connexió, les regles de seguretat (normes antivirus principalment i actualitzacions de seguretat)?

Anton Goma 16:01 16-03-2010

- [x] No.
- [ ] Tota màquina disposa d'un antivirus actualitzat abans de la connexió.
- [ ] Ídem anterior + la majoria de les actualitzacions de seguretat estan aplicades.
- [ ] Ídem anterior + o bé totes les actualitzacions de seguretat són aplicades o bé no es permet la connexió a la xarxa local a la màquina que pertanyi a un tercer.
- [ ] Ídem anterior + es fan regularment controls físics i lògics.

Afegir doc.
Esborrar Resposta

7.4.6.2 Els usuaris coneixen els riscos de seguretat en relació a la connexió d'equips no professionals personals o que pertanyin a un tercer?

Anton Goma 16:04 16-03-2010

- [ ] No.
- [ ] Alguns usuaris.
- [x] Els responsables informàtics únicament .
- [ ] Ha estat difosa una nota de servei demanant a tots els empleats que prenguin contacte amb el responsable informàtic o de seguretat en cas de detectar una connexió física a la xarxa local per un equip que no pertanyi al SAF.
- [ ] Ídem anterior + es fan accions de recordatori periòdiques.

A la xarxa de cable només poden connectar-s'hi equips registrats.

Afegir doc.
Esborrar Resposta

7.4.6.3 Existeixen en la xarxa local equips que estiguin connectats al mateix temps a un terminal mòdem?

Anton Goma 16:05 16-03-2010

- [x] Sí.
- [ ] Sí, es verifica puntualment que la connexió modem només dóna accés punt a punt entre l'equip en qüestió i el terminal remot.
- [ ] Ídem anterior + es revisa periòdicament.
- [ ] No. Aquest tipus de connexions estan prohibides.
- [ ] Ídem anterior + verificacions periòdiques.

Seria possible que passés, però poc probable. Els equips personals haurien d'estar expressament preparats per a admetre les dues connexions simultàniament.

Afegir doc.
Esborrar Resposta

7.4.7 Control de redirecció de xarxa

7.4.7.1 S'han implantat controls d'enrutament garantint que les connexions entre servidors i els fluxos d'informació es produeixen segons la política de controls d'accessos de les aplicacions de negoci?

Anton Goma 16:23 16-03-2010

- [ ] No.
- [ ] Es verifica regularment les màquines i equips puntualment connectades als servidors de negoci.
- [ ] Per alguns sistemes sensibles, s'apliquen controls de routing que verifiquen i autoritzen les connexions per les adreces font i destí.
- [x] S'aplica controls de routing per tots els sistemes sensibles.
- [ ] Ídem anterior + procediments de revisió de les llistes de routatge per tal d'assegurar la concordança amb les especificacions de negoci i la política de seguretat.

Afegir doc.
Esborrar Resposta

7.5 Control d'accessos als sistemes d'explotació

Objectiu: Evitar accessos no autoritzats als sistemes d'explotació.

Utilitats de seguretats dels sistemes operatius han de ser utilitzades per tal de restringir l'accés als sistemes d'explotació als usuaris autoritzats. Aquestes utilitats han de:

a)Autentificar usuaris autoritzats en concordança amb la política definida de control d'accessos.

b)Enregistrar les temptatives d'accés produïdes amb èxit i les fallides.

c)Enregistrar l'ús de privilegis especials de sistema.

d)Indicar alarmes quan la política de seguretat de sistema hagi estat trencada.

e)Subministrar mecanismes adequats d'autentificació.

f)Quan sigui requerit, restringir els temps de connexió dels usuaris a franges horàries d'utilització definides.

7.5.1 Procediments segurs d'obertura de sessió

7.5.1.1 Com es gestiona l'inici de sessió a nivell dels sistemes d'explotació? Anton Goma 16:23 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Usuari local amb identificador i password.
- [ ] El identificadors estan gestionats per un controlador de domini propi del SAF.
- [ ] La gestió d'identificadors usuaris i inicis de sessió està centralitzada en l'Active Directory del Servei Informàtic de la UAB.
- [ ] Ídem anterior + el responsable informàtic del SAF disposa d'un accés al contenidor del AD per gestionar i verificar els identificadors que pertanyin al SAF.

Afegir doc.
Esborrar Resposta

7.5.2 Identificació i autentificació de l'usuari

7.5.2.1 Els usuaris disposen d'un identificador únic? Anton Goma 16:24 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Només per l'inici de sessió Windows.
- [ ] Ídem anterior + i en algunes aplicacions (mail).
- [x] Sí, per l'inici de sessió i per totes les aplicacions.
- [ ] Ídem anterior + existeix un procediment que precisa la obligatorietat d'utilitzar aquest tipus d'identificació per tota nova aplicació.

Afegir doc.
Esborrar Resposta

7.5.2.2 Existeixen en el SAF comptes d'usuari genèriques? Anton Goma 16:24 16-03-2010

- [ ] Sí, i no estan inventariades.
- [x] Sí, però estan identificades i inventariades.
- [ ] Ídem anterior + s'apliquen mesures de control.
- [ ] No. No es permeten aquest tipus de comptes. Tota compte pertany a un únic usuari el qual es fa responsable dels accessos produïts amb la mateixa.
- [ ] Ídem anterior + accions de control i verificacions automàtiques (control de múltiple inici de sessió).

Afegir doc.
Esborrar Resposta

7.5.3 Sistema de gestió de les claus d'accés

7.5.3.1 Els sistemes de gestió de passwords per els sistemes sensibles és interactiu i permet assegurar la qualitat de les mateixes? Anton Goma 16:24 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] El sistema imposa l'ús de contrasenyes individuals. No mostra la paraula clau durant la introducció.
- [ ] Ídem anterior + permet als usuaris escollir i/o canviar les seves contrasenyes a més d'incloure un procediment de confirmació per evitar errors en la creació.
- [x] Ídem anterior + el sistema imposa el canvi periòdic de la contrasenya, així com la modificació de la mateixa durant el primer inici de sessió, si aquesta ha estat proporcionada per l'administració del sistema. També manté el registre de les anteriors contrasenyes utilitzades, per exemple durant l'últim any, impedint la seva reutilització.
- [ ] Ídem anterior + el sistema imposa la creació de contrasenyes de qualitat (veure 7.3.1).

Afegir doc.
Esborrar Resposta

7.5.4 Accés a les aplicacions sistema

7.5.4.2 De quins privilegis disposen els usuaris en la seva estació de treball? Anton Goma 16:25 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] Tots els usuaris disposen de drets d'administració local.
- [ ] Alguns usuaris avançats disposen de drets d'administrador local.
- [x] Tots els usuaris disposen de drets d'utilització restringits. Alguns usuaris se'ls habilita privilegis avançats en el cas que siguin necessaris per la seva funció.
- [ ] Ídem anterior + aquest privilegis són concedits per un temps limitat i es realitzen accions de control regulars.

Afegir doc.
Esborrar Resposta

7.5.5 Desconnexió automàtica de les sessions inactives

7.5.5.1 Les sessions inactives són desactivades després d'un període de temps definit? Anton Goma 16:25 16-03-2010

- [ ] No.
- [ ] Les estacions de treball d'usuari bloquegen la sessió després d'un període determinat d'inactivitat.
- [ ] Alguns sistemes tanquen l'aplicació i les sessions de connexió a la xarxa després d'un període d'inactivitat.
- [x] Ídem anterior + Per tots els sistemes sensibles. El temps definit d'inactivitat es defineix segons els riscos de seguretat del sistema tractat, la informació que gestiona, les aplicacions, i els riscos relacionats amb els usuaris del sistema.
- [ ] Ídem anterior + procediments de verificació regulars.

Afegir doc.
Esborrar Resposta

7.5.6 Limitació dels horaris de connexió

7.5.6.1 Existeixen restriccions de connexió (franges horàries d'utilització o control de temps de connexió) per les aplicacions que impliquin un alt risc de seguretat ? Anton Goma 16:25 16-03-2010

- [x] No.
- [ ] Alguns sistemes sensibles tenen implantats mecanismes per restringir l'ús en l'horari normal d'oficina.
- [ ] Ídem anterior + tots els sistemes sensibles.
- [ ] Ídem anterior + Procediments per la revisió i replantejament dels requeriments.

Afegir doc.
Esborrar Resposta

7.6 Control d'accessos a les aplicacions i la informació

Objectiu: Evitar l'accés no autoritzat a les informacions i aplicacions de sistema.

7.6.1 Restriccions d'accés a les informacions

7.6.1.1 L'accés a la informació i a les funcions de sistema està restringit només als usuaris de l'aplicació i al personal d'administració o suport, seguint una política de seguretat de control d'accessos? Anton Goma 16:28 16-03-2010

- [ ] Cap de les opcions següents.
- [x] L'accés a la informació i a les funcions es realitza a través de menús que controlen l'accés.
- [ ] Ídem anterior + controlen també els drets d'accés, per exemple: la lectura, escriptura, esborrat o execució.
- [ ] Ídem anterior + procediments de verificació.

Afegir doc.
Esborrar Resposta

7.6.2 Aïllament dels sistemes sensibles

7.6.2.1 Els sistemes sensibles es troben en un entorn informàtic dedicat (aïllat)? Anton Goma 16:28 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Les aplicacions, sensibles o no, comparteixen el mateix entorn informàtic (sala tècnica, xarxa de dades, sistema de control d'accessos, servidor físic, etc.).
- [ ] Ídem anterior + Les aplicacions sensibles que comparteixen un mateix entorn i els riscos que aquest fet implica, han estat identificats i acceptats per el propietari de l'aplicació sensible (veure 3.1.2).
- [ ] Les sensibilitat d'una aplicació és explícitament identificada i documentada per part del propietari de l'aplicació (veure 3.1.2) i el seu entorn informàtic dedicat ha estat especificat conjuntament amb els responsables informàtics i de seguretat del servei.
- [ ] Ídem anterior + procediments de verificació.

Afegir doc.
Esborrar Resposta

7.7 Informàtica nòmada o teletreball

Objectiu: Garantir la seguretat de la informació quan s'utilitzin dispositius mòbils o teletreball.

La protecció requerida ha de ser proporcional al riscos que causen aquestes formes específiques de treball. S'han de considerar els riscos de treballar en un entorn desprotegit quan s'utilitza un dispositiu mòbil i aplicar una protecció adequada. En el cas de teletreball, el servei hauria d'implantar una protecció específica en l'estació de treball distant i assegurar que existeixen els acords pertinents per aquest tipus de treball.

7.7.1 Informàtica i comunicacions nòmades

7.7.1.1 Com són protegides les dades sensibles emmagatzemades en els portàtils? ➡ Anton Goma 16:28 16-03-2010

- [ ] Cap de les opcions següents.
- [x] Es demana als usuaris de no emmagatzemar dades sensibles en els portàtils.
- [ ] En alguns portàtil s'hi troba instal•lat una aplicació de xiframent.
- [ ] En tots els portatils amb informació sensible s'ha instal•lat una aplicació de xiframent per tal de protegir les dades crítiques.
- [ ] Ídem anterior + existeix un procediment que ens permet determinar si tot nou PC portàtil ha de ser protegit o no.

Afegir doc.
Esborrar Resposta

7.7.1.2 Quina protecció internet s'ha instal•lat en els portàtils? ➡ Anton Goma 16:30 16-03-2010

- [ ] Cap.
- [ ] Alguns portàtils tenen activat el firewall windows però l'usuari té la possibilitat de desactivar-ho.
- [ ] Alguns portàtils tenen activat el firewall de windows, el windows defender o una sonda ISS (RealSecure Desktop Protector) i el privilegis concedits no li permeten modificar aquesta configuració.
- [x] Ídem anterior + tots els portàtils.
- [ ] Ídem anterior + controls regulars.

Afegir doc.
Esborrar Resposta

7.7.2 Teletreball

7.7.2.1 Hi han mesures específiques en quan al tele-treball? ➡ Anton Goma 16:30 16-03-2010

- [ ] Cap de les opcions següents.
- [ ] El tele-treball està autoritzat en casos particulars.
- [x] Hi han usuaris que tenen instal•lat una aplicació que els permet establir una connexió VPN/RAS des del portàtil personal o professional.
- [ ] Ídem anterior + només es poden connectar des del portàtil professional.
- [ ] Ídem anterior + aquestes connexions són controlades regularment.

Afegir doc.
Esborrar Resposta

8 Adquisició, desenvolupament i manteniment de les Aplicacions

8.1 Necessitat en seguretat dels sistemes d'informació

Objectiu: Assegurar que la seguretat és una part integral en els sistemes d'informació.

Sistema d'informació inclou la infraestructura, les aplicacions de negoci i les aplicacions desenvolupades pels usuaris. El disseny i la implantació del sistemes d'informació que donen servei als processos de negoci, poden ser crucials per la seguretat. Els requeriments de seguretat han de ser identificats i acordats abans del desenvolupament del sistema.

Tots els requeriments de seguretat han de ser identificats i justificats en la fase de requeriments d'un projecte, consensuats i documentats com a part del procés de negoci per un sistema d'informació.

8.1.1 Anàlisis i especificacions de les necessitats en seguretat

8.1.1.1 Disposeu d'un mètode d'expressió de les necessitats de seguretat per ser inclòs en els requeriments de negoci per el desenvolupament o adquisició d'aplicacions noves o millores en sistemes existents? ➡ Anton Goma 13:02 21-04-2010

- [ ] No.
- [x] Les necessitats de seguretat són generalment expressades per el responsable de l'aplicació (o del procés de negoci tractat) al mateix temps que les necessitats funcionals estàndards.
- [ ] Disposem d'un qüestionari que permet al responsable del procés o de la futura aplicació, d'expressar les principals necessitats de seguretat.
- [ ] Disposem d'un mètode d'integració de la seguretat en els processos de desenvolupament o compra d'aplicacions considerades sensibles, des de les especificacions inicials fins la posada en explotació.
- [ ] Ídem anterior + controls periòdics per verificar el compliment del requeriments de seguretat.

Afegir doc.
Esborrar Resposta

8.2 Tractament correcte en el si de les aplicacions

Objectiu: Evitar errors, pèrdues, modificacions no autoritzades o mal ús de les dades en les aplicacions.

S'han de designar controls apropiats en les aplicacions, incloses les aplicacions desenvolupades pels usuaris, per tal d'assegurar un correcte processament de les dades. Aquests controls han d'incloure la validació de les dades d'entrada, processos interns i dades de sortida.

Controls addicionals poden ser requerits per sistemes de procés que tractin informacions sensibles, crítiques o valuoses.

8.2.1 Validació de les dades d'entrada

8.2.1.1 S'efectuen controls durant la introducció d'informacions sensibles per protegir el desenvolupament de possibles errors (doble validació, control de coherència, etc.)? ➡ Anton Goma 13:02 21-04-2010

- [ ] No.
- [x] Alguns controls manuals o automàtics simples es realitzen durant la introducció d'informacions crítiques (ex: detecció de valors fora de rang, verificació del format de les dades, etc.).
- [ ] Controls automàtics complexos (ex:càlcul de versemblança, detecció de caràcters invàlids, detecció de dades incomplertes, detecció de volum excessiu, etc.).
- [ ] Ídem anterior + és creen automàticament fitxers de registre amb les activitats involucrades en els processos d'entrada de dades (veure 6.10.1).
- [ ] Ídem anterior + procediments per verificar regularment els registres de dades d'entrada.

Afegir doc.
Esborrar Resposta

8.2.2 Control dels tractaments

8.2.2.1 Les aplicacions crítiques contenen controls programats que verifiquen automàticament la coherència de les dades i efectuen reconciliacions entre les dades d'entrada i sortida? ➡ Anton Goma 13:02 21-04-2010

- [ ] No.
- [x] Controls manuals ocasionals que permeten verificar la coherència de les dades i efectuar reconciliacions entre les dades d'entrada i sortida.
- [ ] Ídem anterior + controls automàtics periòdics.
- [ ] Ídem anterior + les aplicacions crítiques contenen controls programables que fan les verificacions automàtiques i sistemàtiques.
- [ ] Ídem anterior + les dades son regularment auditades per programes adequats.

Afegir doc.
Esborrar Resposta

8.2.3 Validació de les dades de sortida

8.2.3.1 Es verifica l'exactitud de les dades de sortida en les aplicacions crítiques? ➡ Anton Goma 13:03 21-04-2010

- [ ] No.
- [x] Controls manuals ocasionals permeten verificar l'exactitud de les dades en la sortida de les aplicacions crítiques.
- [ ] Ídem anterior + controls automàtics periòdics.
- [ ] Ídem anterior + les aplicacions crítiques contenen controls programats que realitzen verificacions automàtiques i sistemàtiques.
- [ ] Ídem anterior + les dades son regularment auditades per programes adequats.

Afegir doc.
Esborrar Resposta

8.3 Mitjans criptogràfics

Objectiu: Protegir la confidencialitat, autenticitat o integritat de la informació.

S'han d'utilitzar sistemes i tècniques criptogràfiques per protegir la informació sotmesa a riscos, quan altres mesures i controls no proporcionen la protecció adequada.

8.3.1 Política d'utilització dels mitjans criptogràfics

8.3.1.1 S'han identificat les dades o fluxos que requereixen de tècniques criptogràfiques i /o signatura electrònica? ➡ Anton Goma 13:03 21-04-2010

- [x] No.
- [ ] Els fluxos i dades a protegir criptogràficament són identificades cas per cas.
- [ ] Es realitza un anàlisi de riscos amb la finalitat de determinar el nivell de protecció a subministrar a les dades sensibles. La major part dels fluxes i dades que necessiten de tècniques criptogràfiques i/o signatura electrònica han estat identificats.
- [ ] Ídem anterior + per tot conjunt de dades i fluxos.
- [ ] Ídem anterior + els mitjans criptogràfics requerits han estat implantats.

Afegir doc.
Esborrar Resposta

8.3.1.2 Previ a una implantació de mitjans criptogràfics, us heu informat sobre la legislació aplicable a la criptografia? ➡ Anton Goma 13:03 21-04-2010

- [x] No.
- [ ] Es segueixen les indicacions subministrades per els proveïdors de les solucions criptogràfiques.
- [ ] Ídem anterior + verificacions puntuals amb el servei jurídic.
- [ ] S'han estudiat i seguit les diferents reglamentacions aplicables.
- [ ] Ídem anterior + procediments de verificació de compliment regulars.

Afegir doc.
Esborrar Resposta

8.3.2 Gestió de les claus d'accés

8.3.2.1 Es realitza una gestió segura de les claus de signatura digital o xiframent? ➡ Anton Goma 13:03 21-04-2010

- [x] No.
- [ ] Les claus de xiframent són tractades cas per cas.
- [ ] Totes les claus de signatura digital o xifratge estan centralitzades i a càrrec del responsable de seguretat dels sistemes d'informació.
- [ ] Ídem anterior + existeixen procediments d'actualització i d'intercanvi segurs.
- [ ] Ídem anterior + procediment de verificació dels sistemes criptogràfics i actualització de les reglamentacións vigents.

Afegir doc.
Esborrar Resposta

8.4 Seguretat dels fitxers sistema

Objectiu: Garantir la seguretat dels fitxers de sistema.

L'accés als fitxers de sistema i els codis font, han de ser controlats, i els projectes IT i les activitats de suport han de ser conduïdes de forma segura. S'ha d'evitar l'exposició de dades sensibles en els entorns de desenvolupament.

8.4.1 Controls de les utilitats d'explotació

8.4.1.1 Es controla periòdicament la naturalesa de les aplicacions instal•lades en els sistemes d'explotació o desenvolupament operatius? ➡ Anton Goma 13:04 21-04-2010

- [ ] No.
- [ ] L'actualització de les aplicacions operacionals o llibreries només són realitzades pels administradors sota una gestió d'autoritzacions apropiada (veure 8.4.3). Aquestes aplicacions operatives són codis executables i no codis de desenvolupament o compilacions.
- [x] La implantació de tot codi executable no es realitza mentre no es comprovi el correcte funcionament mitjançant proves, l'acceptació per part de l'usuari i l'actualització de les llibreries de programes font. Aquestes proves de verificació són realitzades en un sistema separat (veure 6.1.4).
- [ ] Ídem anterior + s'ha implantat un control de la configuració del sistemes i aplicacions operatives per mantenir un control de tot software implantat, així com la documentació de sistema.
- [ ] Ídem anterior + es manté un registre d'auditoria de totes les actualització realitzades en els sistemes de producció per tal d'aplicar, sí fos necessari, mesures de contingència. Les versions anteriors són arxivades juntament amb la documentació, procediments, detalls de configuració i de suport, etc.

Afegir doc.
Esborrar Resposta

8.4.2 Protecció de les dades de sistema d'assaig

8.4.2.1 S'assegura que les dades utilitzades en les proves i tests no són confidencials? ➡ Anton Goma 13:05 21-04-2010

- [ ] No.
- [ ] Una copia de les dades són utilitzades per les proves i destruïda a la fi de les mateixes.
- [x] S'utilitza un sol joc de dades extret específicament de les dades estàndards.
- [ ] Ídem anterior + s'ha formalitzat i aplicat un procediment per prohibir la utilització de dades confidencials.
- [ ] Ídem anterior + les dades utilitzades per les proves són verificades anònimes i validades per el responsable del procés de negoci o propietari del desenvolupament.

Afegir doc.
Esborrar Resposta

8.4.3 Control d'accés al codi font de les aplicacions

8.4.3.1 L'accés al codi font dels programes i aplicacions crítiques està restringit al personal habilitat? ➡ Anton Goma 13:05 21-04-2010

- [ ] No.
- [ ] Restringit al departament informàtic.
- [x] Restringit al equip de desenvolupament.
- [ ] Restringit a certs membres de l'equip de desenvolupament.
- [ ] Ídem anterior + els accessos al codi font està prohibit fora de les fases de desenvolupament o evolució validades per el responsable/propietari de l'aplicació.

Afegir doc.
Esborrar Resposta

8.5 Seguretat del desenvolupament i gestió del suport

Objectiu: Mantenir la seguretat de les aplicacions de sistema i de les informacions.

S'han de controlar estrictament els entorns de desenvolupament i suport.

Els responsables de processos i aplicacions de negoci en producció, ho han de ser també de la seguretat dels entorns de desenvolupament i suport. S'han d'assegurar de la revisió de tota modificació proposada en els sistema per verificar que aquesta no debiliti la seguretat.

8.5.1 Procediment del control de canvis i actualitzacions

8.5.1.1 Tot canvi fora del manteniment és objecte d'un procediment d'anàlisi formal abans de la seva posada en producció? ➡ Anton Goma 13:06 21-04-2010

- [ ] No.
- [ ] Tot canvi és identificat i enregistrat.
- [x] Les modificacions majors sobre els programes en producció són objecte de mesures estrictes.
- [ ] Totes les modificacions sobre els entorns de producció crítics, respecten un procediment estricte de control, són sotmesos a una autorització prèvia i a una avaluació de riscos.
- [ ] Ídem anterior + sobre tots els entorns de producció.

Afegir doc.
Esborrar Resposta

8.5.2 Revisió tècnica de les aplicacions després de les modificacions en el sistema d'explotació

8.5.2.1 Les aplicacions són revisades i provades després de cada modificació o actualització sobre el sistema d'explotació (ex: test de no regressió)? Anton Goma 13:06 21-04-2010

- [ ] No.
- [ ] Només les aplicacions crítiques.
- [x] La major part de les aplicacions.
- [ ] Un procediment que defineix com s'han de realitzar els manteniments i evolucions ha estat implantat per tot els sistemes crítics.
- [ ] Ídem anterior + és manté un inventari actualitzat de les modificacions realitzades sobre els sistemes crítics.

Afegir doc.
Esborrar Resposta

8.5.3 Restriccions relatives a les modificacions de paquets d'aplicacions d'editors externs.

8.5.3.1 Les peticions de modificacions sobre els paquets d'aplicacions estan limitades al estrictament necessari i són objecte de mesures de controls i autoritzacions prèvies? Anton Goma 13:10 21-04-2010

- [ ] No.
- [ ] Tota demanda de modificació entra en el marc de gestió de les modificacions definits per l'editor de l'aplicació.
- [x] En cas de refús de modificació, l'aplicació s'utilitza igualment sempre i quan no signifiqui una inadaptació a les necessitats de negoci.
- [ ] Les peticions de modificacions i el seu impacte sobre el manteniment són estudiats abans de l'adquisició definitiva de l'aplicatiu amb una versió de test. L'aplicació no és adquirida fins que s'obté el compromís de desenvolupar les modificacions per part de l'editor.
- [ ] El servei adquireix els drets i les competències sobre les aplicacions crítiques per tal d'efectuar en intern les modificacions indispensables.

Afegir doc.
Esborrar Resposta

8.5.4 Fuita d'informació

8.5.4.1 S'efectuen revisions del codi sobre els desenvolupaments sensibles per tal de protegir-lo contra desenvolupaments fraudulents, canals amagats, portes obertes, desbordament de piles o altres fallides de seguretat? Anton Goma 13:11 21-04-2010

- [x] No.
- [ ] Puntualment sobre algun desenvolupament de sistema sensible.
- [ ] Ocasionalment, sota demanda del responsable de procés o de l'aplicació.
- [ ] Sistemàticament, sobre els desenvolupaments sensibles i seguint un procediment clarament definit, formalitzat i validat.
- [ ] Ídem anterior + es realitzen auditories externes a l'equip de desenvolupament.

Afegir doc.
Esborrar Resposta

8.5.5 Externalització dels desenvolupament d'aplicacions

8.5.5.1 S'apliquen mesures de seguretat particulars en els desenvolupament externs d'aplicacions sensibles (clàusules de seguretat i auditoria en els contractes, certificacions de qualitat, revisió en intern del codi font, etc.)? Anton Goma 13:11 21-04-2010

- [ ] No.
- [x] Les exigències legals generals són recordades en els contractes.
- [ ] S'inclouen clàusules de seguretat específiques en els contractes.
- [ ] S'exigeixen sistemàticament mesures de seguretat en els contractes.
- [ ] Ídem anterior + s'apliquen clàusules d'auditoria.

Afegir doc.
Esborrar Resposta

8.6 Gestió de les vulnerabilitats tècniques

Objectiu: Reduir els riscos resultants de la publicació i explotació de vulnerabilitats tècniques.

La gestió de les vulnerabilitats tècniques ha de ser implantada de forma efectiva i sistemàtica. S'han de considerar tant les vulnerabilitats en els sistemes operatius com en les aplicacions en producció.

8.6.1 Mesures relatives a les vulnerabilitats tècniques

8.6.1.1 Consulteu de forma regular els butlletins de vulnerabilitats publicats pels editors dels sistemes i aplicacions operatives?

➡ Anton Goma 13:11 21-04-2010

- [x] No.
- [ ] Sobre alguns sistemes sensibles.
- [ ] Sobre tots els sistemes sensibles.
- [ ] Ídem anterior + el cap de servei ha establert rols i responsabilitats en la gestió de vulnerabilitats tècniques, inclòs la vigilància continuada, l'avaluació de riscos associada a la vulnerabilitat, l'execució de mesures correctores (patch's), etc. sobre els sistemes sensibles identificats i inventariats.
- [ ] Ídem anterior + aplicació d'un procediment que descriu l'avaluació prèvia, els terminis d'implantació, les prioritats, l'aprovació i validació de les mesures correctores i el registre dels esdeveniments associats.

Afegir doc.

Esborrar Resposta

9 Gestió dels incidents

9.1 Informe dels incidents i les vulnerabilitats de seguretat en els S.I.

Objectiu: Assegurar que els esdeveniments i febleses en la seguretat siguin comunicats de forma que ens permeti realitzar una acció correctiva a temps.

S'han d'implementar informes d'esdeveniments els procediments d'escalada de suport per el tractament dels incidents de seguretat. Tots els empleats, proveïdors i tercers han de ser coneixedors dels procediments per informar dels diferents tipus d'esdeveniments ique poden tenir impacte en la seguretat dels actius del servei. S'ha de requerir que informin de qualsevol esdeveniment o feblesa de seguretat en els sistemes d'informació, de forma ràpida i a la persona de contacte designada.

9.1.1 Informe dels incidents de seguretat en els S.I.

9.1.1.1 S'efectua reporting dels incidents de seguretat al responsable de la seguretat dels sistemes d'informació? Anton Goma 09:05 22-04-2010

- [ ] No.
- [ ] No, el reporting s'efectua només en l'equip d'explotació dels sistemes.
- [x] En casos puntuals, els incidents són reportats al responsable informàtic i seguretat.
- [ ] Sí, existeix un procediment per informar al responsable de seguretat sistemàticament de tot incident d'una gravetat determinada mitjançant un model d'informe preconcebut.
- [ ] Ídem anterior + un reporting periòdic és realitzat cap a la direcció del SAF.

Afegir doc.
Esborrar Resposta

9.1.2 Informe de vulnerabilitats de seguretats en els S.I.

9.1.2.1 S'ha sensibilitzat als usuaris, col•laboradors, proveïdors de fer notar tot esdeveniment inhabitual que podria ser perillós per la seguretat dels sistemes d'informació o per la integritat de les persones? Anton Goma 09:08 22-04-2010

- [x] Cap de les opcions següents.
- [ ] Sí, aquest punt es recordat en les campanyes de sensibilització per la seguretat en el treball.
- [ ] Una nota de servei ha estat difosa amb aquest propòsit.
- [ ] Aquest punt està inclòs en el document de normes d'usuari del sistemes d'informació.
- [ ] Ídem anterior + tots els usuaris coneixen els procediments d'alerta i els contactes a realitzar en el moment que es produeix un esdeveniment inhabitual.

No procedeix. Cap esdeveniment de la seguretat informàtica pot comportar un risc per la seguretat de les persones i, en quant als sistemes d'informació, difícilment.

Afegir doc.
Esborrar Resposta

9.2 Gestió dels incidents i millores de la seguretat dels S.I.

Objectiu: Assegurar una aplicació efectiva en la gestió d'incidents en la seguretat dels sistemes d'informació.

S'han d'establir responsabilitats i procediments per gestionar els esdeveniments de seguretat de forma efectiva des del moment que s'hagi rebut la informació. S'ha d'aplicar un procés de millora continuada en resposta a la vigilància, avaluació i gestió general dels incidents en la seguretat dels sistemes d'informació.

En els casos que es requereixi proves o evidències, aquestes s'han d'enregistrar per tal d'assegurar el compliment de les especificacions legals.

9.2.1 Responsabilitats i procediments

9.2.1.1 Els procediments i responsabilitats en matèria de gestió dels incidents de seguretat estan clarament definits i aplicats de forma que s'asseguri un tractament eficaç i ràpid? Anton Goma 09:08 22-04-2010

- [ ] Cap de les opcions següents.
- [x] No, els incidents són tractats cas per cas.
- [ ] No estan definits completament. Només per certs tipus d'incidents.
- [ ] Sí, estan formalment definits i aplicats a tots els nivells (centre de trucades, suport de nivell 1, suport de nivell 2, contactes proveïdors, responsable del seguiment, comitè de validació, etc.).
- [ ] Ídem anterior + reunió periòdica per el seguiment, verificació de l'estat o per el tancament, si s'escau .

Afegir doc.
Esborrar Resposta

9.2.2 Retorns d'experiència extret dels incidents de seguretat dels S.I.

9.2.2.1 Es fa un seguiment eficaç dels incidents de seguretat que permeti extreure les causes, valorar les conseqüències, l'impacta en el negoci, etc. ? ➡ Anton Goma 09:08 22-04-2010

- ☐ No.
- ☑ Només les incidents més greus són objecte d'un seguiment particular.
- ☐ Existeix un sistema de seguiment dels incidents però aquest és consultat ocasionalment.
- ☐ Existeix un sistema de seguiment formal dels incidents que s'aplica regularment. S'indica l'estat de resolució de l'incident (obert, en curs, tractat, tancat) i la gravetat del mateix.
- ☐ Existeix un conjunt de procediments que permeten tractar i gestionar el incidents de seguretat a diferents nivells funcionals i jeràrquics, que implica el responsable de seguretat i la direcció quan l'incident o requereix. Els incidents de certa gravetat són objecte d'un informe.

Afegir doc.
☐ Esborrar Resposta

9.2.3 Col•lecta de proves

9.2.3.1 Disposeu de procediments per la col•lecta eventual de proves utilitzables davant dels tribunals en cas d'incident greu? ➡ Anton Goma 09:08 22-04-2010

- ☑ No.
- ☐ Només els registres d'esdeveniments dels sistemes operatius.
- ☐ Existeixen mecanismes manuals o automàtics que permeten obtenir informacions en cas d'incidents greus.
- ☐ Un procediment i mecanismes de conservació de proves, completa els registres d'esdeveniments dels sistemes

Afegir doc.
☐ Esborrar Resposta

10 Gestió del pla de continuïtat de l'activitat

10.1 Aspectes de la seguretat dels S.I. en matèria de gestió de la continuïtat de l'activitat

Objectiu: Reaccionar a la interrupció de les activitats de negoci i protegir els processos crítics en front de grans fallides dels sistemes d'informació o desastres.

S'ha d'implantar un procés de gestió de la continuïtat del negoci per reduir, a nivells acceptables, la interrupció causada per desastres naturals, accidents, fallides de seguretat, fallides dels equips, etc., mitjançant una combinació de controls preventius i de recuperació. Aquest procés ha d'identificar els processos crítics de negoci i integrar els requeriments de gestió de la seguretat per la continuïtat del negoci amb altres requeriments de continuïtat relacionats amb aspectes com operacions, proveïdors de serveis i de personal, materials, transport i instal•lacions.

S'han d'analitzar les conseqüències dels desastres, fallides de seguretat, pèrdues de servei i de disponibilitat. S'han de desenvolupar i implantar plans de contingència per assegurar que els processos de negoci es puguin restaurar en els terminis requerits. La seguretat de la informació ha de ser una part integral del pla general de continuïtat del negoci i dels demés processos de gestió dins del servei.

La gestió de la continuïtat del negoci ha d'incloure un procés d'avaluació, controls per la identificació i reducció dels riscos, procediment per limitar les conseqüències de les incidències i assegurar la represa a temps de les operacions essencials.

10.1.1 Integració de la seguretat dels S.I. dins del procediment de gestió del pla de continuïtat

10.1.1.1 Quina és la política de continuïtat (PCA) i de represa de l'activitat informàtica (PRI) del SAF?

➡ Anton Goma 09:09 22-04-2010

- ☐ Cap de les opcions següents.
- ☑ Aquest temes estan en curs d'estudi i seran part del pla d'acció proposat per aquesta auditoria.
- ☐ El PCA està implantat assegurant la continuïtat de l'activitat principal del negoci.
- ☐ Ídem anterior + el PCA integra un pla per la prevenció de riscos informàtics.
- ☐ Ídem anterior + el PRI i el PCA són regularment actualitzats.

Afegir doc.
☐ Esborrar Resposta

10.1.2 Continuïtat de l'activitat i apreciació dels riscos

10.1.2.1 Quins aspectes contempla l'anàlisi de riscos informàtics?

➡ Anton Goma 09:10 22-04-2010

- ☑ Cap de les opcions següents.
- ☐ Només aspectes informàtics.
- ☐ Ídem anterior + una part dels processos de negoci.
- ☐ Ídem anterior + sobre els processos crítics de negoci.
- ☐ Ídem anterior + l'anàlisi de riscos és avaluat periòdicament.

Encara no s'ha fet tal anàlisi.

Afegir doc.
☐ Esborrar Resposta

10.1.3 Elaboració i posada en marxa dels plans de continuïtat integrant la seguretat dels S.I.

10.1.3.1 Existeix en el servei un pla de represa informàtica (PRI)?

➡ Anton Goma 09:10 22-04-2010

- ☐ Cap de les opcions següents.
- ☐ En estudi.
- ☑ Parcialment.
- ☐ Implantat.
- ☐ Ídem anterior + avaluat i actualitzat periòdicament.

No existeix com a pla, sí que existeixen accions independents per a cada servidor crític.

Afegir doc.
☐ Esborrar Resposta

10.1.4 Quadre de planificació i de coherència de la continuïtat de l'activitat

10.1.4.1 S'aplica una metodologia per definir i controlar la coherència dels plans de continuïtat? ➡ Anton Goma 09:10 22-04-2010

- [x] No.
- [ ] Només per els sistemes informàtics.
- [ ] S'aplica una metodologia que implica als responsables dels processos de negoci i a les funcions crítiques del servei.
- [ ] Ídem anterior + per el conjunt de funcions del servei.

Afegir doc.
Esborrar Resposta

10.1.5 Proves, gestió i apreciació constant dels plans de continuïtat de l'activitat

10.1.5.1 El PRI ha estat provat o simulat? ➡ Anton Goma 09:11 22-04-2010

- [ ] Cap de les opcions següents.
- [x] No.
- [ ] Parcialment.
- [ ] Només pels sistemes crítics.
- [ ] Globalment, una vegada a l'any.

Afegir doc.
Esborrar Resposta

11 Conformitat

11.1 Conformitat amb les exigències legals

Objectiu: Evitar els incompliments de qualsevol llei civil o penal, requeriment reglamentari, regulació o obligació contractual, i de tot requeriment de seguretat.

El disseny d'operacions , ús i gestió dels sistemes d'informació port estar subjecte a requeriments estatutaris, reguladors i contractuals envers la seguretat.

El servei ha de demanar assessorament sobre els requeriments legals específics als assessors legals a la seva disposició o a professionals de dret qualificats.

11.1.1 Identificació de la legislació vigent

11.1.1.1 Les lleis relatives a l' utilització de les tecnologies en els projectes i en els contractes amb proveïdors han estat identificades i tingudes en compte? ➡ Anton Goma 09:12 22-04-2010

- ☐ Cap de les opcions següents.
- ☑ Només les principals lleis han estat identificades i aplicades cas per cas.
- ☐ Totes les lleis aplicables sobre projectes que inclouen dades nominatives o personals, signatures electròniques i criptografia.
- ☐ En tots els projectes.
- ☐ Ídem anterior + política formalitzada.

LOPD és acatada.

Afegir doc.

☐ Esborrar Resposta

11.1.2 Drets de la propietat intel•lectual

11.1.2.1 S'apliquen procediments de control per el respecte a la llei de la propietat intel•lectual, principalment pel que fa a les aplicacions i software propietaris? ➡ Anton Goma 09:13 22-04-2010

- ☐ Cap de les opcions següents.
- ☐ La compra d'aplicacions o software la realitza cada departament deixant sota la seva responsabilitat el compliment.
- ☑ Tota compra d'aplicacions o software és realitzada per un servei centralitzat que se'n ocupa.
- ☐ Ídem anterior + totes les instal•lacions són realitzades per el servei informàtic qui s'encarrega de mantenir un inventari actualitzat de les llicències instal•lades.
- ☐ Ídem anterior + inventaris regulars.

Des de fa poc.

Afegir doc.

☐ Esborrar Resposta

11.1.3 Protecció dels registres de la societat

11.1.3.1 Els registres legals (contractes, llicències, permisos, etc.) s'arxiven en condicions de seguretat particular (protecció contra la destrucció o pèrdua de confidencialitat)? ➡ Anton Goma 09:13 22-04-2010

- ☑ Cap de les opcions següents.
- ☐ A criteri de cada cap de departament.
- ☐ Existeix una guia que permet a cada cap de departament identificar i arxivar amb seguretat les informacions legals.
- ☐ Existeix un inventari de les informacions legals que disposa el SAF. Aquestes informacions són arxivades en condicions de seguretat particulars.
- ☐ Ídem anterior + l'inventari determina diferents nivells de criticitat que defineixen diferents necessitats de seguretat.

Afegir doc.

☐ Esborrar Resposta

11.1.4 Protecció de les dades i confidencialitat de les informacions relatives a la vida privada

11.1.4.1 El SAF s'assegura de la conformitat amb la llei relativa a la protecció de les dades personals? ➡ Anton Goma 09:13 22-04-2010

- ☐ Cap de les opcions següents.
- ☑ El personal està sensibilitzat en la necessitat de respecte de la reglamentació estatal o internacional sobre la protecció de les dades personals.
- ☐ El SAF ha implantat un procediment que permet vigilar el respecte a la reglamentació.
- ☐ Ídem anterior + integració en els projectes informàtics.
- ☐ Ídem anterior + revisions regulars del procediment.

Afegir doc.

☐ Esborrar Resposta

11.1.5 Prevenció contra la utilització il•lícita dels mitjans del tractament de les informacions

11.1.5.1 Quines són les mesures aplicades per prevenir una utilització il•lícita dels recursos informàtics? ➡ Anton Goma 09:14 22-04-2010

- ☐ Cap de les opcions següents.
- ☐ Algunes mesures han estat publicades.
- ☐ Els usuaris han estat informats de les regles de bon ús dels recursos informàtics.
- ☑ Ídem anterior + les regles són comunicades via accions de sensibilització periòdiques.
- ☐ Ídem anterior + les regles comunicades són revisades periòdicament.

Afegir doc.
☐ Esborrar Resposta

11.1.6 Legislació sobre els mitjans criptogràfics

11.1.6.1 S'assegura l'aplicació de la legislació en relació a la criptografia? ➡ Anton Goma 09:14 22-04-2010

- ☑ Cap de les opcions següents.
- ☐ Cas per cas en l'adquisició d'un producte.
- ☐ Amb l'assistència del servei jurídic.

Afegir doc.
☐ Esborrar Resposta

11.2 Revisions de la política de seguretat i de la conformitat tècnica

Objectiu: Assegurar la conformitat dels sistemes amb les polítiques i normes de seguretat.

S'han de fer revisions regulars de la seguretat dels sistemes d'informació.

S'ha d'auditar el compliment de les normes d'implantació de la seguretat i els controls de seguretat implantats.

11.2.1 Conformitat amb les polítiques i normes de seguretat

11.2.1.1 Ha adoptat el SAF el pla d'acció seguretat per l'any en curs? ➡ Anton Goma 09:14 22-04-2010

- ☑ Cap de les opcions següents.
- ☐ Sí, parcialment.
- ☐ Sí, completament però no ha estat pressupostat.
- ☐ Si, completament i pressupostat.
- ☐ Ídem anterior + el pla està en acord al pla establert per el Servei Informàtic de la UAB.

Afegir doc.
☐ Esborrar Resposta

11.2.2 Verificació de la conformitat tècnica

11.2.2.1 S'efectua regularment una revisió de la conformitat a les recomanacions establertes per el Servei Informàtic de la UAB? ➡ Anton Goma 09:15 22-04-2010

- ☑ Cap de les opcions següents.
- ☐ Puntualment.
- ☐ Sí, el departament informàtic s'assegura de l'actualització de la seguretat.
- ☐ Ídem anterior + revisió regular.
- ☐ Ídem anterior + una auditoria tècnica externa completa el dispositiu de verificació.

Afegir doc.
☐ Esborrar Resposta

11.3 Consideracions per les auditories de seguretat dels S.I.

Objectiu: Maximitzar l'efectivitat i minimitzar les interferències durant el procés d'auditoria del sistema.

S'han d'establir controls per protegir les aplicacions en producció durant un procés d'auditoria. També es requereix protegir la integritat i evitar el mal ús de les eines d'auditoria.

11.3.1 Mesures de les auditories de seguretat dels S.I.

11.3.1.1 Durant una auditoria o control sobre els sistemes en producció s'assegura la planificació de forma que no hi hagi risc d'interrupció involuntària del sistema? ➨ Anton Goma 09:16 22-04-2010

- [x] Cap de les opcions següents.
- [ ] Es deixa a criteri de l'auditor o persona que realitza el control.
- [ ] Les auditories i controls es realitzen amb privilegis de lectura que no permeten l' interrupció dels sistemes en producció.
- [ ] Ídem anterior + controls realitzats en franges horaries que no afecten a la continuïtat.
- [ ] Ídem anterior + procediment formalitzat.

Encara no s'ha fet una auditoria de control sobre els SI

Afegir doc.

Esborrar Resposta

11.3.2 Protecció de les eines d'auditoria dels S.I. (Apartat definit fora de perímetre)

11.3.2.1 L'accés a les eines d'auditoria està restringit al personal autoritzat? ➨

- [ ] No.
- [ ] Només personal informàtic.
- [ ] Als administradors de sistemes.
- [ ] A les persones habilitades per controlar i auditar la seguretat.
- [ ] Ídem anterior + l'accés es produeix mitjançant autentificació de les credencials d'usuari.

No tenim eines específiques d'auditoria. Si les tinguessim, estarien restringides als administradors dels sistemes. Tot el personal informàtic és a la vegada administrador de sistemes.

Afegir doc.

Annex B: Codi font php del Controlador de la lògica de programa del model MVC

```
<?php
//Controlador de la lògica de programma
//#activació debuger SQL , debugger XAJAX i smarty
//Controller() ens envia a la plantilla base

class Index
{
	//config
	private $config;
	//db
	private $db;
	//smarty
	private $web;

	public function Index($config)
	{
	$this->config = $config;
	$this->db = ADONewConnection($this->config->dbdriver);
	$this->db->Connect($this->config->dbhost, $this->config->dbusuari, $this->config-
	>dbpwd, $this->config->dbnom);
	$this->db->SetFetchMode(ADODB_FETCH_ASSOC);
	$this->db->debug =false;  //activar el debug de les consultes SQL

		$this->web = new smarty_init();

		///control inici de sessió
		session_start();
		$action = isset($_GET['action'])? $_GET['action'] : 'login';

		if(!empty($_SESSION['usr_id']) && $action!='logout'){
			$this->controler();
		}
		else
		{
			switch ($action)
			{
			case 'login':
				$this->web->display("login.tpl");
			break;
			case 'fer_login':
				$usuari = Usuari::login($_POST['usuari'],
				$_POST['contrasenya'],$this->db);
				if($usuari !=null){
					foreach($usuari as $key => $value){
			$_SESSION['id']=session_id();
			if($key=='usr_id') $_SESSION['usr_id']=$value['usr_id'];
			if($key=='usuari') $_SESSION['usuari']=$value['usuari'];
			if($key=='pass') $_SESSION['pass']=$value['pass'];
			if($key=='nom') $_SESSION['nom']=$value['nom'];
			if($key=='rol') $_SESSION['rol']=$value['rol'];
		if($key=='id_quest') $_SESSION['id_quest']=$value['id_quest'];
				$this->quest=$value['id_quest'];
		}
			$this->controler();
	}else
		{
		Usuari::logout();
		$this->web->assign("errlog","Invalid username or password");
		$this->web->display("login.tpl");
	}
	break;
			case 'logout':
				Usuari::logout();
					$this->web->display("login.tpl");
					break;

				default;
			}
		}
		$this->db->Close();
```

```
	}

private function ExecControlForms($instancia){

////CODI PER CONTROLAR LA PAGINA AMB FORMULARIS I LLISTATS
///// Atenció al límit de preguntes a mostrar ficar en fitxer de configuració.

$instancia->Config(-1, 500, -1, $_GET['ord'], $_GET['by'], $_GET['clike'],
$_GET['wlike']);

	$taula=$instancia->Run("GetTaula");

	if($taula=='capitols'){
		list($total, $dadesMostrar, $columnes) = $instancia->Run("GetAllCap");
//list=assignació a una llista de variables
		$this->web->assign("dadesArray", $dadesMostrar);
		$this->web->assign("total", $total);
		$this->web->assign("columnes", $columnes);
		//Capitols('num_cap, num_subcap, num_subsubcap','preguntes', $this->db)
		}

	if($taula=='preguntes'){
		list($totalprg, $dadesMostrarprg) = $instancia->Run("GetAllPrg");
//list=assignació a una llista de variables
		$this->web->assign("dadesArrayprg", $dadesMostrarprg);
		$this->web->assign("totalprg", $totalprg);
		}

	if($taula=='estats'){
		list($difcap,$difnomcap,$nrespxcap,$npxcap,$dhist,$dhistoric)=$instancia-
>Run("GetEstats");
		$this->web->assign("difcap", $difcap);
		$this->web->assign("difnomcap", $difnomcap);
		$this->web->assign("nrespxcap", $nrespxcap);
		$this->web->assign("npxcap", $npxcap);
		$this->web->assign("dhist", $dhist);
		$this->web->assign("dhistoric", $dhistoric);
		}

		if($taula=='historic'){
		list($difcap,$difnomcap,$dhistoric)=$instancia->Run("GetHist");
		$this->web->assign("difcap", $difcap);
		$this->web->assign("difnomcap", $difnomcap);
		$this->web->assign("dhistoric", $dhistoric);
		}

		if($taula=='objectius')
		{
		$dadesobj = $instancia->Run("GetAllObj");
		$this->web->assign("dadesobj", $dadesobj);
		}

		if($taula=='cartografia')
		{
		$dadesper = $instancia->Run("GetAllPer");
		$this->web->assign("dadesper", $dadesper);
		}
		if($taula=='infoquest')
		{
			if($_GET['action']=='fer_login' || !empty($_GET['quest']) ||
$_SESSION['rol']=='Admin'){
				$dadesquest=$instancia->Run('selQ');
				$this->web->assign("dadesq", $dadesquest);
			}
		}

		if($taula=='accio'){
			if($_GET['act']!='del' || $_GET['act']!='doc' ||
$_GET['act']!='ghist') $instancia->Run($_GET['act']);
			$tAct = substr($_GET['act'], 1);
			$this->web->assign("Faction", $tAct);
			$this->web->assign("id", $_GET['id']);
			$this->typ=$_GET['typ'];
```

```
                if($tAct=='add'){
        if ($this->typ=='capnou') $this->web->assign("formadd", 'capnou');
        if ($this->typ=='cap') $this->web->assign("formadd", 'subcap');
        if ($this->typ=='sub') $this->web->assign("formadd", 'subsubcap');
        if ($this->typ=='apt') $this->web->assign("formadd", 'questio');
        if ($this->typ=='obj') $this->web->assign("formadd", 'objectiu');
        if ($this->typ=='per') $this->web->assign("formadd", 'perimetre');
        if ($this->typ=='perfis') $this->web->assign("formadd", 'perfis');
              }
              if($tAct == 'edit'){
                    $instancia->Config($_GET['id']);
        if ($this->typ=='cap') $this->web->assign("formadd", 'cap');
        if ($this->typ=='sub') $this->web->assign("formadd", 'subcap');
        if ($this->typ=='apt') $this->web->assign("formadd", 'subsubcap');
        if ($this->typ=='prg') $this->web->assign("formadd", 'questio');
        if ($this->typ=='obj') $this->web->assign("formadd", 'objectiu');
        if ($this->typ=='per') $this->web->assign("formadd", 'perimetre');
        if ($this->typ=='perfis') $this->web->assign("formadd", 'perfis');
        list($dadesprg,$dadescap, $dobj,$dper)=$instancia->Run('getOne');
        $this->web->assign("dades", $dadesprg);
        $this->web->assign("dadescap", $dadescap);
        $this->web->assign("dobj", $dobj);
        $this->web->assign("dper", $dper);
              }
              if($tAct == 'del'){
                    $missdel=$instancia->Run('del');
              }
              if($tAct == 'ghist'){
                    $instancia->Run('ghist');
              }
        if($tAct == 'doc'){
              if ($this->typ=='afdoc') $this->web->assign("formadd", 'afdoc');
        }

        }
        return array ($totalprg,$dadesMostrarprg,$total);
}

public function LoadComent($formData){
              $objResponse2 = new xajaxResponse();
              //$objResponse2->setCharacterEncoding('utf-8');

              $opcio="";
              $idprg=0;

              foreach($formData as $key => $value){
                    $opcio= $key;
                    $idprg=substr($opcio,0,strlen($opcio)-6);
                    $tipusresp=substr($opcio,-6);
                    $coment=utf8_decode(FuncionsBase::HtmlEntitiesFilter($value));

        if($tipusresp=="coment"){
              $data1=time();
              $data=date ( "H:i      j-m-Y" , $data1 );
              $sql = "INSERT INTO vrespostes (id_preg,id_resp,comentari,usr,data) VALUES
(".$idprg.",".$idprg.",'".$coment."','".$_SESSION['nom']."','".$data."') ON DUPLICATE KEY
UPDATE comentari = '".$coment."', usr= '".$_SESSION['nom']."', data= '".$data."'";
              $this->db->Execute($sql);
              }
        }
return $objResponse2;
}


public function EsbResposta($formData){
        $objResponse4 = new xajaxResponse();
        $opcio="";
        $idprg=0;

        foreach($formData as $key => $value){
              $opcio= $key;
              $idprg=$value;
              $tipusresp=substr($opcio,-6);
              if($tipusresp=="esresp"){
```

```
                    $sql = "INSERT INTO vrespostes
                    (id_preg,id_resp,resposta,usr,data,evol) VALUES
                    (".$idprg.",".$idprg.",99,'','',0) ON DUPLICATE KEY UPDATE resposta=
                    99,usr='',data='',evol=0 ";
              $this->db->Execute($sql);

       $objResponse4->assign($idprg."opcio0","disabled",false);
       $objResponse4->assign($idprg."opcio1","disabled",false);
       $objResponse4->assign($idprg."opcio2","disabled",false);
       $objResponse4->assign($idprg."opcio3","disabled",false);
       $objResponse4->assign($idprg."opcio4","disabled",false);
       $objResponse4->assign($idprg."opcio0","checked",false);
       $objResponse4->assign($idprg."opcio1","checked",false);
       $objResponse4->assign($idprg."opcio2","checked",false);
       $objResponse4->assign($idprg."opcio3","checked",false);
       $objResponse4->assign($idprg."opcio4","checked",false);
       $objResponse4->assign($idprg."prg0","style.color","#000000");
       $objResponse4->assign($idprg."prg1","style.color","#000000");
       $objResponse4->assign($idprg."prg2","style.color","#000000");
       $objResponse4->assign($idprg."prg3","style.color","#000000");
       $objResponse4->assign($idprg."prg4","style.color","#000000");
       $objResponse4->assign($idprg."esresp","disabled","disabled");

       $objResponse4->assign($idprg."reg", "innerHTML", "<IMG SRC='imatges/equal.gif'>");

       $ncap=$this->db->Execute('SELECT id_cap, id_quest FROM preguntes WHERE
id_prg='.$idprg);
       $id_quest=$ncap->fields['id_quest'];
       $id_cap=$ncap->fields['id_cap'];

$npxc=$this->db->Execute('SELECT Count(id_prg) FROM preguntes,capitols WHERE
preguntes.id_cap = capitols.num_cap AND preguntes.id_quest = capitols.id_quest AND
id_subcap = num_subcap AND id_subsubcap = num_subsubcap AND ((preguntes.id_quest
='.$id_quest.') AND (capitols.num_cap='.$id_cap.') AND (capitols.id_excl=0))');

$pregxcap=$npxc->fields['Count(id_prg)'];

$nrxc=$this->db->Execute('SELECT Count(id_prg) FROM capitols, preguntes, vrespostes WHERE
preguntes.id_prg = vrespostes.id_preg AND preguntes.id_cap = capitols.num_cap AND
preguntes.id_subcap = capitols.num_subcap AND preguntes.id_subsubcap =
capitols.num_subsubcap AND preguntes.id_quest = capitols.id_quest AND
((preguntes.id_cap='.$id_cap.') AND (preguntes.id_quest='.$id_quest.') AND
(capitols.id_excl=0) AND (vrespostes.resposta!=99))');

$respxcap=$nrxc->fields['Count(id_prg)'];

$sumr=$this->db->Execute('SELECT SUM(resposta) FROM capitols, preguntes, vrespostes WHERE
preguntes.id_prg = vrespostes.id_preg AND preguntes.id_cap = capitols.num_cap AND
preguntes.id_subcap = capitols.num_subcap AND preguntes.id_subsubcap =
capitols.num_subsubcap AND preguntes.id_quest = capitols.id_quest AND
((preguntes.id_cap='.$id_cap.') AND (preguntes.id_quest='.$id_quest.') AND
(capitols.id_excl=0) AND (vrespostes.resposta!=99))');

$sumresp=$sumr->fields['SUM(resposta)'];

$ind=round($sumresp/$pregxcap,1);

       if($ind<2) $colind="#DF0101";
       if($ind>=2 && $ind<3) $colind="#FF7F00";
       if($ind>=3 && $ind<4) $colind="#04B404";
       if($ind>=4 && $ind<=5) $colind="#2E2EFE";
       $objResponse4->assign($id_cap."ind", "innerHTML", "   <input
STYLE='background-color: ".$colind."' type='text' name='instaval' id='instaval' size='1'
value='".$ind."' readonly>");
       if($respxcap!=$pregxcap) $objResponse4->assign($id_cap."indnrp", "innerHTML",
'<font color="#DF0101">   '.$respxcap.'|'.$pregxcap);
       if($respxcap==$pregxcap)$objResponse4->assign($id_cap."indnrp", "innerHTML",
'<font color="#000000">   '.$respxcap.'|'.$pregxcap);
       $objResponse4->assign("global", "innerHTML", " ");
       $objResponse4->assign("globaln", "innerHTML", " ");

             }
       }
return $objResponse4;
```

```
}

public function PerLog($formData){
	$objResponse3 = new xajaxResponse();
	$idcap=0;
	foreach($formData as $key => $value){
		$idcap=substr($value,0,strlen($value)-3);
		$tipuscheck=substr($value,-3);
			if($tipuscheck=='chk'){
				$sql = "INSERT INTO capitols (id_cap,id_excl) VALUES
(".$idcap.",0) ON DUPLICATE KEY UPDATE id_excl=0";
				$this->db->Execute($sql);
				$objResponse3->assign($idcap."id","disabled","disabled");

			}
			if($tipuscheck=='uck'){
			$sql = "INSERT INTO capitols (id_cap,id_excl) VALUES (".$idcap.",1)
ON DUPLICATE KEY UPDATE id_excl=1";
			$this->db->Execute($sql);
			$objResponse3->assign($idcap."id","disabled","disabled");

			}
		}
	return $objResponse3;
}

public function LoadDada($formData){
	$objResponse = new xajaxResponse();
	$opcio="";
	$idprg=0;
	foreach($formData as $key => $value){
		$opcio= $key;
		$idprg=$value;
		$tipusresp=substr($opcio,-6);

	if($tipusresp!="coment" && $tipusresp!="esresp"){
		$vrespupd=substr($opcio,-1);
		switch($vrespupd){
		case ('0'):
		$objResponse->assign($idprg."opcio0","disabled","disabled");
		$objResponse->assign($idprg."opcio1","disabled",false);
		$objResponse->assign($idprg."opcio2","disabled",false);
		$objResponse->assign($idprg."opcio3","disabled",false);
		$objResponse->assign($idprg."opcio4","disabled",false);
		$objResponse->assign($idprg."opcio1","checked",false);
		$objResponse->assign($idprg."opcio2","checked",false);
		$objResponse->assign($idprg."opcio3","checked",false);
		$objResponse->assign($idprg."opcio4","checked",false);
		$objResponse->assign($idprg."prg0","style.color","#DF0101");
		$objResponse->assign($idprg."prg1","style.color","#000000");
		$objResponse->assign($idprg."prg2","style.color","#000000");
		$objResponse->assign($idprg."prg3","style.color","#000000");
		$objResponse->assign($idprg."prg4","style.color","#000000");
		$vres=$vrespupd;
		break;
		case ('1'):
		$objResponse->assign($idprg."opcio0","disabled",false);
		$objResponse->assign($idprg."opcio1","disabled","disabled");
		$objResponse->assign($idprg."opcio2","disabled",false);
		$objResponse->assign($idprg."opcio3","disabled",false);
		$objResponse->assign($idprg."opcio4","disabled",false);
		$objResponse->assign($idprg."opcio0","checked",false);
		$objResponse->assign($idprg."opcio2","checked",false);
		$objResponse->assign($idprg."opcio3","checked",false);
		$objResponse->assign($idprg."opcio4","checked",false);
		$objResponse->assign($idprg."prg0","style.color","#000000");
		$objResponse->assign($idprg."prg1","style.color","#DF0101");
		$objResponse->assign($idprg."prg2","style.color","#000000");
		$objResponse->assign($idprg."prg3","style.color","#000000");
		$objResponse->assign($idprg."prg4","style.color","#000000");
		$vres=$vrespupd;
		break;
		case ('2'):
		$objResponse->assign($idprg."opcio0","disabled",false);
```

```
            $objResponse->assign($idprg."opcio1","disabled",false);
            $objResponse->assign($idprg."opcio2","disabled","disabled");
            $objResponse->assign($idprg."opcio3","disabled",false);
            $objResponse->assign($idprg."opcio4","disabled",false);
            $objResponse->assign($idprg."opcio0","checked",false);
            $objResponse->assign($idprg."opcio1","checked",false);
            $objResponse->assign($idprg."opcio3","checked",false);
            $objResponse->assign($idprg."opcio4","checked",false);
            $objResponse->assign($idprg."prg0","style.color","#000000");
            $objResponse->assign($idprg."prg1","style.color","#000000");
            $objResponse->assign($idprg."prg2","style.color","#FF7F00");
            $objResponse->assign($idprg."prg3","style.color","#000000");
            $objResponse->assign($idprg."prg4","style.color","#000000");
            $vres=$vrespupd;
            break;
            case ('3'):
            $objResponse->assign($idprg."opcio0","disabled",false);
            $objResponse->assign($idprg."opcio1","disabled",false);
            $objResponse->assign($idprg."opcio2","disabled",false);
            $objResponse->assign($idprg."opcio3","disabled","disabled");
            $objResponse->assign($idprg."opcio4","disabled",false);
            $objResponse->assign($idprg."opcio0","checked",false);
            $objResponse->assign($idprg."opcio1","checked",false);
            $objResponse->assign($idprg."opcio2","checked",false);
            $objResponse->assign($idprg."opcio4","checked",false);
            $objResponse->assign($idprg."prg0","style.color","#000000");
            $objResponse->assign($idprg."prg1","style.color","#000000");
            $objResponse->assign($idprg."prg2","style.color","#000000");
            $objResponse->assign($idprg."prg3","style.color","#04B404");
            $objResponse->assign($idprg."prg4","style.color","#000000");
            $vres=$vrespupd+1;
            break;
            case ('4'):
            $objResponse->assign($idprg."opcio0","disabled",false);
            $objResponse->assign($idprg."opcio1","disabled",false);
            $objResponse->assign($idprg."opcio2","disabled",false);
            $objResponse->assign($idprg."opcio3","disabled",false);
            $objResponse->assign($idprg."opcio4","disabled","disabled");
            $objResponse->assign($idprg."opcio0","checked",false);
            $objResponse->assign($idprg."opcio1","checked",false);
            $objResponse->assign($idprg."opcio2","checked",false);
            $objResponse->assign($idprg."opcio3","checked",false);
            $objResponse->assign($idprg."prg0","style.color","#000000");
            $objResponse->assign($idprg."prg1","style.color","#000000");
            $objResponse->assign($idprg."prg2","style.color","#000000");
            $objResponse->assign($idprg."prg3","style.color","#000000");
            $objResponse->assign($idprg."prg4","style.color","#2E2EFE");
            $vres=$vrespupd+1;
            break;
            }
            $objResponse->assign($idprg."esresp","disabled",false);
            $objResponse->assign($idprg."esresp","checked",false);

            $data1=time();
            $data=date ( "H:i      j-m-Y" , $data1 );
            $evol=0;
            $img="equal";
            //resposta anterior per càlcul evolució
      $rant=$this->db->Execute('SELECT id_resp,resposta FROM vrespostes WHERE
id_preg='.$idprg);

      if (!empty($rant->fields['id_resp']) && $vres>$rant->fields['resposta'] && $rant-
>fields['resposta']!=99) {
            $evol=1;
            $img="up";
      }
      if (!empty($rant->fields['id_resp']) && $vres<$rant->fields['resposta'] && $rant-
>fields['resposta']!=99){
            $evol=-1;
            $img="down";
      }
```

```
	$sql = 'INSERT INTO vrespostes (id_preg,id_resp,resposta,usr,evol,data) VALUES
('.$idprg.','.$idprg.','.$vres.',"'.$_SESSION['nom'].'",'.$evol.',"'.$data.'") ON
DUPLICATE KEY UPDATE resposta = '.$vres.', usr= "'.$_SESSION['nom'].'",
evol='.$evol.',data="'.$data.'"';
	$this->db->Execute($sql);

	$objResponse->assign($idprg.'reg', 'innerHTML', '<IMG SRC="imatges/'.$img.'.gif">
      '.$_SESSION['nom'].'     '.$data);
	$objResponse->assign($idprg."reg","style.color","#04B404");

	$ncap=$this->db->Execute('SELECT id_cap, id_quest FROM preguntes WHERE
id_prg='.$idprg);
	$id_quest=$ncap->fields['id_quest'];
	$id_cap=$ncap->fields['id_cap'];

	$npxc=$this->db->Execute('SELECT Count(id_prg) FROM preguntes,capitols WHERE
preguntes.id_cap = capitols.num_cap AND preguntes.id_quest = capitols.id_quest AND
id_subcap = num_subcap AND id_subsubcap = num_subsubcap AND ((preguntes.id_quest
='.$id_quest.') AND (capitols.num_cap='.$id_cap.') AND (capitols.id_excl=0))');
	$pregxcap=$npxc->fields['Count(id_prg)'];

	$nrxc=$this->db->Execute('SELECT Count(id_prg) FROM capitols, preguntes,
vrespostes WHERE preguntes.id_prg = vrespostes.id_preg AND preguntes.id_cap =
capitols.num_cap AND preguntes.id_subcap = capitols.num_subcap AND preguntes.id_subsubcap
= capitols.num_subsubcap AND preguntes.id_quest = capitols.id_quest AND
((preguntes.id_cap='.$id_cap.') AND (preguntes.id_quest='.$id_quest.') AND
(capitols.id_excl=0) AND (vrespostes.resposta!=99))');
	$respxcap=$nrxc->fields['Count(id_prg)'];

	$sumr=$this->db->Execute('SELECT SUM(resposta) FROM capitols, preguntes,
vrespostes WHERE preguntes.id_prg = vrespostes.id_preg AND preguntes.id_cap =
capitols.num_cap AND preguntes.id_subcap = capitols.num_subcap AND preguntes.id_subsubcap
= capitols.num_subsubcap AND preguntes.id_quest = capitols.id_quest AND
((preguntes.id_cap='.$id_cap.') AND (preguntes.id_quest='.$id_quest.') AND
(capitols.id_excl=0) AND (vrespostes.resposta!=99))');
	$sumresp=$sumr->fields['SUM(resposta)'];

	$ind=round($sumresp/$pregxcap,1);

		if($ind<2) $colind="#DF0101";
		if($ind>=2 && $ind<3) $colind="#FF7F00";
		if($ind>=3 && $ind<4) $colind="#04B404";
		if($ind>=4 && $ind<=5) $colind="#2E2EFE";
	$objResponse->assign($id_cap."ind", "innerHTML", "   <input STYLE='background-
color: ".$colind."' type='text' name='instaval' id='instaval' size='1' value='".$ind."'
readonly>");
	if($respxcap!=$pregxcap) $objResponse->assign($id_cap."indnrp", "innerHTML",
'<font color="#DF0101">   '.$respxcap.'|'.$pregxcap);
	if($respxcap==$pregxcap)$objResponse->assign($id_cap."indnrp", "innerHTML", '<font
color="#000000">   '.$respxcap.'|'.$pregxcap);
	$objResponse->assign("global", "innerHTML", " ");
	$objResponse->assign("globaln", "innerHTML", " ");
		}
	}
return $objResponse;
}

private function loadVarMenus($NMenu,$TMenu){

		$menuSec=array('menuSec1','menuSec2','menuSec3','menuSec4','menuSec5');

	$menuPrin=array('menuPrin1','menuPrin2','menuPrin3','menuPrin4','menuPrin5','menuP
rin6');

		if($TMenu=='msec'){
			for($nums=0; $nums<=4;$nums++)
			{
			$this->web->assign('menuPrin',$this->config->menuprin[$NMenu]);
			$this->web->assign($menuSec[$nums],$this->config-
>menusec[$NMenu][$nums]);
			$this->web->assign('menuSecundari','menusec.tpl');
			}
		}
		if($TMenu='mprin'){
```

```
                    for($nump=0; $nump<=5;$nump++)
                    {
                    $this->web->assign($menuPrin[$nump],$this->config->menuprin[$nump]);
                    }
             }
      }

private function controler(){
      $this->web->assign('menuPrincipal', 'menuprincipal.tpl');
      $this->loadVarMenus(0,'mprin');

      if($_GET['action']=='fer_login' || empty($_GET['quest'])){
             if($this->quest==0) {
                    $this->web->assign('contingut','selquest.tpl');
                    $this->ExecControlForms(new Consulta(' ','infoquest', $this->db,'
',$this->config->updoc_dir));
      }else{
             $this->ExecControlForms(new Consulta(' ','infoquest', $this->db,' ',$this-
>config->updoc_dir));
             $this->web->assign('contingut','default.tpl'); //default no existeix!! es
per que no aparegui la plantilla de estats.tpl (verure base.tpl)
             $this->ExecControlForms(new Consulta('id_cap, id_subcap, id_subsubcap,
num_prg','estats', $this->db,$this->quest,$this->config->updoc_dir));
                    }
             }

             if(!empty($_GET['quest'])){
                    $this->web->assign('menuSecundari','menusec.tpl');
                    $this->web->assign('estats','estats.tpl');
                    $this->quest=$_GET['quest'];
                    //$this->ExecControlForms(new Consulta(' ','accio', $this->db,'
',$this->config->updoc_dir));
                    $_SESSION['id_quest']=$this->quest;
                    if($this->quest==0){
                           $this->web->assign('contingut','selquest.tpl');
                    }
             }

             switch($_GET['load'])
             {
                    case ($this->config->menuprin[0]):
                           $this->loadVarMenus(0,'msec');
                           $this->ExecControlForms(new Consulta(' ','infoquest', $this-
>db,' ',$this->config->updoc_dir));
                           if($this->quest!=0 && $_SESSION['rol']!='Admin') {
                                  $this->web->assign('contingut','default.tpl');
                                  $this->ExecControlForms(new Consulta('','estats',
$this->db,$this->quest,$this->config->updoc_dir));
                           }
                           $this->web->assign('contingut','default.tpl'); //default no
existeix!! es per que no aparegui la plantilla de estats.tpl (verure base.tpl)
                           if($_SESSION['rol']=='Admin'){
                           $this->web->assign('contingut','selquest.tpl');
                           $this->ExecControlForms(new Consulta(' ','infoquest', $this-
>db,' ',$this->config->updoc_dir));
                           }
                           break;
                    case ($this->config->menuprin[1]):
                           $this->loadVarMenus(1,'msec');
                           if($this->quest!=0) {
                                  $this->web->assign('contingut','default.tpl');
                                  //if(!empty($_GET['act']))$this->ExecControlForms(new
Consulta(' ','accio', $this->db,$this->quest,$this->config->updoc_dir)); //acció com
etiqueta no taula
                                  $this->ExecControlForms(new Consulta('','estats',
$this->db,$this->quest,$this->config->updoc_dir));
                                  $this->web->assign('contingut','default.tpl');
//default no existeix!! es per que no aparegui la plantilla de estats.tpl (verure
base.tpl)
                                  $this->ExecControlForms(new Consulta(' ','infoquest',
$this->db,' ',$this->config->updoc_dir));
                           }
                           break;
                    case ($this->config->menuprin[2]):
```

```
                        $this->loadVarMenus(2,'msec');
                        if($this->quest!=0) {
                              $this->ExecControlForms(new Consulta('','estats',
$this->db,$this->quest,$this->config->updoc_dir));
                              $this->web->assign('contingut','default.tpl');
//default no existeix!! es per que no aparegui la plantilla de estats.tpl (verure
base.tpl)
                              $this->ExecControlForms(new Consulta(' ','infoquest',
$this->db,' ',$this->config->updoc_dir));
                        }
                        break;
                  case ($this->config->menuprin[3]):
                        $this->loadVarMenus(3,'msec');
                        if($this->quest!=0) {
                              //$this->web->assign('contingut','avaluacio.tpl');
                              $this->ExecControlForms(new Consulta('','estats',
$this->db,$this->quest,$this->config->updoc_dir));
                              $this->web->assign('contingut','default.tpl');
//default no existeix!! es per que no aparegui la plantilla de estats.tpl (verure
base.tpl)
                              $this->ExecControlForms(new Consulta(' ','infoquest',
$this->db,' ',$this->config->updoc_dir));
                        }
                        break;
                  case ($this->config->menuprin[4]):
                        $this->loadVarMenus(4,'msec');
                        if($this->quest!=0) {
                              //$this->web->assign('contingut','avaluacio.tpl');
                              $this->ExecControlForms(new Consulta('','estats',
$this->db,$this->quest,$this->config->updoc_dir));
                              $this->web->assign('contingut','default.tpl');
//default no existeix!! es per que no aparegui la plantilla de estats.tpl (verure
base.tpl)
                              $this->ExecControlForms(new Consulta(' ','infoquest',
$this->db,' ',$this->config->updoc_dir));
                        }
                        break;
                  case ($this->config->menuprin[5]):
                        $this->loadVarMenus(5,'msec');
                        if($this->quest!=0) {
                              //$this->web->assign('contingut','avaluacio.tpl');
                              $this->ExecControlForms(new Consulta('','estats',
$this->db,$this->quest,$this->config->updoc_dir));
                              $this->web->assign('contingut','default.tpl');
//default no existeix!! es per que no aparegui la plantilla de estats.tpl (verure
base.tpl)
                              $this->ExecControlForms(new Consulta(' ','infoquest',
$this->db,' ',$this->config->updoc_dir));
                        }
                        break;

                  case ($this->config->menusec[0][0]):

                        if($this->quest!=0){
                              $this->loadVarMenus(0,'msec');

                              $this->web->assign('contingut','crespquest.tpl');

                              $pregmost=array();
                              if(!empty($_GET['act']))$this->ExecControlForms(new
Consulta(' ','accio', $this->db,$this->quest,$this->config->updoc_dir)); //acció com
etiqueta no taula
                              $this->ExecControlForms(new Consulta('num_cap,
num_subcap, num_subsubcap','capitols', $this->db,$this->quest,$this->config->updoc_dir));
                              $pregmost=$this->ExecControlForms(new Consulta('id_cap,
id_subcap, id_subsubcap, num_prg','preguntes', $this->db,$this->quest,$this->config-
>updoc_dir));
                              $this->ExecControlForms(new Consulta('','estats',
$this->db,$this->quest,$this->config->updoc_dir));
                              $this->ExecControlForms(new Consulta(' ','infoquest',
$this->db,' ',$this->config->updoc_dir));


                              $xajax = new xajax();
```

```
                                    $xajax->setFlag("debug", false);  //Activació debugger
XAJAX

                                    //$pregmost variable recuperada del formulari per crear
tants mètodes i paràmetres com preguntes mostrades

                                    $xajaxMethods=array();
                                          for($nmth=1; $nmth<=$pregmost[0];$nmth++){
                                                $xajaxMethods[$nmth] =& $xajax-
>register(XAJAX_CALLABLE_OBJECT, $this);
                                          }

for($nprm=1; $nprm<=$pregmost[0];$nprm++){
      $xajaxMethods[$nprm]['loaddada']-
>setParameter(1,XAJAX_FORM_VALUES,"formprg".$nprm);
      $xajaxMethods[$nprm]['loadcoment']-
>setParameter(1,XAJAX_FORM_VALUES,"formprg".$nprm);
      $xajaxMethods[$nprm]['esbresposta']-
>setParameter(1,XAJAX_FORM_VALUES,"formprg".$nprm);
}

$xajax->processRequest();

      $xajaxmeth=array(); //array de punters
      $xajaxmeth2=array();
            for($nxmth=1; $nxmth<=$pregmost[0];$nxmth++){
                  $xajaxmeth[$nxmth]=$xajaxMethods[$nxmth]['loaddada']-
>printScript(true);
                  $xajaxmeth2[$nxmth]=$xajaxMethods[$nxmth]['loadcoment']-
>printScript(true);
                  $xajaxmeth3[$nxmth]=$xajaxMethods[$nxmth]['esbresposta']-
>printScript(true);
                  $this->web->assign("xajax_js", $xajax-
>printJavascript("llibreries/xajax05/"));
                  $this->web->assign('MethodData', $xajaxmeth);
                  $this->web->assign('MethodComent', $xajaxmeth2);
                  $this->web->assign('MethodResp', $xajaxmeth3);
            }
            break;
                  case ($this->config->menusec[0][1]):
                  if($this->quest!=0){
                        $this->loadVarMenus(0,'msec');
                        $this->web->assign('contingut','ceditquest.tpl');
                  if(!empty($_GET['act']))$this->ExecControlForms(new Consulta('
','accio', $this->db,$this->quest,$this->config->updoc_dir)); //acció com etiqueta no
taula
                  $this->ExecControlForms(new Consulta('num_cap, num_subcap,
num_subsubcap','capitols', $this->db,$this->quest,$this->config->updoc_dir));
                  $this->ExecControlForms(new Consulta('id_cap, id_subcap,
id_subsubcap, num_prg','preguntes', $this->db,$this->quest,$this->config->updoc_dir));
                  $this->ExecControlForms(new Consulta('','estats', $this->db,$this-
>quest,$this->config->updoc_dir));
                  $this->ExecControlForms(new Consulta(' ','infoquest', $this->db,'
',$this->config->updoc_dir));
                  }
                  break;

                  case ($this->config->menusec[0][2]):

                        if($this->quest!=0){
                              $this->loadVarMenus(0,'msec');
                              $this->web->assign('contingut','defper.tpl');

                              $capmost=array();
                              if(!empty($_GET['act']))$this->ExecControlForms(new
Consulta(' ','accio', $this->db,$this->quest,$this->config->updoc_dir)); //acció com
etiqueta no taula
                              $this->ExecControlForms(new
Consulta('id_obj','objectius', $this->db,$this->quest,$this->config->updoc_dir));
                              $this->ExecControlForms(new Consulta('','estats',
$this->db,$this->quest,$this->config->updoc_dir));
                              $this->ExecControlForms(new
Consulta('id_element','cartografia', $this->db,$this->quest,$this->config->updoc_dir));
```

```
                                    $capmost=$this->ExecControlForms(new Consulta('num_cap,
num_subcap, num_subsubcap','capitols', $this->db,$this->quest,$this->config->updoc_dir));
                                    $this->ExecControlForms(new Consulta(' ','infoquest',
$this->db,' ',$this->config->updoc_dir));


$xajax = new xajax();
$xajax->setFlag("debug", false);  //Activació debugger XAJAX

       //$pregmost variable recuperada del formulari per crear tants mètodes i paràmetres
com preguntes mostrades

$xajaxMethods=array();
for($nmth=1; $nmth<=$capmost[2];$nmth++){
       $xajaxMethods[$nmth] =& $xajax->register(XAJAX_CALLABLE_OBJECT, $this);
}

for($nprm=1; $nprm<=$capmost[2];$nprm++){
       $xajaxMethods[$nprm]['perlog']-
>setParameter(1,XAJAX_FORM_VALUES,"formperlog".$nprm);
       }

$xajax->processRequest();

$xajaxmeth3=array(); //array de punters
for($nxmth=1; $nxmth<=$capmost[2];$nxmth++){
       $xajaxmeth3[$nxmth]=$xajaxMethods[$nxmth]['perlog']->printScript(true);
       $this->web->assign("xajax_js", $xajax->printJavascript("llibreries/xajax05/"));
       $this->web->assign('MethodPerlog', $xajaxmeth3);
}
break;

case ($this->config->menusec[1][0]):

       if($this->quest!=0){
              $this->loadVarMenus(1,'msec');
              $this->web->assign('contingut','avaluacio.tpl');
              if(!empty($_GET['act']))$this->ExecControlForms(new Consulta(' ','accio',
$this->db,$this->quest,$this->config->updoc_dir)); //acció com etiqueta no taula
              $this->ExecControlForms(new Consulta('','estats', $this->db,$this-
>quest,$this->config->updoc_dir));
              $this->ExecControlForms(new Consulta(' ','infoquest', $this->db,' ',$this-
>config->updoc_dir));
              }
              break;
              case ($this->config->menusec[1][1]):
                     if($this->quest!=0){
                            $this->loadVarMenus(1,'msec');
                            $this->web->assign('contingut','historic.tpl');
                            if(!empty($_GET['act']))$this->ExecControlForms(new Consulta('
','accio', $this->db,$this->quest,$this->config->updoc_dir));
                            $this->ExecControlForms(new Consulta('','historic', $this-
>db,$this->quest,$this->config->updoc_dir));
                            $this->ExecControlForms(new Consulta(' ','infoquest', $this-
>db,' ',$this->config->updoc_dir));
              }
              break;

              case ($this->config->menusec[1][2]):
                     if($this->quest!=0){
                            $this->loadVarMenus(1,'msec');
                            $this->web->assign('contingut','plaaccio.tpl');
                            $this->ExecControlForms(new Consulta('num_cap, num_subcap,
num_subsubcap','capitols', $this->db,$this->quest,$this->config->updoc_dir));
                            $pregmost=$this->ExecControlForms(new Consulta('id_cap,
id_subcap, id_subsubcap, num_prg','preguntes', $this->db,$this->quest,$this->config-
>updoc_dir));
                            $this->ExecControlForms(new Consulta(' ','infoquest', $this-
>db,' ',$this->config->updoc_dir));

              }
              break;

              case ($this->config->menusec[2][0]):
```

```
                        if($this->quest!=0){
                                $this->loadVarMenus(2,'msec');
                                $this->web->assign('contingut','metode.tpl');
                }
                break;

                case ($this->config->menusec[2][1]):
                        if($this->quest!=0){
                                $this->loadVarMenus(2,'msec');
                                $this->web->assign('contingut','guia.tpl');
                }
                break;
                }

                $this->web->display("base.tpl");
                //arranca manual la consola del samrty debugger
                //$this->web->display("debug.tpl");


        }
}

?>
```

Annex C: Qüestionari SIS.

Qüestionari SIS

Àlex Pérez, Pere Ponsa

ID Subjecte: Anton Gomà Data d'avaluació: Abril 2010

N. Document: Títol document: Eina Suport Auditoria Seguretat Sistemes d'informació.

A continuació, li preguem la seva col·laboració per a respondre a aspectes relacionats amb l'activitat que es porta a terme en el SAF i a la tasca de seguretat dels sistemes de la informació; expliqui o digui quina de les opcions s'adiu més amb la seva percepció, segons la pregunta.

1. Quina és la seva activitat principal en el Servei d'Activitat Física?

Direcció de la unitat de sistemes

2. Descrigui breument en què consisteix la seva activitat.

Assegurar el correcte funcionament de les infraestructures informàtiques, cobrir noves necessitats, i gestió dels recursos humans assignats.

3. Desenvolupa activitats sobre seguretat dels sistemes d'informació en el SAF?

1 ☒ SI 2 ☐ NO

4. En cas de resposta afirmativa a la pregunta 3: Quina part de la seguretat considera més rellevant?

Garantir la continuïtat dels sistemes crítics i garantir la integritat de les dades.

5. La tasca a fer sobre el qüestionari de seguretat era difícil d'entendre.
On la puntuació 1 seria "molt difícil d'entendre" i la 4 "molt fàcil d'entendre".

1 ☐ Era molt difícil d'entendre 2 ☐ Era difícil d'entendre 3 ☒ Era fàcil d'entendre 4 ☐ Era molt fàcil d'entendre

6. La tasca ha fer en el qüestionari ha estat llarga.
On la puntuació 1 seria "molt llarga" i la 4 "molt curta".

1 ☐ Ha estat molt llarga 2 ☒ Ha estat llarga 3 ☐ Ha estat curta 4 ☐ Ha estat molt curta

7. M'he sentit confós, sense tenir clar que havia de fer.
On la puntuació 1 seria "no tenia gens clar el que havia de fer" i la 4 "tenia molt clar el que havia de fer".

1 ☐ No tenia gens clar el que havia de fer 2 ☐ No tenia clar el que havia de fer 3 ☒ Tenia clar el que havia de fer 4 ☐ Tenia molt clar el que havia de fer

8. He hagut d'estar molt concentrat per fer eficaçment la tasca en el qüestionari.
On la puntuació 1 seria "molt concentrat" i la 4 "gens concentrat".

1 ☐	2 ☒	3 ☐	4 ☐
He hagut d'estar molt concentrat	He hagut d'estar concentrat	No he hagut d'estar gaire concentrat	No he hagut d'estar gens concentrat

9. M'he sentit pressionat pel temps
On la puntuació 1 seria "molt pressionat" i la 4 "gens pressionat".

1 ☐	2 ☐	3 ☒	4 ☐
M'he sentit molt	M'he sentit pressionat pel temps	No m'he sentit gaire pressionat pel temps	No m'he sentit gens pressionat pel temps

10. Penso que la meva realització sobre el qüestionari ha estat correcta
On la puntuació 1 seria "molt correcta" i la 4 "gens correcta".

1 ☐	2 ☒	3 ☐	4 ☐
La meva realització ha estat molt correcta	La meva realització ha estat correcta	La meva realització no ha estat gaire correcta	La meva realització no ha estat gens correcta

11. Valori la qualitat de l'aplicació informàtica en la que s'ha desenvolupat el qüestionari
On la puntuació 1 seria "baixa" i la 4 "molt bé".

1 ☐	2 ☐	3 ☐	4 ☒
Baixa	Regular	Bé	Molt bé

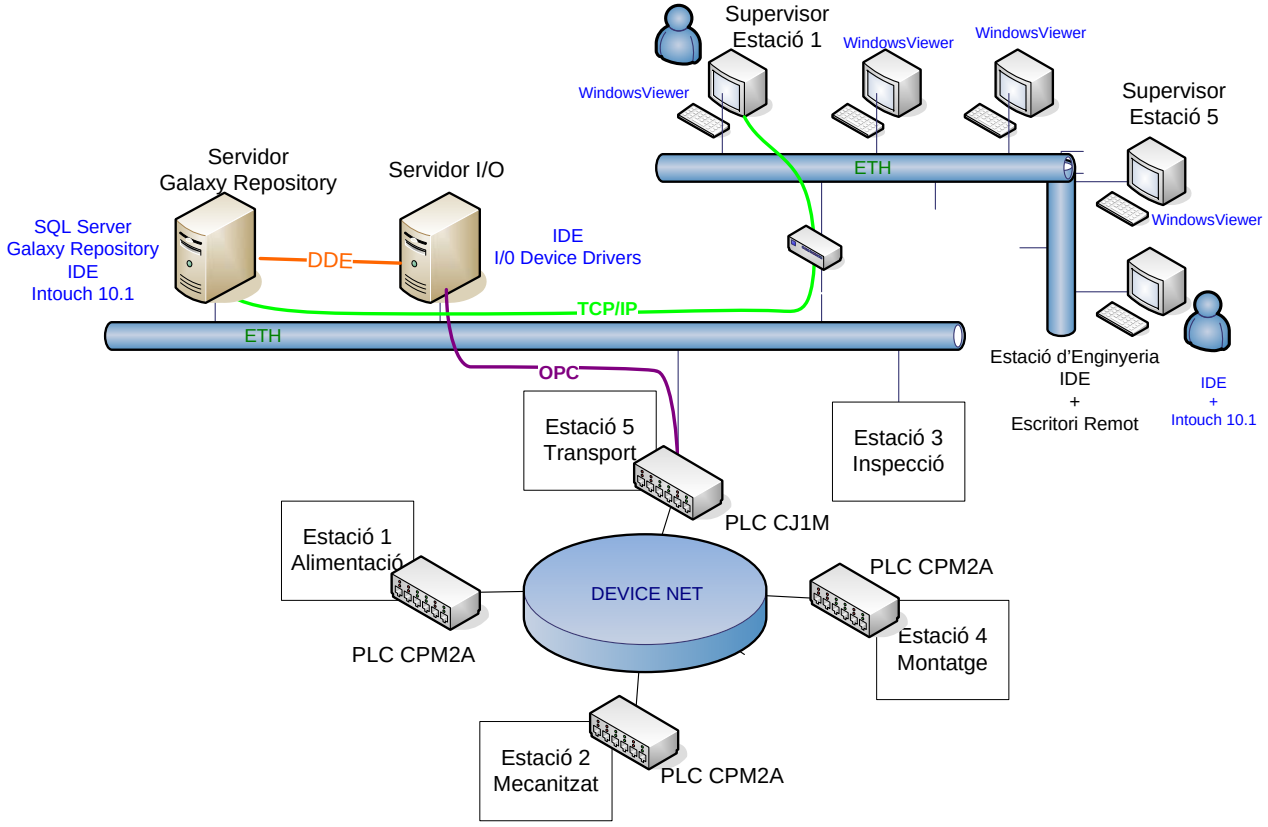
12. Com a usuari/a d'aquesta aplicació informàtica: voldria proposar algun canvi per a la millora del disseny?

Assegurar que pel criteri de resposta primera= poc acompliment, últimes=major acompliment, es manté al llarg de tot el qüestionari.

Annex D: Enginyeria en Automàtica i Electrònica Industrial.

Dins els estudis de segon cicle Enginyeria en Automàtica i Electrònica Industrial del centre EPSEVG s'ha cursat l'assignatura Sistemes de Producció Integrats. En aquesta assignatura es fa una introducció al sistemes automatitzats, la seva supervisió i el lligam amb la gestió de la producció des d'un punt de vista d'organització de l'empresa. En concret, aspectes de sistemes de supervisió (SCADA), execució de la fabricació (MES), gestió de la Producción (ERP) i sistemes de suport a la decisió (DSS).

Per aprofundir en la integració vertical d'aquest nivells, cal disposar d'una plataforma que permeti simplificar programaris de cases comercials diferents i permetin un flux d'informació clar des del nivell de planta fins al nivell de gestió. Mitjançant l'entorn de programació, es treballa en el Laboratori de sistemes de Producció per la posta en marxa d'una plataforma (veure figura següent) que permeti aquesta integració.



L'autor d'aquest PFC ha treballat en aquesta primera fase en la que s'integrin supervisió i automatització. Deixant per més endavant la incorporació de programaris per a la gestió de la producció. Més endavant, fins i tot es podria aplicar l'auditoria explicada en aquest projecte, dins el sistema de producció acadèmic.

Annex E: Article:

Diseño de herramienta de evaluación del grado de cumplimiento de normativas en el ámbito de la interacción entre personas y la gestión de los sistemas de información

Álex Pérez
Depto I. de Sistemas, Automática e Informática Industrial, Escuela Politécnica Superior de Ingeniería de Vilanova i la Geltrú, 08800 Vilanova i la Geltrú, alex.perez@estudiant.upc.edu

Pere Ponsa
Depto Ingeniería de Sistemas, Automática e Informática Industrial, Escuela Politécnica Superior de Ingeniería de Vilanova i la Geltrú, 08800 Vilanova i la Geltrú, pedro.ponsa@upc.edu

Ramon Vilanova
Departament de Telecomunicació i Enginyeria de Sistemes Edifici Q, ETSE Universitat Autònoma de Barcelona, 08193 Bellaterra ramon.vilanova@uab.cat

Resumen

En este artículo se propone un acercamiento entre la interacción persona ordenador y la gestión de los sistemas de información. Se describe una herramienta, desarrollada en lenguaje PHP y soportada por una base de datos MySQL, para la autoevaluación del grado de cumplimiento de normativas estándares, guías o especificaciones de buenas prácticas, que contempla diversas funcionalidades cómo la automatización de la recogida de datos, el seguimiento para la valoración de mejora de los sistemas y la evaluación de la usabilidad y la experiencias de usuario. La finalidad es aplicar esta metodología para poner énfasis en los aspectos humano/sociales del uso de sistemas, y en una primera aproximación se aborda el ámbito de de la gestión de sistemas automatizados en el dominio industrial.

1. Introducción

Por gestión de sistemas de información entendemos un sistema integrado persona-máquina que provee información para dar soporte a la operación, la gestión y la toma de decisiones en una organización [1]. Algunos autores defienden la gestión de los sistemas de información (MIS) como un área interdisciplinar que aúna los conocimientos de la teoría de sistemas, la teoría de control, matemática económica y otras relacionas con la tecnología, la computación y las ciencias sociales. Estas últimas áreas permiten un acercamiento entre la gestión de los sistemas de información y la interacción persona ordenador. Desde el año 2001 el grupo de interés especial en HCI de la *Association for Computing Machinery* ACM, el denominado SIGCHI, creó la asociación para los sistemas de información AIS SIGCHI, de manera que se vertebra la relación entre HCI y ASI (ver Figura 1) y se ilustra cómo incorporar HCI en los planes de estudio de las titulaciones de gestión [2]. En la sinergia entre HCI y MIS se concibe un marco de investigación en el que confluyen la persona, la

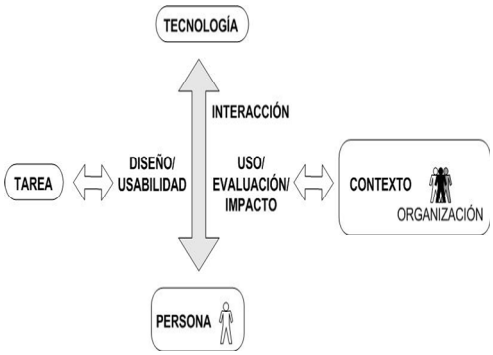


Figura 1. En la sinergia entre HCI y AIS es necesario tener en cuenta el contexto (organizacional, social, global)

tecnología, la tarea, el contexto de uso y la interacción entre persona y tecnología [3]. Por tecnología se entiende aquí todo tipo de hardware, software, aplicaciones, datos, información, conocimiento y procedimientos. Y en concreto se pone especial énfasis en el ámbito de negocio, gestión, organización y contextos culturales [4].

En los siguientes apartados se presenta una metodología que permita fortalecer aspectos de ergonomía, usabilidad y diseño centrado en el usuario en un ámbito de la gestión de los sistemas de información. La sección dos muestra la adaptación de normativas a cuestionarios. La sección tres presenta como ejemplo práctico la creación de herramienta en soporte digital de la guía ergonómica para el diseño de interfaz (guía GEDIS). La sección cuatro muestra cómo preparar la evaluación y el seguimiento de la valoración. La sección cinco indica aspectos de implantación técnica. Finalmente las conclusiones y las líneas futuras de trabajo.

1. Adaptación de normativas

En el mundo empresarial es muy común la necesidad de estudiar el grado de cumplimiento de normativas estándares, códigos de buenas prácticas o guías de implantación y diseño. Por ejemplo, en el caso previo a una certificación ISO en Seguridad de los sistemas de Información, las empresas, directivos o responsables de departamento, es muy probable que necesiten saber cuál es el grado de cumplimiento de su organización con relación a la norma ISO/IEC 27002:2005 [3] (Código de buenas prácticas para la Seguridad de los Sistemas de Información) antes de realizar la inversión en la certificación. O en otro ejemplo, una empresa industrial, es posible que necesite saber si el diseño del sistema de supervisión de su planta de producción, especificado por el proveedor, cumple con la guía GEDIS [5] (Guía Ergonómica para el Diseño de Interfaces de Supervisión) antes de realizar el pedido o validar la entrega. En cualquiera de estos casos, una autoevaluación previa del grado de cumplimiento de las normativas de las cuales se pretende tener la certificación o conocer el grado de implantación de una aplicación con relación a la guía de diseño o un estándar, puede suponer un gran ahorro económico para la empresa, ya sea directamente por la optimización de las inversiones, por un mejor retorno de inversión al mejorar la calidad de las implantaciones o por el ahorro del tiempo que le supone a una organización el hecho de realizar correcciones o modificaciones sobre implantaciones ya entregadas pero no válidas. Si volvemos a los ejemplos anteriores, podemos intuir fácilmente los perjuicios obtenidos si el proceso de certificación no se puede completar al no estar la organización al nivel de cumplimiento necesario o si la interfaz de supervisión puesta en producción fuera necesario modificarla porque el diseño de algunas de sus pantallas o funciones no son las adecuadas y entorpecen la tarea de los operarios de supervisión.

La problemática que una empresa pueda tener al realizar una autoevaluación del grado de cumplimiento de su organización, sistema o aplicación con relación a una normativa, guía de implantación o estándar, la encontramos en que, este tipo de documentos suelen ser extensos y de difícil interpretación y adaptación a las especificidades de la empresa, siendo frecuentemente necesaria la participación (contratación) de un experto auditor para la realización del informe de evaluación correspondiente. Con lo cual, también con frecuencia, la empresa opta por asumir los riesgos de iniciar la inversión sin auditoría previa y los costes de posibles rectificaciones.

La solución a esta problemática pueden ser los cuestionarios de evaluación adaptados en forma de una herramienta útil. Esta herramienta deberá poner a disposición del usuario (evaluador, diseñador, gestor) los estándares, normativas, guías, etc. adaptados y formateados en cuestionarios, de forma que las respuestas recopiladas puedan ser evaluadas, y en función de las mismas, se plasme un seguimiento de la mejora del funcionamiento de los sistemas, una evaluación global y un plan de acción inmediato para corregir funcionamientos anómalos. El trabajo de adaptación y formateo del documento o normativa hace posible que la evaluación sea realizada en el seno de la empresa sin la participación de un auditor experto e incluso facilita que la empresa se introduzca en modelos de calidad sin que ello signifique una gran inversión en recursos humanos y tecnológicos.

Las funciones propias de la aplicación, automatizan la recopilación de las respuestas de los usuarios, consolidación de los datos, evaluación instantánea y detallada, registro de históricos y un seguimiento de la evolución para la mejora continua.

Una vez puesta en marcha esta metodología, queda perfectamente incorporada a los quehaceres de la organización, de manera que se facilita una dirección de trabajo hacia la certificación en estándares de calidad. En este marco de trabajo hay que remarcar la importancia del diseño centrado en el usuario desde las primeras fases del proyecto, por lo que es importante remarcar la colaboración entre expertos en psicología, ergonomía, diseño, interacción y gestión entre otros.

Otra vía de aplicación de la herramienta de cuestionarios es el tratamiento de un conjunto de heurísticos y su evaluación mediante métricas. En concreto estamos trabajando en la versión electrónica de la guía GEDIS, en cómo incorporar las respuestas de diversos evaluadores y a partir de aquí extender el método a incluir la metodología de estudios de usabilidad [6] (análisis de requerimientos CISU-R, informe CIF) y encuestas de satisfacción (usuario del sistema, gestor del sistema). En este caso, la herramienta permite la edición del estudio o encuesta, recopilación de respuestas de forma simultánea a múltiples usuarios (en función de las especificaciones del estudio de usabilidad o encuesta de satisfacción), consolidación de los datos, evaluación, estadísticas y gráficas.

En los apartados siguientes, se describe el método utilizado para la adaptación de los documentos y normativas en cuestionarios de evaluación, la ponderación y consolidación de datos en función del tipo de proyecto y la función de evaluación detallada para la realización de un plan de acción. También se describirán las funciones y la implantación técnica de la herramienta así como las posibles evoluciones.

Estos conceptos son genéricos y para aportar estudios de casos concretos veremos la aplicación en un caso práctico basado en la implantación de la guía GEDIS.

1. Método de Adaptación

La función principal de la herramienta es poner a disposición de la empresa un cuestionario con relación a una normativa, estándar o guía de diseño de forma que el evaluador pueda interactuar con el mismo aportando respuestas, documentos y comentarios. Por tanto, el trabajo de conversión del documento a un cuestionario que nos dé una evaluación eficaz de cada uno de los capítulos tratados, será el más importante por parte del editor de la herramienta.

La primera tarea será identificar en la normativa, estándar o guía los objetivos de control, es decir, dividir el documento en los diferentes apartados de los cuales necesitamos tener una evaluación. Estos objetivos de control los convertiremos en los capítulos del cuestionario de evaluación. La segunda tarea será identificar los controles o indicadores a evaluar. De cada uno de los objetivos de control, qué puntos son necesarios superar para cumplir con el objetivo. Estos controles o indicadores los transcribiremos en las diferentes preguntas del cuestionario de evaluación. La figura 2 describe cómo podemos estructurar el documento estándar, guía o normativa para convertirlo en un cuestionario de evaluación.

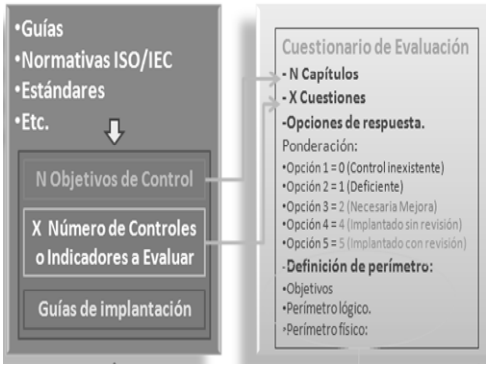


Figura 1. Conversión documento estándar a cuestionario de evaluación

A modo de ejemplo, en el caso práctico de implantación de la guía GEDIS sobre el diseño de una interfaz de supervisión determinada, las tareas de identificación de los objetivos de control y los

diferentes controles o indicadores nos vienen dados por la tabla de indicadores descrita en la misma guía. En la Tabla 1 se numeran cinco de los diez indicadores que contiene la guía GEDIS.
En el ejemplo, los objetivos de control están marcados en negrita (Estructura, Distribución, navegación…) y los controles son cada uno de los sub-indicadores. En el caso del objetivo Estructura, necesitamos evaluar la existencia de mapas, número de niveles y división. De esta forma, la conversión del objetivo de control de Estructura a un cuestionario de evaluación seria como se muestra en la Figura 3.

Para la migración de encuestas de satisfacción, como por ejemplo la escala SUS, las tareas de identificación de los objetivos de control e indicadores para su posterior conversión a un cuestionario de evaluación, no son necesarias, ya que la propia encuesta define claramente al cuestionario de evaluación [7].

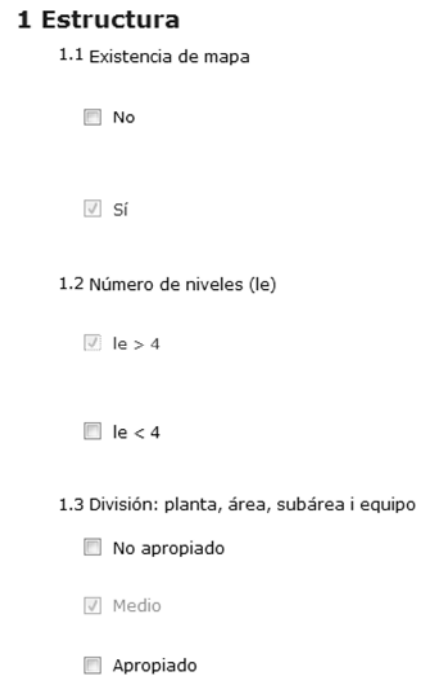


Figura 1. Cuestionario de evaluación Indicador Estructura (guía GEDIS)

Nombre_indicador y nombre_subindicador	Rango numérico/cualitativo y valor numérico	
Estructura	**1,7**	
Existencia de mapa	[SI, NO] [5, 0]	0
Número de niveles le	[le<4, le>4] [5, 0]	0
División: planta, área, subárea, equipo	[a, m, na] [5, 3, 0]	5
Distribución	**3**	
Comparación con modelo	[a, m, na] [5, 3, 0]	3
Flujo del proceso	[claro, medio, no claro] [5, 3, 0]	3
Densidad	[a, m, na] [5, 3, 0]	3
Navegación	**3**	
Relación con Estructura	[a, m, na] [5, 3, 0]	3
Navegación entre pantallas	[a, m, na] [5, 3, 0]	3
Color	**5**	
Ausencia de combinaciones no apropiadas	[SI, NO] [5, 0]	5
Número de colores c	[4<c<7, c>7] [5, 0]	5
Ausencia de intermitencia (caso sin alarma)	[SI, NO] [5, 0]	5
Contraste entre fondo pantalla y los objetos gráficos	[a, m, na] [5, 3, 0]	5
Relación con Texto	[a, m, na] [5, 3, 0]	5
Texto	**3,2**	
Número de fuentes f	[f<4, f>4]	5
Ausencia de fuentes pequeñas (mínima fuente 8)	[SI, NO] [5, 0]	0
Ausencia de combinaciones no apropiadas	[SI, NO] [5, 0]	5
Uso de abreviaciones	[a, m, na] [5, 3, 0]	3

Tabla 1. Resumen de indicadores de la guía GEDIS

1. Evaluación

Se recomienda utilizar la guía GEIDS en las primeras fases del diseño de una interfaz. En otras situaciones, puede aplicarse la guía GEDIS a una interfaz creada por terceros y que ya esté en desarrollo. En estos casos se recomienda un conjunto de evaluadores externos (3 personas por ejemplo) que sean las encargadas, por separado, de aplicar la guía GEDIS. De forma global puede realizarse una valoración media entre estos evaluadores. En caso de duda de cómo proceder ante la respuesta a un sub-indicador puede ser necesario la intervención del personal que trabaja directamente con la interfaz.

Cada pregunta dispone de dos a cinco opciones de respuestas ponderadas de 0 a 5. La ponderación por defecto es lineal, aunque otro tipo de ponderaciones pueden ser aplicadas en función del proyecto tratado. A su vez, cada uno de los capítulos puede tener una ponderación determinada (peso), con relación al resto de capítulos, en función de la implantación evaluada. Las ponderaciones se definirán durante el proceso de edición del cuestionario de evaluación. Siguiendo el caso práctico de implantación de la guía GEDIS, en la Tabla 1 se indica las ponderaciones de cada una de las respuestas de los diferentes sub-indicadores (Rango numérico/cualitativo y valor numérico). El capítulo Estructura podría tener, por ejemplo, un peso de 1.5, el de Distribución 0.5 y el resto de 1, sí se quisiera dar más importancia a los aspectos de estructura que a los de distribución, durante el diseño de una interfaz determinada.

1.1. Evaluación por capítulo

En función de las respuestas dadas, la ponderación aplicada y el número de preguntas, obtendremos la evaluación por capítulo aplicando la siguiente fórmula:

$$Evaluación\ \ Capítulo = \frac{\sum_{i=1}^{n} valor\ respuesta_i}{n} \qquad (1)$$

Donde *n* es el número de preguntas del capítulo evaluado.

Esta valoración cuantitativa nos indicará si es necesario o no actuar sobre los indicadores del objetivo de control (capítulo) tratado antes de iniciar una inversión, ya sea en una certificación o en un desarrollo.

Siguiendo el ejemplo, la evaluación para el capítulo estructura sería:

$$Ev.\ Estructura = \frac{5+0+3}{3} = 2{,}7$$

Esta puntuación nos indica que es necesario mejorar el diseño reduciendo a menos de 4 el número de niveles de la estructura de la interfaz, antes de validar el desarrollo.

1.2. Evaluación global

En función del número de capítulos, de la evaluación y del peso de cada uno de ellos, obtenemos la evaluación global aplicando la siguiente fórmula:

$$Ev.\ Global = \frac{\sum_{j=1}^{c} p_j \cdot Ev.Capítol}{\sum_{j=1}^{c} p_j} \qquad (2)$$

Donde *c* es el número total de capítulos y P_j es el peso correspondiente al capítulo.

Esta puntuación nos puede servir para el seguimiento de la evaluación del proyecto. En la Figura 4 se muestra un ejemplo de la función de evaluación para un proyecto de desarrollo de interfaz de supervisión aplicando la guía GEDIS. Donde *nºR*, es el número de respuestas, *nºC*, el número de controles por capítulo, *aval*, la evaluación por capítulo y *Global*, la evaluación global del proyecto.

Figura 1. Función de evaluación, ejemplo guía GEDIS

En el caso de los estudios de usabilidad y de encuestas de satisfacción, las evaluaciones por capítulos y globales quedarán definidas por el propio estudio, teniendo en cuenta, el número de muestras (cuestionarios respondidos).

La herramienta debe ofrecer la posibilidad de seleccionar el tipo de evaluación en función del proyecto tratado. Para un estudio de usabilidad o encuesta de satisfacción se está valorando cómo incorporar las métricas oportunas.

1.1. Proceso de mejora continua.

La herramienta ofrece una recopilación de la evaluación cualitativa de cada uno de los controles de forma que, de la misma, se pueda extraer un plan de acción para la mejora del proyecto o la toma de decisiones previas a iniciar un procedimiento de certificación o desarrollo.

En la Figura 5 vemos un ejemplo correspondiente a la aplicación de la guía GEDIS a un desarrollo de interfaz de supervisión. En el ejemplo, están indicados con un círculo negro aquellos indicadores sobre los cuales será necesario actuar para la mejora o validación del proyecto.

1	**Estructura**	
1.1	Existencia de mapa	✓
1.2	Número de niveles (le)	●
1.3	División: planta, área, subárea i equipo	○
2	**Distribución**	
2.1	Comparación con modelo	○
2.2	Flujo de proceso	✓
2.3	Densidad	●
3	**Navegación**	
3.1	Relación con la estructura	○
3.2	Navegación entre pantallas	●
4	**Color**	
4.1	Ausencia de combinaciones no apropiadas	●
4.2	Número de colores (c)	●
4.3	Ausencia de intermitencia (caso sin alarma)	●
4.4	Contraste entre fondo de pantalla y los objetos graficos	○
4.5	Relación con Texto	○
5	**Texto**	
5.1	Número de fuentes (f)	✓
5.2	Ausencia de fuentes pequeñas (mínima fuente 8)	●
5.3	Ausencia de combinaciones no apropiadas	✓
5.4	Uso de abreviaciones	○

Figura 1. Ejemplo evaluación detallada: aplicación guía GEDIS

El objetivo de la evaluación detallada es servir de soporte para la creación de un plan de acción para la mejora del sistema evaluado. En ocasiones, según la complejidad del proyecto o cuestionario de evaluación, la conversión de la evaluación detallada a un plan de acción será inmediata, en otras, será necesario realizar un estudio de la evaluación detallada para analizar las prioridades. En el siguiente ejemplo, para la mejora del grado de cumplimiento de una organización con relación a la norma ISO/IEC 27002:2005 (Seguridad de los Sistemas de Información) [3], se realizó el estudio representado en el diagrama de la figura 6.

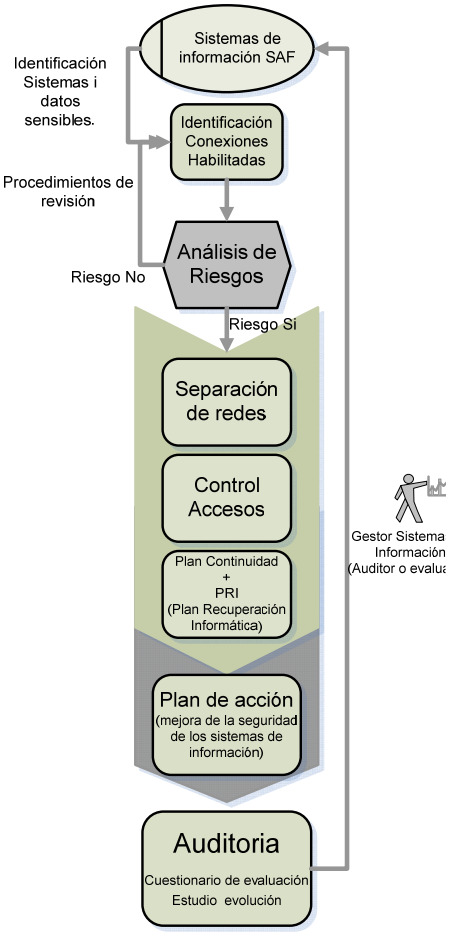


Figura 2. Ejemplo estudio evaluación detallada: aplicación ISO/IEC 27002:2005

En primer lugar, el gestor de los sistemas de información (rol de Auditor o evaluador) responde al cuestionario de evaluación correspondiente a la norma ISO/IEC 27002:2005 para la gestión de la Seguridad de los sistemas de información. Destacar que este cuestionario cuenta con 10 capítulos y 153 objetivos de control, por tanto, este proceso puede durar varias semanas en función de la disponibilidad de la información a recopilar y los recursos utilizados. En segundo lugar, al completar el cuestionario, disponemos de la evaluación global, por capítulos y detallada en cuanto al grado de cumplimiento de nuestra organización con relación a la norma ISO/IEC 27002:2005. En este punto, y antes de realizar el estudio de la evaluación, el gestor tiene que tener claramente identificados los objetivos de seguridad y los sistemas e informaciones sensibles para los cuales se lleva a cabo la evaluación. En el ejemplo que nos ocupa (figura 6), el gestor fijó los objetivos de continuidad del los servicios de negoció y la preservación de los datos personales (Asegurar el cumplimiento de la ley de protección de datos personales). La herramienta de evaluación dispone de una función (Definición de Perímetro) para la definición de los objetivos i la descripción de los sistemas e informaciones sensibles. Seguidamente, con el soporte de la evaluación detallada, se realiza un análisis de riesgos. Es decir, para cada uno de los controles detectados como deficientes o no implantados, analizar sí afectan negativamente a la consecución de los objetivos prefijados. En nuestro ejemplo, del análisis de riesgos, se detectó que era prioritario actuar sobre los siguientes aspectos: Separación de las redes ofimática e industrial, control de accesos y confección de un plan de contingencia (Plan de continuidad del negoció en modo degradado y plan de recuperación informática). Tras la definición de los aspectos prioritarios a tratar y, una vez más, con el soporte de la evaluación detallada, se confecciona el plan de acción con las actuaciones concretas a realizar para la mejora de los controles deficientes o la implantación de los controles inexistentes. La definición de la tarea a realizar queda definida por el propio título del control en la evaluación detallada. En el caso de evaluación de normas ISO/IEC, contamos también con las guías de implantación descritas para cada uno de los controles, dónde se detallan las tareas precisas para cumplir con el objetivo de control. Ejecutado el plan de acción, el gestor de los sistemas de información está en disposición de realizar una nueva auditoría retomando el cuestionario de evaluación para recoger en él las mejoras realizadas. Con la nueva evaluación, el gestor puede reiniciar el proceso descrito anteriormente para la evaluación y mejora continuada de la seguridad de sus sistemas de información.

De forma genérica y a modo de resumen, en el diagrama de la figura 7 se describe el proceso de mejora continua destacando los roles de interactuación de la persona con el sistema de evaluación.

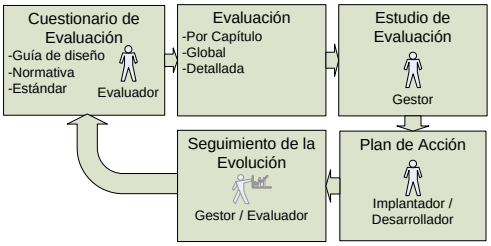


Figura 1. Diagrama proceso mejora continua.

Para el seguimiento de la evolución de un proyecto, la herramienta dispone de la función de históricos, dónde se recopilan las evaluaciones por capítulos y global de las evaluaciones realizadas. En la figura 8 tenemos un ejemplo de la función de históricos para el de seguimiento de la evolución en un proyecto de diseño de interface de supervisión aplicando la guía GEDIS.

	Capítol	nºR	nºC	nºO	aval	ev	nºR	nºC	nºO	aval	ev
1	Estructura	3	3		2.7	➡	3	3		4.3	⬆
2	Distribución	3	3		3.7	➡	3	3		3.7	➡
3	Navegación	2	2		4	➡	2	2		4	➡
4	Color	5	5		4.2	➡	5	5		4.2	➡
5	Texto	4	4		1.2	➡	4	4		4.5	⬆
6	Estado de los dispositivos	2	2		4	➡	2	2		4	➡
7	Valores de proceso	2	2		3	➡	2	2		3	➡
8	Graficos y Tablas	4	4		2.2	➡	4	4		3	⬆
9	Comandos de Entrada de Datos	3	3		3.7	➡	3	3		3.7	➡
10	Alarmas	5	5		3.8	➡	5	5		3.8	➡
	Global:	33	33		3.21	➡	33	33		3.85	⬆

Figura 2. Ejemplo seguimiento evolución implantación guía GEDIS.

1. Implantación técnica

El cuestionario de un proyecto en concreto queda a disposición (online) de los usuarios (evaluadores) a través de un servidor Web (apache) que ejecuta PHP [8]. Cuando el usuario responde a cada una de las preguntas, las respuestas son registradas en la base de datos MySql [9] instantáneamente y síncronamente gracias a la clase XAJAX [10] de PHP. Las funciones de evaluación desarrolladas en PHP se encargan de realizar los cálculos necesarios para poner a disposición del usuario auditor (responsable del proyecto) las evaluaciones por capítulo, global y detallada, de forma que, éste pueda realizar la toma de decisión, la mejora continua o el plan de acción que corresponda.

En estos momentos los Servicios de Tecnología de la Información y la Comunicación de nuestro centro universitario nos han facilitado la puesta en marcha de la herramienta en un servidor del centro. Hemos incorporado y desarrollado la adaptación de la norma ISO/IEC 17799:2005 (Seguridad de los Sistemas de Información) y la guía GEDIS.

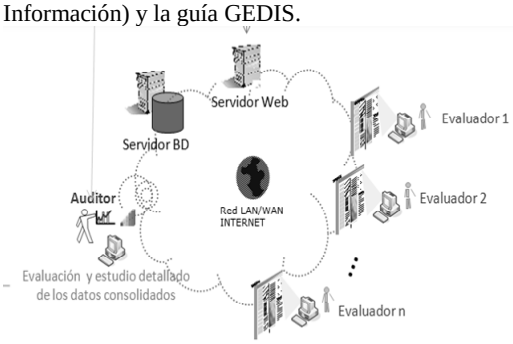


Figura 1. Esquema implantación técnica

Las empresas que están respondiendo al cuestionario relacionado con la seguridad son el Servicio de Actividad Física SAF de la Universidad Autónoma de Barcelona UAB y el Servicio STIC de nuestro centro docente.

En el caso de la entidad SAF, ésta actúa en el rol de empresa vinculada a la UAB y presta servicio a los usuarios (estudiantes, profesores, personal de administración) que utilizan las instalaciones deportivas del campus. EL SAF se encarga de la gestión de los sistemas automatizados, acceso de los usuarios, mantenimiento de las instalaciones. Desde la Universitat Politécnica de Catalunya, en los últimos tres años les hemos prestado soporte también en el ámbito de la mejora de interfaz de supervisión mediante la aplicación de la guía GEDIS, entrevista con los gestores, análisis de requerimientos, rediseño de sala de control y valoración de la satisfacción de los gestores.

La valoración de la seguridad de los sistemas de información en los servicios TIC de nuestro centro universitario permiten que el responsable acceda a una funcionalidad con poca inversión de recursos y permite una incursión en la mejora de la calidad de los sistemas informáticos.

2. Conclusiones

En el presente trabajo se ha buscado potenciar la sinergia entre la interacción persona ordenador y la gestión de los sistemas de información. La introducción del diseño centrado en el usuario permite introducir con facilidad funcionalidad HCI dentro de la gestión de las organizaciones.
El favorecer el diseño ergonómico, la seguridad de los sistemas de información, la evaluación de la usabilidad, la valoración de la satisfacción dentro del ciclo de vida de procesos y productos permite incorporar elementos que redundan en la mejora de la calidad de los sistemas y aportan de forma clara un marco de colaboración entre profesionales de distintas áreas.

Este acercamiento está planteado de forma sistemática genérica. Así por ejemplo, la herramienta para la valoración de la seguridad de los sistemas de información creada se adapta con facilidad a la organización que la necesita (en este trabajo la hemos presentado para los servicios SAF y STIC).

Tras el esfuerzo inicial de conversión de los documentos estándares, normativas o guías a cuestionarios de evaluación siguiendo el método descrito, éstos pueden ponerse a disposición de las empresas de forma que puedan auto-auditarse con relación a un proyecto especifico, previo al inicio del proceso de certificación o validación del desarrollo.

El primer autor de este trabajo está en estos momentos colaborando con el gestor principal del SAF para poner en marcha a corto plazo un plan de acción de mejora de los servicios, gracias a la metodología desarrollada en este trabajo.

Agradecimientos

Los autores agradecen la ayuda económica de la Universitat Politécnica de Catalunya. Proyecto: Diseño centrado en el usuario en sistemas de control supervisado.

Los autores agradecen a David Raya y Rubén Menéndez de los Servicios STIC de la Universitat Politécnica de Catalunya su apoyo para la puesta en marcha de la herramienta citada en este trabajo. Y a Antón Gomà, gestor de los servicios SAF por su colaboración en la aplicación de la herramienta en un entorno real de funcionamiento.

Referencias

[1] Davis, G.B. Management Information Systems: conceptual foundations, structure and development. McGraw-Hill, New York. 1974

[2] Carey, J., Galleta, D., Kim, J., Te'eni, D., Wildemuth, B., Zhang, P. The role of human-computer interaction in management information systems curricula: a call to action. Communications of the Association for Information Systems, Vol 13, pp. 357-379, 2004

[3] Zhang, P., Nah, F., Preece, J. HCI studies in Management Information Systems. Behaviour & Information Technology, V 23, Nº 3, pp. 1-13, 2004

[4] Association for Information Systems. En URL: http://www.linknet1.com/sighci/. Última visita: 27/mayo/2010

[5] ISO. ISO/IEC 17799. Information technology-Security Techniques – Code of practices for information security management, 2005

[6] Ponsa, P., Amante, B., Díaz, M. Ergonomic design applied in a sugar mill interface. Latin American Applied Research Journal, Vol 40, N 1,, pp. 27.34, 2010

[7] ISO. ISO/IEC 25062 Software engineering, software product quality requirements and evaluation (SQuaRE), Common Industry Format (CIF) for usability test reports, 2006

[8] Brooke, J. SUS: A "quick and dirty" usability scale. En Jordan, P.W., Thomas, B.T. y Weerdmeester, B.A. (eds.), Usability Evaluation in Industry. UK: Taylor and Francis, pp. 189-194, 1996

[9] PHP Group. Hypertext Preprocessor. En URL: http://www.php.net/manual/es/preface.php. Último acceso: 9 abril de 2010

[10] Mysql Enterprise. En URL: http://www.mysql.com/products/enterprise/, Último acceso: 9 abril de 2010

[11] XAjax Community. En URL: http://xajaxproject.org/, Último acceso: 9 abril de 2010