Sistemes de Gestió de la Seguretat de la Informació

Nom Estudiant: Iván Arocas Martínez

Programa: Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Consultor: Arsenio Tortajada Gallego

Professor/a responsable de l'assignatura: Carles Garrigues Olivella

Centre: Universitat Oberta de Catalunya

Data Lliurament: 6 de juny de 2016

Títol del treball:	*Sistemes de Gestió de la Seguretat de la Informació*
Nom de l'autor:	*Iván Arocas Martínez*
Nom del consultor/a:	*Arsenio Tortajada Gallego*
Nom del PRA:	*Carles Garrigues Olivella*
Data de lliurament (mm/aaaa):	*06/2016*
Titulació o programa:	Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)
Idioma del treball:	*Català*
Paraules clau	*Sgsi, seguretat, gestió*

Resum del Treball (màxim 250 paraules):

Al llarg de les fases de la creació del pla director de seguretat s'ha anat construint tota la base necessària per a la preparació de la certificació de la ISO/IEC 27001:2013.

En primer moment s'ha realitzat un anàlisi inicial de l'estat en què es troba l' organització respecte a la ISO/IEC 27002:2013 per tal de tindre una visió global de l'estat actual i on es vol arribar respecte al nivell d'adaptació a la norma.

Posteriorment s'ha construït la base per elaborar el sistema documental exigit per la SO/IEC 27001:2013, almenys els element més importants, com la política de seguretat o la metodologia d'anàlisi de riscos.

En tercer lloc s'ha realitzat l'anàlisi de riscos de l'organització. Aquest anàlisi s'ha realitzat seguint la metodologia Magerit. En aquest punt s'ha realitzat l'inventari d'actius i la seva valoració per l'organització. També s'han enumerat les amenaces que poden afectar a l'organització i el seu impacte en ella.

Després de l'anàlisi de riscos i els seus resultats s'ha definit un conjunt de projectes per tal de minimitzar els efectes de les amenaces detectades en el punt anterior i s'ha valorat el cost de la seva implantació.

Per últim, s'ha realitzat un anàlisi de compliment respecte la ISO/IEC 27002:2013 considerant que els projectes anterior han sigut implantats. Els resultats obtinguts marcaran els aspectes a millorar del sistema de gestió de la seguretat.

Abstract:

During the phases of creation of the security director plan the necessary base for the preparation of the certification according to the ISO/IEC 27001:2013 was constructed.

First, an initial analysis about the actual status of the organisation regarding the ISO/IEC 27001:2013 was realised in order to get a global vision of the actual status and the level of adaption to the norm that we want to achieve.

Second, a base for creating the documentary system demanded from ISO/IEC 27001:2013 - at least the most important elements like the security police or the method of risks analysis - was constructed.

Third, the analysis of risks of the organisation was carried out with the method Magerit. With this analysis the inventary and the evaluation of assets was done for the organisation. Also the dangers that can affect the organisation and their impact on it were counted.

After knowing the results of the analysis of risks, several projects which minimize the effects of the detected dangers were defined and the costs of their implementation were calculated.

At last, another analysis regarding the ISO/IEC 27001:2013 was done considering that the projects have been implemented. The results show the aspects of the system of security management that need to be improved.

Índex

Llista de figures

1. Introducció

1.1 Context i justificació del Treball

Amb aquest treball de fi de màster es volen construir les bases per implantar un SGSI a una organització.

Per a aquesta organització, la seguretat de la informació és un valor molt important atès que ofereix serveis TIC on hi ha molta informació i serveis que estan exposats a Internet. Amb el treball s'intentaran crear unes pautes i procediments fruit d'un anàlisi previ seguint les pautes de la norma.

Una de les avantatges que es té a l'empresa es l'interès de la direcció en la seguretat de la informació i l'adequació dels procediments a un estàndard que garanteixi la qualitat dels seus serveis. Per tant, un dels punts més importants en la implantació de qualsevol SGSI, que és el suport per part de la direcció, ja es té, així que és un bon inici per a la correcta implantació del sistema gestor.

Com a objectiu final, el projecte permetrà a l'organització implantar un SGSI per la posterior certificació de la ISO 27001.

1.2 Objectius del Treball

Els objectius del treball són:

- Implantar un Sistema de Gestió de la Seguretat de la Informació que satisfaça les necessitats d'una empresa real.
- Obtenir experiència en l'anàlisi de les característiques d'una organització per tal de documentar-les.
- Crear documentació i procediments en base a les exigències de la ISO 27001.

1.3 Enfocament i mètode seguit

L'estratègia a seguir es utilitzar l'experiència de l'organització i els seus empleats per utilitzar-la de base per crear els procediments per garantir la seguretat de la informació.

Aquest coneixements adquirits durant els anys son essencials per crear normes per actuar en diverses situacions crítiques.

També es seguiran mètodes reconeguts per tal de realitzar tasques de forma objectiva com el mètode Magerit a l'anàlisi de riscos.

Tot el SGSI se emmarcara dins del cicle de Demming (PDCA), basat en la planificació d'activitats, la seva implementació i operació, la seva revisió i la seva posterior millora.

1.4 Planificació del Treball

Una possible planificació de les fases del treball en forma de diagrama de Gantt podria ser la següent:

Nombre	Trab...
Fase 1: Situació actual	**9d**
Introducció al Projecte	3d
Realització del pla de treball	3d
Definició dels objectius del Pla	3d
Entrega de la Fase 1	
Fase 2: Sistema de Gestió Documental	**20d**
Introducció i descripció del projecte	10d
Declaració de l'aplicabilitat i documentació del SGSI	10d
Entrega de la Fase 2	
Fase 3: Anàlisis de riscos	**27d**
Elaboració d'una metodologia d'anàlisis de riscos	27d
Entrega de la Fase 3	
Fase 4: Proposta de Projectes	**20d**
Revisió de la documentació del projecte	10d
Quantificació econòmica i temporal d'aquests	10d
Entrega de la Fase 4	
Fase 5: Auditoria de Compliment de la ISO/IEC 27002:2013	**14d**
Avaluació de controls, maduresa i nivell de compliment.	14d
Entrega de la Fase 5	
Fase 6: Presentació de Resultats i entrega de Informes	**10d**
Consolidació dels resultats obtinguts durant el procés d'anàlisis	5d
Realització dels informes i presentació executiva a Direcció	5d
Entrega de la Fase 6	

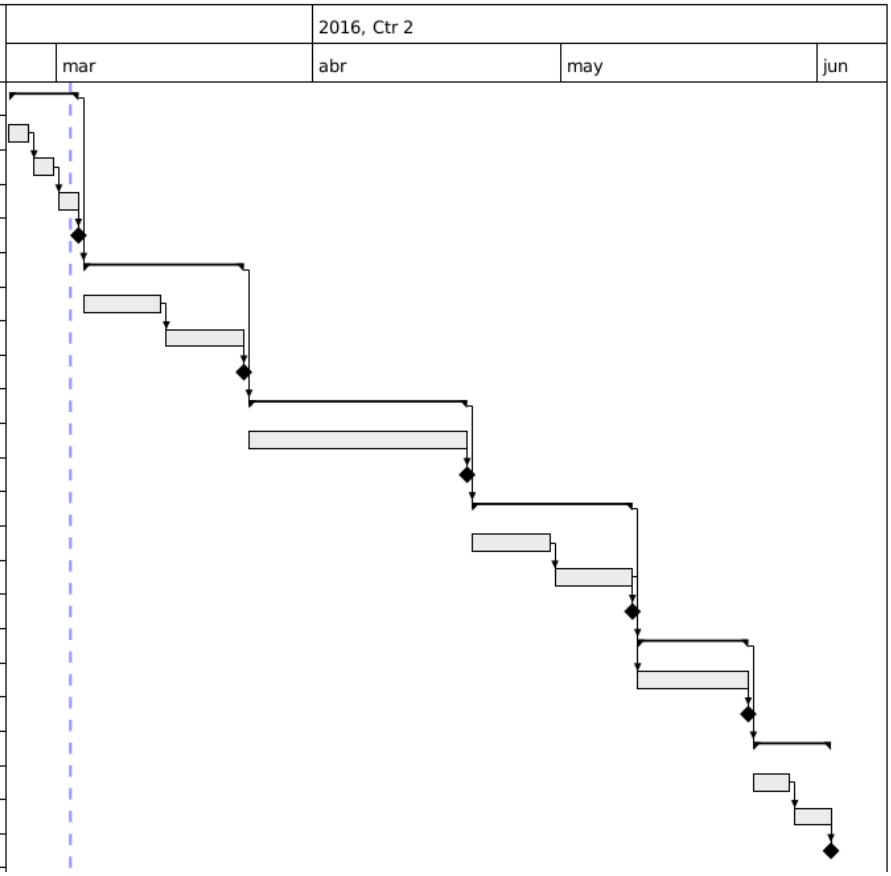


Figura 1: Diagrama de Gantt

2. Fase 1: Situació actual: Contextualització, objectius i anàlisi de compliment

2.1 Descripció detallada de l'organització

Visió general:

L'organització escollida per realitzar el pla de seguretat l'anomenarem amb les sigles "ON SL".

L'organització es troba dins de les que ofereixen un servei de tipus IaaS (Infrastructure as a Service). Es a dir, es posa a disposició dels clients una infraestructura informàtica adequada a les seves necessitats.

Concretament aquesta empresa esta orientada a:

- La gestió de infraestructures virtualitzades mitjançant hipervisors.
- Creació i manteniment de sistemes distribuïts visualitzats sobre equips físics amb l'hipervisor XenServer anomenats Clouds.
- Disponibilitat de la informació, mitjançant tecnologies de replicat de dades.
- Capacitat d'escalat dinàmic de les infraestructures dels clients amb la possibilitat d'augmentar recursos de forma transparent.
- Serveis d'assessorament per iniciar nous projectes amb necessitats de disponibilitat i velocitat.

L'empresa ofereix aquests serveis gestionats mitjançant Clouds privats, aquests estan composats per servidors HP DL 165 G7 situats en 3 armaris Rack a un CPD de València. Aquests servidors utilitzen el software XenServer com a hipervisor i Debian com a SO virtualitzat, tots ells estan monitoritzats mitjançant serveis com Opsview i StatusCake. El servidors estan connectats a Internet mitjançant switches HP, un router Mikrotik i els routers BGP de l'empresa proveïdora de serveis d'Internet (el Data Center) mitjançant connexions de fibra òptica.

A la Figura 2 es pot veure la infraestructura de xarxa, en aquest gràfic podem observar la part que es troba al Data Center i la part corresponent a les oficines per a la gestió de la infraestructura. Podem diferenciar els 3 armaris interconnectats a través del switch i el router. El router connecta per una banda amb el firewall que es troba protegint els equips de les oficines i per l'altra banda es connecta amb els equips de xarxa del Data Center de forma redundada, aquests a la vegada connecten a Internet pels diferents proveïdors de servei, fins un total de 8.

Els empleats de ON SL, composat per 7 persones, treballen des de les oficines situades al mateix edifici que el CPD, oferint un servei de 24x7 utilitzant els equips d'oficina amb Ubuntu i telèfons VoIP Cisco.

Segons la descripció anterior, podem veure a la Figura 5 la situació de les oficines, assenyalades amb el punt 14 al dibuix.

Altres elements importants del plànol son la localització de l'entrada del CPD (Punt 2) on es realitza el control d'accés, garantint la seguretat física. La localització dels armaris Rack (Punts 7 i 8) on estan situats els servidors, en el cas d'ON SL a la sala 2. Y les sales UPS (Punts 4 i 5) que garanteixen disponibilitat de tota la infraestructura.

L'organització del personal es troba a la Figura 3. La gestió i interacció amb clients es realitza amb un sistema de tiquets WHMCS, contacte telefònic i correu electrònic.

Tota aquesta infraestructura té com a finalitat donar serveis gestionats a diversos clients que gestionen tendes online de tipus Magento, Prestashop i altres projectes a mida, tenint com a principal valor garantir la disponibilitat i el rendiment i utilitzant com a base els sistemes distribuïts disponibles.

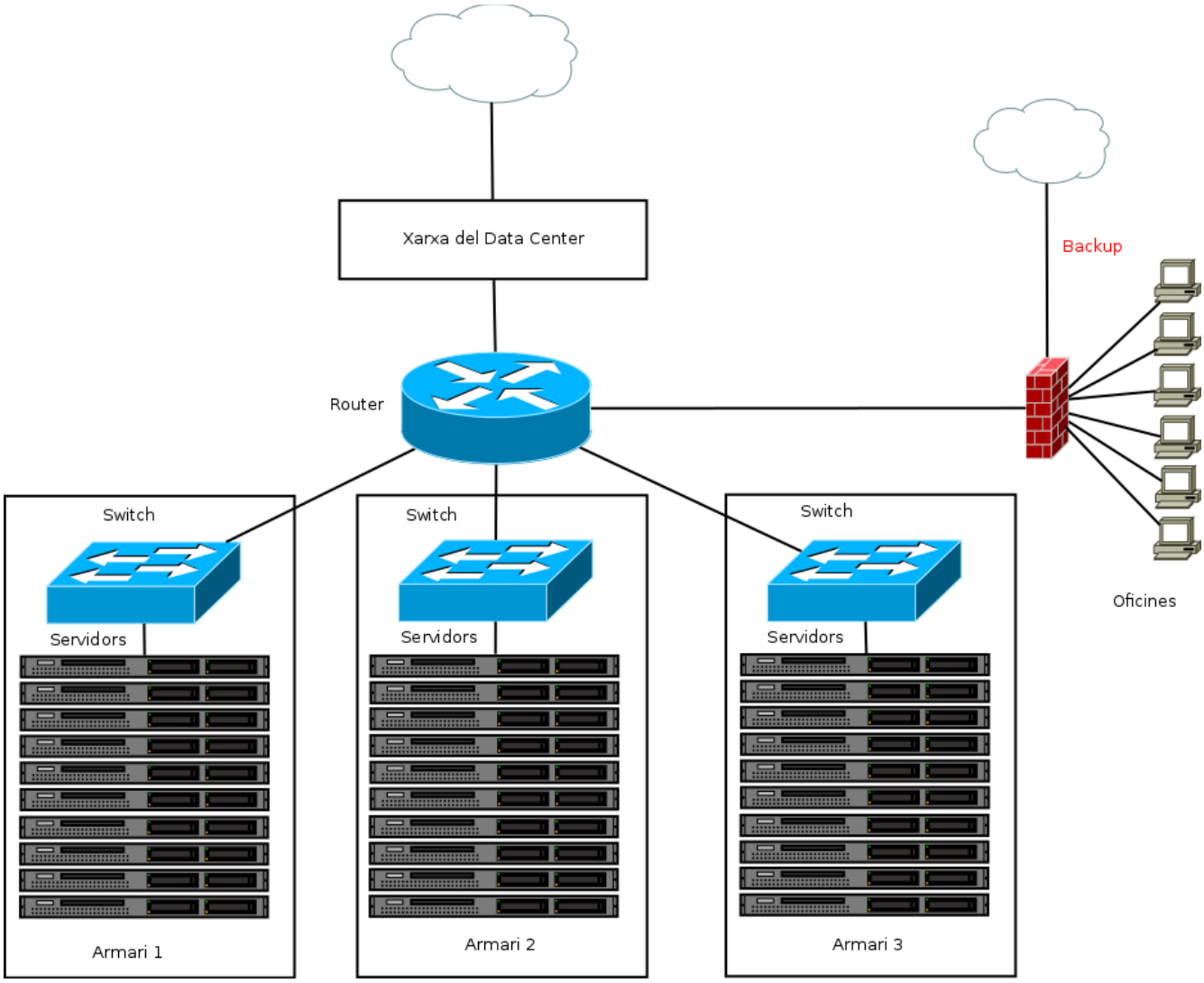


Figura 2: Diagrama de Xarxa

Departaments:

L'organització està dividida en diferents departaments amb una funció específica:

Departament Directiu: Té una visió general de l'organització la qual li permet marcar els objectius utilitzant la resta de departaments de forma adequada.

Departament Administratiu: S'encarrega de la gestions administratives, nòmines, compres i vendes de serveis.

Departament RRHH: S'encarrega de les noves incorporacions i fa un seguiment sobre aquestes, investiga antecedents i aconsella sobre la adequació o necessitat de llocs de treball.

Departament de Compres: S'encarrega d'adquirir nou material per a que els tècnics puguen configurar els nous sistemes.

Departament Tècnic: Té l'objectiu d'atendre les necessitats dels clients i complir els objectius marcats per la direcció per part del responsable del departament tècnic. Hi ha dos grups distints de tècnics que s'ocupen de tasques diferenciades:

- **Tècnics Nivell 1:** És el primer nivell d'atenció als clients, s'ocupa de resoldre problemes menors, gestionar incidències en primeria instància i escalar els problemes greus o que no pot resoldre algun dels tècnics de nivell superior.
- **Tècnics Nivell 2:** S'ocupen de gestionar els sistemes i la xarxa, de construir nous sistemes i de resoldre les incidències escalades per altres tècnics.

Degut a que l'organització no es extremadament gran, membres de l'equip directiu realitzen tasques en diferents departaments, ja siga de forma autònoma o donant suport a altres empleats.

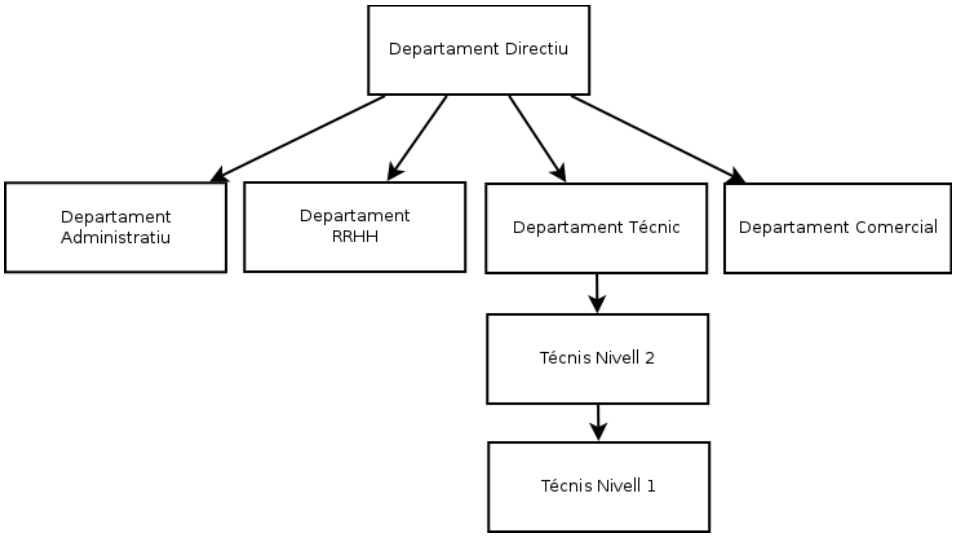


Figura 3: Organigrama

Tecnologia:

Com s'ha dit a la descripció general, el servei oferit als clients son els «Clouds Gestionats». Aquest servei es tracta d'una combinació de dos o més màquines físiques HP DL 165 G7 amb un sistema operatiu Xen Server per tal de crear les distintes màquines virtuals per oferir el servei. Aquestes màquines virtuals contenen un sistema operatiu Debian GNU/Linux per executar les distintes aplicacions i servidors.

Tal com es pot veure a la Figura 4 hi ha un exemple de Cloud Gestionat bàsic, composat de dues màquines físiques per garantir la disponibilitat. Cadascuna de les màquines físiques està composada per les següents màquines virtuals:

2 Balancejadors: Fan la funció de porta d'entrada al servei, estan duplicats per a què en el cas de que un quede indisponible, l'altre entraria en funcionament. El principal software utilitzat es Nginx.

4 O més Servidors web: Són els que executen el codi de les aplicacions web. Hi ha 2 o més per màquina física per garantir la disponibilitat en cas de que una màquina no estiga disponible. El principal software utilitzat es Apache, que serà el que execute les distintes aplicacions web.

2 Servidors de base de dades: Encarregats de contindre les bases de dades necessàries per a les aplicacions. Estan replicats, el software utilitzat es Mysql.

2 Servidors de fitxers NAS: Aquests servidors contenen els fitxers de l'aplicació web i que són accedits pels servidors web al igual que les basea de dades. Estan replicats per a mantindre el servei en el cas necessari. El principal software utilitzat es NFS.

Maquina de backups: Existeix una màquina de backups per a cada Cloud Gestionat que incorpora un software per tal de fer còpies segons la política definida. El principal software utilitzat es Dirvish.

Aquestes són les màquines mínimes que pot tindre un d'aquests Cloud Gestionats, no obstant, el nombre de màquines es pot augmentar segons les necessitats del servei, però la tecnologia a utilitzar no canviarà.

Actualment existeixen un total de 22 Clouds Gestionats repartits en tres armaris al CPD, pel que fa un total de 44 màquines físiques que contenen en total 220 màquines virtuals que gestionar si consideremt que totes contenen 5 màquines virtuals com a l'exemple.

Per altra banda, tota aquesta infraestructura es gestionada des de les oficines d'«ON SL». Cada empleat compta amb un ordinador amb un sistema operatiu Ubuntu 14 LTS. Les aplicacións mes utilitzades son:

Terminal de comandes: Per a la gestió i administració de servidors.

Libreoffice: Per a la generació de documentació.

WHCMS: Per a la interacció amb clients i suport.

També existeix una màquina per a la visualització de la monitorització a través del navegador web connectada a vàries pantalles per tal de veure des d'els llocs de treball l'estat de les distintes màquines.

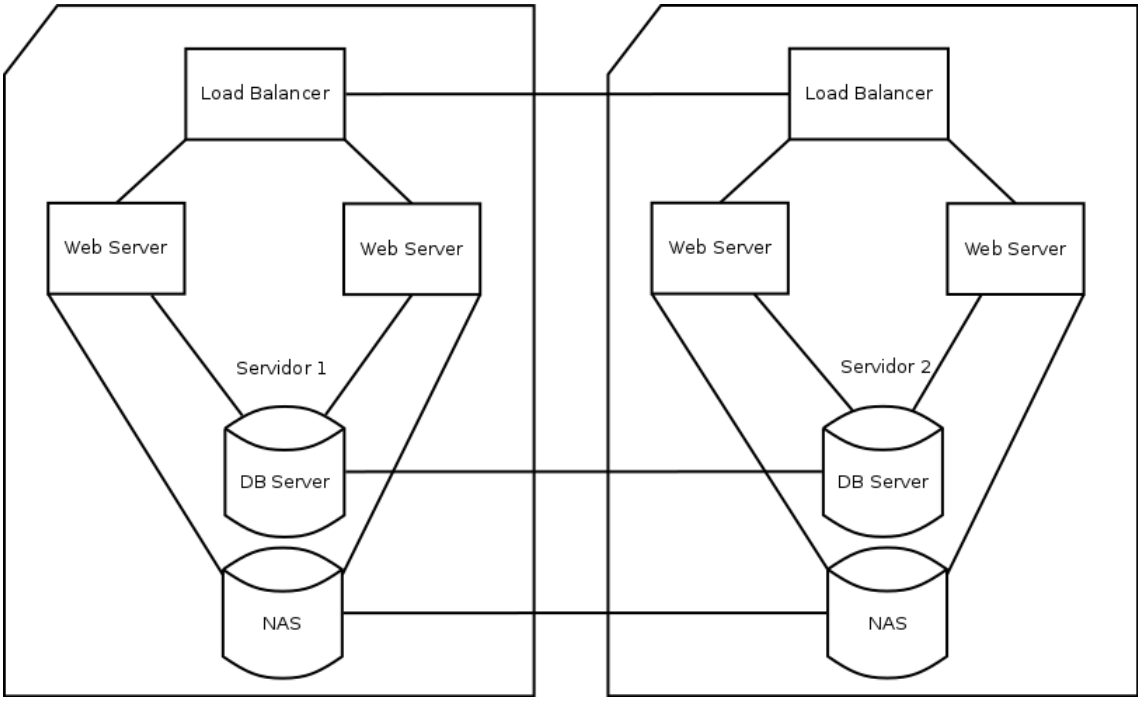


Figura 4: Cloud Gestionat

Topologia de xarxa:

L'estructura de la xarxa es pot veure a la Figura 2. Hi ha 2 parts totalment diferenciades amb necessitats de protecció distintes, els servidor situats dins del CPD i l'equipament d'oficines, situats dins de les oficines d'«ON SL».

El hardware que es troba dins del CPD és:

- 3 armaris HP de 42 U.
- 3 switches de tipus modular model HP ProCurve amb fonts redundades
- 1 router Mikrotik CCR amb font redundada.
- Cablejat d'interconnexió a Internet i a les oficines.
- Cablejat redundat dels servidors físics als switch

Aquest equipament de xarxa és el necessari per fer accessibles els serveis dels «Clouds Gestionats». En estar situats dins del CPD tenen redundància d'energia i de connexió a Internet. Cada Cloud es troba separat lògicament de la resta amb VLAN's per independitzar la xarxa i mantindre l'aïllament de clients.

Per altra banda, les oficines compten amb 1 router Mikrotik CCR bàsic que realitza les funcions de firewall i interconnecta la xarxa d'oficines amb la que es troba dins del CPD directament i a Internet. També compta amb una connexió a Internet secundària de backup en el cas de que el router/firewall d'oficines quedara sense servei. Els telèfons VoIP també segueixen el mateix patró, i estan preparats per utilitzar la connexió de backup en cas de caiguda.

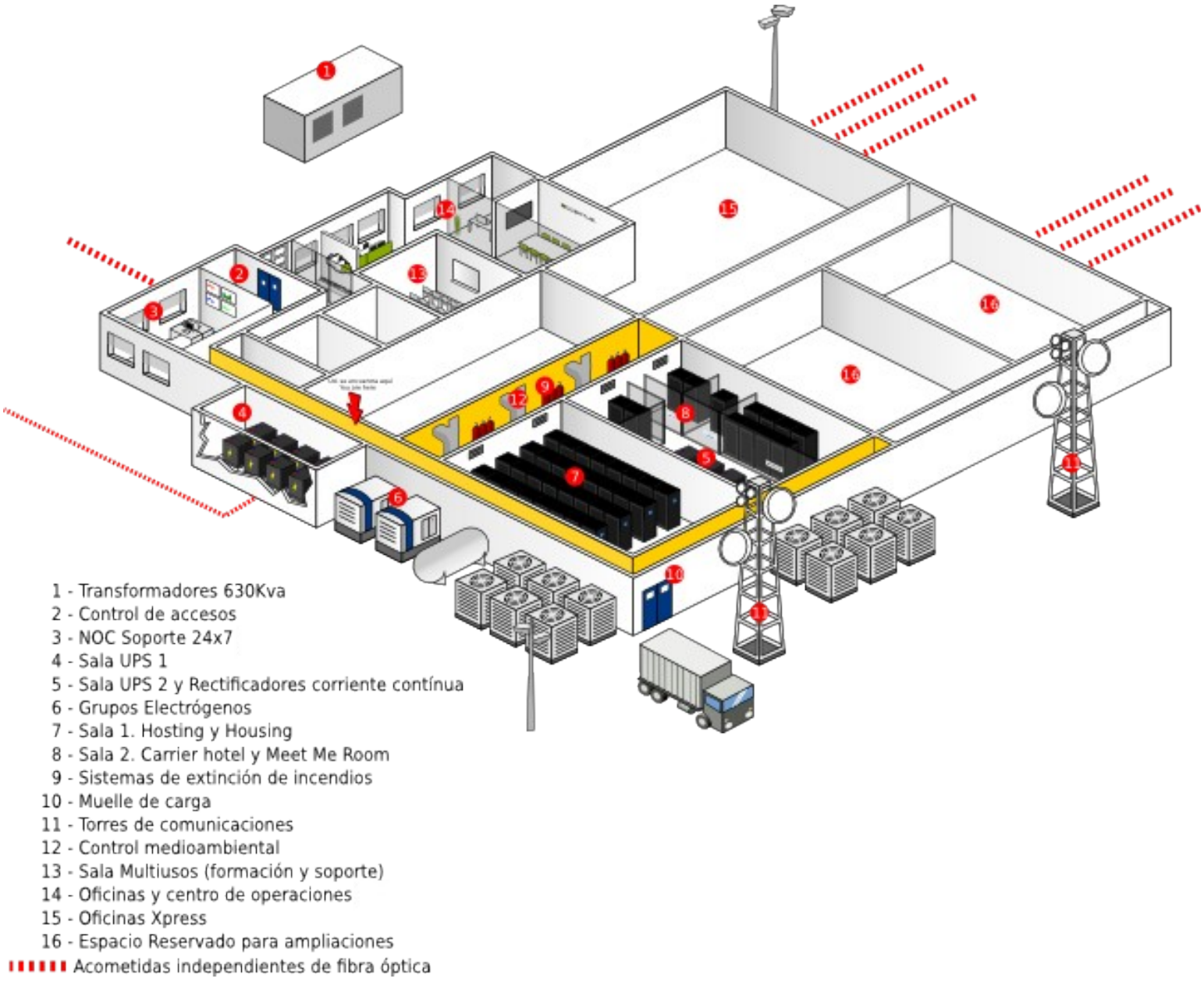


Figura 5: Infraestructura Física

Infraestructura Física:

A la Figura 5 podem observar en detall l'organització física de l'empresa i la del CPD del qual es fa servir per tal de garantir el mínim de qualitat que els clients esperen. L'organització que s'està tractant es troba dins del mateix edifici on es troba el CPD. En aquest edifici també es troben tres altres empreses independents al igual que «ON SL».

A la imatge podem diferenciar aquests elements:

Oficines d'«ON SL» (14): Les oficines es poden veure amb detall a la Figura 6. Aquestes consten d'una sala d'operacions on estan situats els empleats amb els seus llocs de treball (punt 1 de la Figura 6). El despatx de direcció es troba al punt 2 de la Figura 6, i la sala de reunions al punt 3 de la Figura 6. Els punts 4 i 5 de la Figura 6 corresponen a les sales de laboratori i emmagatzematge de material. La sala de laboratori és de gran utilitat per realitzar tests abans d'incorporar nous sistemes a producció.

Aquestes oficines estan tancades amb clau i protegides amb alarma. Cal tenir en compte que només es pot accedir a l'edifici si un empleat del CPD obri la porta principal d'accés.

Accés al CPD (2): L'accés està protegit per portes amb clau i que només s'obrin si es sol·licita l'accés mitjançant un timbre. Una vegada s'accedeix a la sala de control d'accés un empleat del CPD comprovarà que la persona que sol·licita l'accés està autoritzada a fer-ho i a quina secció del CPD pot tindre accés. L'empleat facilitarà una targeta d'accés limitada segons el nivell d'autorització que tinga el sol·licitant d'accés al CPD. El CPD incorpora personal 24x7 per garantir la seguretat i, a més, compta amb controls de vídeo vigilància interior i exterior.

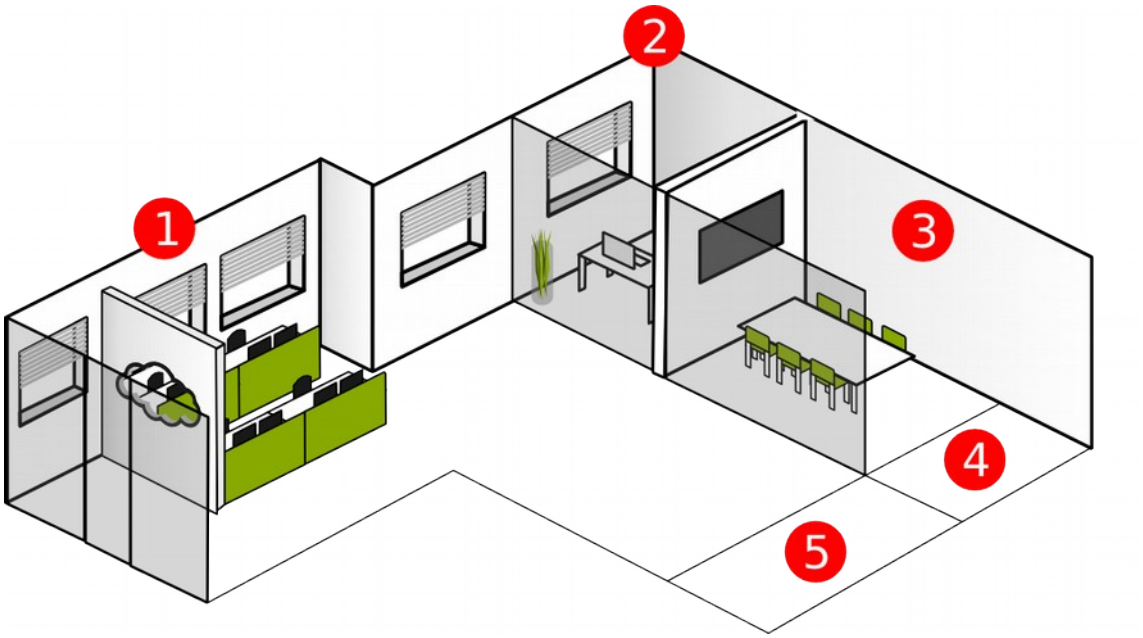


Figura 6: Oficines

Sala UPS 1 i 2 (4): Infraestructura per garantir la disponibilitat d'energia del CPD oferint als clients del CPD redundància en els serveis d'energia.

Sala 2 (8): A aquesta sala es troben els 3 armaris d'«ON SL». La sala està protegida amb un control d'accés biomètric mitjançat l'empremta dactilar, que el personal del CPD ha habilitat prèviament a l'accés a les sales. Els armaris estan situats dins d'una estructura de metall tancada amb clau al qual només té accés l'empresa i el CPD per realitzar revisions o tasques de tipus «mans remotes».

Connexions de servei (Línies discontinues): El CPD proporciona 10 connexions de servei de fibra òptica de 8 proveïdors distints per garantir la disponibilitat als clients. El que permet redundar les connexions dels servidors de dins de les sales.

2.2 Abast del pla director de Seguretat i objectius

El pla director de seguretat estarà delimitat per les àrees de vital importància per a que l'organització puga treballar amb normalitat per garantir una qualitat de servei determinada. Les àrees que conformen l'abast son:

- Equipament informàtic, servidors de virtualització enrackables necessaris per al funcionament dels «Clouds Gestionats».
- Equipament de xarxa, switch i routers.
- Equipament d'oficines, ordinadors, mòbils i telèfons.
- Repositoris de documentació, clients i fitxers.

Amb el Pla director de seguretat s'intentarà satisfer els següents objectius:

- Assegurar la confidencialitat, integritat i disponibilitat de les dades.
- Complir els requisits legals aplicables a l'organització.
- Tenir un pla de continuïtat de negoci que permeta recuperar-se d'un desastre en el menor temps possible.
- Protegir els elements essencials per al funcionament de l'organització.
- Crear un pla de formació per als empleats en matèria de seguretat de la informació.
- Registrar els incidents de seguretat.

- Crear plans de millora de la seguretat de la informació de l'organització mitjançant revisions periòdiques.

2.3 Anàlisi de compliment inicial

A continuació es presenten els resultats de l'anàlisi diferencial inicial en forma de taula de la implantació dels controls de la ISO/IEC 27002:2013. Aquest anàlisi es presenta en detall a **l'Annex G. Anàlisi de compliment inicial**, indicant el grau de maduresa actual a l'empresa. Cal destacar els resultats de dues àrees:

- L'àrea 11, seguretat física i ambiental té un grau de maduresa molt alt, 95%. Degut a que gran part d'aquest aspectes son gestionats pel centre de dades que garanteix aquest nivell de implantació.
- Els controls centrats en el desenvolupament de software (control 14.2) i l'accés per part de subministradors (àrea 15), estan marcats com a N/A, ja que l'organització no realitza tals accions.

El grau d'implantació de cada àrea es calculat segons la mitjana de les seves subàrees.

Control	Implantació
5. POLÍTICAS DE SEGURIDAD.	30%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	44%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	50%
8. GESTIÓN DE ACTIVOS.	66%
9. CONTROL DE ACCESOS.	50%
10. CIFRADO.	10%
11. SEGURIDAD FÍSICA Y AMBIENTAL.	95%
12. SEGURIDAD EN LA OPERATIVA.	46%
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	50%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	25%
15. RELACIONES CON SUMINISTRADORES.	0%

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	0%
17. SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	28%
18. CUMPLIMIENTO.	50%

Els diferents graus d'implantació estan indicats amb percentatge, cada nivell està definit a la Figura 7.

Percentatge	Nivell
0%	Inexistent
10%	Inicial
50%	Reproduïble, però intuïtiu
90%	Procés definit
95%	Gestionat i Mesurable
100%	Optimitzat

Figura 7: Nivells

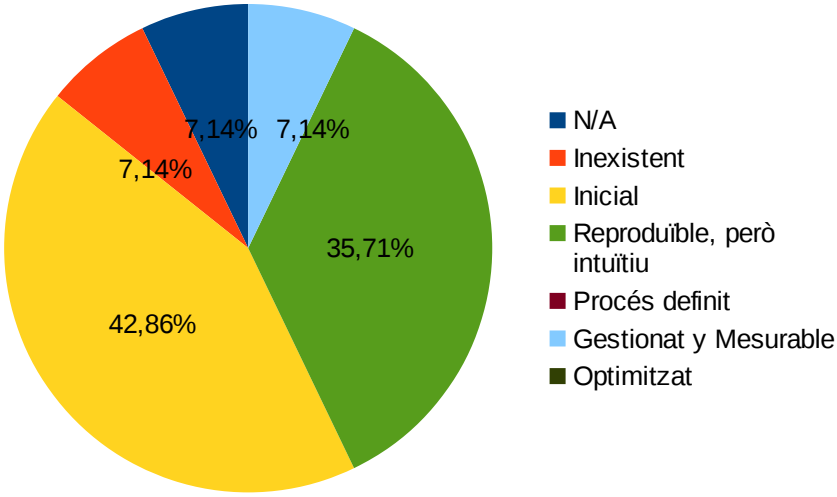


Figura 8: CMM

A la Figura 8 s'observa el percentatge d'àrees que tenen un nivell determinat representat pel gràfic, la majoria es inicial o reproduïble, no obstant hi ha poques àrees amb un nivell inexistent.

A la Figura 9 es compara el nivell actual de maduresa del SGSI amb el nivell desitjat.

L'obtenció d'aquests valors es troba detallat a l'adjunt **«controls_analisi_inicial.ods»**.

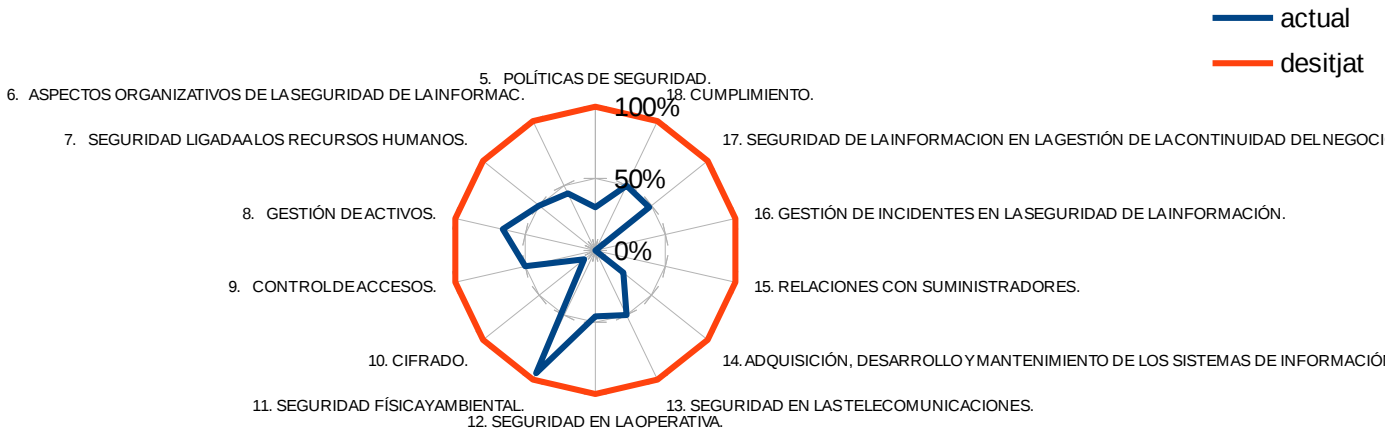


Figura 9: Nivell de compliment inicial

3. Fase 2. Sistema de Gestió Documental

3.1 Política de Seguretat

La política de seguretat està inclosa a **l'Annex A. Política de seguretat de la informació**, aquesta política és d'obligat compliment per al personal de l'organització per garantir la seguretat de la informació i mantindre una qualitat en el servei. Per aquest motiu, es troba accessible de forma fàcil per a tots els empleats de la organització.

Es pot consultar una versió adaptada als usuaris centrant-se en les seves responsabilitats en qualsevol moment a la plataforma documental web de tipus wiki a la secció corresponent, com es pot veure a la Figura 10. Aquesta plataforma serveix també per fer accessibles els distints documents relatius al SGSI :

Figura 10: Gestor documental

La informació i els serveis són els principals valors de l'organització, ja siguen de la pròpia de l'empresa o d'altres organitzacions que posen en les mans d'ON SL els seus sistemes.

3.2 Procediment d'Auditories Internes

Les auditories internes són de vital importància per comprovar que el controls, processos i procediments:

- Compleixen els requeriments de l'estàndard, legislació o regulació rellevants.
- Compleixen el requeriments de la seguretat de la informació.
- Els controls i procediments siguen implementats i mantinguts de forma efectiva i que es efectuen com s'esperava.

El procediment a seguir per a les auditories internes està exposat a **l'Annex B. Procediment d'Auditories Internes**. Les idees principals són les següents:

- Els auditors no deuen auditar el seu treball per tal de no alterar el seus resultats.
- Les no-conformitats s'han de resoldre el més aviat possible.
- Els resultats hauran de ser presentats a la gerència així com la resolució de les no conformitats.

3.3 Gestió d'Indicadors

L'emmagatzematge dels registres es realitza a través de diverses ferramentes segons el tipus de control que s'estiga revisant.

Aquestes ferramentes, manuals o automàtiques, garanteixen la generació de mostres dels distints controls implantats. A més, permeten l'emmagatzematge en el temps dels resultats registrats.

Les distintes mostres serviran per a avaluar l'estat dels controls de seguretat implantats, A **l'Annex C. Gestió d'Indicadors** s'indica en forma de taula els distints indicadors amb els umbrals de tolerància per tal d'indicar si un control no funciona.

3.4 Procediment de Revisió per Direcció

Per garantir la aprovació per par de la direcció de les millores del sistema de gestió de la seguretat, es planificaran reunions periòdiques on s'avaluaran les propostes de millora o les necessitats del sistema. Aquestes reunions seguiran el procediment definit a **l'Annex D. Procediment de Revisió per Direcció**.

3.5 Gestió de Rols i Responsabilitats

Per tal de gestionar el SGSI s'han definit una sèrie de rols i responsabilitats, aquestes es troben a **l'Annex E. Gestió de Rols i Responsabilitats.**

El comitè de seguretat està composat per 4 persones. Per una banda 2 tècnics de nivell 2 que s'encarreguen de realitzar procediments, revisar e informar dels distints incidents de seguretat. Un d'aquests membres és el responsable de seguretat.

Els altres dos membres del comitè son dues persones de la direcció, per tal d'avaluar i aprovar i validar les distintes decisions preses i donar suport de recursos ja siga per assignar recursos de temps o econòmics.

3.6 Metodologia d'Anàlisi de Riscos

La metodologia a seguir per tal d'identificar el actius i valorar les seves vulnerabilitats està basada amb la Magerit.

Aquesta permetrà de forma objectiva conèixer l'estat de la seguretat dels sistemes de la informació, conèixer les seves vulnerabilitats i aplicar millores per tal de minimitzar les amenaces trobades. A **l'Annex F. Metodologia de Anàlisis de Riscos.**

3.7 Declaració de Aplicabilitat

A l'**Annex F. Declaració de Aplicabilitat** es descriu el motiu de si un control és aplicable a l'organització o no.

4. Fase 3. Anàlisi de Riscos

A aquesta fase s'analitzen els actius de l'organització per tal d'enumerar-los i decidir quins tenen un valor més alt en l'organització, quins son els més crítics i el seu cost. També es veurà la relació que tenen els distints actius entre ells, elaborant un diagrama de dependències entre actius, per indicar quins afecten a la resta.

Posteriorment s'analitzen les possibles amenaces que poden afectar als actius definits, per tal de decidir quin és l'impacte que tindrà la materialització d'una amenaça en les cinc dimensions de la seguretat per cada actiu.

Per últim, a partir de les dades recopilades es valora el risc de cadascun dels actius per a l'organització.

4.1 Inventari i valoració d'actius

A la taula següent es recopilen els distints actius de l'organització, agrupats segons l'àmbit al que pertanyen. La classificació dels actius s'ha realitzat seguint les pautes del punt 2, llibre II de Magerit i tenint en compte el document intern que defineix el procediment d'anàlisi de riscos, a l'Annex F. Metodologia de Anàlisis de Riscos.

Cada actiu serà classificat en una de les següents categories:

- [D] Dades / Informació: Dades de qualsevol tipus i format.
- [L] Instal·lacions: Elements físics que alberguen actius de l'organització.
- [HW] Equipament informàtic (hardware): Dispositius electrònics.
- [SW] Software: Aplicacions informàtiques: Aplicacions de tot tipus, com ofimàtica, desenvolupament, administració, gestió de sistemes, etc.
- [P] Personal: Empleats de l'organització.
- [COM] Xarxes de comunicacions: Xarxes i dispositius de xarxa.

Àmbit	Actiu	Valor Qualitatiu	Valor Quantitatiu
[HW] Equipament informàtic (hardware)	Routers BGP	Molt Alt	10
[HW] Equipament informàtic (hardware)	Switches	Molt Alt	10

[HW] Equipament informàtic (hardware)	Servidors	Molt Alt	9
[HW] Equipament informàtic (hardware)	Router Mikrotik	Molt Alt	10
[HW] Equipament informàtic (hardware)	Equips d'oficina	Mig	4
[HW] Equipament informàtic (hardware)	Firewall	Mig	4
[HW] Equipament informàtic (hardware)	DNS	Alt	9
[HW] Equipament informàtic (hardware)	Telèfons VoIP	Mig	5
[P] Personal	Personal tècnic	Alt	7
[P] Personal	Direcció	Alt	8
[SW] Software - Aplicacions informàtiques	Sistemes Operatius	Alt	8
[SW] Software - Aplicacions informàtiques	Servidors Web	Alt	7
[SW] Software - Aplicacions informàtiques	Servidors Base de dades	Alt	8
[SW] Software - Aplicacions informàtiques	Servidors de fitxers	Alt	7
[SW] Software - Aplicacions informàtiques	Hipervisors	Alt	8
[SW] Software - Aplicacions informàtiques	Aplicacions internes de gestió	Mig	6
[D] Dades / Informació	Fitxers web	Alt	8
[D] Dades / Informació	Documentació Interna	Mig	5
[COM] Xarxes de comunicacions	Xarxa Interna	Mig	6

[COM] Xarxes de comunicacions	Connexions Fibra Òptica	Alt	7
[COM] Xarxes de comunicacions	Connexió telefònica / VoIP	Mig	6
[S] Serveis	Serveis de Cloud Gestionat	Alt	8
[L] Instal·lacions	CPD	Molt Alt	9
[L] Instal·lacions	Armaris / Gàbia	Alt	8
[AUX] Equipament auxiliar	Hardware de recanvi	Molt Baix	1

El valor de l'actiu es representa en valors qualitatius i quantitatius. El valor quantitatiu representa el cost econòmic de cada actiu per a l'organització. La equivalència entre el valor quantitatiu i el cost econòmic es la següent:

Valor Quantitatiu	Valor Econòmic
10	Mes de 100000€
7-9	Entre 50000€ i 100000€
4-6	Entre 10000€ i 50000€
1-3	Entre 1000€ i 10000€
0	Menys de 1000€

Els actius de la taula anterior estan relacionats entre ells, alguns depenen d'altres ja que en el cas de que un sigui afectat per alguna amenaça, els actius superiors (dependents) serien afectats també. A la Figura 11 es mostren les dependències entre actius, s'observa en la part superior l'actiu més dependent, la informació web que qualsevol pot consultar amb el navegador.

Aquest actiu depèn de quasi la resta d'actius, qualsevol vulneració de la seguretat en la resta el pot afectar.

Al diagrama s'observa com l'actiu més dependent són els serveis web, tota la resta existeixen per garantir la disponibilitat d'aquest servei.

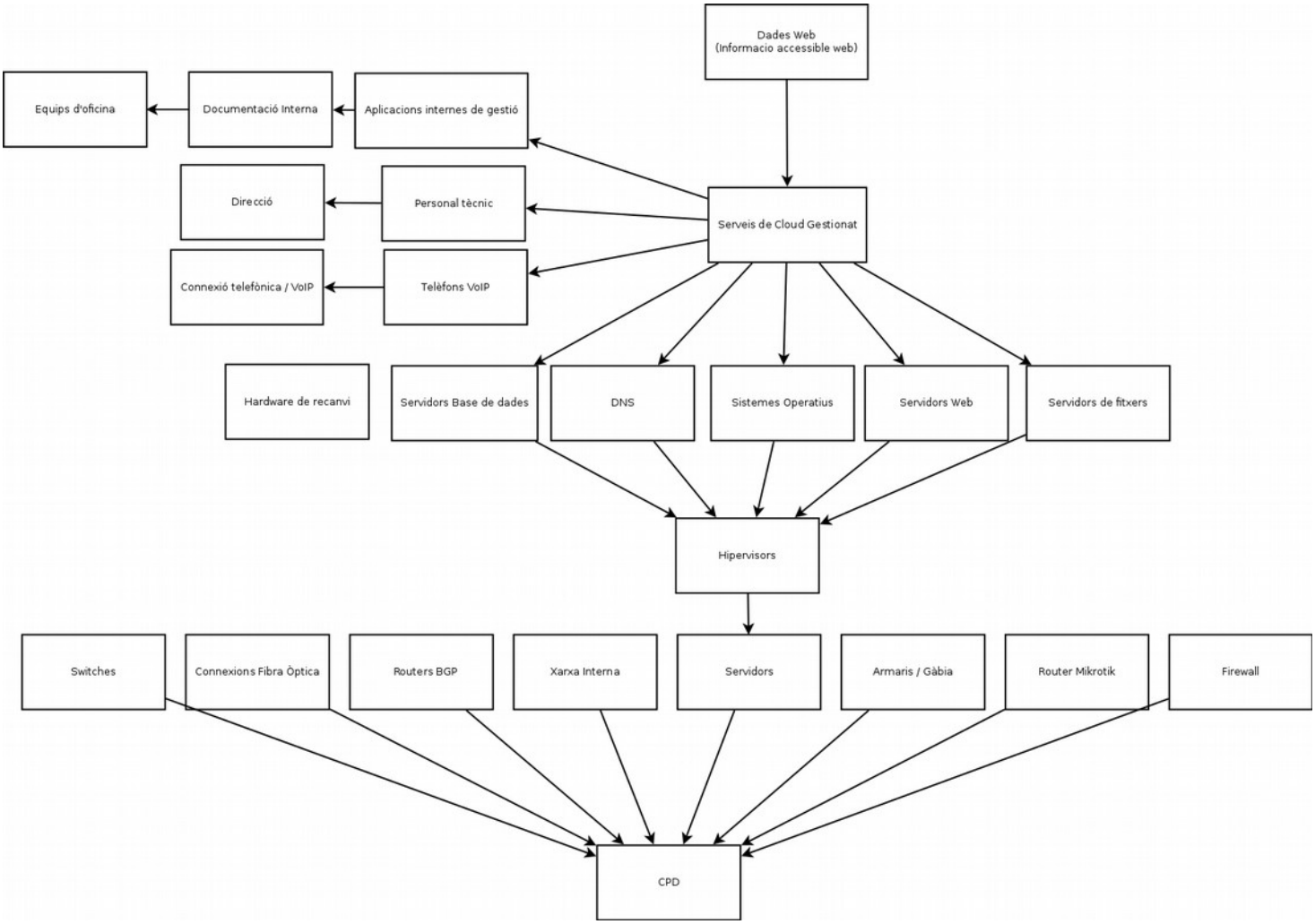


Figura 11: Dependències entre actius

Una vegada que els actius s'hagen categoritzat, es realitzarà una valoració qualitativa dels mateixos, definint la següent informació de cadascun:

- Àmbit
- Actiu
- Valor
- Impacte ACIDA

A la taula següent s'indica la seua valoració desglossada.

Les dimensions de la seguretat de la informació que son tractades son:

C → Confidencialitat, una pèrdua de confidencialitat pot derivar en incidències de seguretat quan un usuari no autoritzat accedeix a la informació del actiu. Aquest usuari pot adquirir coneixement que l'utilitze per perjudicar els interessos de l'organització.

Conseqüències segons el seu valor:

Valor qualitatiu	Valor quantitatiu	Criteri
Molt alt	10	Fer-ho pública suposa una pèrdua total de la confiança de l'opinió pública.
Alt	7-9	Fer-ho pública suposa una pèrdua important de la confiança de l'opinió pública.
Mig	4-6	Fer-ho pública suposa una pèrdua lleu de la confiança de l'opinió pública.
Baix	1-3	Fer-ho pública suposa una pèrdua mínima de la confiança de l'opinió pública.
Molt baix	0	Es pot fer públic.

I → Integritat, es refereix a l'exactitud de la informació. Una pèrdua d'integritat pot fer que les dades siguen incoherents. En relació a altres categories d'actius, la pèrdua d'integritat es tradueix a un mal funcionament.

Conseqüències segons el seu valor:

Valor qualitatiu	Valor quantitatiu	Criteri
Molt alt	10	No es pot funcionar sense ell
Alt	7-9	Es produeix mal funcionament en el servei
Mig	4-6	Es produeixen errors lleus

Baix	1-3	Es produeixen errors inapreciables
Molt baix	0	No afecta al servici

D → Disponibilitat, la disponibilitat d'un actiu pot afectar negativament al negoci, provocant que certs processos se vegen mermats o cancel·lats durant el temps que l'actiu es trobe in-operatiu. Un actiu disponible ha de ser accessible en el moment en que es necessite.

Conseqüències segons el seu valor:

Valor qualitatiu	Valor quantitatiu	Criteri
Molt alt	10	No es pot prescindir de l'actiu més de 2 hores
Alt	7-9	No es pot prescindir de l'actiu més de 4 hores
Mig	4-6	No es pot prescindir de l'actiu més de 1 dia
Baix	1-3	No es pot prescindir de l'actiu més de 2 dies
Molt baix	0	Es pot prescindir de l'actiu 2 dies o més

A(T) → Traçabilitat, es poden assignar les interaccions d'una entitat determinada inequívocament.

A → Autenticitat, indica que qui presenta una identitat és qui diu ser.

A continuació tenim la taula d'actius i la seva valoració en les cinc dimensions:

Àmbit	Actiu	Valor Qualitatiu	A	C	I	D	A
[HW] Equipament informàtic (hardware)	Routers BGP	Molt Alt	9	9	9	10	9
[HW] Equipament informàtic (hardware)	Switches	Molt Alt	9	9	9	10	9
[HW] Equipament informàtic (hardware)	Servidors	Molt Alt	9	9	9	10	9
[HW] Equipament informàtic (hardware)	Router Mikrotik	Molt Alt	9	9	9	10	9
[HW] Equipament informàtic (hardware)	Equips d'oficina	Mig	5	5	5	3	5
[HW] Equipament informàtic (hardware)	Firewall	Mig	5	5	5	5	5
[HW] Equipament informàtic (hardware)	DNS	Alt	9	9	9	10	9

[HW] Equipament informàtic (hardware)	Telèfons VoIP	Mig	6	6	6	5	5
[P] Personal	Personal tècnic	Alt	8	8	8	9	8
[P] Personal	Direcció	Alt	9	9	9	9	9
[SW] Software - Aplicacions informàtiques	Sistemes Operatius	Alt	8	8	8	9	8
[SW] Software - Aplicacions informàtiques	Servidors Web	Alt	7	7	7	9	7
[SW] Software - Aplicacions informàtiques	Servidors Base de dades	Alt	8	8	8	9	8
[SW] Software - Aplicacions informàtiques	Servidors de fitxers	Alt	7	7	7	9	7
[SW] Software - Aplicacions informàtiques	Hipervisors	Alt	8	8	8	9	8
[SW] Software - Aplicacions informàtiques	Aplicacions internes de gestió	Mig	5	5	5	5	5
[D] Dades / Informació	Fitxers web	Alt	8	8	8	7	8
[D] Dades / Informació	Documentació Interna	Mig	9	9	9	5	8
[COM] Xarxes de comunicacions	Xarxa Interna	Mig	8	5	8	9	8
[COM] Xarxes de comunicacions	Connexions Fibra Òptica	Alt	8	5	8	9	8
[COM] Xarxes de comunicacions	Connexió telefònica / VoIP	Mig	7	7	7	9	7
[S] Serveis	Serveis de Cloud Gestionat	Alt	8	8	8	9	8
[L] Instal·lacions	CPD	Molt Alt	8	10	10	10	8
[L] Instal·lacions	Armaris / Gàbia	Alt	5	10	10	10	8
[AUX] Equipament auxiliar	Hardware de recanvi	Molt Baix	0	0	5	5	5

4.2 Anàlisi d’amenaces

Per tal d'identificar les amenaces s'ha revisat el llistat de possibilitats indicades per la metodologia Magerit, llibre II punt 5. També la metodologia definida a l'Annex F. Metodologia de Anàlisis de Riscos.

A les taules següents s'analitza cadascun dels tipus d'actius, indicant en cada cas el grau d'afectació que té la materialització de l'amenaça sobre l'actiu en les cinc dimensions de la seguretat.

La valoració de l'impacte es fa en forma de percentatge, següent 100% el màxim d'impacte i 0% el mínim.

La freqüència indica la probabilitat de què l'amenaça es produeixi en l'interval d'un any segons la taula vista a l'Annex F. Metodologia de Anàlisis de Riscos:

Les amenaces poden trobar-se dins de les següents categories:

- [N] Desastres naturals → Successos que poden ocòrrer sense la intervenció dels éssers humans com a causa directa o indirecta.
- [I] D'origen industrial → Successos que poden ocòrrer de forma accidental, derivats de l'activitat humana de tipus industrial. Aquestes amenaces poden donar-se de forma accidental o intencionada.
- [E] Errors i fallades no intencionades → Errors no intencionats causats per les persones.
- [A] Ataques intencionats → Errors intencionats causats per les persones.

Freqüència		
Valor qualitatiu	**Valor quantitatiu**	**Criteri**
Molt alt	10	Ocorre a diari o vàries vegades al dia
Alt	7-9	Ocorre vàries vegades a la setmana
Mig	4-6	Ocorre una vegada al mes
Baix	1-3	Ocorre vàries vegades a l'any
Molt baix	0	Ocorre como a molt una vegada a l'any

L'anàlisi d'amenaces es fa a nivell de tipus d'actius per maximitzar la claredat i lectura de la informació, però es perd en definició.

Per tant, per a cada agrupació d'actius segons els seu tipus, l'impacte que provoca l'actiu per la materialització d'una amenaça en les cinc dimensions està definit per l'impacte més alt d'alguna de les amenaces que puguen afectar al grup d'actius.

Seguint la mateixa norma, la freqüència en què es produeix l'amenaça sobre l'actiu és la màxima de les amenaces que afecten al grup d'actius.

Actiu / Amenaça	Freqüència	A	C	I	D	A
[HW] Equipament informàtic (hardware)						
Routers BGP	3		100%	100%	100%	
Switches	3		100%	100%	100%	
Servidors	3		100%	100%	100%	
Router Mikrotik	3		100%	100%	100%	
Equips d' oficina	3		100%	100%	100%	
Firewall	3		100%	100%	100%	
DNS	3		100%	100%	100%	
Telèfons VoIP	3		100%	100%	100%	
[N.1] Foc	0				100%	
[N.2] Danys per aigua	0				75%	
[N.*] Desastres naturals	0				100%	
[I.6] Tall del subministre elèctric	0				100%	
[I.7] Condicions inadequades de temperatura o humitat	1				75%	
[E.2] Errors de l'administrador	3		50%	50%	50%	
[E.23] Errors de manteniment / actualització d'equips (hardware)	3				50%	
[E.24] Caiguda del sistema per esgotament de recursos	3				100%	
[A.6] Abús de privilegis d'accés	0		100%	100%	75%	
[A.7] Ús no previst	3		5%	5%	75%	
[A.11] Accés no autoritzat	0		100%	100%		
[A.23] Manipulació dels equips	0		100%		50%	
[A.24] Denegació de servici	0				100%	
[A.25] Robatori	0		50%		100%	
[A.26] Atac destructiu	0				100%	

Actiu / Amenaça	Freqüència	A	C	I	D	A
[P] Personal						
Direcció	3		50%	25%	50%	
Personal tècnic	3		50%	25%	50%	
[E.7] Deficiències en l'organització	3				25%	
[E.19] Fugues d'informació	0		50%			
[E.28] Indisponibilitat del personal	3				50%	
[A.30] Ingenieria social (picaresca)	0		25%	25%	25%	

Actiu / Amenaça	Freqüència	A	C	I	D	A
[SW] Software - Aplicacions informàtiques						
Sistemes Operatius	6	90%	100%	90%	90%	
Servidors Web	6	90%	100%	90%	90%	
Servidors Base de dades	6	90%	100%	90%	90%	
Servidors de fitxers	6	90%	100%	90%	90%	
Hipervisors	6	90%	100%	90%	90%	
Aplicacions internes de gestió	6	90%	100%	90%	90%	
[I.5] Averia d'origen físic o lògic	6				75%	
[E.1] Errors dels usuaris	5		50%	50%	50%	
[E.2] Errors de l'administrador	5		90%	90%	90%	
[E.8] Difusió de malware	4		90%	90%	90%	
[E.19] Fugues d'informació	0		100%			
[E.20] Vulnerabilitats dels programes (software)	6		90%	90%	90%	
[E.21] Errors de manteniment / actualització de programes (software)	3			75%	75%	
[A.5] Suplantació de la identitat de l'usuari	0	90%	90%	90%		
[A.6] Abús de privilegis d'accés	0		75%	75%	75%	
[A.11] Accés no autoritzat	0		75%	75%		
[A.22] Manipulació de programes	6		85%	85%	85%	

Actiu / Amenaça	Freqüència	A	C	I	D	A
[D] Dades / Informació						
Fitxers web	6	90%	100%	90%	95%	
Documentació Interna	6	90%	100%	90%	95%	

[E.1] Errors dels usuaris	6		90%	50%	85%	
[E.2] Errors de l'administrador	6		90%	50%	85%	
[E.15] Alteració accidental de la informació	5				50%	
[E.18] Destrucció d'informació	1				95%	
[E.19] Fugues d'informació	0		100%			
[A.5] Suplantació de la identitat de l'usuari	0	90%	90%	90%		
[A.6] Abús de privilegis d'accés	0		90%	90%	90%	
[A.11] Accés no autoritzat	1		90%	90%		
[A.15] Modificació deliberada de la informació	1			90%		

Actiu / Amenaça	Freqüència	A	C	I	D	A
[COM] Xarxes de comunicacions						
Xarxa Interna	1		100%	90%	100%	
Connexions Fibra Òptica	1		100%	90%	100%	
Connexió telefònica / VoIP	1		100%	90%	100%	
[I.8] Fallada de serveis de comunicacions	0				100%	
[E.2] Errors de l'administrador	0		75%	75%	100%	
[E.9] Errors de [re-]encaminament	0		75%	75%	100%	
[E.24] Caiguda del sistema por esgotament de recursos	0				100%	
[A.7] Ús no previst	1		75%	75%	75%	
[A.9] [Re-]encaminament de missatges	0		100%			
[A.10] Alteració de seqüència	0			75%		
[A.11] Accés no autoritzat	0		90%	90%		
[A.12] Anàlisi de tràfic	0		90%			
[A.14] Captura d'informació (escolta)	0		90%			
[A.15] Modificació deliberada de la informació	0			90%		
[A.24] Denegació de servei	1				100%	

Actiu / Amenaça	Freqüència	A	C	I	D	A
[S] Serveis						
Serveis de Cloud Gestionat	3		90%	90%	100%	
[E.2] Errors de l'administrador	3		90%	90%	90%	
[E.24] Caiguda del sistema por esgotament de recursos	3				90%	
[A.5] Suplantació de la identitat del usuari	0	90%	90%		90%	
[A.18] Destrucció d'informació	0				75%	

[A.24] Denegació de servei	0				100%	

Actiu / Amenaça	Freqüència	A	C	I	D	A
[L] Instal·lacions						
CPD	0		75%		100%	
Armaris / Gàbia	0		75%		100%	
[N.1] Foc	0				90%	
[N.2] Danys per aigua	0				90%	
[N.*] Desastres naturals	0				90%	
[A.26] Atac destructiu	0				100%	
[A.27] Ocupació enemiga	0		75%		100%	

Actiu / Amenaça	Freqüència	A	C	I	D	A
[AUX] Equipament auxiliar						
Hardware de recanvi	0		10%	10%	10%	
[N.1] Foc	0		10%		10%	
[N.2] Danys per aigua	0				10%	
[N.*] Desastres naturals	0				10%	
[I.6] Tall del subministre elèctric	0				10%	
[I.7] Condicions inadequades de temperatura o humitat	0				10%	
[A.11] Accés no autoritzat	0			10%	10%	
[A.25] Robatori	0		10%		10%	

4.3 Impacte potencial

Per calcular l'impacte potencial, es fa calculant el valor de l'actiu en cadascuna de les cinc dimensiones pel percentatge corresponent d'impacte de la materialització d'amenaces en les cinc dimensions:

Impacte potencial: (Valor actiu) * (% Impacte)

Aquests càlculs es troben detallats a l'adjunt **«AARR.ods»**.

La taula següent mostra la relació valor/criteri corresponent al valor d'impacte potencial obtingut per cada actiu i el seu criteri per l'organització.

Valor	Criteri
10	Dany molt greu a l'organització

7-9	Dany greu a l'organització
4-6	Dany important a l'organització
1-3	Dany menor a l'organització
0	Dany irrellevant a l'organització

A continuació es presenta la taula amb els càlculs realitzats. La columna «Impacte Pot.» indica l'impacte potencial de cada actiu en cadascuna de les dimensions de la seguretat.

Actius		Valor					% Impacte					Impacte Pot.				
Actiu	Valor	A	C	I	D	A	A	C	I	D	A	A	C	I	D	A
Routers BGP	10	9	9	10	10	9		100%	100%	100%		0	9	10	10	0
Switches	10	9	9	10	10	9		100%	100%	100%		0	9	10	10	0
Servidors	9	9	9	10	10	9		100%	100%	100%		0	9	10	10	0
Router Mikrotik	10	9	9	10	10	9		100%	100%	100%		0	9	10	10	0
Equips d' oficina	4	5	5	4	1	5		100%	100%	100%		0	5	4	1	0
Firewall	4	5	5	4	1	5		100%	100%	100%		0	5	4	1	0
DNS	9	9	9	8	10	9		100%	100%	100%		0	9	8	10	0
Telèfons VoIP	5	6	6	4	5	5		100%	90%	100%		0	6	3,6	5	0
Direcció	7	8	8	7	6	8		50%	25%	50%		0	4	1,7	3	0
Personal tècnic	8	9	9	7	6	9		50%	25%	50%		0	4,5	1,7	3	0
Sistemes Operatius	8	8	8	8	10	8	90%	100%	90%	90%		7,2	8	7,2	9	0
Servidors Web	7	7	7	8	10	7	90%	100%	90%	90%		6,3	7	7,2	9	0
Servidors Base de dades	8	8	8	8	10	8	90%	100%	90%	90%		7,2	8	7,2	9	0
Servidors de fitxers	7	7	7	8	10	7	90%	100%	90%	90%		6,3	7	7,2	9	0
Hipervisors	8	8	8	9	9	8	90%	100%	90%	90%		7,2	8	8,1	8,1	0
Aplicacions internes de gestió	6	5	5	9	9	5	90%	100%	90%	90%		4,5	5	8,1	8,1	0
Fitxers web	8	8	8	9	10	8	90%	100%	90%	95%		7,2	8	8,1	9,5	0
Documentació Interna	5	9	9	1	1	8	90%	100%	90%	95%		8,1	9	0,9	0,95	0
Xarxa Interna	6	8	5	8	5	8		100%	90%	100%		0	5	7,2	5	0
Connexions Fibra Òptica	7	8	5	8	10	8		100%	90%	100%		0	5	7,2	10	0
Connexió telefònica / VoIP	6	7	7	5	5	7		100%	90%	100%		0	7	4,5	5	0

Serveis de Cloud Gestionat	8	8	8	8	10	8		90%	90%	100%		0	7,2	7,2	10	0
CPD	9	8	10	10	10	8		75%		100%		0	7,5	0	10	0
Armaris / Gàbia	8	5	10	10	10	8		75%		100%		0	7,5	0	10	0
Hardware de recanvi	1	0	0	0	1	0		10%	10%	10%		0	0	0	0,1	0

4.4 Nivell de Risc Acceptable i Risc Residual

El nivell de risc acceptable per l'organització es mig o menor. En valors quantitatius s'accepten els riscos amb un valor igual a 6 o menor. Aquestes amenaces tenen un impacte assumible per l'organització. Les amenaces amb un valor superior a 6 han de ser tractades amb controls fins que el nivell de risc de l'amenaça siga igual o menor a 6, el risc residual.

Risc Acceptable	
Valor qualitatiu	**Valor quantitatiu**
Molt alt	10
Alt	7-9
Mig	4-6
Baix	1-3
Molt baix	0

Per tal de centrar els esforços en els actius que presenten un problema major, s'haurà de calcular el risc que representa cada actiu.

Una vegada es té l'impacte potencial de cadascun dels actius en les distintes dimensions, es calcula la seva mitjana per tindre un valor d'impacte únic. Es presenta també el valor de l'actiu en format numèric i la probabilitat de que es materialitze una amenaça. Amb aquests 3 valors es realitza la mitjana aritmètica per calcular el nivell de risc de què una amenaça afecte a l'actiu.

Els actius nivells de risc superior a 6 seran l'eix central per a la implantació de nous controls.

Valor → valor econòmic de l'actiu

Impacte Pot → mitjana impacte 5 dimensions

Probabilitat → major probabilitat d'amenaça

Actiu	Valor	Impacte Pot.	Probabilitat	Risc
Routers BGP	10	9,67	3	7,56
Switches	10	9,67	3	7,56
Servidors	9	9,67	3	7,22
Router Mikrotik	10	9,67	3	7,56
Equips d' oficina	4	3,33	3	3,44
Firewall	4	3,33	3	3,44
DNS	9	9,00	3	7,00
Telèfons VoIP	5	4,87	3	4,29
Direcció	7	2,92	3	4,31
Personal tècnic	8	3,08	6	5,69
Sistemes Operatius	8	7,85	6	7,28
Servidors Web	7	7,38	6	6,79
Servidors Base de dades	8	7,85	6	7,28
Servidors de fitxers	7	7,38	6	6,79
Hipervisors	8	7,85	6	7,28
Aplicacions internes de gestió	6	6,43	6	6,14
Fitxers web	8	8,20	6	7,40
Documentació Interna	5	4,74	1	3,58
Xarxa Interna	6	5,73	1	4,24
Connexions Fibra Òptica	7	7,40	1	5,13
Connexió telefònica / VoIP	6	5,50	3	4,83
Serveis de Cloud Gestiont	8	8,13	0	5,38
CPD	9	5,83	0	4,94
Armaris / Gàbia	8	5,83	0	4,61
Hardware de recanvi	1	0,03	0	0,34

A la taula anterior, es ressalten amb roig els actius amb un risc major. Si consultem les taules d'amenaces d'aquests riscos vegem que aquests actius son afectats per 31 amenaces amb un risc major a l'acceptable.

El següent pas és crear controls que minimitzen el risc dels actius amb un valor superior a l'acceptable.

Com a exemple, podem considerar l'actiu «Servidors de fitxers» és afectat per les següents amenaces:

Amenaça	Freqüència	A	C	I	D	A
[I.5] Averia d'origen físic o lògic	6				75%	
[E.1] Errors dels usuaris	5		50%	50%	50%	
[E.2] Errors de l'administrador	5		90%	90%	90%	
[E.8] Difusió de malware	4		90%	90%	90%	
[E.19] Fugues d'informació	0		100%			
[E.20] Vulnerabilitats dels programes (software)	6		90%	90%	90%	
[E.21] Errors de manteniment / actualització de programes (software)	3			75%	75%	
[A.5] Suplantació de la identitat de l'usuari	0	90%	90%	90%		
[A.6] Abús de privilegis d'accés	0		75%	75%	75%	
[A.11] Accés no autoritzat	0		75%	75%		
[A.22] Manipulació de programes	6		85%	85%	85%	

A la taula es marquen les més crítiques. El següent pas seria aplicar els controls apropiats per reduir l'impacte i la probabilitat d'aquestes amenaces, per tal de reduir el risc.

Per exemple, aplicant controls sobre el Servidor de fitxers, es podria reduir el risc als següents valors:

Actiu	Valor	Impacte Pot.	Probabilitat	Risc
Servidors de fitxers	7	4.6	3	4.8

Com s'observa, fent els càlculs necessaris com els vists a l'adjunt **«AARR.ods»** per obtindre l'impacte potencial i el risc, s'ha aconseguit reduir el valor un risc acceptable d'amenaces sobre l'actiu. Aquest valor anomenat risc residual es podrà millorar en les següents revisions.

5. Fase 4. Propostes de projectes

A la fase anterior s'ha seguit el procés per tal d'identificar els actius que necessiten de l'aplicació de controls per tal de reduir el seu nivell de risc.

Per tant, els projectes hauran d'estar orientats a minimitzar els efecte de les amenaces que afecten als actius i, si és possible, eliminar-les.

Les propostes de projectes tindran com a principal objectiu ser aplicables als següents actius:

Actiu	Risc
Routers BGP	7,56
Switches	7,56
Servidors	7,22
Router Mikrotik	7,56
DNS	7,00
Sistemes Operatius	7,28
Servidors Web	6,79
Servidors Base de dades	7,28
Servidors de fitxers	6,79
Hipervisors	7,28
Aplicacions internes de gestió	6,14
Fitxers web	7,40

5.1 Projecte «Router Mikrotik redundat (VRRP)»

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: ROUTER MIKROTIK REDUNDAT (VRRP)			Pàgina : 1 de 2

Descripció

Com s'ha vist al diagrama de xarxa de la Figura 2. tota la xarxa de l'organització es comunica amb l'exterior a través d'un router Mikrotik a través de la xarxa del CPD.

Aquest router interconnecta la xarxa del CPD amb la de l'organització de forma redundada, és a dir, el router de l'organització es connecta a dos routers del CPD, per tant existeix una connexió de backup en cas de que un dels routers del CPD quede inoperatiu. No obstant, en el cas de què el router Mikrotik quedara indisponible tota la xarxa de l'organització es quedaria sense servei, menys les oficines que compten amb una connexió de backup.

La caiguda d'aquest router implicaria que els serveis oferits pels clouds gestionats serien inaccessibles.

Per tant, es proposa l'adquisició d'un segon router Mikrotik de les mateixes característiques que el que ja existeix, per tal de substituir el primer en cas de que es quede sense servei.

El segon router no serà un element passiu a l'espera de que entre en funcionament, sinò que, mitjançant el protocol VRRP i l'acció humana per tal de mantindre els canvis del que es troba en funcionament, permetrà l'activació d'aquest segon router de forma automàtica en cas de que el primer quedara sense servei. A més, cada un d'aquests routers estarà connectat als routers BGP del CPD de forma redundada, permetent la caiguda de 2 routers sense que la disponibilitat siga afectada.

Objectius

Amb el projecte s'intenta, per una banda, tenir un hardware de backup de forma activa i per l'altra, augmentar la seguretat afegint redundància a la interconnexió amb el CPD. Açò permetrà assimilar els error i averies que aquests equips puguen sofrir afegint redundància a la infraestructura de xarxa.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [E.2] Errors del administrador
- [E.23] Errors de manteniment / actualització d'equips (hardware)

- [E.24] Caiguda del sistema per esgotament de recursos
- [A.11] Accés no autoritzat
- [A.23] Manipulació dels equips
- [A.24] Denegació de servici
- [A.25] Robatori

Sobre els següents actius:

- Router Mikrotik

Recursos

Recurs	Descripció	Cost
Router Mikrotik	Element hardware	4000€
Administrador xarxes	Hores de l'administrador de xarxes per tal d'implementar la solució, personal especialitzat extern.	3000€
Cablejat xarxes	Element hardware	200€
		Total: 7200€

Planificació

Pas	Tasca	Duració
1	Estudi de la infraestructura actual	5d
2	Adquisició de hardware	2d
3	Implementació de la solució	5d
4	Proves	3d
5	Millores	5d
		Total: 20 dies

Dominis de la norma ISO/IEC 27002 tractats

- 17.1.1 Planificación de la continuidad de la seguridad de la información
- 17.1.2 Implantación de la continuidad de la seguridad de la información
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

5.2 Projecte «Router Mikrotik redundat (backup)»

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: ROUTER MIKROTIK REDUNDAT (BACKUP)			Pàgina : 1 de 2

Descripció

Aquest projecte és una segona opció al projecte anterior per tal de minimitzar els riscos del router principal de l'organització i la seva interconexió amb el CPD.

Per tant, es proposa l'adquisició d'un segon router Mikrotik de les mateixes característiques que el que ja existeix, per tal de substituir el primer en cas de que es quede sense servei, en aquest cas, de forma manual.

Es crearà un procediment pel qual es podrà possar en funcionament el router de backup. Per tal de que el procediment tinga exit, es crearà un sistema de backups del router de producció, el qual crearà un backup de la seva configuració a un servidor extern, per tal de que es puga utilitzar per deixar en funcionament el router de backup en cas de necessitat.

El procediment serà aproximadament:

1. Tenir en funcionament el sistema de backup del router principal, per tenir un repositori d'arxius de configuració.
2. Obtenir l'última còpia realitzada.
3. Importació en el router de backup.
4. Connexió del router de backup a la resta de infraestructura.
5. Comprovacions.

Objectius

Amb el projecte s'intenta, per una banda, tenir un hardware de backup de forma activa i per l'altra, augmentar la seguretat afegint redundància a la interconnexió amb el CPD.

En aquesta ocasió, aquest segon router és un element passiu a l'espera de ser posat en producció.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [E.2] Errors del administrador
- [E.23] Errors de manteniment / actualització d'equips (hardware)

Sobre els següents actius:

- Router Mikrotik

Recursos

Recurs	Descripció	Cost
Router Mikrotik	Element hardware	4000€
Administrador xarxes	Hores de l'administrador de xarxes per tal d'implementar la solució, personal intern.	0€ (cost intern)
Cablejat xarxes	Element hardware	200€
		Total: 7200€

Planificació

Pas	Tasca	Duració
1	Estudi de la infraestructura actual	4d
2	Adquisició de hardware	2d
3	Creació del procediment	1d
4	Implementació de la solució	1d
5	Proves	1d
6	Millores	1d
		Total: 10 dies

Dominis de la norma ISO/IEC 27002 tractats

- 17.1.1 Planificación de la continuidad de la seguridad de la información
- 17.1.2 Implantación de la continuidad de la seguridad de la información
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

5.3 Projecte «Documentació de nous projectes»

Elaborat per: **Iván Arocas**	Revisat per: **Direcció**	Aprovat per: **Comitè Seguretat**	Data: **04/04/16** Versió: **1.0**
Document: **DOCUMENTACIÓ DE NOUS PROJECTES**			Pàgina : **1** de **3**

Descripció

El projecte consisteix en desenvolupar un format de document per tal de registrar els nous projectes que es van a implantar a l'organització, ja siga per la incorporació de nous clients o la expansió d'altres.

Abans de començar qualsevol projecte es registraran tots els components en la següent plantilla:

Projecte: Nom del projecte.	**Codi:** Codi del projecte	**Aprovat per:** Direcció	**Data: 04/04/16** **Versió: 1.0**
Components			**Referencia**
Components hardware			
Component hardware 1			Ref1
Component hardware 2			Ref2
Components software			
Components software 1			Ref1
Components software 2			Ref2
Altres			
Altres 1			Ref1
Altres 2			Ref2
Descripció del projecte:			
Més informació:			
Client:			
Data d'entrega estimada:			

Aquest document, on es detallaran les característiques dels projectes serà entregat als tècnics que hauran d'implantar la solució al client.

Posteriorment aquests tècnics afegiran informació al document degut a les variacions en l'execució dels projectes per tal de servir per futures referències.

Objectius

L'objectiu d'aquest projecte és tindre una fitxa de treball on centralitzar la informació referent als nous projectes desenvolupats per l'organització. Amb aquests documents s'intenta que els tècnics tinguen clar el que s'ha de fer en cada cas, el producte final, la data d'entrega que s'ha de complir i els components en els quals està dividit el projecte.

També permetrà en cas de dubtes d'actuació adreçar-se al document per trobar més informació dels sistema que s'està tractant, ja siga en els moments inicials del projecte o quan duga un temps en producció.

Permetrà ajudar al tècnics per realitzar intervencions i modificacions evitant errors del personal de l'organització.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [E.1] Errors dels usuaris
- [E.2] Errors del administrador
- [E.21] Errors de manteniment / actualització de programes (software)

Sobre les següents categories d'actius:

- [SW] Software - Aplicacions informàtiques
- [HW] Equipament informàtic (hardware)
- [S] Serveis

Recursos

Recurs	Descripció	Cost
Comité Seguretat	El projecte consistirà en posar-se d'acord amb la direcció per tal de veure quina informació ha de contenir la fitxa de projecte. També en acordar el compromís d'enregistrar les dades a l'inici del projecte.	0€ (cost temporal intern)
Direcció	Assistència a les reunions.	0€ (cost temporal intern)
		Total: 0€

Planificació

Pas	Tasca	Duració
1	Reunions per crear el document	5d
2	Millores del document	1d
		Total: 6 dies

Dominis de la norma ISO/IEC 27002 tractats

- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.

5.4 Projecte «Revisió d'instal·lacions, compliment de requisits»

Elaborat per: **Iván Arocas**	Revisat per: **Direcció**	Aprovat per: **Comitè Seguretat**	Data: **04/04/16** Versió: **1.0**
Document: **REVISIÓ D'INSTAL·LACIONS, COMPLIMENT DE REQUISITS**			Pàgina : **1** de **3**

Descripció

El projecte consisteix en tenir un procediment per tal de comprovar que tant nous projectes com antics projectes, compleixen la política de seguretat, les normes de qualitat i les configuracions adequades.

Per tal de registrar les revisions realitzades s'ha d'utilitzar el següent document:

Projecte:" Nom del projecte.	**Codi:** Codi del projecte	**Revisat per:** Tècnic 1	**Data: 04/04/16** **Versió: 1.0**
Objectiu			**Estat**
Monitorització activa			OK
Backups programats			NOK
Firewall			No aplica
Actualitzacions			OK
Tests de carrega			OK
Test serveis redundats			OK
Entrega client			OK

Al document quedarà registrada la informació del projecte per tal de referenciar-lo i els objectius a revisar, com pot ser la monitorització activada o els backups programats.

Aquesta fitxa serà creada pel tècnic responsable del projecte una vegada finalitzat.

Objectius

Evitar incidents de seguretat per mala configuració, errors intencionats o fortuïts.

Evitar errors produïts per les ajustades dates d'entrega de projectes.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [A.6] Abús de privilegis d'accés
- [A.7] Uso no previst
- [A.11] Accés no autoritzat
- [A.23] Manipulació dels equips
- [A.24] Denegació de servici

Sobre les següents categories d'actius:

- [SW] Software - Aplicacions informàtiques
- [HW] Equipament informàtic (hardware)
- [D] Dades / Informació
- [COM] Xarxes de comunicacions
- [S] Serveis

Recursos

Recurs	Descripció	Cost
Comité Seguretat	El projecte consistirà en posar-se d'acord amb la direcció per tal de veure quins requisits i de qui serà la responsabilitat de revisar les instal·lacions.	0€ (cost temporal intern)
Direcció	Assistència a les reunions.	0€ (cost temporal intern)
		Total: 0€

Planificació

Pas	Tasca	Duració
1	Reunions per crear el document	5d
2	Millores del document	1d
		Total: 6 dies

Dominis de la norma ISO/IEC 27002 tractats

- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.3.1 Copias de seguridad de la información.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 12.7.1 Controles de auditoría de los sistemas de información.

5.5 Projecte «Pen-tests interns, prevenció d'incidents»

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: PEN-TESTS INTERNS, PREVENCIÓ D'INCIDENTS			Pàgina : 1 de 3

Descripció

Realització de tests de penetració interns per tal de descobrir vulnerabilitats a les aplicacions webs que es serveixen a través dels clouds gestionats i dels serveis del que es composen els clouds gestionats.

Les tasques d'auditoria es realitzaran mitjançant eines automàtiques com nessus, arachni o nikto. Si es detecta alguna anomalia greu es realitzarà un estudi manual.

Els pent-tests realitzats generaran informes on es podrà valorar l'estat dels distints projectes i les necessitats d'actuació en matèria de la seguretat de la informació.

Objectius

Millorar la seguretat dels actius evitant problemes causats per males configuracions o errors de desenvolupament.

Evitar possibles atacs de fonts externes. Aquests tests ajudaran a la detecció de software desactualitzat i vulnerable.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [A.6] Abús de privilegis d'accés
- [A.11] Accés no autoritzat
- [A.23] Manipulació dels equips
- [A.24] Denegació de servici

  [A.9] [Re-]encaminament de missatges
- [A.10] Alteració de seqüencia
- [A.12] Anàlisi de tràfic
- [A.14] Captura d'informació (escolta)

- [A.15] Modificació deliberada de la informació
- [A.24] Denegació de servei

Sobre les següents categories d'actius:

- [SW] Software - Aplicacions informàtiques
- [HW] Equipament informàtic (hardware)
- [D] Dades / Informació
- [COM] Xarxes de comunicacions
- [S] Serveis

Recursos

Recurs	Descripció	Cost
Tècnics	Encarregats de llençar, analitzar i gestionar els informes generats per les eines automàtiques. Revisions manuals de les anomalies detectades.	24000€ - 30000 (contractació de més personal)
Aplicacions d'anàlisi de vulnerabilitats	Aplicacions d'anàlisi de vulnerabilitats com nessus, arachni o nikto.	2000€
		Total: 32000€

Planificació

Pas	Tasca	Duració
1	Reunions per acordar la forma de realitzar les auditories	10d
2	Realització de auditories	2d
3	Millores	5d
		Total: 17 dies

Dominis de la norma ISO/IEC 27002 tractats

- 12.2.1 Controles contra el código malicioso.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.
- 12.7.1 Controles de auditoría de los sistemas de información.

5.6 Projecte «Pla d'actuació front a incidents de seguretat»

Elaborat per: **Iván Arocas**	Revisat per: **Direcció**	Aprovat per: **Comitè Seguretat**	Data: **04/04/16** Versió: **1.0**
Document: **PLA D'ACTUACIÓ FRONT A INCIDENTS DE SEGURETAT**			Pàgina : **1** de **2**

Descripció

El projecte especifica la forma d'actuar davant d'un incident de seguretat. De qui serà responsabilitat de gestionar els incidents. Qui tindrà que realitzar les accions de contenció oportunes. Com registrar l'incident. Les acciones correctives per evitar que es torne a produir.

Cada incident s'haurà de registrar en un document per a tal fi, de cada un dels incidents registrats s'haurà d'incloure la següent informació:

Incident: Nom del incident.	**Codi:** Codi del incident	**Revisat per:** Tècnic 1	**Data: 04/04/16** **Versió: 1.0**
Font de notificació: Font externa, interna, client, etc.			
Descripció: Descripció de l'incident.			
Accions de contenció/correcció: Accions preses.			
Accions de prevenció: Accions preses per evitar que e l'incident torne a produir-se.			

Objectius

Minimitzar l'impacte d'un incident de seguretat gracies a la ràpida actuació del personal encarregat.

Obtenir informació i experiència dels incidents registrats.

Millorar les condicions de seguretat de l'organització.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [E.8] Difusió de malware

- [E.19] Fugues d'informació
- [A.22] Manipulació de programes
- [A.15] Modificació deliberada de la informació

Sobre les següents categories d'actius:

- [SW] Software - Aplicacions informàtiques
- [D] Dades / Informació

Recursos

Recurs	Descripció	Cost
Tècnics	Encarregats de gestionar els incidents de seguretat.	24000€ - 30000 (contractació de més personal)
		Total: 30000€

Planificació

Pas	Tasca	Duració
1	Reunions per acordar la forma de gestionar els incidents	15d
2	Millores	5d
		Total: 20 dies

Dominis de la norma ISO/IEC 27002 tractats

- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.

5.7 Projecte «Creació cloud de backup»

Elaborat per: **Iván Arocas**	Revisat per: **Direcció**	Aprovat per: **Comitè Seguretat**	Data: **04/04/16** Versió: **1.0**
Document: **CREACIÓ CLOUD DE BACKUP**			Pàgina : **1 de 2**

Descripció

El projecte consisteix en la creació d'un entorn cloud genèric de backup, per tal de suplir a qualsevol dels clouds en producció si per qualsevol problema queda indisponible.

La instal·lació i configuració d'aquests clouds és un procés llarg i costos, per tant, tenir un preconfigurat, a falta d'adaptar al client afectat, incorporant un increment en la seguretat dels actius que depenen d'aquest element ja que es podria posar en funcionament en poques hores.

Aquest backup consistirà en dos equips físics amb l'hipervisor XenServer instal·lat i l'esquelet bàsic de màquines virtuals ja creades, per tal de que es puga restaurar un backup de fitxers, base de dades i configuració de qualsevol client per tal de restablir el servei.

Objectius

Obtenir un «cloud gestionat» preparat per entrar en producció en el menor temps possible.

Evitar una caiguda de servei superior al establert per el SLA de l'organització.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [E.2] Errors del administrador
- [E.23] Errors de manteniment / actualització d'equips (hardware)
- [E.24] Caiguda del sistema per esgotament de recursos
- [A.11] Accés no autoritzat
- [A.23] Manipulació dels equips
- [A.24] Denegació de servici
- [A.25] Robatori

Sobre les següents categories d'actius:

1. [HW] Equipament informàtic (hardware)
2. [SW] Software - Aplicacions informàtiques

Recursos

Recurs	Descripció	Cost
Administrador de Sistemes	Instal·lació i configuració del cloud	0€ (cost intern)
Servidor HP DL 165 G7	Servidor	1000€x2
		Total: 2000€

Planificació

Pas	Tasca	Duració
1	Adquisició del hardware	15d
2	Instal·lació i configuració	5d
		Total: 20 dies

Dominis de la norma ISO/IEC 27002 tractats

- 12.3.1 Copias de seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

5.8 Projecte «Noves controladores switchs»

Elaborat per: **Iván Arocas**	Revisat per: **Direcció**	Aprovat per: **Comitè Seguretat**	Data: **04/04/16** Versió: **1.0**
Document: **NOVES CONTROLADORES SWITCHS**			Pàgina : **1 de 2**

Descripció

El switch que conté cadascun dels armaris és de tipus modular, a més de tenir doble font d'alimentació, permet instal·lar una segona controladora.

Aquesta controladora s'encarrega de fer funcionar la resta de mòduls i les funcions de switch. Tenint aquest component redundat es guanyaria en disponibilitat. També es guanyaria en tolerància a fallades, ja que permetria proves de configuració al tenir dos controladores permetent utilitzar una per a configuracions de proves.

Objectius

L'objectiu és afegir redundància a l'equipament hardware de tipus switch per tal de protegir-los front a diverses amenaces.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

[E.2] Errors del administrador

[E.23] Errors de manteniment / actualització d'equips (hardware)

[E.24] Caiguda del sistema per esgotament de recursos

[A.24] Denegació de servici

Sobre els següents actius:

- Switches

Recursos

Recurs	Descripció	Cost
Controladora	Component hardware	5000€x3
Técnic de xarxes	Instal·lació del hardware	0€ (cost temporal intern)

	Total: 15000€

Planificació

Pas	Tasca	Duració
1	Adquisició del hardware	15d
2	Instal·lació	2d
3	Proves	5d
		Total: 22 dies

Dominis de la norma ISO/IEC 27002 tractats

17.1.1 Planificación de la continuidad de la seguridad de la información

17.1.2 Implantación de la continuidad de la seguridad de la información

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

5.9 Projecte «Xifrat discos oficines»

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: XIFRAT DISCOS OFICINES			Pàgina : 1 de 2

Descripció

El sistema operatiu utilitzat en les oficines és Ubuntu, aquest permet de forma senzilla xifrar completament els disc durs dels ordinadors o les carpetes personals.

Per tant es preparara un manual d'usuari per tal de realitzar el xifrat del disc tant a la instal·lació com realitzar el proces després d'instal·lar amb un ordinador no xifrat.

Es definiran els actius que han de xifrar les dades, com els ordinadors de les oficines o els ordinadors portàtils.

Objectius

L'objectiu es evitar l'accés a d'informació interna de l'organització.

Si l'empresa sofreix un robatori dels ordinadors d'oficines, l'atacant podria tenir a accés a informació sensible de l'organització i posar en perill altres actius molt més importants que cal protegir.

S'inclourà el requisit de realitzar el xifrat de la informació seguint el procediment a la política de seguretat de l'organització, per tal de tenir les dades protegides.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [E.19] Fugues d'informació
- [A.11] Accés no autoritzat

Sobre els següents actius:

- Documentació Interna

Recursos

Recurs	Descripció	Cost

Procediment de xifrat	Procediment de xifrat de la informació	0€ (cost intern)
		Total: 0€

Planificació

Pas	Tasca	Duració
1	Reunions per a la redacció del procediment	5d
2	Revisió dels equips per complir el requisit	1d
		Total: 6 dies

Dominis de la norma ISO/IEC 27002 tractats

- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

5.10 Projecte «Open Xchange»

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: OPEN XCHANGE			Pàgina : 1 de 2

Descripció

El projecte consisteix en posar en funcionament la plataforma de software col·laboratiu Open Xchange per emmagatzemar la documentació personal dels empleats i informació del projecte. També per tal d'accedir al correu. De tal forma que es tindria un software centralitzat per tal de gestionar documents i correu dels empleats de l'organització, facilitant la tasca de compartició de fitxers i backups.

Aquesta plataforma incorpora entra altres característiques el xifrat de fitxers i correus de forma senzilla.

Objectius

Aquest projecte intenta ser una ferramenta per tal de centralitzar i protegir la informació.

Es tracta d'evitar la diversificació de la informació. Mantenir vàries plataformes per a cada necessitat pot ser beneficiós en ocasions, però arriba un moment que és inoperatiu, ja que la informació es replica en cada plataforma i o dificulta la seva cerca.

Per altra banda, al tenir tanta informació, documents, dades i correu de forma centralitzada ajuda a la seva protecció, no és el mateix intentar protegir 10 sistemes que un en concret.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [E.19] Fugues d'informació
- [A.11] Accés no autoritzat

Sobre els següents actius:

- Documentació Interna

Recursos

Recurs	Descripció	Cost
Procediment de xifrat	Procediment de xifrat de la informació	0€ (cost intern)
		Total: 0€

Planificació

Pas	Tasca	Duració
1	Reunions per a la redacció del procediment	5d
2	Revisió dels equips per complir el requisit	1d
		Total: 6 dies

Dominis de la norma ISO/IEC 27002 tractats

- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.
- 14.1.3 Protección de las transacciones por redes telemáticas.

5.11 Projecte «Actualització del Pla de continuïtat de negoci»

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: ACTUALITZACIÓ DEL PLA DE CONTINUÏTAT DE NEGOCI			Pàgina : 1 de 2

Descripció

Existeix un pla de concinnitat però està desactualitzat degut a canvis en l'organització en els últims anys.

L'actualització d'aquest pla de continuïtat es essencial per tal de implantar completament el SGSI, per tant es proposa com a projecte de millora.

Els aspectes del pla a actualitzar son:

- Actualització de responsabilitats sobre la substitució de hardware.
- Ampliació dels escenaris de desastre.
- Actualització de proveïdors de servei.
- Modificació dels processos segons la seva categoria, crítics, o no crítics.
- Revisió dels activadors del pla de continuïtat de negoci.
- Actualització del pla de recuperació

Els canvis més importants son referents a la infraestructura física dins del CPD on les condicions han canviat respecte a les responsabilitats de l'organització sobre els actius.

Objectius

Tenir un pla de continuïtat de negoci de qualitat actualitzat per tal de permetre la identificació, elaboració i desenvolupament de les accions, responsabilitats i procediment que permeten respondre front a una interrupció significativa dels processos de forma que les funcions crítiques de l'organització es restablisquen de la forma més rapida possible dins dels paràmetres adequats.

Aquest pla de continuïtat considera la situació de contingència a aplicar després de la materialització d'un desastre per tal de recuperar el nivell de servici habitual.

Amenaces a mitigar

La implantació d'aquest projecte mitigaria les amenaces següents:

- [N.1] Foc
- [N.2] Danys per aigua
- [N.*] Desastres naturals
- [I.6] Tall del subministre elèctric
- [I.7] Condicions inadequades de temperatura o humitat
- [E.2] Errors del administrador
- [E.23] Errors de manteniment / actualització d'equips (hardware)
- [E.24] Caiguda del sistema per esgotament de recursos

Sobre les següents categories d'actius:

- [HW] Equipament informàtic (hardware)

Recursos

Recurs	Descripció	Cost
Pla de continuïtat de negoci	Document del pla de continuïtat	0€ (cost intern)
		Total: 0€

Planificació

Pas	Tasca	Duració
1	Reunions per a la redacció del pla de continuïtat	15d
2	Adquisició de recursos per complir el pla	5d
		Total: 20 dies

Dominis de la norma ISO/IEC 27002 tractats

- 17.1.1 Planificación de la continuidad de la seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

5.12 Resultats i planificació global

La implantació dels projectes vists anteriorment tindrà un efecte positiu en l'estat del SGSI, però també representa un cost alt en temps i recursos. Per resumir tots aquest valors, es representen a continuació les dades de la planificació i cost del conjunt de projectes.

Planificació dels projectes:

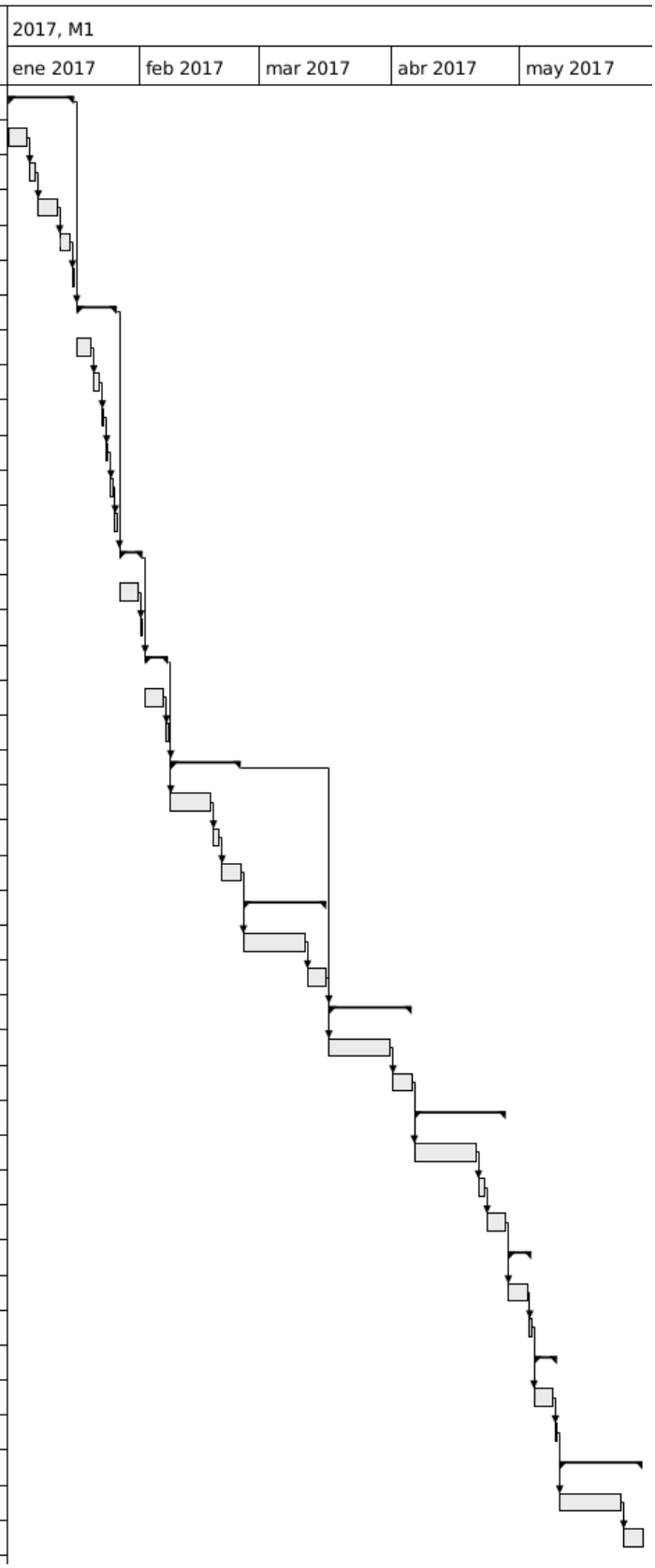
La durada total per a la implantació dels projectes es de 123 dies, uns 4 mesos. No es un temps excessiu, no obstant, el compliment d'aquesta pot ser superior tenint en compte les incidències i tasques que surten en el dia a dia i que rep la organització. Es molt probable que la duració per a la implantació de projectes es puga allargar dos mesos més.

	Tasca	Inici	Fi	Duracio
1	Router Mikrotik redundat (VRRP)	Ene 1	Ene 16	16d
1.1	Estudi de la infraestructura actual	Ene 1	Ene 5	5d
1.2	Adquisició de hardware	Ene 6	Ene 7	2d
1.3	Implementació de la solució	Ene 8	Ene 12	5d
1.4	Proves	Ene 13	Ene 15	3d
1.5	Millores	Ene 16	Ene 16	1d
2	Router Mikrotik redundat (backup)	Ene 17	Ene 26	10d
2.1	Estudi de la infraestructura actual	Ene 17	Ene 20	4d
2.2	Adquisició de hardware	Ene 21	Ene 22	2d
2.3	Creació del procediment	Ene 23	Ene 23	1d
2.4	Implementació de la solució	Ene 24	Ene 24	1d
2.5	Proves	Ene 25	Ene 25	1d
2.6	Millores	Ene 26	Ene 26	1d
3	Documentació de nous projectes	Ene 27	Feb 1	6d
3.1	Reunions per crear el document	Ene 27	Ene 31	5d
3.2	Millores del document	Feb 1	Feb 1	1d
4	Revisió d'instal·lacions, compliment de normes	Feb 2	Feb 7	6d
4.1	Reunions per crear el document	Feb 2	Feb 6	5d
4.2	Millores del document	Feb 7	Feb 7	1d
5	Pen-tests interns, prevenció d'incidents	Feb 8	Feb 24	17d
5.1	Reunions per acordar la forma de realitzar	Feb 8	Feb 17	10d

	les auditories			
5.2	Realització de auditories	Feb 18	Feb 19	2d
5.3	Millores	Feb 20	Feb 24	5d
6	Pla d'actuació front a incidents de seguretat	Feb 25	Mar 16	20d
6.1	Reunions per acordar la forma de gestionar els incidents	Feb 25	Mar 11	15d
6.2	Millores	Mar 12	Mar 16	5d
7	Creació cloud de backup	Mar 17	Apr 5	20d
7.1	Adquisició del hardware	Mar 17	Mar 31	15d
7.2	Instal·lació i configuració	Abr 1	Abr 5	5d
8	Noves controladores switchs	Abr 6	Abr 27	22d
8.1	Adquisició del hardware	Abr 6	Abr 20	15d
8.2	Instal·lació	Abr 21	Abr 22	2d
8.3	Proves	Abr 23	Abr 27	5d
9	Xifrat discos oficines	Abr 28	May 3	6d
9.1	Reunions per a la redacció del procediment	Abr 28	May 2	5d
9.2	Revisió dels equips per complir el requisit	May 3	May 3	1d
10	Open Xchange	May 4	May 9	6d
10.1	Reunions per a la redacció del procediment	May 4	May 8	5d
10.2	Revisió dels equips per complir el requisit	May 9	May 9	1d
11	Actualització del Pla de continuïtat de negoci	May 10	May 29	20d
11.1	Reunions per a la redacció del pla de continuïtat	May 10	May 24	15d
11.2	Adquisició de recursos per complir el pla	May 25	May 29	5d
			Total:	123d

Al següent diagrama de Gant es pot observar la planificació d'implantació dels projectes:

Nombre	Trab...
Router Mikrotik redundat (VRRP)	**16d**
Estudi de la infraestructura actual	5d
Adquisició de hardware	2d
Implementació de la solució	5d
Proves	3d
Millores	1d
Router Mikrotik redundat (backup)	**10d**
Estudi de la infraestructura actual	4d
Adquisició de hardware	2d
Creació del procediment	1d
Implementació de la solució	1d
Proves	1d
Millores	1d
Documentació de nous projectes	**6d**
Reunions per crear el document	5d
Millores del document	1d
Revisió d'instal·lacions, compliment de normes	**6d**
Reunions per crear el document	5d
Millores del document	1d
Pen-tests interns, prevenció d'incidents	**17d**
Reunions per acordar la forma de realitzar les auditories	10d
Realització de auditories	2d
Millores	5d
Pla d'actuació front a incidents de seguretat	**20d**
Reunions per acordar la forma de gestionar els incidents	15d
Millores	5d
Creació cloud de backup	**20d**
Adquisició del hardware	15d
Instal·lació i configuració	5d
Noves controladores switchs	**22d**
Adquisició del hardware	15d
Instal·lació	2d
Proves	5d
Xifrat discos oficines	**6d**
Reunions per a la redacció del procediment	5d
Revisió dels equips per complir el requisit	1d
Open Xchange	**6d**
Reunions per a la redacció del procediment	5d
Revisió dels equips per complir el requisit	1d
Actualització del Pla de continuïtat de negoci	**20d**
Reunions per a la redacció del pla de continuïtat	15d
Adquisició de recursos per complir el pla	5d



Cost total dels projectes:

A la següent taula es recopila el cost total de cada projecte i el seu total:

Recurs	Cost
Router Mikrotik redundat (VRRP)	
Router Mikrotik	4000 €
Administrador xarxes	3000 €
Cablejat xarxes	200 €
Router Mikrotik redundat (backup)	
Router Mikrotik	4000 €
Administrador xarxes	0,00 €
Cablejat xarxes	200 €
Documentació de nous projectes	
Comité Seguretat	0,00 €
Direcció	0,00 €
Revisió d'instal·lacions, compliment de normes	
Comité Seguretat	0,00 €
Direcció	0,00 €
Pen-tests interns, prevenció d'incidents	
Tècnics	30.000,00 €
Aplicacions d'anàlisi de vulnerabilitats	2.000,00 €
Pla d'actuació front a incidents de seguretat	
Comité Seguretat	0,00 €
Direcció	0,00 €
Creació cloud de backup	
Administrador de Sistemes	0,00 €
Servidor HP DL 165 G7	2.000,00 €
Noves controladores switchs	
Controladora	15.000,00 €
Técnic de xarxes	0,00 €
Xifrat discos oficines	
Tècnics	30.000,00 €
Open Xchange	
rocediment de xifrat	0,00 €
Actualització del Pla de continuïtat de negoci	
la de continuïtat de negoci	0,00 €
Total:	90.400,00 €

Dominis ISO tractats als projectes:

Si la implantació de tots els projecte es fa efectiva els dominis de la ISO/IEC 27002 afectats o tractats per els projectes s'enumeren a continuació. S'ha intentat que els projectes es centren en la millora i l'aplicació de controls que minimitzen el risc dels actius més vulnerables o crítics:

- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.
- 14.1.3 Protección de las transacciones por redes telemáticas.
- 17.1.1 Planificación de la continuidad de la seguridad de la información
- 17.1.2 Implantación de la continuidad de la seguridad de la información
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
- 12.3.1 Copias de seguridad de la información.
- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.
- 12.2.1 Controles contra el código malicioso.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 8.1.1 Inventario de activos.

- 8.1.2 Propiedad de los activos.

Estimació del grau de compliment

A la següent taula s'observa el grau de compliment abans i després de l'aplicació dels projectes, les millores estan marcades amb color verd.

Control	Abans dels projectes	Després dels projectes
5. POLÍTICAS DE SEGURIDAD.	30%	90%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	44%	44%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	50%	50%
8. GESTIÓN DE ACTIVOS.	66%	66%
9. CONTROL DE ACCESOS.	50%	50%
10. CIFRADO.	10%	90%
11. SEGURIDAD FÍSICA Y AMBIENTAL.	95%	95%
12. SEGURIDAD EN LA OPERATIVA.	46%	65%
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	50%	50%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	25%	63%
15. RELACIONES CON SUMINISTRADORES.	0%	0%
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	0%	90%
17. SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	28%	90%
18. CUMPLIMIENTO.	50%	50%

Per últim, les dades de la taula anterior s'han representat a uns gràfic radar per tal de comprar de forma visual la evolució del nivell de maduresa del diferents dominis de la ISO/IEC 27002.

Abans de la implantació dels projectes:

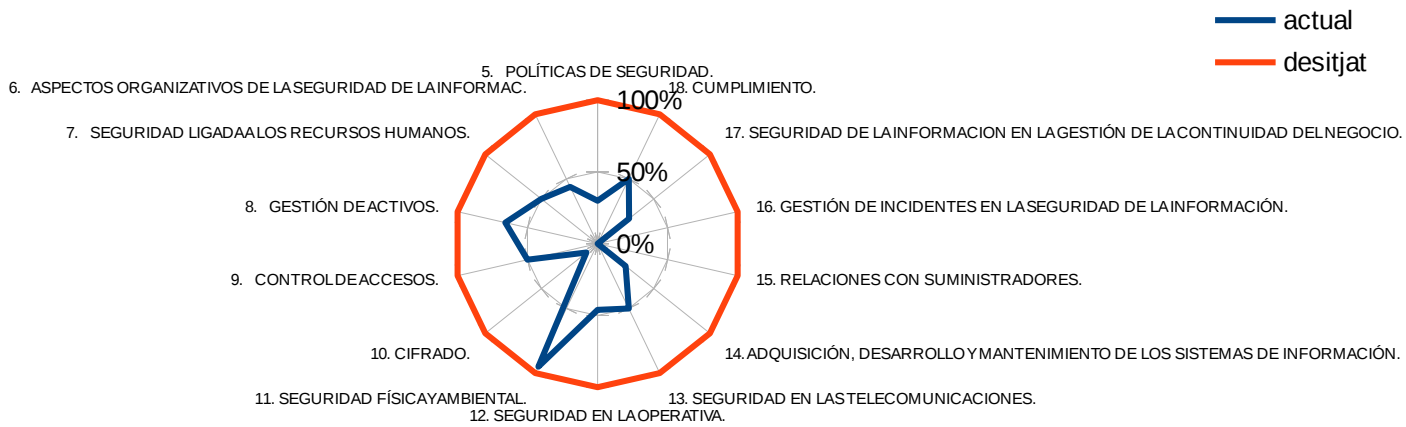


Figura 12: Nivell de compliment inicial

Després de la implantació dels projectes:

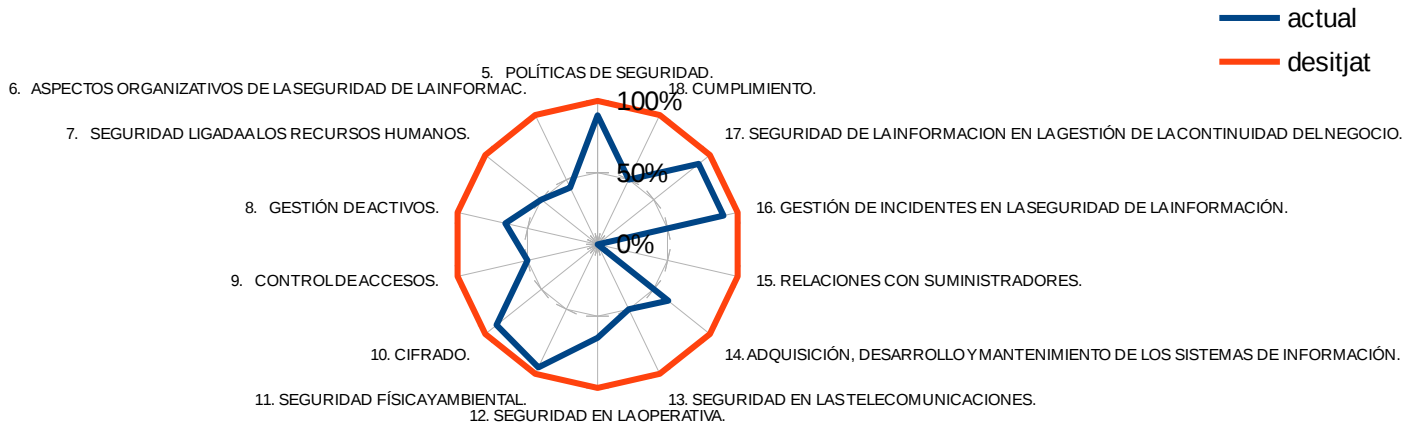


Figura 13: Nivell de compliment amb projectes

L'obtenció d'aquests valors es troba detallada als adjunts **«controls_analisi_inicial.ods»** i **«controls_amb_projectes.ods»**.

Com s'ha vist en l'evolució dels gràfics radial, la implantació dels projectes ha millorat considerablement el nivell de compliment de la ISO/IEC 27002 en les àrees següents:

- POLÍTICAS DE SEGURIDAD.
- CIFRADO
- SEGURIDAD EN LA OPERATIVA.
- GESTIÓN DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

La implantació de controls dels dominis anteriors afecten positivament als actius més crítics de l'organització, el que produiria una reducció del risc associat a cada actiu, ja que es millorarien els valors d'impacte i probabilitat cas de produir-se una amenaça.

Aquesta implantació tindria un cost econòmic d'uns 100.000 euros i la duració total de la implantació seria d'uns 4 mesos si la dedicació es del 100%.

6. Fase 5. Auditoria de compliment

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: AUDITORIA DE COMPLIMENT			Pàgina : 1 de 10

6.1 Introducció

Al següent document s'analitzarà l'estat de l'organització respecte al grau de compliment dels controls proposats per la ISO/IEC 27002:2013. S'analitzaran un a un els distints controls per tal de veure el grau d'implantació en l'organització.

El grau d'implantació de cada domini de la norma es calcularà a partir de la mitjana dels valors del controls del qual es composa.

Una vegada obtingut el grau de compliment actual, es farà una comparació respecte al grau de compliment inicial, per tal de valorar si les millores son notables.

No obstant, el grau de implantació no serà perfecte, per tant, es buscaran les no conformitat majors, menor i observacions respecte a la norma, del qual s'obtindran les àrees de millora per a optimitzar el SGSI.

Les no conformitats menors indiquen una discrepància respecte a un punt d'un domini de la norma. Les majors en canvi indicaran una falta de incompliment d'un domini complet. Per altra banda, les observacions seran indicacions que no es poden considerar no conformitats al no estar considerades a la norma però que cal reflectir-les a l'informe per la seva importància.

6.2 Abast

L'auditoria esta orientada a comprovar el grau de compliment de la norma ISO/IEC 27002:2013 de l'organització. S'analitzarà el grau d'implantació dels 14 dominis de la norma i els seus 114 controls, tenint especial atenció als dominis amb menys grau de compliment segons la auditoria anterior, en aquest cas l'inicial.

6.3 Planificació

L'encarregat de realitzar l'auditoria serà el responsable de seguretat de l'organització. Aquest serà la persona encarregada de fer els anàlisis necessaris per poder donar una valoració de l'estat de l'organització.

Les dades de l'auditoria son les següents:

Lloc de l'auditoria: Oficines de l'organització, Centre de dades. A la Figura 14 s'observa el detall de les zones auditades.

Personal auditat: Responsables de l'organització, personal tècnic, tant nivell 1 com nivell 2.

Duració: 1 mes.

Auditoria: Auditoria interna de complimenta de la ISO/IEC 27002:2013

Auditor: Auditor intern.

Actius auditats: Els inventiarats segons l'analisi de riscos, la documentació referent al SGSI elaborada per la organització, com la política de seguretat. Processos que representen controls, com el control d'accés al CPD.

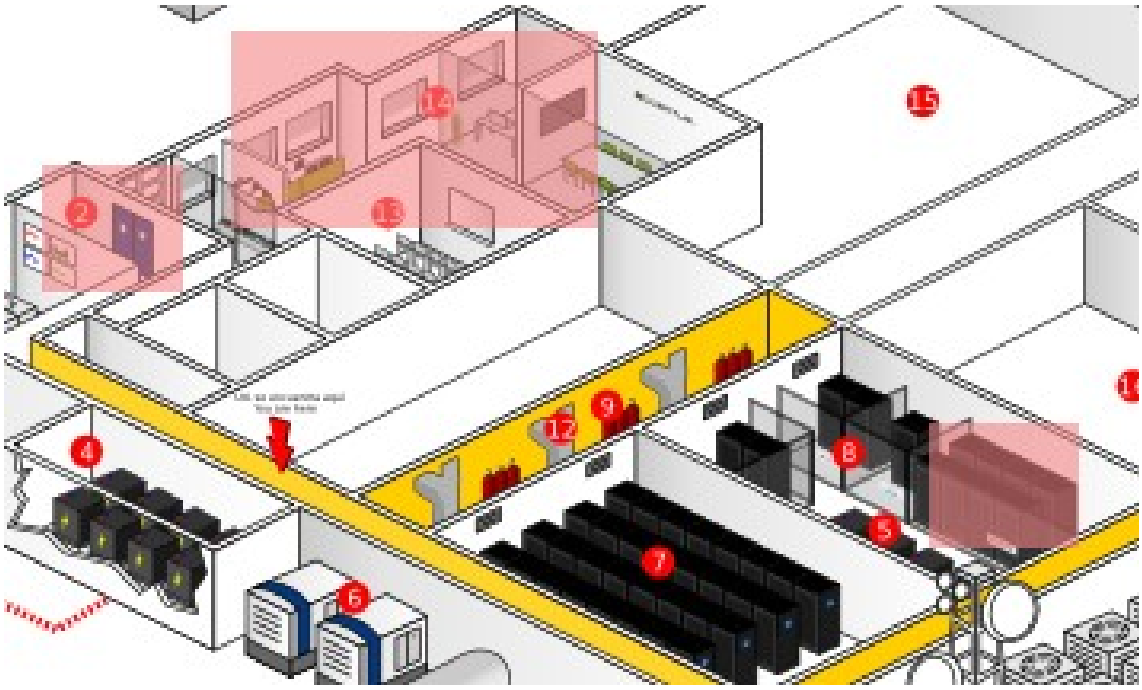


Figura 14: Àrees auditades

L'auditor utilitzarà els seus recursos i experiència per tal de calcular de forma objectiva el grau d'implantació de cadascun dels controls de la norma aplicable a cada àrea auditada.

6.4 Objectius

Obtenir l'estat de l'organització i permetre definir les àrees de millora. Comprovar l'efectivitat dels controls incorporats gracies a la implantació dels projectes definits a les fases anteriors.

6.5 Anàlisi de compliment

Una vegada s'ha realitzat la implantació dels projectes cal valorar en quin estat de la seguretat es troba l'organització.

Per tant, al igual que al punt 2.3 Anàlisi de compliment inicial, es realitzarà un anàlisi del grau d'implantació dels controls de la ISO/IEC 27002:2013 tenint en compte la implantació dels projectes definits al punt anterior.

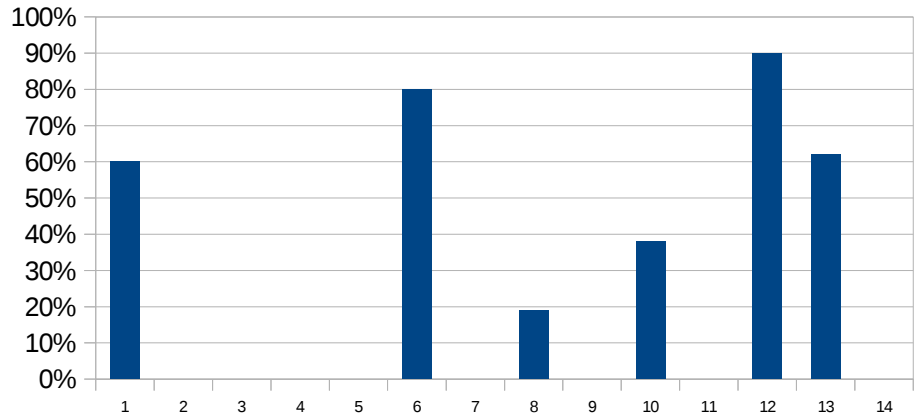
A l'**Annex H. Anàlisi de compliment**, es presenta amb detall el grau d'aplicació de cadascun dels controls dels distints dominis.

El resultat es repren a la taula següent on el grau d'implantació de cada domini és calculat segons la mitjana dels seus controls, també es representa el grau de millora de cada control respecte a l'inicial

Control	Abans dels projectes	Després dels projectes	Millora
5. POLÍTICAS DE SEGURIDAD.	30%	90%	60%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	44%	44%	0%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	50%	50%	0%
8. GESTIÓN DE ACTIVOS.	66%	66%	0%
9. CONTROL DE ACCESOS.	50%	50%	0%
10. CIFRADO.	10%	90%	80%
11. SEGURIDAD FÍSICA Y AMBIENTAL.	95%	95%	0%
12. SEGURIDAD EN LA OPERATIVA.	46%	65%	19%
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	50%	50%	0%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	25%	63%	38%
15. RELACIONES CON SUMINISTRADORES.	0%	0%	0%
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	0%	90%	90%
17. SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	28%	90%	62%

18. CUMPLIMIENTO.	50%	50%	0%

Al gràfic de barres es pot observar el percentatge de millora dels distints controls.



Als següents gràfics es pot observar els Models de Maduresa de la Capacitat (CMM) a l'anàlisi inicial de compliment i a l'actual:

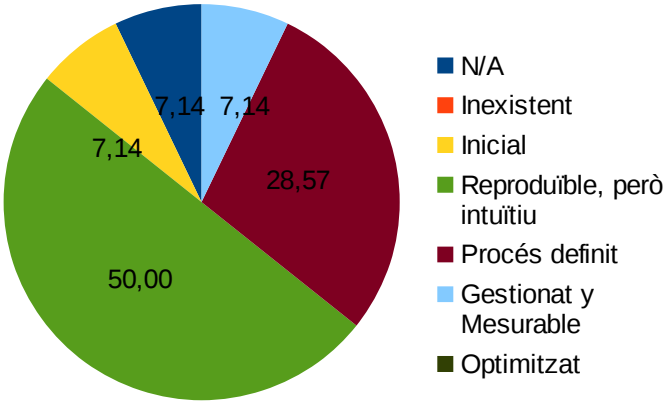


Figura 15: Compliment

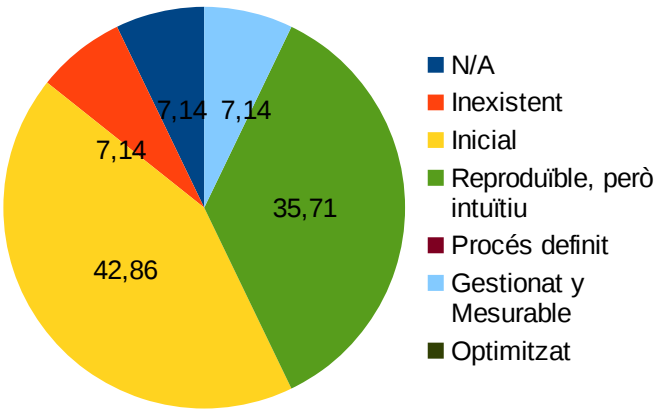


Figura 16: Compliment inicial

Els càlculs per obtindre els gràfics CMM es troben als adjunts **«controls_analisi_inicial.ods»** i **«controls_amb_projectes.ods»**

Com s'observa a la Figura 15 s'ha arribat a un valor del 50% de controls reproduïbles i quasi un 30% de control amb nivell de procés definit.

En comparació amb l'anàlisi de compliment anterior (l'anàlisi inicial) es veu una evolució positiva clara, ja que abans no es tenien controls amb nivell adequats quan ara hi ha un 43% (processos definits, gestionats o optimitzats).

També cal destacar que hi ha un 50% de controls que, centrant els esforços en ells, a les pròximes auditories de compliment, es possible que el percentatge de processos amb nivell desitjable augmente fins a un 93% si s'aconsegueix la implantació correcta dels controls adequats.

A la Figura 13 es compara el nivell actual de maduresa del SGS amb el nivell desitjat.

Grau de maduresa global:

Per tal de donar el grau de maduresa global de l'organització, podem fer una aproximació fent una mitja dels percentatges de implantació, el qual dóna com a resultat un 63,7% d'implantació respecte a l'ideal, que és el 100%

6.6 No conformitats

Encara que la evolució de l'estat del SGSI és positiva i el nivell de compliment de la ISO/IEC 27002:2013 va augmentant, s'han detectat algunes no conformitats que cal registrar per al seu tractament i resoldre-les en el menor temps possible.

A continuació es detallen les no conformitat trobades per a la seva posterior resolució:

No Conformitat:	**Auditor:**	**Data: 04/04/16**
NC1: Control d'accessos	Auditor	

Descripció de la no conformitat:

Falta informació de com gestionar l'assignació de control d'accessos dels usuaris i com actuar front les sol·licituds de modificació de privilegis d'accés.

És habitual rebre sol·licitud de clients demanant modificacions dels seus comptes d'usuari, canvis de privilegis d'accés o permetre accés remot. També el crear nous usuaris o deshabilitar altres.

No està definit si aquestes modificacions es poden realitzar, si cal realitzar-les però registrar els canvis en algun lloc o avisar al client dels perills de certes peticions.

Seria convenient detallar unes normes al respecte per tal de facilitar la tasca d'atendre aquestes peticions.

Categoria:

Menor

Control ISO/IEC 27002:2013 associat:

9.1.1 Política de control de accesos

9.1.2 Control de acceso a las redes y servicios asociados

9.2.1 Gestión de altas/bajas en el registro de usuarios

No Conformitat:	**Auditor:**	**Data: 04/04/16**
NC2: Documentació hardware incompleta	Auditor	

Descripció de la no conformitat:

S'ha detectat que un dels últims hardwares adquirits (HPE BladeSystem), no disposa de documentació adequada per al seu manteniment, gestió i operació.

Aquesta falta de informació perjudica la disponibilitat de l'actiu en el cas d'haver algun incident.

Seria convenient documentar a les plataformes per a tal fi, la forma de administrar i mantenir aquest nou hardware.

Categoria:

Menor

Control ISO/IEC 27002:2013 associat:

11.2.4 Mantenimiento de los equipos

12.1.1 Documentación de procedimientos de operación

No Conformitat:	**Auditor:**	**Data: 04/04/16**
NC3: Política d'actualitzacions	Auditor	

Descripció de la no conformitat:

No existeix una política o procediment per tal de gestionar les actualitzacions disponibles dels sistemes operatius ni de la seva paquetera oficial.

Al sistemes operatiu GNU/Linux, com Debian, Ubuntu o CentOS és habitual tenir disponibles actualitzacions que reparen deficiències en la programació del software disponible en la seva paqueteria. Aquestes actualitzacions es solen aplicar quan surt alguna vulnerabilitat greu, però no existeix un procediment per tal de actualitzar de forma programada, així que les actualitzacions depenen de si una vulnerabilitat es coneguda per algun membre del equip i es posa en marxa un procediment de actualització manual.

Categoria:

Menor

Control ISO/IEC 27002:2013 associat:

12.1.1 Documentación de procedimientos de operación

12.6.1 Gestión de las vulnerabilidades técnicas

No Conformitat:	**Auditor:**	**Data: 04/04/16**
NC4: Sobreasignament de rescursos	Auditor	
Descripció de la no conformitat: Es habitual el sobreasignament de recursos i d'utilització d'actius per a un fi en el que inicialment no varen ser pensats en moments de necessitat. Aquestes situacions generen situacions caòtiques o de descontrol, ja que aquestes modificacions poques vegades son documentades.		
Categoria: Menor		
Control ISO/IEC 27002:2013 associat: 8.1.3 Uso aceptable de los activos		

No Conformitat:	**Auditor:**	**Data: 04/04/16**
NC5: Formació periòdica	Auditor	
Descripció de la no conformitat: No existeix formació programada orientada a la seguretat de la informació ni cal donar a conèixer la política de seguretat i les bones pràctiques, fet indicat en la política de seguretat.		
Categoria: Menor		
Control ISO/IEC 27002:2013 associat: 7.2.2 Concienciación, educación y capacitación en segur. de la informac		

No Conformitat:	**Auditor:**	**Data: 04/04/16**
NC6: Política sobre teletreball	Auditor	
Descripció de la no conformitat: S'ha detectat que ocasionalment es fa ús del teletreball, no existeix un procediment de seguretat per aquestes ocasions, encara que sí bones pràctiques fruit de l'experiència. Existeix la necessitat de formalitzar una política d'actuació en el teletreball que contemple aspectes sobre com es deuen connectar els empleats als serveis interns de l'organització, per exemple l'obligació d'ús de VPN per tal de accedir a la xarxa interna.		
Categoria: Menor		
Control ISO/IEC 27002:2013 associat: 6.2.2 Teletrabajo		

No Conformitat:	**Auditor:**	**Data: 04/04/16**
NC7: Registre d'esdeveniments d'activitat	Auditor	
Descripció de la no conformitat: Els events d'activitat no estan centralitzats per a la posterior revisió, tampoc estan protegits front a l'eliminació o alteració d'aquests. Aquesta no conformitat pot fer no fiables els registres de sistema a l'hora de revisar-los per tal de realitzar un anàlisi d'incidents de seguretat.		
Categoria: Menor		
Control ISO/IEC 27002:2013 associat: 12.4.2 Protección de los registros de información		

No Conformitat:	**Auditor:**	**Data: 04/04/16**
NC8: Canals de comunicació alternatius	Auditor	
Descripció de la no conformitat:		
S'ha detectat la falta de canals alternatius per a la comunicació dels clients en els casos en què l'única via de comunicació és el correu electrònic. És habitual que aquest tipus de clients tinguen problemes amb el correu i no puguen ser notificats sobre esdeveniments dels seus servidors, com averies o falta de pagament.		
Categoria:		
Menor		
Control ISO/IEC 27002:2013 associat:		
13.2.3 Mensajería electrónica		

6.7 Observacions

Per altra banda, s'han observat les següents característiques que mereixen ser registrades:

Observació:	**Auditor:**	**Data: 04/04/16**
OB1: Control de capacitat dels backups	Auditor	
Descripció de la observació:		
No existeix un procediment per controlar el augment de ocupació dels backups, tampoc existeix una disposició conservadora de l'espai ocupat, permetent que augmente sense control el que pot causar un bloqueig complet de les tasques de copia.		
Categoria:		
Observació		
Control ISO/IEC 27002:2013 associat:		
12.3.1 Copias de seguridad de la información		

Observació:	**Auditor:**	**Data: 04/04/16**
OB2: Evidències de proves de recuperació	Auditor	
Descripció de la observació: No s'observen evidències de què els mecanismes de recuperació i de continuïtat de negoci d'alguns actius es revisen i proven periòdicament. Dhauria d'haver procediments i registres dels processos d'execució dels processos de recuperació de la informació per tal de verificar la seva utilitat.		
Categoria: Observació		
Control ISO/IEC 27002:2013 associat: 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información		

6.8 Valoració de les no conformitats

A l'informe d'auditora s'han trobat 8 no conformitats les quals son de caràcter menor i poden ser eliminades de forma relativament ràpida. A més de 2 observacions.

A la següent taula s'indiquen la correspondència entre els dominis de la ISO/IEC 27002:2013 i les no conformitats i observacions detectades:

Control	Maduresa	No conformitats	Observacions
5. POLÍTICAS DE SEGURIDAD.	90%		
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	44%	1	
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	50%	1	
8. GESTIÓN DE ACTIVOS.	66%	1	
9. CONTROL DE ACCESOS.	50%	1	
10. CIFRADO.	90%		
11. SEGURIDAD FÍSICA Y AMBIENTAL.	95%	1	
12. SEGURIDAD EN LA OPERATIVA.	65%	4	1
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	50%	1	

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	63%		
15. RELACIONES CON SUMINISTRADORES.	0%		
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	90%		
17. SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	90%		1
18. CUMPLIMIENTO.	50%		

La majoria de les no conformitats es troben a àrees de la ISO/IEC 27002:2013 amb un nivell de implantació baix, pel que serà necessari l'anàlisi i creació de projectes que ajuden a l'augment de la implantació d'aquests dominis, per tant caldria atacar els següents dominis de la ISO:

- 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 9. CONTROL DE ACCESOS.
- 13. SEGURIDAD EN LAS TELECOMUNICACIONES.

Altres no conformitats i observacions es troben emmarcades dins de dominis amb un grau de compliment alt, el que indica és que encara queden detalls que millorar o ajustar, aquests objectius marcaran el camí de les millores a incorporar al SGSI.

7. Fase 6. Conclusions

La realització del pla director ha permès valorar de forma real en quin estat es troba l'organització per tal de optar a la certificació ISO/IEC 27001:2013.

La documentació exigida per la norma ha sigut incorporada al gestor documental utilitzat per l'organització permetent la visualització dels documents interessants per al personal de l'organització, com la política de seguretat.

La fase d'anàlisi de riscos, tant la valoració de riscos com l'anàlisi d'amenaces possibles i el seu impacte en els actius, ha permès donar una visió formal de les amenaces a les que els sistemes de la informació de l'organització estan exposats en el dia a dia.

Aquest anàlisi de riscos ha fet que surta la necessitat d'idear projectes i solucions per millorar i protegir els actius, alguns dels projectes proposats a la fase corresponen del treball ja estan en implantació.

La valoració general de la realització del treball ha sigut positiva, ja que ha avançat considerablement la preparació de la certificació i s'ha pogut valorar en quins aspectes destaca l'organització i en quins altres cal concentrar els esforços.

Els principals avantatges a destacar són:

- Implicació de la direcció en la implantació d'un SGSI de qualitat.
- Coneixements i aptituds del personal de l'organització.
- Llarga experiència

En canvi, les necessitats de millora es centren en:

- Elaboració de documentació.
- Formalització de procediments basats en l'experiència.
- Definició de responsabilitats

La implantació d'alguns dels projectes proposats actua directament en les necessitats de millora, per tant el següent pas després d'aquest pla director, és completar la materialització dels projectes per al posterior anàlisi de resultats.

8. Glossari

IaaS: *Infraestructura* com a servei, model de «cloud computing» basat en l'oferiment de recursos en forma de màquines virtuals accessibles de forma remota.

VRRP: Protocol de redundància no propietari definit en el RFC 3768.

Mikrotik: És una empresa letona proveïdora de tecnologia de xarxes.

BGP: Protocol mitjançant el qual s'intercanvien rutes entre sistemes autònoms per tal de fer accessibles les direccions ip de forma global.

HPE BladeSystem: Sistema modular de servidors composat per un chasis i diversos servidors anomenats «Blade».

XenServer: Plataforma de virtualització open source.

9. Bibliografia

1. **Estandar Internacional:** ISO/IEC 17799, http://www.17799.com/papers/iso17799scope.pdf, 01/03/16
2. **Web:** http://iso27000.es/iso27002.html, 01/03/16
3. **Llibre:** Diseño de un sistema de gestión de seguridad de información, Alberto G. Alexander
4. **Llibre:** Sistema de gestión de la seguridad de la información (UOC). Daniel Cruz Allende, Silvia Garre Gui
5. **Metodologia:** MAGERIT versión 3

Annex A. Política de seguretat de la informació

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓ			Pàgina : 1 de 3

Objectiu:

La política de seguretat te com a objectius establir les directrius necessàries per assegurar els sistemes de la informació indispensables per a la prestació dels serveis que la organització ofereix als clients. Totes aquestes directrius estaran emmarcades en les obligacions legals aplicables a la organització.

També reunir tots el components dels que forma part el servei oferit baix control per tal de seguir prestant els serveis seguint els estàndards de qualitat que esperen els clients, evitant problemes que puguen afectar a la seguretat dels sistemes i els serveis o actuar adequadament davant d'un incident de seguretat.

Aquesta política de seguretat no és immutable i està en continua revisió, per tant la seva estructura, al igual que el SGSI, està basada en un cicle PDCA (plan do check act) el que ajuda a què es millore contínuament.

Objectius de seguretat:

- Assegurar la confidencialitat, integritat i disponibilitat de les dades.
- Complir els requisits legals aplicables a l'organització.
- Tenir un pla de continuïtat de negoci que permeta recuperar-se d'un desastre en el menor temps possible.
- Protegir els elements essencials per al funcionament de l'organització.
- Crear un pla de formació per als empleats en matèria de seguretat de la informació.
- Registrar els incidents de seguretat.
- Crear plans de millora de la seguretat de la informació de l'organització mitjançant revisions periòdiques.

Planificació:

Les actuacions a realitzar per part de l'organització per tal de complir amb els objectius de seguretat passen per la planificació, implantació, operació i manteniment del sistema de gestió de la seguretat de la informació que està en coherència amb aquesta política.

Per tal de garantir una correcta gestió de la seguretat, l'organització realitza un estudi exhaustiu de la seguretat a través de l'anàlisi de riscos i l'establiment de un pla de tractament de riscos per tal de reduir l'impacte del riscos acordats a tractar per el comitè de seguretat i aprovats per la direcció.

El procediment seguit per realitzar l'anàlisi de riscos es tracta en profunditat a **l'Annex F. Metodologia de Anàlisis de Riscos.**

Actuació dels responsables

Una vegada realitzat la avaluació de riscos, en funció dels resultats obtinguts en la fase de planificació, serà tasca del Responsable de Seguretat junt amb el Comitè de Seguretat creat per a tal fi, implantar els controls necessaris per a les amenaces detectades i acordades a tractar.

Serà la seva responsabilitat actuar davant dels incidents de seguretat seguint els procediments creats per al seu tractament.

Responsabilitat dels usuaris

- Els usuaris dels sistemes de la informació hauran d'esforçar-se en promoure i utilitzar eficientment aquest amb el fi d'evitar tràfic i transaccions innecessàries a la xarxa.
- És responsabilitat dels usuaris la correcta utilització i custòdia dels actius que tinguen en possessió per al desenvolupament de les seves tasques, ordinadors, telèfons, servidors, etc.
- No divulgar ni utilitzar la informació a la que es tinga accés durant la relació laboral amb l'organització. Aquest compromís haurà d'aplicar-se inclòs després de finalitzada la relació laboral.

- Assegurar que tots els empleats i tercers entenguen les seves responsabilitats i són adequades per a realitzar les seves funcions de cara a reduir el risc de robatori, frau o ús indegut dels recursos posats a la seva disposició.
- Es previndrà tot tipus de accés físic no autoritzat i es duran a terme mesures de seguretat per a evitar pèrdues, danys, robatoris o circumstàncies que posen en perill els actius o que puguen provocar la interrupció de les activitats.
- Els usuaris d'Internet i correu electrònic huran de fer accés eficient de les xarxes i preservant la confidencialitat i integritat de les dades transmeses per aquests mitjans.
- S'evitarà qualsevol tipus d'incompliment de les lleis u obligacions legals, reglamentaries o contractuals i els requisits de seguretat que afecten als sistemes de la informació.
- Es seguiran les distintes normes a l'hora de crear nous serveis o projectes, com per exemple, l'ús de contrasenyes segures o configuracions de firewalls.

Revisió i millora

Tant la política de seguretat com el sistema gestor de la seguretat de la informació son revisats regularment a intervals planificats, o si ocorren canvis significatius per tal d'assegurar la contínua idoneïtat, eficàcia i efectivitat de la política. De forma genèrica, son revisats anualment mitjançant la auditoria interna del SGSI o la revisió del sistema per part de la direcció, realitzant un profund anàlisi del sistema i detectant possibles millores i deficiències.

Les millores del sistema de seguretat de la informació són establertes durant les fases de revisió o mitjançant aportacions del personal que se consideren interessants, incentivant i animant a que es produeixin aquest tipus d'intervencions.

Aquestes idees seran posteriorment revisades per el responsable i el comitè de seguretat per tal de incorporar-les al SGSI.

Annex B. Procediment d'Auditories Internes

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: PROCEDIMENT D'AUDITORIES INTERNES			Pàgina : 1 de 4

Objectiu:

Aquest procediment te l'objectiu de servir de guia a l'hora de realitzar les auditories internes de seguretat periòdiques. Tasca essencial per verificar que el conjunt de controls, objectius, processos i procediments es troben en bon estat, seguint les directrius de la norma i el requeriments especificats per l'organització.

Per tal de que les tasques d'auditoria es realitzen sempre de la forma adequada es crea aquest programa de auditoria.

1. Responsable

La gestió del programa estarà a càrrec del responsable de seguretat de l'empresa. Aquest serà l'encarregat de que el programa d'auditoria s'execute tal com s'ha programat. També serà tasca seva la organització del personal, realitzar les gestions necessàries per obtindre el recursos necessàries per realitzar les auditories i justificar la necessitat del programa.

També seran responsables el comitè de seguretat, l'auditor intern i la direcció.

2. Objectius, exclusions, prioritats i extensió

L'objectiu del programa d'auditoria es comprovar que el SGSI funciona perfectament, trobar fallades i punts de millora.

Els principals actius de l'organització son 44 servidors físics que contenen 220 máquines virtuals, diversos dispositius de xarxa com routers i switches, i també 6 equips de treball que utilitzen el operadors i administradors. Per tant el programa d'auditoria tindrà preferència en l'anàlisi d'aquests objectes per ser els més susceptibles de que siguen afectats per alguna amenaça.

El servidors accessibles des d'Internet tindran prioritat front a la resta per ser més vulnerables. Els equips dels usuaris i administradors també tindran una prioritat alta ja que els usuari interactuen contínuament amb ells i poden no seguir les pautes del SGSI.

3. Recursos

Com s'ha vist al punt anterior la infraestructura a auditar te una grandària considerable, 44 servidors físics, 220 entorns virtuals i gran quantitat d'equipament de xarxa i de equips de usuari.

Segons l'organigrama l'empresa caldria incorporar els recursos necessaris per realitzar l'auditoria ja que no compta d'un departament complet de seguretat informàtica actualment.

Per l'extensió, un petit departament de seguretat amb un responsable seria suficients per complir els objectius del programa d'auditoria si no tingues que ocupar-se de les incidències habituals del dia a dia.

Per el qual va a ser impossible disposar de l'equip complet per a l'auditoria.

També, per garantir la independència, el personal que realitzes les auditories no deuria conèixer amb detall les característiques del sistema a auditar, com es probable que algun membre del personal coneguí aquest detalls, aquest grup es redueix encara més.

Per tant, seria recomanable comptar amb l'ajuda de personal extern en el moments de realitzar les auditories programades per unir-se al equip d'auditors.

Auditor Intern: L'auditor intern deurà posseir alguna titulació relacionada amb el marc de referencia a auditar i tindre experiència demostrable en almenys dos auditories. Aquesta persona tindrà les següents funcions i obligacions:

- Comprendre i complir amb els criteris per realitzar l'auditoria.
- Verificar la definició i correcta aplicació dels procediments de l'auditoria interna.
- Presentar els informes d'auditoria.
- Guardar en secret les dades obtingudes al realitzar l'auditoria.
- Conèixer la normativa interna.

4. Planificació

Les auditories es realitzaran anualment. La durada de les auditories serà d'aproximadament una setmana, una part per als objectes més crítics i l'altra per a la resta. L'elaboració de documentació o d'informes no està inclosa en aquesta setmana.

5. Implementació

Serà tasca del responsable del programa fer el seguiment de la seva execució i recopilar els resultats per als posteriors informes, aquest informes tindran el format indicat a l'apartat 7. Format de l'informe d'auditoria.

Abans d'executar les accions d'auditoria es comunicarà als responsables del sistemes a auditar.

6. Revisió i millora

Després de l'auditoria es farà una revisió d'aquesta per trobar fallades i punts de millora.

Deguts a les necessitats del programa i a la rapidesa de canvi de les noves tecnologies, almenys, es realitzaran 2 cicles de formació a l'any per als tècnics encarregats de realitzar les auditories.

7. Format de l'informe d'auditoria

Elaborat per: Auditor	Revisat per: Responsable de Seguretat	Data: 04/04/16
Document: Informe d'auditoria Interna		Pàgina : 1 de X

Resultat de l'informe:

Redacció del resultat de l'informe per part del responsable, indicant els objectius, anàlisis realitzats, les conclusions i les propostes de millora.

No conformitats:

Actiu	Amenaça	Descripció / Recomanacions	Impacte
Exemple 1: Apache Web Server	Múltiples vulnerabilitats. CVE-2013-2249 CVE-2011-3192 CVE-2012-0883	Permet realitzar ataques DOS i XSS entre altres. Actualitzar la versió del servei. O aplicar pegats de seguretat	Mitja
Exemple 2: Servidor Armari1-79	Sobreasignament dels recursos	Inestabilitat del servidor. Possible caiguda del servei. Reducció de càrrega o augment de recursos.	Greu

Annex C. Gestió d'Indicadors

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: GESTIÓ D'INDICADORS			Pàgina : 1 de 3

Objectiu

Per tal de valorar l'eficàcia dels controls implantats a l'organització es crea aquest procediment.

S'indicarà la forma de procedir per tal de gestionar les mesures dels indicadors per avaluar els controls corresponents i es proporciona la metodologia per registrar aquestes mesures.

Realització de mesures

La realització de mesures es realitzarà de forma automàtica quan siga possible, sent necessària l'acció humana per part del membre designat per tal de valorar les mostres al registre de controls i indicadors definit al procediment.

- El registre dels distints elements hardware i software, maquinari, xarxes, i PDU i tot dispositiu amb connexió de xarxa, es realitzarà a través de l'eina de monitorització OPSVIEW. Aquesta registra les distintes mesures generant un històric de mesures i genera alertes segons els umbrals definits.
- El registre de l'estat de la xarxa i subxarxes es realitzarà a través de l'eina CACTI, aquest registra l'estat del tràfic de xarxa que passa a través dels distints routers i firewalls.
- Les mostres que tinguen que ser registrades de forma manual s'introduiran en plantilles de tipus full de calcul, com per exemple, els processos manuals de revisió de backups, el processos de revisió d'aplicacions instal·lades o els processos d'anàlisi d'incidents de seguretat per al posterior anàlisi.

Registre d'Indicadors

Per tal d'organitzar i valorar totes les mostres generades manualment o automàticament i decidir si els controls implants són adequats, es consultarà la

següent taula on es definiran els umbrals per comprovar que un control ha deixat de ser efectiu. A la taula es defineixen els indicadors més rellevants implantats actualment.

Control	Indicador	Descripció	Umbral	Mostres
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.				
7.1.1 Investigación de antecedentes.	Investigació d'antecedents	Abans de la contractació s'investiga per valorar que el candidat te la formació adequada	<1 investigacions	Abans d'una contractació
7.2.2 Concienciación, educación y capacitación en segur. de la informac.	Formació de l'empleat adequada	Es necessari mantindre un pla de formació adequat per a que els empleats puguen realitzar la tasca adequadament	<2 cursos de formació anuals	Anual
7.3.1 Cese o cambio de puesto de trabajo.	Aplicació de procediment al produir-se un acomiadament	S'ha de aplicar el procediment que indica els actius que ha de tornar a l'organització i el canvi de passwords corresponent	<1 aplicacions del procediment	Al produirse un acomiadament
8. GESTIÓN DE ACTIVOS.				
8.1.3 Uso aceptable de los activos.	Ús de recursos dels sistemes i xarxes	Controlar l'ús que es fa dels actius	95%	Cada 5 minuts
9. CONTROL DE ACCESOS.				
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Accés limitat als servidors	No es permet accés complet als sistemes per part del personal extern de no ser absolutament necessari	>10 accessos no controlats	Mensual
9.4.3 Gestión de contraseñas de usuario.	Canvi periòdic de contrasenyes	Canvi periòdic de les passwords d'accés	>1 canvis no efectuats	Anual
11. SEGURIDAD FÍSICA Y AMBIENTAL.				
11.1.1 Perímetro de seguridad física.	Accés físic acotat	L'accés a l'organització esta protegit baix clau i un edifici.	>0 violacions del perímetre	Al produïrse la mostra
11.1.2 Controles físicos de entrada.	Registre d'accessos	Revisió dels accessos al CPD registrats en nom de l'organització	>0 accessos no autorizats	Anual
11.1.3 Seguridad de oficinas, despachos y recursos.	Alarmes	Registre d'activació de l'alarma	>0 alarmes activades	Al produïrse la mostra
11.2.1 Emplazamiento y protección de equipos.	Equips protegits mitjançant estructures metàliques	Nombre d'equips afectats per accidents	>2 equips afectats	Anual

11.2.2 Instalaciones de suministro.	UPS del CPD	Registre de les caigudes de tensió i activació dels UPS	>0 caigudes totals de l'energia	Al produirse la mostra
11.2.4 Mantenimiento de los equipos.	Realització de manteniment	Registre de les actuacions de manteniment realitzades	>2 actuacions no realitzades	Anual
12. SEGURIDAD EN LA OPERATIVA.				
12.3.1 Copias de seguridad de la información.	Còpies automàtiques d'arxius	Control manual de la realització de les còpies programades mitjançant scripts d'anàlisi.	Fallades anuals <10	Setmanal
13. SEGURIDAD EN LAS TELECOMUNICACIONES.				
13.1.1 Controles de red	Instal·lació de firewall individual a cada equip	Incidències detectades al no aplicar correctament les configuracions de firewall adecuades	<5 incidències detectades	Al detectar-se una incidència

Annex D. Procediment de Revisió per Direcció

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: PROCEDIMENT DE REVISIÓ PER DIRECCIÓ			Pàgina : 1 de 2

Objectiu

Segons la ISO 27001, es necessari que la Direcció realitze revisions periòdiques de l'estat. Aquestes revisions pretenen que es cree una visió de l'estat del SGSI des d'un punt de vista gerencial, ja que la gerència o direcció és la responsable d'assignar i aportar recursos per a que el sistema de la informació funcione amb garanties.

Amb aquestes revisions pot saber de primera mà si tot funciona correctament i si el SGSI es adequat, assignant o eliminant recursos segons el seu estat.

Procediment

La direcció tindrà per norma revisar l'estat del SGSI una vegada a l'any. Aquestes revisions quedaran registrades segons aquest procediment.

Es tindrà que indicar:

- La data de la reunió
- Lloc de la reunió
- Hora de la reunió
- Assistents a la reunió

Al començar la revisió per part de la direcció es comptarà amb els següents elements d'entrada:

- Resultats de les auditores i revisions anteriors.
- Retroalimentació de les parts interessades.
- Tècniques, productes o procediments que es puguen utilitzar en la organització i l'efectivitat del SGSI.
- Estat de les accions preventives i correctives.

- Vulnerabilitats o amenaces no tractades adequadament en l'avaluació de riscos prèvia.
- Resultats dels indicadors dels controls.
- Accions de seguiment de les revisions gerencials prèvies.
- Qualsevol canvi que puga afectar al SGSI.
- Recomanacions per part dels empleats per al millorament.
- Revisió de la formació dels empleats.

Una vegada realitzada l'anàlisi, es tindrà com a resultat:

- Modificacions que milloren l'efectivitat del SGSI.
- Actualització de la avaluació de riscos i el pla de tractament de riscos.
- Modificació de procediments i controls que afecten a la seguretat de la informació.
- Necessitats de recursos.
- Millora de com es valora l'efectivitat dels controls.

Planificació

Es planificaran les revisions gerencials per realitzar-les una vegada a l'any després de l'auditoria interna i abans de l'auditoria de l'entitat certificadora si es donara el cas.

Annex E. Gestió de Rols i Responsabilitats

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: GESTIÓ DE ROLS I RESPONSABILITATS			Pàgina : 1 de 3

Objectiu

El procediment té com objectiu definir els rols i les responsabilitats de cada actor implicat en el SGSI.

Gestió de responsabilitats

L'organització estableix i gestiona un sistema de la seguretat de la informació amb el fi de protegir els actius d'aquesta. Per a tal motiu cal assignar un conjunt de rols i responsabilitats per garantir que les normes descrites en el sistema de gestió es compleixen.

Per a tal fi es creen les següents figures:

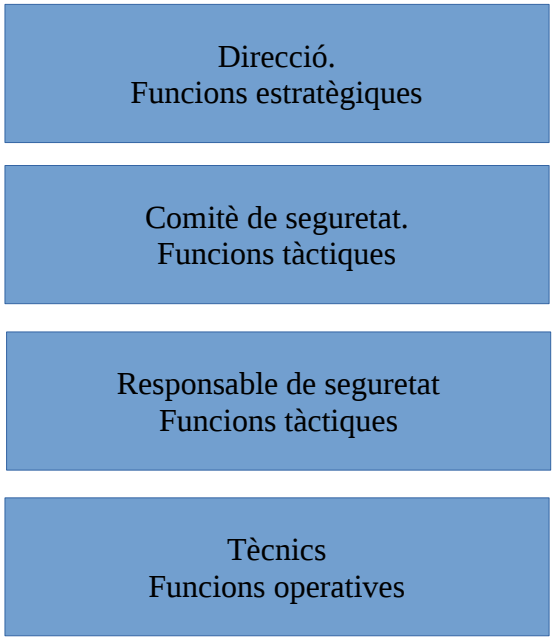


Figura 17: Rols

Cadascun d'aquests rols s'ocuparà principalment de:

Direcció. Estarà integrat pels membres que formen part de la direcció de l'organització, s'ocuparan de:

- Garantir que la seguretat siga un tema a tractar a les reunions programades amb el grup de direcció de l'organització.
- Fer els nomenaments de la resta de rols, com per exemple el responsable de seguretat i el comitè de seguretat.
- Donar suport econòmic i organitzacional per tal de poder dur a terme la implantació i millora del SGSI.
- Aprovar els distints plans de seguretat.

Comitè de seguretat. Estarà integrat per membres que formen part de la direcció de l'organització a més del responsable de seguretat i tècnics de nivell 2, s'ocuparan de:

- Implantar les decisions preses pel comitè de direcció en matèria de seguretat.
- Assignar rols i responsabilitats amb un paper important en el SGSI.
- Validar el pla de seguretat de la informació. Supervisar la implantació i fer el seguiment.
- Fer complir la legislació que sigui aplicable a l'organització en matèria de seguretat.
- Promoure l'ús del sistema de la informació segons la política de seguretat.
- Revisar les incidències més important.
- Revisió del SGSI en general.

Responsable de seguretat:

- Implantar les decisions preses pel comitè de seguretat.
- Promoure l'ús del sistema de la informació segons la política de seguretat, millorar aquest política i mantenir-la.
- Fer de punt central del SGSI, sent el principal enllaç entre el personal amb funcions tàctiques, operatives i estratègiques.

- Coordinació en la implantació de controls del SGSI.

Tècnics. Aquest rol estarà integrat per totes les persones que formen part del departament tècnic de l'organització, s'ocuparan de:

- Complir les polítiques, les normes i els procediments en matèria de seguretat de la informació.
- Implantar els controls definits pel comitè de seguretat.
- Col·laboració amb el responsable de seguretat per a la millora i definició de procediments i normes.
- Implantar mesures per protegir la informació.

Annex F. Metodologia de Anàlisis de Riscos

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: METODOLOGÍA DE ANÀLISI DE RISCOS			Pàgina : 1 de 5

Objectius

Es tracta de definir els criteris i la metodologia a seguir per a realitzar l'inventari d'actius de la organització i el posterior anàlisi de riscos que puguen afectar a la seguretat de la organització. Aquesta metodologia estarà basada amb la Magerit amb les modificacions oportunes per adequar-la a l'organització.

Inventari de actius

Per a realitzar l'inventari d'actius d'ON SL es tindran en compte les següents consideracions:

Cada actiu serà classificat en una de les següents categories:

- **[D] Dades / Informació:** Dades de qualsevol tipus i format (BBDD, codi font, manuals), independentment de com estiguen organitzats i on estiguen allotjats. És un actiu intangible.
- **[L] Instal·lacions:** Elements físics que alberguen actius de l'organització, com puguen ser oficines, seus, despatxos o el CPD.
- **[HW] Equipament informàtic (hardware):** Considerant tant el dispositiu electrònic com la configuració necessària per a què funcione. No es té en compte la informació que conté, categoritzada com a informació.
- **[SW] Software:** Aplicacions informàtiques: Aplicacions de tot tipus, com ofimàtica, desenvolupament, administració, gestió de sistemes, etc. Les dades que puguen gestionar se consideren dades de tipus informació.
- [**P] Personal:** Empleats de l'organització, sense els quals no podria funcionar.
- **[COM] Xarxes de comunicacions:** Xarxa local de l'organització, dispositius de xarxa com el router, switch, firewall, etc. Junt a la seva configuració.

Una vegada que els actius s'hagen categoritzat, es realitzarà una valoració qualitativa dels mateixos, definint la següent informació de cadascun:

- Nom del actiu.
- Unitats.
- Categoria (Descrita anteriorment).
- Propietari de l'actiu: Persona o càrreg que l'administra, autoritza l'ús, regula o gestiona l'actiu.

Realitzada la valoració inicial dels actius, el següent pas es valorar la importància que tenen per a la organització, analitzant els actius en base a cinc dimensions, com son:

- **Integritat:** Es refereix a l'exactitud de la informació. Una pèrdua d'integritat pot fer que les dades siguen incoherents. En relació a altres categories d'actius, la pèrdua d'integritat es tradueix a un mal funcionament.

Valor qualitatiu	Valor quantitatiu	Criteri
Molt alt	10	No es pot funcionar sense ell
Alt	7-9	Es produeix mal funcionament en el servei
Mig	4-6	Es produeixen errors lleus
Baix	1-3	Es produeixen errors inapreciables
Molt baix	0	No afecta al servici

- **Confidencialitat**: Una pèrdua de confidencialitat pot derivar en incidències de seguretat quan un usuari no autoritzat accedeix a la informació del actiu. Aquest usuari pot adquirir coneixement que l'utilitze per perjudicar els interessos de l'organització.

Valor qualitatiu	Valor quantitatiu	Criteri
Molt alt	10	Fer-ho pública suposa una pèrdua total de la confiança de l'opinió pública.
Alt	7-9	Fer-ho pública suposa una pèrdua important de la confiança de l'opinió pública.
Mig	4-6	Fer-ho pública suposa una pèrdua lleu de la confiança de l'opinió pública.
Baix	1-3	Fer-ho pública suposa una pèrdua mínima de la confiança de l'opinió pública.
Molt baix	0	Es pot fer públic.

Disponibilitat: La disponibilitat d'un actiu pot afectar negativament al negoci, provocant que certs processos se vegen mermats o cancel·lats durant el temps que l'actiu es trobe inoperatiu. Un actiu disponible ha de ser accessible en el moment en que es necessite.

Cal considerar el temps necessari en substituir l'actiu i deixar-lo com estava abans de que ocorreguera l'incident de seguretat.

Valor qualitatiu	Valor quantitatiu	Criteri
Molt alt	10	No es pot prescindir de l'actiu més de 2 hores
Alt	7-9	No es pot prescindir de l'actiu més de 4 hores
Mig	4-6	No es pot prescindir de l'actiu més de 1 dia
Baix	1-3	No es pot prescindir de l'actiu més de 2 dies
Molt baix	0	Es pot prescindir de l'actiu 2 dies o més

També es valorarà la **autenticitat** i la **traçabilitat. L**a primera indica que qui presenta una identitat es qui diu ser, la segona indica que es poden assignar les interaccions d'una entitat determinada inequívocament.

Anàlisi de riscos

Una vegada acabada la valoració dels actius, se procedirà a fer un estudi per examinar les amenaces, vulnerabilitats, impacte i risc als que estan exposats cadascun dels actius de l'organització:

1. Amenaces. Per a cada tipus d'actiu es definiran les amenaces que poden afectar-li. Aquestes són accions voluntàries o involuntàries que es poden desencadenar en un incident en la organització, produint danys materials o pèrdues immaterials en els actius. Aquestes poden ser d'un d'aquest tipus:

- D'origen natural [N]
- D'origen industrial [I]
- Atacs intencionats [A]
- Errors no intencionats [E]

2. Probabilitat o freqüència. Identificar la probabilitat de que la amenaça es materialitze segons l'experiència de l'organització. Aquesta es representarà segons la taula:

Valor qualitatiu	Valor quantitatiu	Criteri
Molt alt	10	Ocorre a diari o vàries vegades al dia
Alt	7-9	Ocorre vàries vegades a la setmana
Mig	4-6	Ocorre una vegada al mes
Baix	1-3	Ocorre varies vegades a l'any
Molt baix	0	Ocorre com a molt una vegada a l'any

3. Impacte. En cas d'ocurrència de l'amenaça es determinarà el grau de degradació que es produiria en l' organització. L'impacte es desglossarà en les cinc dimensions de la seguretat descrites anteriorment segons l'impacte que cause en cadascuna d'aquestes. Aquest valor es representa en forma de percentatge.

Posteriorment es calcularà l'impacte potencial, a partir del valor de l'actiu i l'impacte en les cinc dimensions de la seguretat que ens donarà un valor segons la taula següent.

Valor qualitatiu	Valor quantitatiu	Criteri
Molt alt	10	Dany irrecuperable, afecta a la eficàcia de la seguretat de l'organització.
Alt	7-9	Dany recuperable a llarg termini (mesos).
Mig	4-6	Dany recuperable a mig termini (dies), penalitza les activitats pròpies de l'organització.
Baix	1-3	Dany recuperable a curt termini (hores), causa petites interrupcions en les activitats.
Molt baix	0	Dany irrellevant.

A continuació es calcularà el risc de cada actiu, amb la mitjana dels valors de probabilitat, impacte i valor de cada actiu.

El comitè decidirà quins nivells de riscs no són assumibles per l'organització (alt o molt alt). Per a aquells actius pels quals no s'assumisquen riscos associats, es deurà establir un pla de tractament de riscos que es traduirà en la definició de controls a implementar, responsabilitats, planificacions i activitats a realitzar.

Annex F. Declaració de Aplicabilitat

Elaborat per: Iván Arocas	Revisat per: Direcció	Aprovat per: Comitè Seguretat	Data: 04/04/16 Versió: 1.0
Document: DECLARACIÓ DE APLICABILITAT			Pàgina : 1 de 6

Al següent document es valora l'aplicabilitat dels distints controls definits per la ISO/IEC 27002:2013 i el motiu pel que s'apliquen o no. Aquesta taula és d'utilitat per mantindre un registre dels controls implantats i l'estat d'aquests.

Control	Aplica	Motiu
5. POLÍTICAS DE SEGURIDAD.		
5.1 Directrices de la Dirección en seguridad de la información.		
5.1.1 Conjunto de políticas para la seguridad de la información.	Si	Necessitat de la creació de la política de seguretat de l'organització, aprobada per la direcció.
5.1.2 Revisión de las políticas para la seguridad de la información.	Si	Necessitat de l'actualització de la política de seguretat de l'organització degut a les noves amenaces.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.		
6.1 Organización interna.		
6.1.1 Asignación de responsabilidades para la segur. de la información.	SI	Es necessari definir responsables per tal de fer-se càrrec del bon funcionament del SGSI.
6.1.2 Segregación de tareas.	SI	Les tasques s'han d'assignar a la persona adequada per realitzar-les.
6.1.3 Contacto con las autoridades.	SI	Cal estar en contacte amb les autoritats per tal de fer complir les lleis adients.
6.1.4 Contacto con grupos de interés especial.	SI	Cal estar en contacte amb blogs, notícies i organitzacions per tal d'estar al dia sobre els nous incidents de seguretat que puguen aparèixer.
6.1.5 Seguridad de la información en la gestión de proyectos.	SI	La seguretat de la informació s'ha d'aplicar també en les fases de gestió de projectes.
6.2 Dispositivos para movilidad y teletrabajo.		
6.2.1 Política de uso de dispositivos para movilidad.	SI	Cal definir una política per a l'ús de dispositius mòbils.
6.2.2 Teletrabajo.	SI	Cal desenvolupar una política per tractar les ocasions en que es treballa des de casa, però cobrint guàrdies.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.		
7.1 Antes de la contratación.		
7.1.1 Investigación de antecedentes.	SI	Abans de cada contractació és molt important revisar el CV de cada candidat. (Ja implementat)
7.1.2 Términos y condiciones de contratación.	SI	Es necessari llegir i signar el document on s'exposen les condicions de treball.
7.2 Durante la contratación.		
7.2.1 Responsabilidades de gestión.	SI	Tots les persones que tinguen relació amb l'organització han de complir la política de seguretat.

7.2.2 Concienciación, educación y capacitación en segur. de la informac.	SI	Cal fer conèixer i formar als empleats sobre la importància de la seguretat de la informació. (Ja implementat)
7.2.3 Proceso disciplinario.	SI	Ha d'existir un procés d'amonestació en cas de no seguir les normes de seguretat.
7.3 Cese o cambio de puesto de trabajo.		
7.3.1 Cese o cambio de puesto de trabajo.	SI	Procediment per tal de gestionar l'abandonament d'un empleat del seu lloc de treball orientat a garantir la seguretat dels actius. (Ja implementat)
8. GESTIÓN DE ACTIVOS.		
8.1 Responsabilidad sobre los activos.		
8.1.1 Inventario de activos.	SI	Etiquetatge i registre dels actius de l'organització.
8.1.2 Propiedad de los activos.	SI	Tots el actius pertanyen a l'organització.
8.1.3 Uso aceptable de los activos.	SI	Control de l'ús que es fa dels actius. (Ja implementat)
8.1.4 Devolución de activos.	SI	Acord en el què s'han de tornar els actius prestats.
8.2 Clasificación de la información.		
8.2.1 Directrices de clasificación.	SI	Classificació de la informació segons importància.
8.2.2 Etiquetado y manipulado de la información.	SI	Etiquetatge i registre de la informació de l'organització.
8.2.3 Manipulación de activos.	SI	Normes de manipulació d'actius donat el seu valor.
8.3 Manejo de los soportes de almacenamiento.		
8.3.1 Gestión de soportes extraíbles.	NO	No s'utilitzen.
8.3.2 Eliminación de soportes.	SI	Eliminació de suports físics i lògics mitjançant mètodes segurs.
8.3.3 Soportes físicos en tránsito.	NO	No es trauen actius fora de l'organització.
9. CONTROL DE ACCESOS.		
9.1 Requisitos de negocio para el control de accesos.		
9.1.1 Política de control de accesos.	SI	Es presenta una política de control d'accessos bàsica.
9.1.2 Control de acceso a las redes y servicios asociados.	SI	Garantir l'accés només als recursos autoritzats.
9.2 Gestión de acceso de usuario.		
9.2.1 Gestión de altas/bajas en el registro de usuarios.	SI	Procediment per habilitar/deshabilitar l'accés dels usuaris.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	SI	Accés als servidors limitat. (Ja implementat)
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	SI	Gestió d'accessos amb privilegis especials. (Ja implementat)
9.2.4 Gestión de información confidencial de autenticación de usuarios.	SI	Emmagatzematge segur de les credencials d'accés dels usuaris. (Ja implementat)
9.2.5 Revisión de los derechos de acceso de los usuarios.	SI	Creació de procediment de revisió d'accessos.
9.2.6 Retirada o adaptación de los derechos de acceso	SI	Creació de procediment de retirada d'accessos.
9.3 Responsabilidades del usuario.		
9.3.1 Uso de información confidencial para la autenticación.	SI	El empleats tenen accés a ús d'informació per a la autentificació.
9.4 Control de acceso a sistemas y aplicaciones.		

9.4.1 Restricción del acceso a la información.	SI	Existeix un control d'accessos selectiu.
9.4.2 Procedimientos seguros de inicio de sesión.	SI	Els comptes d'usuari estan protegits amb password.
9.4.3 Gestión de contraseñas de usuario.	SI	(Ja implementat)
9.4.4 Uso de herramientas de administración de sistemas.	SI	Estandardització de les ferramentes a utilitzar.
9.4.5 Control de acceso al código fuente de los programas.	NO	No es desenvolupa software a l'organització.
10. CIFRADO.		
10.1 Controles criptográficos.		
10.1.1 Política de uso de los controles criptográficos.	SI	Necessitat de xifrar la informació dels equips d'oficines.
10.1.2 Gestión de claves.	SI	Existeixen claus de xifratge dels equips d'oficines.
11. SEGURIDAD FÍSICA Y AMBIENTAL.		
11.1 Áreas seguras.		
11.1.1 Perímetro de seguridad física.	SI	Control implantat per el CPD. (Ja implementat)
11.1.2 Controles físicos de entrada.	SI	Control implantat per el CPD. (Ja implementat)
11.1.3 Seguridad de oficinas, despachos y recursos.	SI	Control implantat per el CPD. (Ja implementat)
11.1.4 Protección contra las amenazas externas y ambientales.	SI	Control implantat per el CPD. (Ja implementat)
11.1.5 El trabajo en áreas seguras.	SI	Control implantat per el CPD. (Ja implementat)
11.1.6 Áreas de acceso público, carga y descarga.	SI	Control implantat per el CPD. (Ja implementat)
11.2 Seguridad de los equipos.		
11.2.1 Emplazamiento y protección de equipos.	SI	Existeixen equips sensibles.
11.2.2 Instalaciones de suministro.	SI	Control implantat per el CPD. (Ja implementat)
11.2.3 Seguridad del cableado.	SI	Control implantat per el CPD. (Ja implementat)
11.2.4 Mantenimiento de los equipos.	SI	Es realitza manteniment dels equips.
11.2.5 Salida de activos fuera de las dependencias de la empresa.	NO	No es trauen actius fora de les instal·lacions.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	NO	No es trauen actius fora de les instal·lacions.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	SI	Es realitza un esborrat segur dels dispositius reutilitzats.
11.2.8 Equipo informático de usuario desatendido.	SI	Tot equip ha de contenir una mínima protecció.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	SI	Existència de bloquejos de pantalla als equips de oficines.
12. SEGURIDAD EN LA OPERATIVA.		
12.1 Responsabilidades y procedimientos de operación.		
12.1.1 Documentación de procedimientos de operación.	SI	Existència de plataforma per al registre de informació.
12.1.2 Gestión de cambios.	SI	Els canvis es registren segons les peticions de servei.
12.1.3 Gestión de capacidades.	SI	Equips monitoritzats.

12.1.4 Separación de entornos de desarrollo, prueba y producción.	SI	Separació física dels entorns de producció i proves (laboratori).
12.2 Protección contra código malicioso.		
12.2.1 Controles contra el código malicioso.	SI	Ús de distribucions GNU/Linux per minimitzar l'existència de virus.
12.3 Copias de seguridad.		
12.3.1 Copias de seguridad de la información.	SI	Es realitzen copies. (Ja implementat)
12.4 Registro de actividad y supervisión.		
12.4.1 Registro y gestión de eventos de actividad.	SI	Es fan revisions periòdiques, no planificades.
12.4.2 Protección de los registros de información.	SI	No es protegeixen els registres.
12.4.3 Registros de actividad del administrador y operador del sistema.	SI	Registre automàtic en històrics de cada màquina.
12.4.4 Sincronización de relojes.	SI	Unificació d'hores d'equips d'oficina i servidors.
12.5 Control del software en explotación.		
12.5.1 Instalación del software en sistemas en producción.	SI	No es produeixen instal·lacions no autoritzades.
12.6 Gestión de la vulnerabilidad técnica.		
12.6.1 Gestión de las vulnerabilidades técnicas.	SI	Tractament de les vulnerabilitats greus que es publiquen als mitjans.
12.6.2 Restricciones en la instalación de software.	SI	Als equips d'oficina no es controla la instal·lació de software.
12.7 Consideraciones de las auditorías de los sistemas de información.		
12.7.1 Controles de auditoría de los sistemas de información.	SI	No existeix el control.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.		
13.1 Gestión de la seguridad en las redes.		
13.1.1 Controles de red.	SI	(Ja implementat)
13.1.2 Mecanismos de seguridad asociados a servicios en red.	SI	Existeixen acords de tipus SLA.
13.1.3 Segregación de redes.	SI	Separació de clients amb VLAN's.
13.2 Intercambio de información con partes externas.		
13.2.1 Políticas y procedimientos de intercambio de información.	SI	S'intercanvia informació amb tercers.
13.2.2 Acuerdos de intercambio.	SI	S'intercanvia informació amb tercers.
13.2.3 Mensajería electrónica.	SI	S'utilitza la missatgeria electrònica.
13.2.4 Acuerdos de confidencialidad y secreto.	SI	Existeixen contractes amb aquests tipus d'acords.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.		
14.1 Requisitos de seguridad de los sistemas de información.		
14.1.1 Análisis y especificación de los requisitos de seguridad.	SI	Falta de procediment per complir aquest control necessari.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	SI	Necessitat d'estandardització d'ús de SSL.
14.1.3 Protección de las transacciones por redes telemáticas.	SI	Necessitat d'estandardització d'ús de SSL.
14.2 Seguridad en los procesos de desarrollo y soporte.		

14.2.1 Política de desarrollo seguro de software.	NO	L'organització no desenvolupa software.
14.2.2 Procedimientos de control de cambios en los sistemas.	NO	L'organització no desenvolupa software.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	NO	L'organització no desenvolupa software.
14.2.4 Restricciones a los cambios en los paquetes de software.	NO	L'organització no desenvolupa software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.	NO	L'organització no desenvolupa software.
14.2.6 Seguridad en entornos de desarrollo.	NO	L'organització no desenvolupa software.
14.2.7 Externalización del desarrollo de software.	NO	L'organització no desenvolupa software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	NO	L'organització no desenvolupa software.
14.2.9 Pruebas de aceptación.	NO	L'organització no desenvolupa software.
14.3 Datos de prueba.		
14.3.1 Protección de los datos utilizados en pruebas.	SI	Protecció de dades en entorns de laboratori.
15. RELACIONES CON SUMINISTRADORES.		
15.1 Seguridad de la información en las relaciones con suministradores.		
15.1.1 Política de seguridad de la información para suministradores.	NO	Hi ha un intercanvi inapreciable d'informació amb els subministradors.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	NO	Hi ha un intercanvi inapreciable d'informació amb els subministradors.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	NO	Hi ha un intercanvi inapreciable d'informació amb els subministradors.
15.2 Gestión de la prestación del servicio por suministradores.		
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	NO	Hi ha un intercanvi inapreciable d'informació amb els subministradors.
15.2.2 Gestión de cambios en los servicios prestados por terceros.	NO	Hi ha un intercanvi inapreciable d'informació amb els subministradors.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.		
16.1 Gestión de incidentes de seguridad de la información y mejoras.		
16.1.1 Responsabilidades y procedimientos.	SI	Existència d'incidents de seguretat.. Necessitat d'establir responsabilitats i procediments front els incidents de seguretat.
16.1.2 Notificación de los eventos de seguridad de la información.	SI	Existència d'incidents de seguretat. Falta de procediment.
16.1.3 Notificación de puntos débiles de la seguridad.	SI	Existència d'incidents de seguretat. Falta de procediment.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	SI	Existència d'incidents de seguretat. Falta de procediment.
16.1.5 Respuesta a los incidentes de seguridad.	SI	Existència d'incidents de seguretat. Falta de procediment.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	SI	Existència d'incidents de seguretat. Falta de procediment.
16.1.7 Recopilación de evidencias.	SI	Existència d'incidents de seguretat. Falta de procediment.
17. SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.		
17.1 Continuidad de la seguridad de la información.		

17.1.1 Planificación de la continuidad de la seguridad de la información.	SI	Necessitat de la creació d'un pla de continuïtat de negoci. Existència d'un pla bàsic.
17.1.2 Implantación de la continuidad de la seguridad de la información.	SI	Necessitat de la creació d'un pla de continuïtat de negoci. Existència d'un pla bàsic.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	Necessitat de la creació d'un pla de continuïtat de negoci. Existència d'un pla bàsic.
17.2 Redundancias.		
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	SI	Necessitat de la creació d'un pla de continuïtat de negoci. Existència d'un pla bàsic.
18. CUMPLIMIENTO.		
18.1 Cumplimiento de los requisitos legales y contractuales.		
18.1.1 Identificación de la legislación aplicable.	SI	Coneixement exhaustiu de la Llei per part de la direcció. Per defecte es compleixen els requisits legals.
18.1.2 Derechos de propiedad intelectual (DPI).	SI	Coneixement exhaustiu de la Llei per part de la direcció. Per defecte es compleixen els requisits legals.
18.1.3 Protección de los registros de la organización.	SI	Coneixement exhaustiu de la Llei per part de la direcció. Per defecte es compleixen els requisits legals.
18.1.4 Protección de datos y privacidad de la información personal.	SI	Coneixement exhaustiu de la Llei per part de la direcció. Per defecte es compleixen els requisits legals.
18.1.5 Regulación de los controles criptográficos.	SI	Coneixement exhaustiu de la Llei per part de la direcció. Per defecte es compleixen els requisits legals.
18.2 Revisiones de la seguridad de la información.		
18.2.1 Revisión independiente de la seguridad de la información.	SI	Necessitat d'auditories externes e independents de l'estat de la seguretat.
18.2.2 Cumplimiento de las políticas y normas de seguridad.	SI	Necessitat d'auditories de l'estat de la seguretat.
18.2.3 Comprobación del cumplimiento.	SI	Necessitat d'auditories de l'estat de la seguretat.

Annex G. Anàlisi de compliment inicial

Control	Implantació
5. POLÍTICAS DE SEGURIDAD.	30%
5.1 Directrices de la Dirección en seguridad de la información.	30%
5.1.1 Conjunto de políticas para la seguridad de la información.	50%
5.1.2 Revisión de las políticas para la seguridad de la información.	10%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	44%
6.1 Organización interna.	38%
6.1.1 Asignación de responsabilidades para la segur. de la información.	10%
6.1.2 Segregación de tareas.	50%
6.1.3 Contacto con las autoridades.	0%
6.1.4 Contacto con grupos de interés especial.	50%
6.1.5 Seguridad de la información en la gestión de proyectos.	90%
6.2 Dispositivos para movilidad y teletrabajo.	50%
6.2.1 Política de uso de dispositivos para movilidad.	50%
6.2.2 Teletrabajo.	50%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	50%
7.1 Antes de la contratación.	70%
7.1.1 Investigación de antecedentes.	50%
7.1.2 Términos y condiciones de contratación.	90%
7.2 Durante la contratación.	30%
7.2.1 Responsabilidades de gestión.	90%
7.2.2 Concienciación, educación y capacitación en segur. de la informac.	0%
7.2.3 Proceso disciplinario.	0%
7.3 Cese o cambio de puesto de trabajo.	10%
7.3.1 Cese o cambio de puesto de trabajo.	10%
8. GESTIÓN DE ACTIVOS.	66%
8.1 Responsabilidad sobre los activos.	80%
8.1.1 Inventario de activos.	90%
8.1.2 Propiedad de los activos.	90%
8.1.3 Uso aceptable de los activos.	50%
8.1.4 Devolución de activos.	90%
8.2 Clasificación de la información.	70%
8.2.1 Directrices de clasificación.	90%
8.2.2 Etiquetado y manipulado de la información.	50%
8.2.3 Manipulación de activos.	50%
8.3 Manejo de los soportes de almacenamiento.	50%
8.3.1 Gestión de soportes extraíbles.	50%
8.3.2 Eliminación de soportes.	50%
8.3.3 Soportes físicos en tránsito.	50%

9. CONTROL DE ACCESOS.	50%
9.1 Requisitos de negocio para el control de accesos.	50%
9.1.1 Política de control de accesos.	50%
9.1.2 Control de acceso a las redes y servicios asociados.	50%
9.2 Gestión de acceso de usuario.	50%
9.2.1 Gestión de altas/bajas en el registro de usuarios.	50%
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	50%
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	50%
9.2.4 Gestión de información confidencial de autenticación de usuarios.	50%
9.2.5 Revisión de los derechos de acceso de los usuarios.	50%
9.2.6 Retirada o adaptación de los derechos de acceso	50%
9.3 Responsabilidades del usuario.	50%
9.3.1 Uso de información confidencial para la autenticación.	50%
9.4 Control de acceso a sistemas y aplicaciones.	50%
9.4.1 Restricción del acceso a la información.	50%
9.4.2 Procedimientos seguros de inicio de sesión.	50%
9.4.3 Gestión de contraseñas de usuario.	50%
9.4.4 Uso de herramientas de administración de sistemas.	50%
9.4.5 Control de acceso al código fuente de los programas.	50%
10. CIFRADO.	10%
10.1 Controles criptográficos.	10%
10.1.1 Política de uso de los controles criptográficos.	10%
10.1.2 Gestión de claves.	10%
11. SEGURIDAD FÍSICA Y AMBIENTAL.	95%
11.1 Áreas seguras.	95%
11.1.1 Perímetro de seguridad física.	95%
11.1.2 Controles físicos de entrada.	95%
11.1.3 Seguridad de oficinas, despachos y recursos.	95%
11.1.4 Protección contra las amenazas externas y ambientales.	95%
11.1.5 El trabajo en áreas seguras.	95%
11.1.6 Áreas de acceso público, carga y descarga.	95%
11.2 Seguridad de los equipos.	95%
11.2.1 Emplazamiento y protección de equipos.	95%
11.2.2 Instalaciones de suministro.	95%
11.2.3 Seguridad del cableado.	95%
11.2.4 Mantenimiento de los equipos.	95%
11.2.5 Salida de activos fuera de las dependencias de la empresa.	95%
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	95%
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	95%
11.2.8 Equipo informático de usuario desatendido.	95%
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	95%

12. SEGURIDAD EN LA OPERATIVA.	46%
12.1 Responsabilidades y procedimientos de operación.	63%
12.1.1 Documentación de procedimientos de operación.	90%
12.1.2 Gestión de cambios.	50%
12.1.3 Gestión de capacidades.	50%
12.1.4 Separación de entornos de desarrollo, prueba y producción.	50%
12.2 Protección contra código malicioso.	50%
12.2.1 Controles contra el código malicioso.	50%
12.3 Copias de seguridad.	100%
12.3.1 Copias de seguridad de la información.	100%
12.4 Registro de actividad y supervisión.	50%
12.4.1 Registro y gestión de eventos de actividad.	50%
12.4.2 Protección de los registros de información.	50%
12.4.3 Registros de actividad del administrador y operador del sistema.	50%
12.4.4 Sincronización de relojes.	50%
12.5 Control del software en explotación.	10%
12.5.1 Instalación del software en sistemas en producción.	10%
12.6 Gestión de la vulnerabilidad técnica.	50%
12.6.1 Gestión de las vulnerabilidades técnicas.	50%
12.6.2 Restricciones en la instalación de software.	50%
12.7 Consideraciones de las auditorías de los sistemas de información.	0%
12.7.1 Controles de auditoría de los sistemas de información.	0%
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	50%
13.1 Gestión de la seguridad en las redes.	50%
13.1.1 Controles de red.	50%
13.1.2 Mecanismos de seguridad asociados a servicios en red.	50%
13.1.3 Segregación de redes.	50%
13.2 Intercambio de información con partes externas.	50%
13.2.1 Políticas y procedimientos de intercambio de información.	50%
13.2.2 Acuerdos de intercambio.	50%
13.2.3 Mensajería electrónica.	50%
13.2.4 Acuerdos de confidencialidad y secreto.	50%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	25%
14.1 Requisitos de seguridad de los sistemas de información.	50%
14.1.1 Análisis y especificación de los requisitos de seguridad.	50%
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	50%
14.1.3 Protección de las transacciones por redes telemáticas.	50%
14.2 Seguridad en los procesos de desarrollo y soporte.	N/A
14.2.1 Política de desarrollo seguro de software.	N/A
14.2.2 Procedimientos de control de cambios en los sistemas.	N/A
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	N/A

14.2.4 Restricciones a los cambios en los paquetes de software.	N/A
14.2.5 Uso de principios de ingeniería en protección de sistemas.	N/A
14.2.6 Seguridad en entornos de desarrollo.	N/A
14.2.7 Externalización del desarrollo de software.	N/A
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	N/A
14.2.9 Pruebas de aceptación.	N/A
14.3 Datos de prueba.	N/A
14.3.1 Protección de los datos utilizados en pruebas.	N/A
15. RELACIONES CON SUMINISTRADORES.	N/A
15.1 Seguridad de la información en las relaciones con suministradores.	N/A
15.1.1 Política de seguridad de la información para suministradores.	N/A
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	N/A
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	N/A
15.2 Gestión de la prestación del servicio por suministradores.	N/A
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	N/A
15.2.2 Gestión de cambios en los servicios prestados por terceros.	N/A
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	0%
16.1 Gestión de incidentes de seguridad de la información y mejoras.	0%
16.1.1 Responsabilidades y procedimientos.	0%
16.1.2 Notificación de los eventos de seguridad de la información.	0%
16.1.3 Notificación de puntos débiles de la seguridad.	0%
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	0%
16.1.5 Respuesta a los incidentes de seguridad.	0%
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	0%
16.1.7 Recopilación de evidencias.	0%
17. SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	48%
17.1 Continuidad de la seguridad de la información.	6%
17.1.1 Planificación de la continuidad de la seguridad de la información.	10%
17.1.2 Implantación de la continuidad de la seguridad de la información.	10%
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	0%
17.2 Redundancias.	50%
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	50%
18. CUMPLIMIENTO.	50%
18.1 Cumplimiento de los requisitos legales y contractuales.	90%
18.1.1 Identificación de la legislación aplicable.	90%
18.1.2 Derechos de propiedad intelectual (DPI).	90%
18.1.3 Protección de los registros de la organización.	90%
18.1.4 Protección de datos y privacidad de la información personal.	90%
18.1.5 Regulación de los controles criptográficos.	90%
18.2 Revisiones de la seguridad de la información.	10%
18.2.1 Revisión independiente de la seguridad de la información.	10%

18.2.2 Cumplimiento de las políticas y normas de seguridad.	10%
18.2.3 Comprobación del cumplimiento.	10%

Annex H. Anàlisi de compliment

Control	Implantació
5. POLÍTICAS DE SEGURIDAD.	90%
5.1 Directrices de la Dirección en seguridad de la información.	30%
5.1.1 Conjunto de políticas para la seguridad de la información.	50%
5.1.2 Revisión de las políticas para la seguridad de la información.	10%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	44%
6.1 Organización interna.	38%
6.1.1 Asignación de responsabilidades para la segur. de la información.	10%
6.1.2 Segregación de tareas.	50%
6.1.3 Contacto con las autoridades.	0%
6.1.4 Contacto con grupos de interés especial.	50%
6.1.5 Seguridad de la información en la gestión de proyectos.	90%
6.2 Dispositivos para movilidad y teletrabajo.	50%
6.2.1 Política de uso de dispositivos para movilidad.	50%
6.2.2 Teletrabajo.	50%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	50%
7.1 Antes de la contratación.	70%
7.1.1 Investigación de antecedentes.	50%
7.1.2 Términos y condiciones de contratación.	90%
7.2 Durante la contratación.	30%
7.2.1 Responsabilidades de gestión.	90%
7.2.2 Concienciación, educación y capacitación en segur. de la informac.	0%
7.2.3 Proceso disciplinario.	0%
7.3 Cese o cambio de puesto de trabajo.	10%
7.3.1 Cese o cambio de puesto de trabajo.	10%
8. GESTIÓN DE ACTIVOS.	66%
8.1 Responsabilidad sobre los activos.	80%
8.1.1 Inventario de activos.	90%
8.1.2 Propiedad de los activos.	90%
8.1.3 Uso aceptable de los activos.	50%
8.1.4 Devolución de activos.	90%
8.2 Clasificación de la información.	70%
8.2.1 Directrices de clasificación.	90%
8.2.2 Etiquetado y manipulado de la información.	50%

8.2.3 Manipulación de activos.	50%
8.3 Manejo de los soportes de almacenamiento.	50%
8.3.1 Gestión de soportes extraíbles.	50%
8.3.2 Eliminación de soportes.	50%
8.3.3 Soportes físicos en tránsito.	50%
9. CONTROL DE ACCESOS.	50%
9.1 Requisitos de negocio para el control de accesos.	50%
9.1.1 Política de control de accesos.	50%
9.1.2 Control de acceso a las redes y servicios asociados.	50%
9.2 Gestión de acceso de usuario.	50%
9.2.1 Gestión de altas/bajas en el registro de usuarios.	50%
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	50%
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	50%
9.2.4 Gestión de información confidencial de autenticación de usuarios.	50%
9.2.5 Revisión de los derechos de acceso de los usuarios.	50%
9.2.6 Retirada o adaptación de los derechos de acceso	50%
9.3 Responsabilidades del usuario.	50%
9.3.1 Uso de información confidencial para la autenticación.	50%
9.4 Control de acceso a sistemas y aplicaciones.	50%
9.4.1 Restricción del acceso a la información.	50%
9.4.2 Procedimientos seguros de inicio de sesión.	50%
9.4.3 Gestión de contraseñas de usuario.	50%
9.4.4 Uso de herramientas de administración de sistemas.	50%
9.4.5 Control de acceso al código fuente de los programas.	50%
10. CIFRADO.	90%
10.1 Controles criptográficos.	90%
10.1.1 Política de uso de los controles criptográficos.	90%
10.1.2 Gestión de claves.	90%
11. SEGURIDAD FÍSICA Y AMBIENTAL.	95%
11.1 Áreas seguras.	95%
11.1.1 Perímetro de seguridad física.	95%
11.1.2 Controles físicos de entrada.	95%
11.1.3 Seguridad de oficinas, despachos y recursos.	95%
11.1.4 Protección contra las amenazas externas y ambientales.	95%
11.1.5 El trabajo en áreas seguras.	95%
11.1.6 Áreas de acceso público, carga y descarga.	95%

11.2 Seguridad de los equipos.	95%
11.2.1 Emplazamiento y protección de equipos.	95%
11.2.2 Instalaciones de suministro.	95%
11.2.3 Seguridad del cableado.	95%
11.2.4 Mantenimiento de los equipos.	95%
11.2.5 Salida de activos fuera de las dependencias de la empresa.	95%
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	95%
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	95%
11.2.8 Equipo informático de usuario desatendido.	95%
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	95%
12. SEGURIDAD EN LA OPERATIVA.	65%
12.1 Responsabilidades y procedimientos de operación.	63%
12.1.1 Documentación de procedimientos de operación.	90%
12.1.2 Gestión de cambios.	90%
12.1.3 Gestión de capacidades.	90%
12.1.4 Separación de entornos de desarrollo, prueba y producción.	50%
12.2 Protección contra código malicioso.	90%
12.2.1 Controles contra el código malicioso.	90%
12.3 Copias de seguridad.	100%
12.3.1 Copias de seguridad de la información.	100%
12.4 Registro de actividad y supervisión.	50%
12.4.1 Registro y gestión de eventos de actividad.	50%
12.4.2 Protección de los registros de información.	50%
12.4.3 Registros de actividad del administrador y operador del sistema.	50%
12.4.4 Sincronización de relojes.	50%
12.5 Control del software en explotación.	10%
12.5.1 Instalación del software en sistemas en producción.	10%
12.6 Gestión de la vulnerabilidad técnica.	50%
12.6.1 Gestión de las vulnerabilidades técnicas.	50%
12.6.2 Restricciones en la instalación de software.	50%
12.7 Consideraciones de las auditorías de los sistemas de información.	90%
12.7.1 Controles de auditoría de los sistemas de información.	90%
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	50%
13.1 Gestión de la seguridad en las redes.	50%
13.1.1 Controles de red.	50%
13.1.2 Mecanismos de seguridad asociados a servicios en red.	50%

13.1.3 Segregación de redes.	50%
13.2 Intercambio de información con partes externas.	50%
13.2.1 Políticas y procedimientos de intercambio de información.	50%
13.2.2 Acuerdos de intercambio.	50%
13.2.3 Mensajería electrónica.	50%
13.2.4 Acuerdos de confidencialidad y secreto.	50%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	63%
14.1 Requisitos de seguridad de los sistemas de información.	50%
14.1.1 Análisis y especificación de los requisitos de seguridad.	50%
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	50%
14.1.3 Protección de las transacciones por redes telemáticas.	90%
14.2 Seguridad en los procesos de desarrollo y soporte.	N/A
14.2.1 Política de desarrollo seguro de software.	N/A
14.2.2 Procedimientos de control de cambios en los sistemas.	N/A
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	N/A
14.2.4 Restricciones a los cambios en los paquetes de software.	N/A
14.2.5 Uso de principios de ingeniería en protección de sistemas.	N/A
14.2.6 Seguridad en entornos de desarrollo.	N/A
14.2.7 Externalización del desarrollo de software.	N/A
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	N/A
14.2.9 Pruebas de aceptación.	N/A
14.3 Datos de prueba.	0%
14.3.1 Protección de los datos utilizados en pruebas.	0%
15. RELACIONES CON SUMINISTRADORES.	N/A
15.1 Seguridad de la información en las relaciones con suministradores.	N/A
15.1.1 Política de seguridad de la información para suministradores.	N/A
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	N/A
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	N/A
15.2 Gestión de la prestación del servicio por suministradores.	N/A
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	N/A
15.2.2 Gestión de cambios en los servicios prestados por terceros.	N/A
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	90%
16.1 Gestión de incidentes de seguridad de la información y mejoras.	90%
16.1.1 Responsabilidades y procedimientos.	90%
16.1.2 Notificación de los eventos de seguridad de la información.	90%
16.1.3 Notificación de puntos débiles de la seguridad.	90%

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	90%
16.1.5 Respuesta a los incidentes de seguridad.	90%
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	90%
16.1.7 Recopilación de evidencias.	90%
17. SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	90%
17.1 Continuidad de la seguridad de la información.	90%
17.1.1 Planificación de la continuidad de la seguridad de la información.	90%
17.1.2 Implantación de la continuidad de la seguridad de la información.	90%
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	90%
17.2 Redundancias.	90%
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	90%
18. CUMPLIMIENTO.	50%
18.1 Cumplimiento de los requisitos legales y contractuales.	90%
18.1.1 Identificación de la legislación aplicable.	90%
18.1.2 Derechos de propiedad intelectual (DPI).	90%
18.1.3 Protección de los registros de la organización.	90%
18.1.4 Protección de datos y privacidad de la información personal.	90%
18.1.5 Regulación de los controles criptográficos.	90%
18.2 Revisiones de la seguridad de la información.	10%
18.2.1 Revisión independiente de la seguridad de la información.	10%
18.2.2 Cumplimiento de las políticas y normas de seguridad.	10%
18.2.3 Comprobación del cumplimiento.	10%