Universitat Autònoma de Barcelona

Disseny i implementació d'un sistema de seguretat de sistemes d'informació

Memòria del projecte d'Enginyeria Tècnica en

Informàtica de Gestió realitzat per

Aleix Carbajal Brossa

i dirigit per

Xavier Verge Mestre

Escola Universitària d'Informàtica

Sabadell, Setembre de 2009

El sotasignant, Xavier Verge Mestre,

professora de l'Escola Universitària d'Informàtica de la UAB,

CERTIFICA:

Que el treball al que correspon la present memòria ha estat realitzat sota la seva direcció per en Aleix Carbajal Brossa

I per a que consti firma la present. Sabadell, *Setembre* de *2009*

Resum

El principal actiu de qualsevol empresa és, avui en dia, la **informació**. Tectura Espanya com empresa, està subjecta a la possibilitat de patir qualsevol incident amb la gestió de la seva informació, susceptible de posar en perill la **continuïtat de negoci.**

La manca de protecció de la informació, un virus, el mal ús i gestió dels recursos, i qualsevol tipus d'intrusió poden ocasionar pèrdues de temps i de recursos que incideixen directament en la operativa diària de Tectura Espanya, que, en nombroses ocasions, es pot traduir en una repercussió directa en la qualitat del servei donat al client.

La informació, com altres actius importants per Tectura Espanya, té un valor i com a conseqüència requereix d'una protecció adequada.

La finalitat, doncs, de la realització d'aquest projecte és vetllar per la seguretat de la informació; entenent per seguretat de la informació, la protecció dels interessos de negoci, en el nostre cas del negoci de Tectura Espanya.

Tectura Espanya es un proveïdor mundial de serveis de consultoria de negoci, desenvolupament y suport de IT a indústries de la construcció, ciències biològiques, distribució, fabricació i serveis. Els seus serveis es centren en l'aplicació de solucions basades en tecnologies Microsoft com Microsoft Dynamics AX, Microsoft Dynamics NAV, Microsoft Dynamics CRM i altres solucions tecnologies que pot oferir com a Microsoft Gold Partner.

Es presenta com a projecte el disseny e implantació d'un Sistema de Gestió de Seguretat de la Informació a Tectura Espanya.

Índex

1. Introducció

1.1 Presentació

Aquest projecte "Disseny i implementació d'un sistema de seguretat de sistemes d'informació" pretén crear, implementar i implantar un SGSI dins de Tectura Espanya per tal de preservar la confidencialitat, la integritat i la disponibilitat de la informació així com del sistemes implicats en el tractament d'aquesta dins de l'empresa.

S'ha escollit un SGSI ja que és la base de la ISO 27001 i perquè es tracta d'un estàndard basat en una metodologia de procés cíclic, el PDCA, de l'anglès Plan (planificar), Do (fer), Check (comprobar) i Act (actuar). D'aquesta manera, s'aconsegueix una situació segura i continuada al llarg del temps. Per altra banda i no per això menys important, és perquè és un estàndard de mercat, que es centra en la millora continua que proporciona la metodologia PDCA (veure aparat b del punt 2.3). S'espera doncs, que com més cicles de la metodologia PDCA vagin passant, és a dir, a mesura que passi el temps, un cop començat el cicle per la implantació d'un SGSI basat en la ISO 27001, aquest serà més efectiu.

Un SGSI és un sistema de gestió que comprèn uns controls molt extensos i un seguiment continu. Per aquest motiu, en el marc d'aquest projecte, només s'han tractat el disseny i la implementació del SGSI, donat també que el projecte de final de carrera està limitat a un cert número d'hores.

En la actualitat, Tectura Espanya disposa d'alguns procediments i normes de la utilització dels *sistemes* dins de l'empresa. Aquests procediments, normes i controls només estan disponibles i son coneguts pel departament de TI.

Els procediments, controls i normes son pobres i pocs. Dels pocs que hi han, tots estan quedant obsolets, no hi ha revisions d'aquests, ningú assegura que es duguin a terme i que siguin coneguts pels treballadors. Tampoc hi ha un document "pare" que especifiqui i recopili un seguit de bones pràctiques necessàries per garantir la continuïtat de negoci, és a dir, garantir la informació. Per aquests motius, Tectura Espanya necessita algun estàndard per garantir la seguretat de la informació.

1.2 Estat de l'art

Avui en dia, la informació es tractada com un actiu i com actiu s'ha de protegir. Per protegir-la i garantir la seva disponibilitat, calen un conjunt de normes, procediments i controls que assegurin el bon ús, la protecció, la disponibilitat, la integritat i la confidencialitat d'aquesta. Donat que sense la informació, la continuïtat de negoci perilla.

Existeixen moltes normes i formes de preservar la informació; des de les formés més complexes i extenses fins a les més simples. A continuació, es fa referència a alguns exemples de normatives a seguir per garantir la protecció de la informació.

CobIT – Control Objectives for Information and related Technology

És un conjunt de bones pràctiques pel tractament de la informació creat per l'Institut d'Administració de les Tecnologies de la Informació (ITGI) i distribuït per la Associació de l'Auditoria i Control de Sistemes de Informació (ISACA).

ISO/IEC 27K

La sèrie de normes de la ISO/IEC 27000 son estàndards de seguretat publicats per la Organització Internacional per la Estandardització (ISO) i la Comissió electrotècnica Internacional (IEC).

La sèrie conté les millors pràctiques recomanades en la Seguretat de la Informació, per desenvolupar, implementar i mantenir especificacions pels Sistemes de Gestió de la Seguretat de la Informació (SGSI).

Algunes destacades:

- ISO/IEC 27000
  Vocabulari estàndard per el SGSI, es troba en desenvolupament.
- ISO/IEC 27001
  Norma que especifica els requisits per la implantació del SGSI.
- ISO/IEC 27002
  Codi de bones pràctiques per la gestió de la seguretat de la informació.

La ISO/IEC 27003 y 27004 es troben en desenvolupament i es preveu que es publiquin a finals de l'any 2009.

La evolució d'aquesta norma ha estat constant des de la seva creació l'any 1995:

1995: BS7799 part 1. Codi de bones practiques.

1998: BS7799 part 2. Especificacions del SGSI.

1999: Revisions de ambdues.

2000: La part 1 s'adopta como ISO 17799:2000.

2002: Nova revisió de BS7799-2.

2004: UNE-71502:2004: Tecnologia de la Informació. Especificacions pel sistemes de Gestió de la seguretat de la Informació.

2005: Revisió de la part 1 en ISO 17799:2005.

2005: Adopció de la part 2 en ISO 27001:2005.

2007: ISO 17799:2005 canvia de nombre a ISO27002:2005.

BS25999

Ha sigut desenvolupada per un ampli grup d'experts de primera categoria que constitueixen una mostra representativa de sectors de la indústria i de l'administració per establir els processos, els principis i la terminologia de la gestió de continuïtat de l'activitat comercial. Proporciona una base per comprendre, desenvolupar i implantar la continuïtat de negoci en una organització i atorga confiança en els negocis de B2B i de B2C.

NIST 800-30

La sèrie 800 de la NIST son un conjunt de documents d'interès general sobre la seguretat de la informació. Es van començar a publicar l'any 1990 gràcies a organitzacions, indústries i universitats que volien garantir la seguretat de la informació. Concretament la SP 800-30 és una guia de com tractar els riscos en els sistemes de TI.

PCI – DSS

Significa en anglès *Payment Card Industry Data Security Santard*. Aquest estàndard, com indica el seu nom, ha estat desenvolupat per un comitè format per les companyies de targetes de dèbit i crèdit més importats, intentant crear una guia que ajudi a les organitzacions que processen, emmagatzemen i/o transmeten dades de titulars de targetes, assegurant dita informació amb la finalitat de prevenir fraus. Aquest estàndard es pot implantar en altres empreses que no treballin amb targetes de pagament però que treballin amb dades/informació confidencial.

1.3 Actualitat

En els últims anys s'està observant una clara tendència a la creació de normes estàndards o bones pràctiques per garantir la informació i la continuïtat de negoci. Algunes d'elles, creades i basades en l'àmbit de treball de dites empreses que creen els estàndards/normes.

Les organitzacions son cada com més conscients de la importància de garantir una correcta gestió de la seguretat de la informació i, per tant, de la necessitat d'invertir en recursos. S'observa doncs, una clara tendència de les organitzacions i empreses a la utilització d'aquestes normes, estàndards o bones pràctiques que garanteixin la confidencialitat, integritat i disponibilitat de la informació assegurant la continuïtat i progressió constant del negoci.

1.4 Objectiu

L'objectiu d'aquest projecte és la implantació d'una d'aquestes normes per la gestió de la seguretat de la informació a Tectura Espanya.

De tot el conjunt de normes i possibles polítiques de seguretat, s'ha seguit la **norma ISO 27001** per la implantació d'un Sistema de Gestió de la Seguretat de la Informació (SGSI) a Tectura Espanya.

Resulta indiscutible el fet que a l'actualitat la informació constitueix un dels actius més rellevants per qualsevol organització. És a dir, que ha de ser considerada com un recurs corporatiu i protegir-la contra qualsevol forma d'accés, ús, divulgació, modificació o destrucció no autoritzada.

La realització del SGSI té com a objectius gestionar la seguretat de la informació, mitjançant la realització de processos sistemàtics, documentats i coneguts per a tota l'organització.

Garantir un nivell de protecció total és virtualment impossible, inclús disposant d'un pressupost il·limitat. Es per això que amb la implementació d'aquest sistema, es pretén reduir les possibilitats de pèrdua d'informació relacionada amb el negoci de Tectura Espanya.

El propòsit de la implantació d'un SGSI és també garantir que els riscos de la seguretat de la informació siguin coneguts, assumits, gestionats i minimitzats per l'organització d'una forma documentada, sistemàtica, estructurada, repetible, eficient i adaptada als canvis que es puguin produir en l'entorn i les tecnologies.

2. Estudi de Viabilitat

2.1 Introducció

El departament de Tecnologies de la Informació (en endavant TI) pretén dissenyar un SGSI seguint la norma ISO 27001 per tal de gestionar la seguretat de la informació per a una pyme a nivell nacional, Tectura Espanya.

2.2 Objecte

a) Descripció de la situació actual

Actualment, Tectura Espanya no disposa de cap tipus de pla de gestió de la seguretat de la informació, ni a nivell d'infraestructures tecnològiques ni a nivell documental. Només es disposa d'alguns documents que contenen procediments d'instal·lació d'algun software o algun procediment de configuració de llocs de treball.
Avui en dia, a Tectura Espanya la seguretat es basa en la confiança que es té en els treballadors en relació a la no vulnerabilitat i transgressió de la informació. Per aquest motiu, es fàcil que pugui haver-hi pèrdues d'informació, filtratges d'informació confidencial i inestabilitat en la continuïtat del negoci.
Tot això provoca situacions de desconfiança entre els directius de Tectura Espanya.

b) Perfil del client – usuari

Els usuaris que està previst que utilitzin o, més concretament, que compleixin el SGSI, son tots els treballadors interns de l'empresa indistintament del càrrec que ocupin dins de l'organització, treballadors subcontractats i empreses externes o subcontractades.
Per tant, els documents que comprendran el SGSI hauran de ser clars, llegibles, entenedors, no ambigus i adequats a les necessitats de Tectura Espanya.

c) Objectius

Els objectius que es busquen amb la implantació del SGSI son:

- Evitar que la informació no es posi a disposició ni es reveli a persones, entitats o processos no autoritzats.
- Mantenir la exactitud i complexitat de la informació i dels mètodes de processament.
- Garantir l'accés i utilització de la informació i dels sistemes de tractament de la mateixa per part de les persones, entitats o processos autoritzats que ho requereixin.

Així doncs es vol garantir la **confidencialitat, integritat i disponibilitat** de la informació; tot això, a partir de la implantació de polítiques, procediments, normes i estàndards.
La raó del SGSI està directament relacionada amb la generalització de l'ús de mitjans electrònics, informàtics i telemàtics amb beneficis tangibles per Tectura Espanya. Aquesta generalització, inherentment, dóna lloc a certs riscos que deuen ser minimitzant amb mesures de seguretat que generin confiança en l'ús de recursos que tracten informació.
L'objectiu també és aconseguir un 80% d'aplicabilitat del SGSI segons el qüestionari de l'annex-1 d'aquesta memòria.

d) Fonts d'informació

Després d'estudiar les diferents normes i controls vistos en el punt 1.2 d'aquest document, es va optar per implantar un SGSI basat en la mesura del possible en la norma ISO 27001.
La informació la podem trobar a:

- Norma ISO 27001
- ISO/IEC 17799
- Controls ISO 27002-2005
- Articles, documents i blogs relacionats amb la ISO 27001 i la implantació d'un SGSI

També caldrà realitzar auditories sobre el material informàtic de tractament de dades que disposa l'empresa. Fer un anàlisi de l'empresa des d'on està fins on es vol arribar, per tal garantir la seguretat de la informació. També s'hauran de realitzar entrevistes amb els directius i caps de departament per enfocar i emfatitzar on calgui els diferents punts del SGSI.

2.3 Sistema a realitzar

a) Descripció del Sistema a realitzar

Es vol implantar un sistema que permeti gestionar la seguretat de la informació de Tectura Espanya. Aquest sistema a realitzar és un SGSI que s'implantarà seguint la ISO 27001 i la ISO/IEC 27002:2005. A continuació, es descriuen les principals parts del SGSI de Tectura Espanya

· Política de Seguretat
Document de contingut genèric que estableix el compromís de la direcció i de la organització en la gestió de la seguretat de la informació.

· Gestió d'Actius
Conjunt de documents que permetran garantir i assegurar que els actius de que disposa Tectura Espanya son controlats en tot moment, d'inici a fi, amb la finalitat d'aconseguir i mantenir la protecció adequada per a cada actiu davant la possibilitat d'amenaces internes o externes, deliberades o accidentals.

· Seguretat Física i Ambiental
Conjunt de documents que permetran impedir i prevenir accessos no autoritzats, danys i interferències al conjunt d'oficines, instal·lacions i informació de Tectura Espanya, així com protegir els equips que processen informació i la informació utilitzada pel personal a les oficines, dins del marc normal de les seves tasques habituals.

· Gestió de Comunicacions i Operacions
Conjunt de documents que garantiran el funcionament correcte i segur de les instal·lacions de processament d'informació i les comunicacions.

· Control d'accés
Conjunt de documents que permetran garantir l'accés no autoritzat als sistemes d'informació, bases de dades i serveis d'informació per tal de:

a) Controlar els accessos dels usuaris mitjançant tècniques d'identificació i autentificació.
b) Controlar la seguretat de connexió a la xarxa interna, i entre aquesta i les xarxes publiques.

· Adquisició, desenvolupament i manteniment dels sistemes de la informació

Conjunt de documents que asseguraran la inclusió de controls de seguretat i validació de les dades en el desenvolupament dels sistemes d'informació. Documentació de les normes i procediments que s'utilitzaran durant el cicle de vida de les aplicacions que treballen amb informació. Definir els mètodes de protecció de la informació crítica.

· Gestió d'incidències en la seguretat de la informació

Conjunt de documents que permetran garantir una bona identificació de les incidències relacionades amb el tractament de la informació, per tal de poder-les acotar i solucionar amb la major brevetat. Tot documentant, d'inici a fi, amb la història de la incidència.

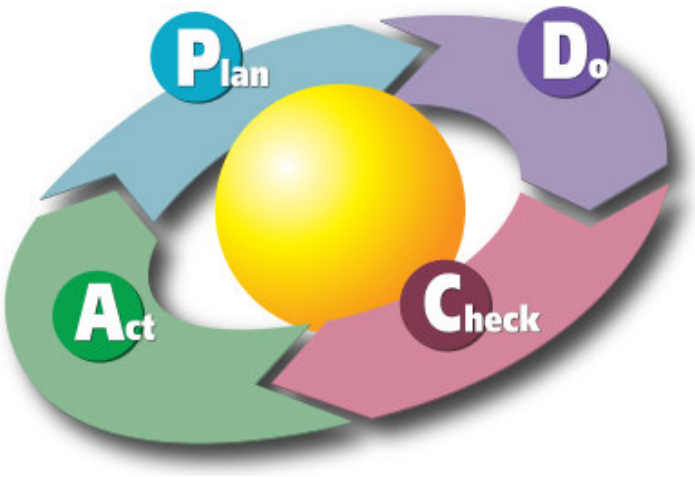
· Compliment

Conjunt de documents que permetran complir amb les disposicions legals, normes, procediments i polítiques que componen el SGSI de Tectura Espanya, amb la finalitat d'evitar la pèrdua d'informació o problemes derivats de la seguretat de la informació.

b) Model a desenvolupar

El model de desenvolupament que seguirem serà el cicle de *Deming* o model PDCA (Plan, Do, Check, Act).

- Plan (**planificar**): establir el SGSI.
- Do (**fer**): implementar i utilitzar el SGSI.
- Check (**verificar**): monitoritzar i revisar el SGSI.
- Act (**actuar**): mantenir i millorar el SGSI.



1 Cicle PDCA

c) Recursos

Serà necessari un PC amb sistema operatiu Windows XP, un processador de text, un programa d'inventari d'equips i un programa de generació de fluxos de treball (Visio).

d) Anàlisi cost – benefici

Un cop vistos els escassos recursos necessaris pel desenvolupament del projecte, el cost bàsicament serà el de la mà d'obra de l'enginyer tècnic informàtic del departament de TI de Tectura Espanya.
Per contra, els beneficis que s'obtindrà seran:

. Ampliar el coneixement real dels actius que es disposen (control i calcificació).
a. Desenvolupar polítiques formals d'obligat compliment.
b. Involucrar la direcció en la Seguretat de la Informació.
c. Realitzar anàlisis de riscos per el desenvolupament del negoci.
d. Reforçar la seguretat lligada al personal.
e. Disposar de plans de contingència davant incidents.
f. Disposar de plans de continuïtat de negoci i recuperació d'informació davant desastres.
g. Disminuir els riscos a nivells acceptables.

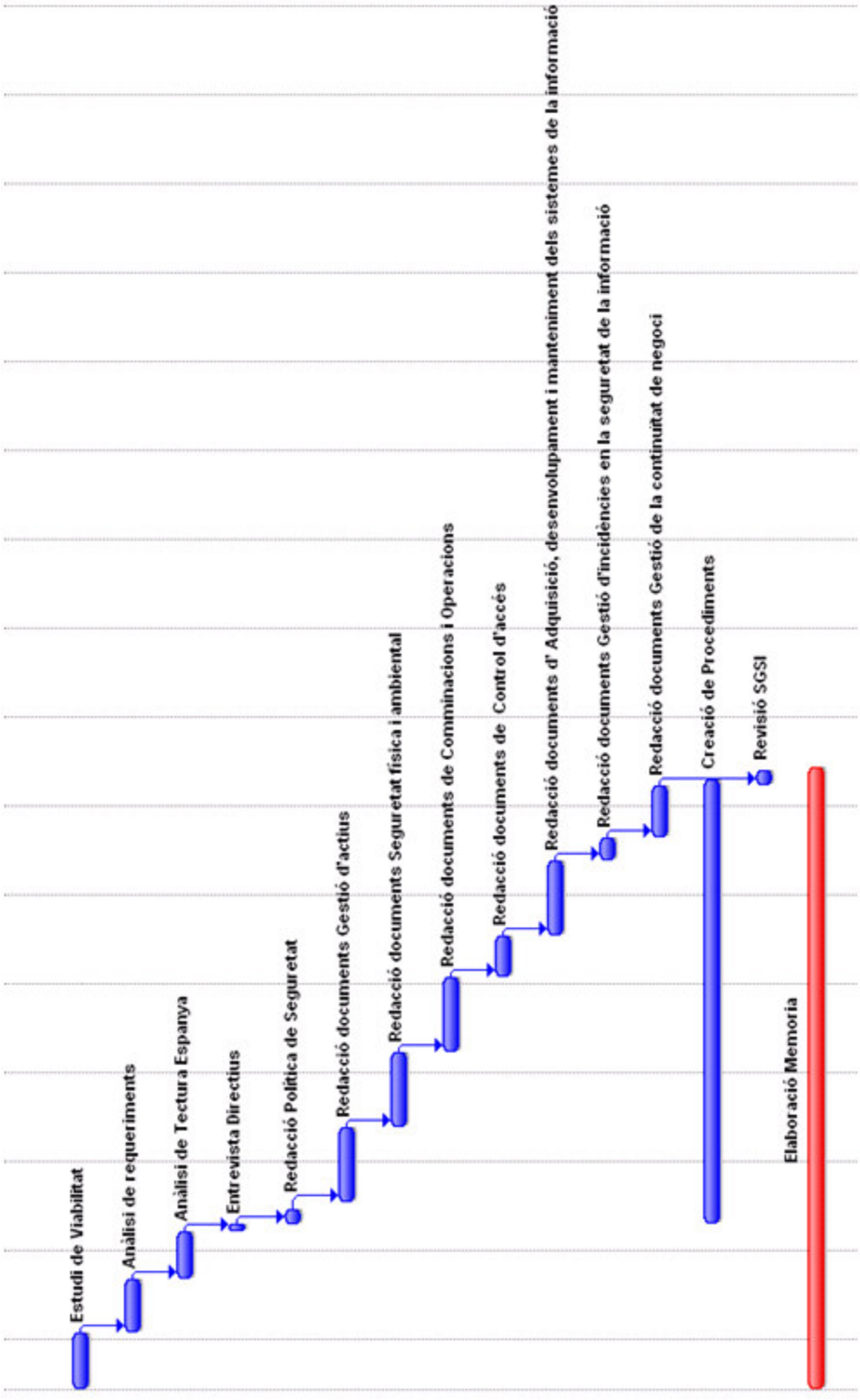
e) Avaluació de riscos

El principal problema serà implantar el SGSI a una empresa on els treballadors i la direcció no estan acostumats a tenir cap tipus de control ni restricció en les accions que realitzen respecte al tractament de la informació. Una altre dels problemes o dificultats, serà aconseguir abarcar i enfortir totes les febleses referents a seguretat de la informació que té l'empresa.

2.4 Planificació

A continuació, es mostra una taula amb les diferents tasques que es duran a terme i la durada de cada una. Donat que la realització del projecte està acotada per un número determinat d'hores, la implantació i la verificació del SGSI no estaran contemplades.

Fase	Concepte	Durada en Hores	Durada en dies
Planificació del SGSI	Estudi de Viabilitat	18	6
	Anàlisi de requeriments	36	12
	Anàlisi situació seguretat Tectura Espanya	12	4
	Entrevista Directius	6	2
Disseny i implementació del SGSI	Redacció Política de Seguretat	12	4
	Redacció documents Gestió d'actius	30	10
	Redacció documents Seguretat física i ambiental	30	10
	Redacció documents de Comunicacions i Operacions	30	10
	Redacció documents de Control d'accés	30	10
	Redacció documents d' Adquisició, desenvolupament i manteniment dels sistemes de la informació	30	10
	Redacció documents Gestió d'incidències en la seguretat de la informació	12	4
	Redacció documents Compliment	18	6
	Creació de Procediments	30	10
	Revisió SGSI	12	4
Implantació SGSI			
Verificació SGSI			
TOTAL		**309**	**103**


Estudi de Viabilitat
Anàlisi de requeriments
Anàlisi de Tectura Espanya
Entrevista Directius
Redacció Política de Seguretat
Redacció documents Gestió d'actius
Redacció documents Seguretat física i ambiental
Redacció documents de Comminacions i Operacions
Redacció documents de Control d'accés
Redacció documents d' Adquisició, desenvolupament i manteniment dels sistemes de la informació
Redacció documents Gestió d'incidències en la seguretat de la informació
Redacció documents Gestió de la continuïtat de negoci
Creació de Procediments
Revisió SGSI
Elaboració Memoria

2.5 Conclusions

La informació, juntament amb els processos i sistemes que en fan ús, son actius molt importants d'una organització. Garantir la informació i els seus sistemes de tractament arriba a ser essencial per a mantenir els nivells de competitivitat, rendibilitat, conformitat legal i imatge empresarials necessaris per assolir els objectius de Tectura Espanya i assegurar per aquesta uns beneficis econòmics.

Tectura Espanya i els seus sistemes d'informació estan exposats a un nombre cada vegada més elevat d'amenaces que, aprofitant qualsevol de les vulnerabilitats existents, poden sotmetre a actius crítics d'informació a diverses formes de frau, espionatge, sabotatge o vandalisme. Els virus informàtics, el "hacking" o els atacs de denegació de servei son alguns exemples comuns i coneguts, però també s'han de considerar els riscos de patir incidents de seguretat causats voluntària o involuntàriament des de dins de la pròpia organització o aquells provocats accidentalment per catàstrofes naturals o fallades tècniques.

Amb l'aplicació del SGSI, tots aquests problemes i riscos esmentats estaran contemplats i s'estarà preparat i previngut davant de tots els elements que puguin posar en perill la informació. Així l'empresa podrà garantir una continuïtat de negoci, garantir la seguretat de la informació sabent que s'ha de complir el SGSI.

Un cop realitzat l'estudi de viabilitat i havent comprovat la possibilitat de realització, i havent valorat els aspectes positius i negatius de la implementació del SGSI, es considera que **el projecte es viable.**

3. Anàlisi i especificació

3.1 Introducció

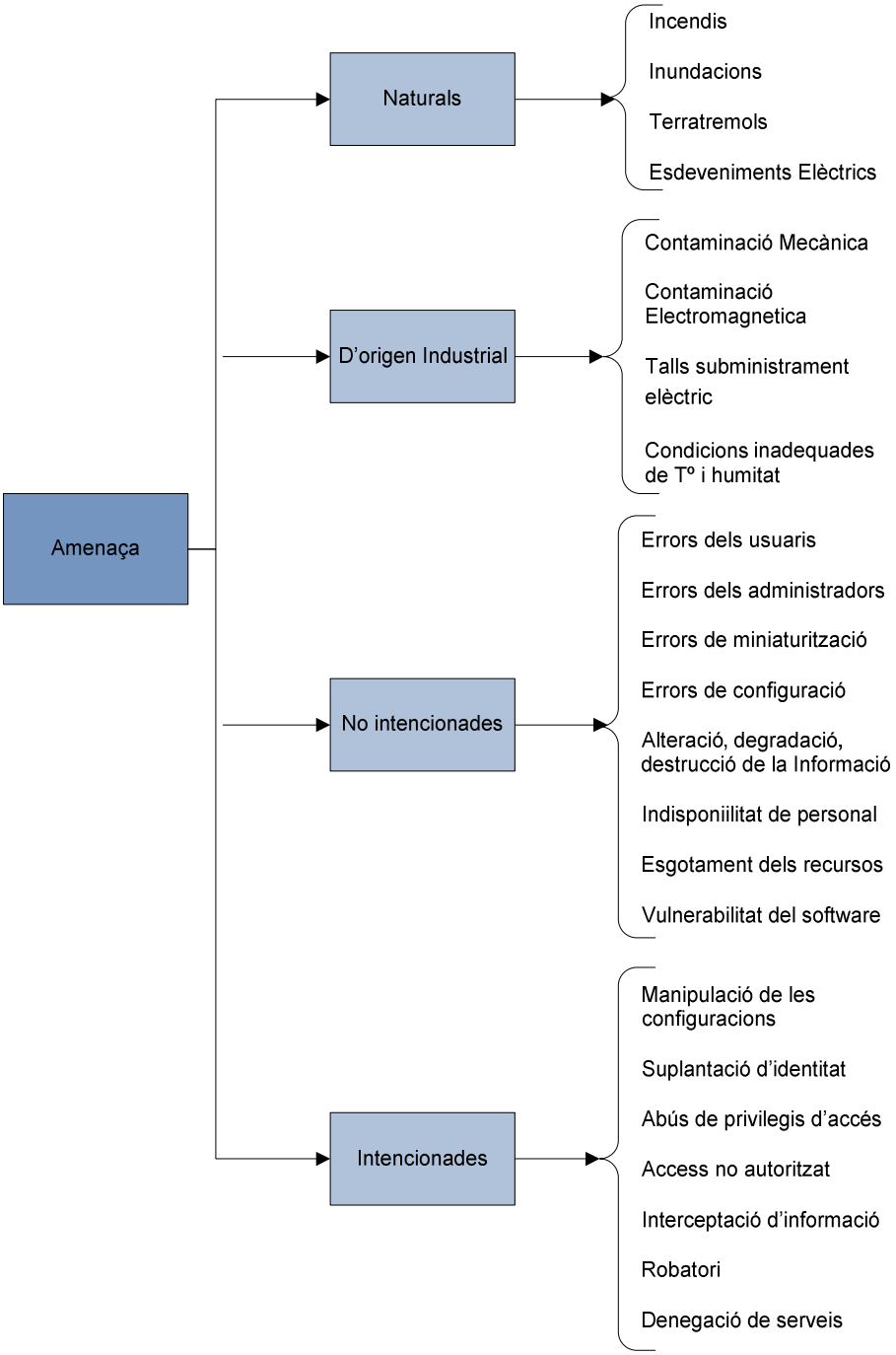
La finalitat d'aquest projecte és dictar un seguit de normes administratives per protegir la informació, les xarxes, els sistemes de processament de la informació, les instal·lacions, els equips, els serveis, el software, el personal i tot element relacionat amb les funcions del negoci, d'una amplia gama d'amenaces, a fi de garantir la continuïtat de les activitats, minimitzar els danys i maximitzar el retorn sobre les inversions i el desenvolupament de les oportunitats.

La informació pot existir de moltes formes. Pot estar impresa o escrita en paper, emmagatzemada electrònicament, transmesa per correu, transmesa per correu electrònic o utilitzant mitjans electrònics, transmesa oralment en una conversa o presentada en imatges. Qualsevol quina sigui la forma en que es presenta la informació, o els mitjans per els quals es distribueix o s'emmagatzema, sempre ha de ser protegida de forma adequada.

S'entén per seguretat de la informació la preservació de les següents característiques elementals:

- *Confidencialitat:* garantir que la informació es accessible només a aquelles persones i/o processos autoritzats a tenir accés a ella.
- *Integritat:* mantenir la exactitud i totalitat de la informació i dels seus mètodes de tractament.
- *Disponibilitat:* garantir que els usuaris autoritzats i/o processos tinguin accés a la informació i als recursos relacionats amb ella cada cop que ho requereixin.

Com hem esmentat anteriorment, la informació l'haurem de protegir contra amenaces. Una amenaça es una violació potencial de la seguretat, sense ser necessari que la violació succeeixi perquè l'amenaça existeixi.



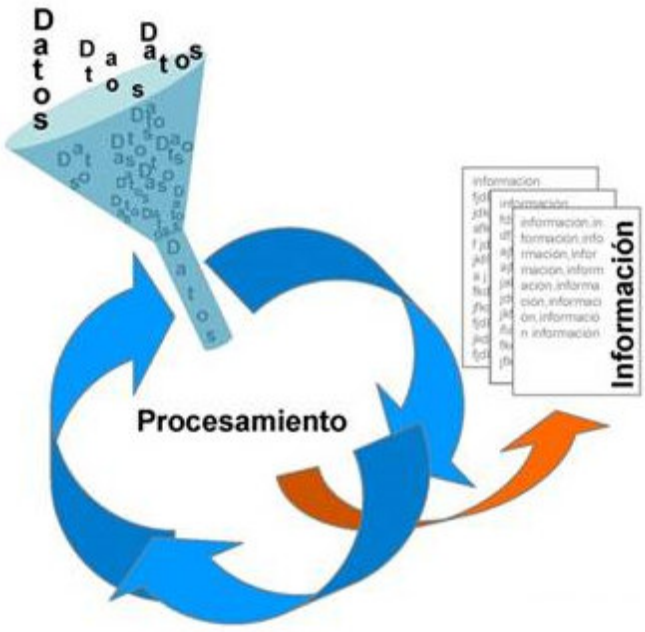
2 Calcificació amenaces segons Magerit

Per protegir-nos de les esmentades amenaces, s'implementaran un conjunt de controls, que comprendran polítiques, normes, estàndards, procediments, estructures organitzatives, equips, dispositius i suports físics, lògics i administratius. Les polítiques, normes i estàndards és el que defineix el SGSI que realitzem com a projecte per Tectura Espanya.

3.2 Què és un SGSI?

El SGSI (Sistema de Gestió de Seguretat de la Informació) és el concepte central sobre el que es construeix la ISO 27001. La gestió de la seguretat de la informació s'ha de realitzar mitjançant un procés sistemàtic, documentat i conegut per tota l'organització. Aquest procés és el que constitueix un SGSI, que es podria considerar com el sistema de qualitat per la seguretat de la informació.

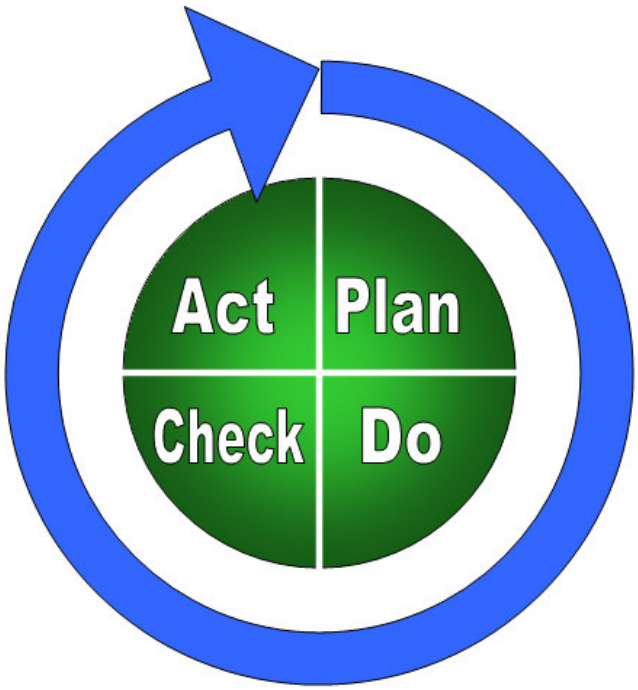
Garantir un nivell de protecció total és impossible; el propòsit, doncs, del SGSI és garantir que els riscos de la seguretat de la informació siguin coneguts, assumits, gestionats i minimitzats per Tectura Espanya de forma documentada, sistemàtica, estructurada, repetible, eficient i adaptada als canvis.
El SGSI ajudarà a establir les polítiques, procediments, estàndards, normes, etc. en relació als objectius de negoci de Tectura Espanya.
Es tindrà coneixement dels riscos a què està sotmesa la informació, es podran assumir, minimitzar, controlar i prevenir d'una manera sistemàtica, definida, documentada i coneguda per tots, que es revisarà i millorarà constantment.



3 **Processament de la informació**

3.3 Com s'implementa un SGSI

Per establir i gestionar un Sistema de Gestió de la Seguretat de la Informació en base a la ISO 27001, s'utilitza un cicle continu PDCA, tradicional en els sistemes de gestió de la qualitat.



4 Cicle de Deming

Plan (planificar): establir el SGSI.

Do (fer): implementar i utilitzar el SGSI.

Check (verificar): monitoritzar i revisar el SGSI.

Act (actuar): mantenir i millorar el SGSI.

En el marc d'aquest projecte només estan reflectides les fase Plan i Do, donat que les de monitoritzar i revisar el SGSI (Check) i mantenir i millorar el SGSI (Act) es realitzen un cop s'ha implantat el SGSI i tenen una dura i continuïtat més llarga en el temps, gairebé indefinida.

3.3.1 *Plan*: Establir el SGSI

- S'analitza la situació actual de la organització:
  - Objectius de control i controls que ja estan implantats, en base a la Norma ISO/IEC 27002:2005.
  - Recopilació de documents relatius a la seguretat, ja existents.
- Es seleccionen els nous objectius de control i els controls per el tractament de les amenaces, vulnerabilitats o riscos, en base a la Norma ISO/IEC 27002:2005.
- S'involucra a la direcció i els caps de departament en la implantació i ús del SGSI.
- Es defineix la política de seguretat.

En aquesta etapa es verifica on està actualment la companyia a partir d'uns controls i s'establiran quins dominis i controls s'aplicaran. Es defineix la política de seguretat i l'abast del SGSI.

3.3.2 *Do*: Implementar i utilitzar el SGSI

- Implementar els controls anteriorment seleccionats que porten als objectes de control.
- Agrupar els controls en diferents dominis de control.
- Elaborar i estructurar els procediments, normes, estàndards i controls que permetin garantir la seguretat de la informació, la detecció i la resposta davant de possibles incidents.
- Formar i conscienciar al personal de l'empresa en relació a l'ús i coneixement del SGSI.

4. Disseny (PLAN)

4.1 Situació Actual

S'analitza la situació actual de l'empresa per tal de saber l'estat de la implantació del SGSI seguint un conjunt de dominis, objectes de control i controls establerts a la ISO/IEC 27002:2005.
De la ISO/IEC 27002:2005 ens centrarem en els dominis:

- Política de seguretat
- Gestió d'actius
- Seguretat física i ambiental
- Gestió de les comunicacions i operacions
- Control d'accessos
- Gestió d'incidències en la seguretat de la informació
- Gestió de continuïtat de negoci
- Compliment

Donat que el departament de RRHH té les seves pròpies normatives i gestionen a partir d'una empresa externa tot el relacionat amb l'empleat, el domini "Seguretat lligada als recursos humans" l'obviarem.

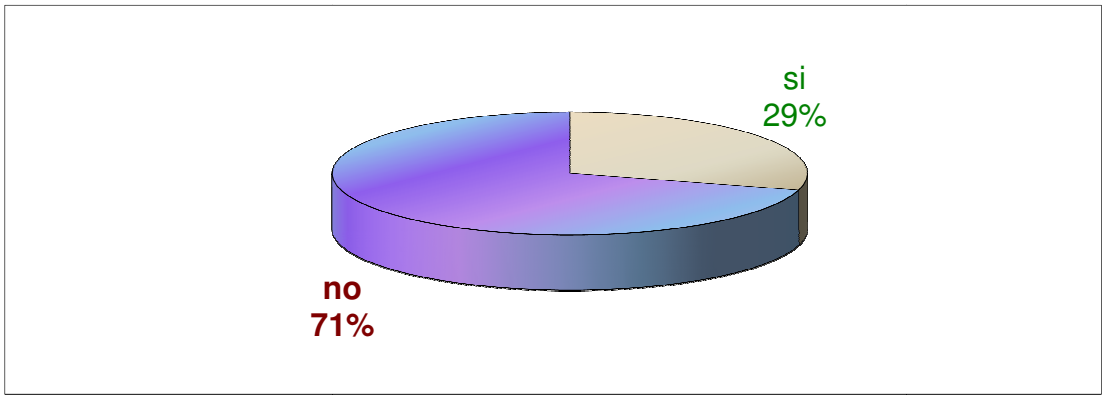
D'altra banda, el domini "Aspectes organitzatius de la seguretat de la informació" tan sols tindrem en compte el control *6.1.1 Compromís de la direcció amb la seguretat de la informació* i estarà reflectit en el punt 3 del document SGSI Tectura - Políticas de Seguridad.

4.1.1 Controls Anàlisi Inicial

Un cop analitzats els dominis de la norma ISO/IEC 27002:2005 que utilitzarem pel SGSI de Tectura Espanya, el següent pas consisteix a realitzar un seguit de qüestions referents a cada un dels dominis seleccionats per tal de saber l'estat actual en que es troba Tectura Espanya a nivell de seguretat de la informació.

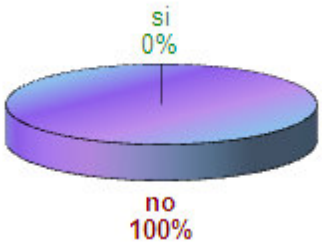
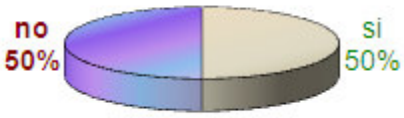
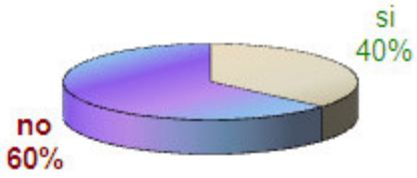
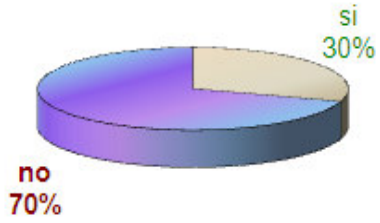
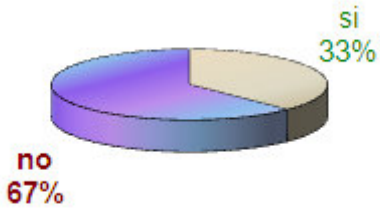
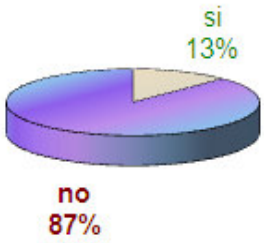
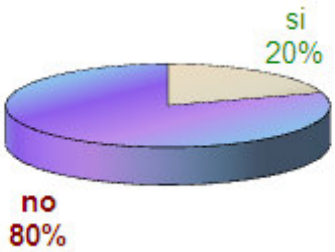
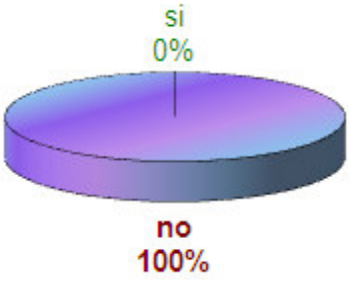
Per obtenir aquesta informació es realitza el qüestionari de l'annex-1

En una visió general, s'observa que no s'està complint en un 71% els controls per garantir la seguretat de la informació, contra un 29% que si que garanteixen algun tipus de control:



Observem un clar forat en la seguretat de la informació donat que sense l'aplicació del SGSI tant sols s'estan complint un **29%** dels controls inclosos a la ISO/IEC 27002:2005. Per tant, s'observa una clara manca de seguretat que fa perillar la informació i, en conseqüència, la continuïtat del negoci de Tectura Espanya.

Si separem l'anàlisi inicial en els diferents dominis que analitzarem i implantarem dins del marc del SGSI i dins de Tectura Espanya, s'obtenen els següents resultats:

Política de Seguretat	Gestió d'actius
	
Seguretat física i ambiental	**Gestió de les comunicacions i operacions**
	
Control d'accessos	**Adquisició, desenvolupament i manteniment dels Sistemes de la Informació**
	
Gestió d'incidències en la seguretat de la informació	**Compliment**
	

S'observa que tant sols s'arriba a un 50% de seguretat de la informació en el domini "Gestió d'actius".

Tectura Espanya no arriba al nivells mínims (80% en cada un dels dominis), per tant, la urgència de l'aplicació de controls en la seguretat de la informació mitjançant la implantació d'un SGSI és d'una importància considerable. Un cop realitzat el SGSI, tornarem a realitzar l'anàlisi anterior per observar com la implantació del SGSI ha ajudat a garantir la seguretat de la informació a Tectura Espanya.

4.1.2 On volem arribar

Mitjançant aquest projecte, es vol arribar a tenir una arquitectura de gestió de la seguretat que identifiqui els riscos que poden afectar al negoci de Tectura Espanya a través de la implantació del SGSI.

El que es pretén és:

- Conèixer realment dels actius que es disposa.
- Involucrar a la Direcció en la seguretat de la Informació.
- Desenvolupar politiques formals, d'obligat compliment.
- Desenvolupar normes, procediments i estàndards d'obligat compliment.
- Reforçar la seguretat lligada als empleats.
- Disposar de plans de continuïtat de negoci i recuperació.
- Prevenir davant de possibles amenaces.
- Evitar inversions innecessàries, ineficients o mal dirigides produïdes de contrarestar amenaces.
- Assignar funcions i responsabilitats.
- Garantir una resposta puntual i adequada davant les incidències.

4.2 Estructura SGSI Tectura Espanya

L'estructura seguida en els diferents documents que composen el SGSI de Tectura Espanya manté, en el possible, l'estructura de la ISO/IEC 27002:2005. El nom dels Controls a seguir pot no correspondre amb el nom dels controls de la ISO/IEC 27002:2005. Tant sols s'agafa dita norma com a referència i guia per la realització del SGSI de Tectura Espanya.
S'ha triat utilitzar l'estructura de la ISO/IEC 27001:2005 ja que facilita el disseny, desenvolupament, manteniment i realització del SGSI.

El SGSI de Tectura Espanya consta de 7 dominis de control, agrupats en 7 documents independents, els quals contenen col·lectivament 18 procediments, 20 normes, 7 estàndards, 2 polítiques i un total de 17 controls i subcontrols de seguretat.

Tots els dominis han estat redactats respectant la següent estructura:

1) Es dedica un document per cada un dels dominis seleccionats:
    a. Els dominis constitueixen àrees d'aplicació del SGSI.
    b. S'han fet coincidir els títols dels documents amb els dominis de la ISO/IEC 27001:2005 amb l'objectiu de facilitar la recerca de referències.

2) Cada un dels dominis queda caracteritzat per:
    a. Objectiu: breu descripció del domini i del seu context d'aplicació.
    b. Abast: camp d'aplicació del domini.
    c. Responsabilitat: persones, treballadors a qui va dirigit el domini.
    d. Directives: una o més d'una norma, procediment, estàndard en el context del domini que han de ser aplicats per aconseguir els objectius de control del domini.

4.3 Reunió amb els directius

Es reuneixen els directius de Tectura Espanya, així com els cap de departament per tal d'implicar-los en la realització del SGSI. S'acorda i s'aprova que el departament de TI gestioni la seguretat de la informació, exceptuant els dominis que entren dins l'àmbit del departament de recursos humans que seran gestionats per dit departament.
Un cop finalitzada la implementació del SGSI, la direcció de Tectura Espanya es tornarà a reunir amb el departament de IT per comprovar l'abast, realització i estructura del SGSI i que encaixi en l'àmbit empresarial de Tectura i no repercuteixi en les operacions de negoci.

5. Implementació (DO)

A continuació, es detalla cadascun dels dominis de control que s'han implementant per la realització del SGSI Tectura Espanya, amb els seus pertinents procediments, normes i estàndards.

5.1 SGSI Tectura - Políticas de Seguridad

La política de seguretat de la informació és un document fonamental per la gestió adequada i efectiva dels processos de seguretat de Tectura Espanya.
Té com a objectiu garantir i assegurar la implementació de mesures de seguretat compreses al SGSI Tectura Espanya, així com en els documents que el comprenen, per protegir els recursos de la informació de la empresa i la tecnologia utilitzada per el processament, transmissió, emmagatzament i eliminació, davant amenaces, internes o externes, deliberades o accidentals.

Document complet - Annex 2

5.2 SGSI Tectura - Gestión de Activo

Amb aquest domini es pretén garantir i assegurar que els actius que disposa Tectura Espanya són controlats en tot moment, d'inici a fi de la vida de cada actiu, amb la finalitat d'assolir i mantenir la protecció adequada per a cada actiu davant possibles amenaces internes o externes, deliberades o accidentals.

5.2.1 Inventario Activos

Conjunt de normes i procediments que garanteixen l'inventariat d'actius tecnològics que disposa Tectura Espanya.

- TECTURA - Procedimiento Auditoria Software

  Procediment amb els passos a seguir per auditar correctament el software de tots els equips.

- TECTURA - Entrega Activo Móvil

  Document que certifica l'entrega i bona utilització per part del treballador d'un actiu mòbil.

- TECTURA - Entrega Activo NB

  Document que certifica l'entrega i bona utilització per part del treballador d'un actiu mòbil.

5.2.2 Inventario Software

Procediment que garanteix l'inventariat de software que disposa Tectura Espanya.

- TECTURA - Procedimiento Inventario Software

  Procediment amb els passos a seguir per inventariar el software del que Tectura Espanya disposa.

5.2.3 Auditoria

Normes i Procediments que garanteixen l'auditoria de tots els equips informàtics connectats a la xarxa de Tectura Espanya.

- TECTURA - Procedimiento Auditoria Software

  Procediment amb els passos a seguir per auditar correctament el software de tots els equips.

Document complet - Annex 3

5.3 SGSI Tectura - Seguridad Física y Ambiental

Amb les normes, controls i procediments descrits en aquest domini es pretén protegir l'equipament que processa informació ubicant-lo en àrees protegides amb mesures de seguretat i controls d'accés, així com controlar els factors ambientals que poguessin perjudicar el correcte funcionament de l'equipament informàtic i llocs de treball que puguin albergar informació de Tectura Espanya. S'implementen mesures per protegir la informació que utilitza el personal a les oficines de Tectura España en el marc de les seves tasques habituals.

5.3.1 Normes de Seguretat

Conjunt de normes que garantiran la protecció dels llocs de treball, equips de processament d'informació, sistemes operatius, entorns de comunicació i altre material que treballi amb informació rellevant per Tectura.

- TECTURA - Procedimiento Solicitud Acceso fuera horario oficina

  Procediment amb els passos a seguir per sol·licitar accés fora de l'horari laboral.

5.3.2 Norma, Juegos / Salvapantallas y temas de escritorio

Conjunt d'especificacions de com s'ha de configurar el salva pantalles, el fons d'escriptori i normatives referents a jocs de PC.

Document complet - Annex 4

5.4 SGSI Tectura - Gestión de Comunicaciones y Operaciones

Es pretén garantir el funcionament correcte i segur de tots els dispositius i instal·lacions que processen informació rellevant per Tectura Espanya així com les comunicacions.

5.4.1 Copias de seguridad y gestión de soportes de copias

Procediment de com s'han de realitzar les còpies de seguretat de la informació amb que treballa Tectura Espanya.

5.4.2 Normas Correo electrónico Email

Conjunt de normes per la correcta utilització i distribució del correu electrònic que Tectura Espanya disposa als seus empleats.

- TECTURA - Procedimiento de Limitaciones y configuraciones de Exchange

  Normes i procediments de limitacions de configuració de Exchange.

- TECTURA - Procedimiento de configuración del buzón personal

  Procediment de configuració de la bústia personal per la utilització del correu Tectura.

5.4.3 Normas FTP

Normativa per la correcta utilització de les comptes FTP que els treballadors de Tectura Espanya poden disposar.

- TECTURA - Procedimiento de Normas de Acceso a FTP
  Normes d'accés a les comptes personals de FTP.
- TECTURA – Procedimiento Creación cuenta FTP para Trabajadores
  Procediment per crear les comtes FTP dels treballadors de Tectura Espanya.

5.4.4 Normas Acceso FTP clientes

Normativa per la correcta utilització de les comptes FTP que es disposa per els clients Tectura Espanya.

- TECTURA - Procedimiento Solicitud FTP Cliente
  Procediment per la sol·licitud d'una compta FTP de client.

5.4.5 Descargas de Internet

Normativa de com es tracten les descàrregues d'Internet.

5.4.6 Norma sobre la Música / Archivos de video(películas)

Normativa sobre l'emmagatzematge en equips de treball d'arxius de musica (mp3, wav, wmv, ra, etc) com d'arxius de vídeo (mpeg, avi, mp4, mpg, etc.)

5.4.7 Virus y código malicioso

Normes sobre la correcta eliminació i prevenció de virus i codi maliciós

- TECTURA - Procedimiento para Instalación cliente Sophos
  Procediment d'instal·lació de l'antivirus corporatiu.

5.4.8 Normas de acceso a internet y redes públicas

Normatives per la bona utilització d'Internet i xarxes públiques.

- TECTURA - Estándar Configuración Standard Firewall
  Configuració estàndard del firewall que disposa Tectura Espanya.

5.4.9 Normas sobre el cableado de red, HSRP en MPLS y ADSL

Conjunt de normes sobre el funcionament i configuració de les MPLSentre oficines, la sortida a internet (ADSL) aixi com el cablejat de xarxa.

5.4.10 Estándar Planes de Mantenimiento Servidores SQL

Estàndard per la realització dels plans de manteniment per els servidors de SQL inclouen copies de seguretat i optimització de les BBDD.

Document complet - Annex 5

5.5 SGSI Tectura – Control de Accesos

El domini Control d'accessos es marca com a objectiu impedir l'accés no autoritzat als sistemes d'informació de Tectura Espanya, bases de dades, serveis que gestionen informació i equips que treballen amb informació. Es pretén implementar seguretat en els accessos dels treballadors als sistemes d'informació per mitja de tècniques d'identificació i autentificació, així com controlar la seguretat en les connexions a la xarxa.

5.5.1 Gestión de acceso de usuarios

Conjunt de normes de seguretat que garanteixen la unicitat d'usuaris pels treballador, així com altres aspectes de la seguretat refent als treballadors com la identificació i la autentificació.

- TECTURA - Procedimiento cambio de password
  Procediment amb els passos per canviar el password d'identificació en el domini Tecturacorp

5.5.2 Normas de acceso a la red Tectura

Conjunt de normes per garantir el correcte accés a la xarxa de Tectura.

5.5.3 Normas de descargas de Internet

Normativa referent a les descàrregues realitzades des d'Internet.

5.5.4 Acceso no autorizado / Piratería Informática

Normativa pel control de la pirateria i d'accessos no autoritzats.

5.5.5 Normativa DMZ

Existeix una zona de la xarxa totalment aïllada utilitzada per l'accés a segons quines aplicacions des de fora de la xarxa de Tectura.

- TECTURA - Procedimiento de conexión remota por Terminal Server

  Procediment per la connexió remota al servidor de terminal server de Tectura Espanya.

5.5.6 Normas acceso a Sites, Sharepoint

Condicions i normes d'accés als diferents site de la intranet de Tectura Sharepoint.

5.5.7 Normas Utilización licencias Microsoft

Normes d'utilització de llicencies Microsoft de que disposa Tectura Espanya com a *Gold Partner*.

5.5.8 Normas Utilización licencias Tectura Navision/Axapta

Tectura España, al disposar de llicències completes de desenvolupament pel software de Microsoft Dynamis, necessita normes que garanteixin la bona utilització d'aquestes.

5.5.9 Normas de acceso servidores de desarrollo

Conjunt d'especificacions de com s'ha d'accedir als servidors de desenvolupament.

5.5.10 Normas de acceso a BBDD

Conjunt d'especificacions de com s'ha d'accedir a las diferents bases de dades (bbdd) que hi ha disponibles.

5.5.11 Normas de uso de la VPN

Conjunt de procediments i normes per la correcta connexió des de l'exterior de la LAN de Tectura utilitzant una connexió VPN.

- TECTURA – Procedimiento configuración VPN

  Procediment per la connexió i configuració de la VPN de Tectura.

5.5.12 Norma de Protección de Datos

Norma que estableix l'encriptació de les dades que continguin informació confidencial en els diferents sistemes que la puguin procesar.

5.5.13 Estándar Asignación de móviles

Mètode d'assignació de mòbils als treballadors de Tectura Espanya.

5.5.14 Normas de utilización de teléfonos móviles

Conjunt de punts sobre la utilització dels telèfons mòbils.

5.5.15 Estándar Nomenclatura Equipos

Estàndard que assegura la correcta nomenclatura dels equips del domini Tecturacorp.

- TECTURA - Estándar Nomenclatura Equipos Tectura
  Estàndard de com identificar els equips de Tectura Espanya.

5.5.16 Estándar Configuración equipos nuevos

Mètode de configuració dels nous equips per als treballadors de Tectura Espanya.

- TECTURA - Procedimiento de Instalación y configuración de un nuevo equipo
  Procediment amb els passos a seguir per la instal·lació i configuració dels nous equips de Tectura Espanya.

5.5.17 Estándar Alta usuario

Estàndard per l'alta dels nous treballadors de Tectura Espanya.

- TECTURA - Procedimiento para Alta Usuarios
  Procediment a seguir per la configuració de nous usuaris.

5.5.18 Estándar Baja usuario

Estàndard per la baixa dels treballadors de Tectura Espanya.

- TECTURA - Procedimiento Baja Usuarios
  Procediment a seguir per donar de baixa els usuaris de Tectura Espanya.

5.5.19 Normas de acceso a Internet y redes públicas

Normatives per la bona utilització de Internet i xarxes públiques.

5.5.20 Normas de acceso al SGSI de Tectura España

Normes que estableixen qui te accés al SGSI de Tectura España

Document complet - Annex 6

5.6 SGSI Tectura – Adquisición, desarrollo y mantenimiento de los sistemas de información

L'objectiu d'aquest domini és assegurar la inclusió de controls en la validació de les dades que utilitzen els sistemes d'informació, així com definir i documentar les normes i procediments que s'aplicaran durant el cicle de vida del software.

5.6.1 Normes de control del Software

Conjunt de normes i procediments que declaren i expliquen com s'ha d'utilitzar el software que disposa Tectura Espanya per realitzar-ne un bon ús, tot garantint la seguretat de la informació.

- TECTURA - Procedimiento Solicitud Software

  Procediment que s'utilitza per la sol·licitud de software quan Tectura Espanya no en disposa.

5.6.2 Norma de Tratamiento del freeware y shareware

El freeware i shareware també és una variant de software que ha de ser considerat pel que també existeixen normes per garantir un bon ús d'aquest.

5.6.3 Actualizaciones Sistema Operativo

Normativa que estableix el funcionament de les actualitzacions dle sistema operatiu.

5.6.4 Seguridad en el almacenamiento

Norma que recull diferents punts per garantir la confidencialitat de les dades que continguin informació confidencial.

5.6.5 Normas de usuarios de móvil y dispositivos móviles

Normes d'utilització de dispositius mòbils.

5.6.6 Seguridad en el almacenamiento

Normativa que preserva la seguretat de la informació confidencial en equips portàtils o mòbils

5.6.7 Normas de Encriptación

Norma que garanteix la protecció de les dades confidencials en equips portàtils o dispositius mòbils

5.6.8 Normes de desarrollo de software

Conjunt de normes que garanteixen unes bones practiques en el desenvolupament del sofware

Document complet - Annex 7

5.7 SGSI Tectura - Gestión Incidencias

L'objectiu d'aquest domini és gestionar les incidències per poder restablir la seguretat en la major brevetat i amb el mínim impacte pel negoci; així com, permetre el registre de les incidències per avaluar-les i poder-les prevenir en un futur.

5.7.1 Procedimiento para la gestión de incidencias

Passos a seguir per la notificació i resolució de les possibles incidències.

- TECTURA – Procedimiento de Gestión de incidencias
  Procediment a seguir per la gestió de les incidències que poguessin sorgir.

Document complet - Annex 8

5.8 SGSI Tectura – Cumplimiento

Domini que assegura el compliment i utilització del SGSI als treballadors de Tectura Espanya. Així com que els sistemes, els organismes i els treballadors compleixin els procediments, estàndards, normes i polítiques que el formen, com també el compliment d'altres lleis governamentals.

5.8.1 Política de la Propiedad intelectual del Software

Document que assegura una utilització correcta i legal del software.

- TECTURA - Política para uso de programas de Tectura España

  Política per la correcta utilització del software.

5.8.2 Normativa para el cumplimiento del SGSI

Garanteix que tot treballador de Tectura Espanya utilitzarà i seguirà les normes, procediments i estàndards descrits al SGSI Tectura Espanya.

5.8.3 Infracción de las políticas

Mesures per l'incompliment del SGSI Tectura Espanya.

5.8.4 Revisión de las políticas/procedimientos

Política que garanteix una revisió del SGSI Tectura Espanya assegurant que no quedi obsolet amb el temps.

Document complet - Annex 9

6. Implantació

Un cop finalitzades les etapes de disseny i implementació del SGSI per Tectura Espanya es durà a terme la posada en pràctica a tota l'organització.
Els passos ha seguir son:

1) Reunió amb la direcció

   Es reunirà el departament de IT juntament amb la direcció de Tectura Espanya, per tal de presentar-li el SGSI que s'aplicarà a tota l'organització.
   S'exposaran breument els dominis de control que garantiran la seguretat de la informació. Un cop la direcció comprengui els objectius del sistema realitzat, i un cop comprovat que no repercutirà en el desenvolupament del negoci de Tectura, es signarà la política de seguretat, donant així conformitat, validesa i suport a la implantació i utilització per tota l'organització.

2) Reunió amb el departament de RRHH

   Es reunirà el departament de IT amb el departament de RRHH, donat que els treballadors de Tectura Espanya tenen un rellevància fonamental per l'èxit del SGSI.
   S'establiran els protocols de com es donarà a conèixer el SGSI als nous treballadors així com a la totalitat de la plantilla de Tectura Espanya. S'establiran els processos de formació que s'impartiran als treballadors per donar a conèixer el SGSI.

3) Reunió responsables de departament

   Es reunirà el departament de IT juntament amb el caps de departament per tal que tinguin coneixement de quins dominis de seguretat s'aplicaran al conjunt del seu departament, i d'aquest manera els facilitin i transmetin als seus membres i vetllin pel compliment d'aquests.

4) Donar a conèixer el SGSI als treballadors

   Un dels punts més importants per l'èxit del SGSI és la formació i conscienciació de l'ús dels procediments, normes i controls que garantiran la seguretat de la informació al conjunt dels treballadors. Aquesta formació es donarà per departaments on s'exposaran els dominis de control que afectaran a l'àmbit del departament així com els dominis generals per tota l'empresa. La formació dels treballadors és molt important ja que no hem d'oblidar que el component principal de la seguretat és el factor humà, i que tot el que es proposa al SGSI no complirà l'objectiu d'incrementar la seguretat, sinó s'involucra al treballadors.

5) Empreses subcontractades i clients

   Es donarà a conèixer a les empreses subcontractades i clients de Tectura Espanya la implementació d'aquest nou sistema de seguretat informant d'aquells procediments, normes i estàndards que els puguin implicar.

6) Accés al document

   Tots els documents que comprenen el SGSI estaran a l'abast de tots els treballadors en el Sharepoint corporatiu dins del Site de IT. Hi haurà un accés restringit a aquells procediments i estàndards que el departament de IT cregui convenient.

7. Proves i manteniment

Al ser un projecte que s'implanta un cop ha estat tot realitzat, no s'han pogut realitzar proves, tant sols revisions dels diferents documents que componen el SGSI de Tectura Espanya.
Seguint el cicle PDCA, les proves i el manteniment s'aniran fent a mesura que passin els dies, setmanes, mesos i anys, i es vagi veien com evoluciona l'empresa.
Un cop finalitzi la implantació del SGSI es seguiran les següents fases del cicle de *Deming*: Check i Act.

8. Conclusions

A partir de l'elaboració d'aquest projecte hem pogut comprovar que la seguretat de la informació no només es basa en estàndards i procediments sinó que també es basa en les persones, en com elles tenen la capacitat i coneixement de gestionar-la. No sense abans haver-les instruït en com fer-ho.

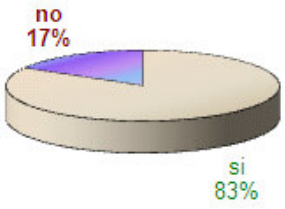
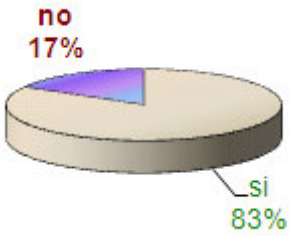
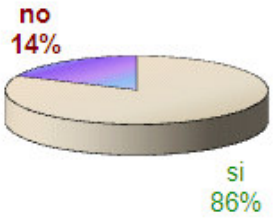
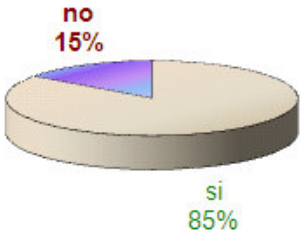
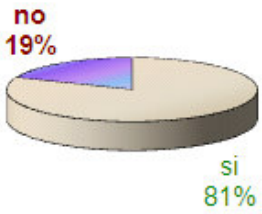
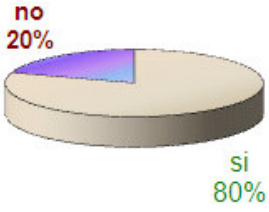
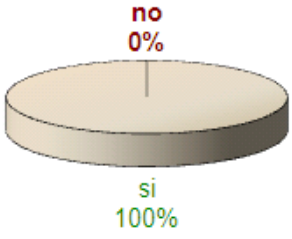
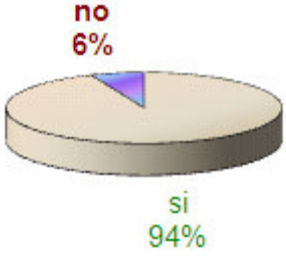
Al mateix temps s'ha observat la necessitat de tota empresa de disposar d'unes normes, polítiques o estàndards que protegeixin la seva informació. Tectura Espanya ho està aconseguint gràcies al SGSI que aporta seguretat, millores continues, és útil i molt rentable. Una possible debilitat és que per l'èxit del SGSI és indispensable la implicació de la direcció així com de tota l'organització.

Mentre es realitzava aquest projecte, s'han anat trobant diferents dificultats; la més rellevant ha estat la problemàtica de no saber quin estàndard seguir per gestionar la seguretat de la informació que englobés tots els procedimentals, normes, controls, etc. en una política global. Fins que, juntament amb el tutor d'aquest projecte (Xavier Verge), es va decidir seguir la ISO 27001 que redacta la implementació i implantació d'un SGSI.

Al temps que s'anaven redactant les diferents polítiques, normes, procediments i estàndards va sorgir el dubte de com agrupar-los ja que no només teníem un sol document. Finalment, es decideix seguir la ISO/IEC 27002:2005 com a guia de referència, sense que els noms dels controls que apareixen fossin els mateixos que els controls realitzats en el SGSI de Tectura Espanya.

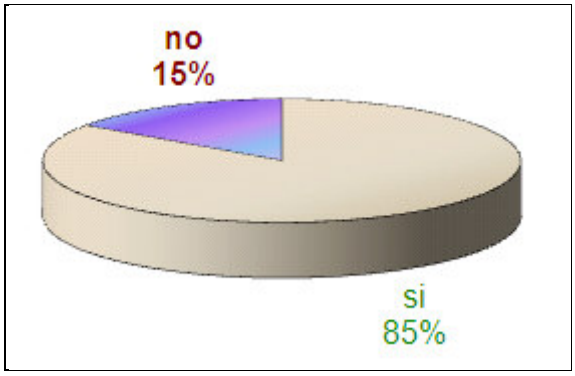
7.1 Objectius aconseguits

Un cop s'ha implementat el SGSI tornem a realitzar les qüestions sobre la seguretat de la informació de l'annex-1 per saber el nivell de seguretat que aconseguim amb el sistema implantat.

<table>
<tr><th>Política de Seguretat</th><th>Gestió d'actius</th></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><th>Seguretat física i ambiental</th><th>Gestió de les comunicacions i operacions</th></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><th>Control d'accessos</th><th>Adquisició, desenvolupament i manteniment dels Sistemes de la Informació</th></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><th>Gestió d'incidències en la seguretat de la informació</th><th>Compliment</th></tr>
<tr><td> 
</td><td> 
</td></tr>
</table>

Observem doncs que el nivell assolit en tots els dominis és superior o igual al 80%, per tant, podem afirmar que a Tectura Espanya es segueixen una sèrie de controls per garantir la seguretat de la informació gràcies a la implantació del SGSI.

A nivell global el nivell assolit en l'aplicació de controls per garantir la seguretat de la informació es d'un 85%.



No obstant, no podem afirmar al 100% que hem complert els objectius d'aquest projecte, donat que el SGSI ha de concloure amb el cicle de *Deming*. Un cop finalitzat tot el cicle, es valorarà amb la direcció de Tectura Espanya si s'han assolit els objectius que es van marcar.

Bibliografia

·Informació general sobre la ISO 27000

http://www.iso27000.es/herramientas.html

http://www.27000.org/

·Informació sobre les amenaces, Margerit

http://www.csae.map.es/csi/pg5m20.htm

·Informació general sobre la ISO 27001

http://es.wikipedia.org/wiki/ISO/IEC_27001

·Informació sobre la ISO 27001

http://www.iso27001security.com/

·Informació sobre els estàndards ISO

http://www.iso.org

·Informació sobre SGSI

http://sgsi-iso27001.blogspot.com/

http://www.iso27000.es/doc_sgsi_all.htm

·Informacion general ISO/IEC 27002

http://es.wikipedia.org/wiki/ISO/IEC_17799

·Informacio Seguretat de la informació

http://www.inteco.es/

http://seguridadit.blogspot.com/

http://seguridad-de-la-informacion.blogspot.com/

·Informació d'amenaces i riscos

http://www.csae.map.es/csi/pg5m20.htm

·ISO/IEC 27001: "Information technology – Security techniques – Information security management systems – Requirements".

·ISO/IEC 27002:2005: "Information technology – Security techniques – Code of practice for information security management