Treball Final de Màster

"Implementació d'un Pla Director de Seguretat"

Alumne: Adrián Infiesta Aguilá
Professor: Arsenio Tortajada Gallego

Índex

Fase 6: Presentació de Resultats i Entrega d'Informes

Memòria

- *Característiques de l'empresa:*

Primerament començarem parlant del que serà el nostre client i objecte del projecte. Es tracta de *Hotel XXXX*, un petita societat limitada, formada per la junta directiva i uns pocs treballadors. Aquesta organització té les característiques del que es coneix com a PIME (Petita i Mitjana Empresa). Tal i com el seu nom indica, treballa en el sector del turisme i hoteleria, oferint allotjament i altres activitats a tota mena de públic. Localitzada en una vila propera a la ciutat de Barcelona, porta donant servei durant més de 40 anys. Durant aquest temps s'ha consolidat en el seu sector, i és un hotel de referència a nivell provincial. Per tal de seguir al capdavant del sector, la junta directiva ha sol·licitat que es dugin a terme les tasques necessàries per obtenir la certificació entorn a la norma ISO/IEC 27001. Degut a que no disposa d'un SGSI implantat, ens veiem obligats a plantejar un Pla Director de Seguretat per adaptar la situació a la posterior implantació del SGSI. Les finalitats principals que ha requerit la junta directiva són que aquestes tasques serveixin principalment per:

- Dotar a Hotel XXXX d'un valor afegit en els seus productes
- Obtenir uns anàlisis que serveixin per determinar les vulnerabilitats relacionades amb la seguretat de la informació que existeixen actualment
- Deixar a la organització en un punt proper a la implantació del SGSI.

Per aquests motius comencem esmentant les principals característiques de la empresa:

- **Personal i treballadors:** està formada per dos persones que composen la junta directiva, i cinc treballadors fixes més. Depenent de l'època de l'any poden intervenir treballadors esporàdics.
- **Ubicació:** tot el complexe està situat en un antic edifici típic del casc antic dels pobles. L'edifici es propietat exclusiva de Hotel XXXX i totes les activitats que es duen a terme estan relacionades amb el negoci. Consta de tres plantes, pati interior, pati exterior, terrassa i jardins.
- **Sistemes d'Informació:** entre els sistemes més destacables podem trobar una pàgina web, amb la opció de fer reserves online en temps real; també una plataforma de pagament segura. Un cop dintre de la empresa, existeixen diferents aparells que manegen informació en diferents etapes del seu cicle de vida. Podem trobar ordinadors, telèfons, fax, videocàmeres de seguretat, lectors de targetes, llibres de registres, llibretes, contractes, etc.
- **Departaments:** a part de la junta directiva, existeix una relació amb terceres parts. Aquestes impliquen la comunicació de diferents informacions. Entre aquests tercers, podem trobar aquells que mantenen un vincle per prestació de serveis, com el hosting o les plataformes bancàries. Altrament trobem el que seria el departament jurídic, que en aquest cas queda

representat en forma d'assessoria jurídica. Recentment es crearà un departament amb un especialista en sistemes informàtics, i que serà el responsable de la seguretat de la informació entre d'altres tasques.

Donades aquestes característiques ens trobem amb diferents relacions que intervenen en el cicle de vida de la informació. El primer que observem és que tota la presa de decisions ve determinada per la junta directiva, que són els màxims responsables de Hotel XXXX. En aquest cas, i per exemple davant d'un imprevist, els empleats han de contactar amb els directius per saber com actuar, i si no és possible, actuar segons el seu coneixement i la seva experiència. Ràpidament detectem una carència de qualsevol mena de documentació que contingui plans d'actuació o guies bàsiques amb protocols als quals referenciar-se en cas de dubte.

Un altre punt feble que s'ha detectat és la poca formació del personal en matèria de gestió de la informació i dels elements de seguretat que hi intervenen. La falta de cultura en aquest camp queda patent, i per aquest motiu són ben rebudes les bones intencions per part de la junta directiva de posar-se al dia en aquest aspecte. Per tant, un dels punts en els que caldrà treballar és en la formació i conscienciació de tots els implicats en qualsevol procés que prengui part en el SGSI. En el cas que ens ocupa, i degut a que Hotel XXXX és un negoci familiar, tots els treballadors intervenen en algun moment en processos de manipulació d'informació. Per això serà altament important tenir en compte que cada vegada que es contracti ma d'obra extra a temps parcial, caldrà que quedin ben definides les seves implicacions i limitacions al desenvolupar les tasques quotidianes. Tant és així que cal revisar i modificar els contractes que existeixen, per tal d'adequar algunes clàusules, per exemple de confidencialitat, que ara mateix no existeixen. Tots aquests punts adquiriran importància a mesura que avancem en la creació del SGSI.

Les estructures i els canals de comunicació que hem descobert també són un punt calent. Per motius aliens a la direcció, la implantació de les noves tecnologies s'ha fet de manera desordenada, i el creixement dels suports físics existents no guarda cap relació ni cap ordre. En molts casos s'han instal·lat ordinadors o telèfons en punts arbitraris que simplement presentaven un accés més fàcil o que en aquell moment estaven disponibles per acollir un nou element. Particularment trobem que a la planta baixa, darrera d'un mostrador de recepció, es concentren elements com el telefon principal, el fax, un servidor, un ordinador, un lector de targetes, una impressora, i altres elements relacionats. La seguretat en aquesta zona és pràcticament nul·la, i no existeixen responsabilitats sobre els actius més enllà de les que se suposa al treballador que ocupa aquella zona durant el seu torn. Com es pot veure, la seguretat de la informació quedarà compromesa greument. La falta de coneixements en aquest aspecte, tal i com ja hem comentat, agreugen el problema. Serà necessari trobar solucions a aquests problemes.

L'edifici i la seva antiguitat són el motiu principal per el qual la junta directiva ha efectuat una remodelació recent, incloent una ampliació, però en la qual no s'ha tingut en compte aspectes bàsics i recomanacions que ens ajudaran a superar els diferents objectius de control dels estàndards que busquem assolir. Un exemple concret el trobem en la distribució de les oficines, en aquest cas despatx de la junta directiva, el qual pràcticament no existeix com a tal, i no disposa de mobiliari adequat per acollir actius puntuals i amb rellevant importància. També trobem que les estàncies que existeixen han estat creades aprofitant diversos espais antics, reformant-los, però deixant al descobert carències de seguretat. Aquestes mancances venen donades per la ubicació concreta, on existeixen espais que queden comunicats físicament entre ells, o que no estan prou ben vigilats.

Finalment, la relació amb diferents departaments que existeixen es basa en la contractació de serveis a terceres parts. En els casos de l'assessoria jurídica, o el servei de hosting, estarem parlant

de terceres parts que intervenen en el procés de gestió de la seguretat de la informació. Tot i això, la junta directiva no era conscient del que això implica, i per tant, es tracten com a simples relacions comercials. Caldrà doncs, revisar els acords existents, i posar-los al dia adequadament per tal que compleixin la normativa legal vigent. El mateix passarà amb el servei que ofereix la entitat bancària o les plataformes de reserves des de webs de tercers. Tots aquests serveis i altres que puguin sorgir seran motiu d'estudi i de valoració.

Amb totes aquestes dades, creiem que hem destacat les principals característiques que existeixen dins de la empresa en relació amb la seguretat de la informació i dels processos en els que intervenen. La manera de treballar concreta s'explicarà en els apartats que sigui necessaris. Fins aquí, simplement hem citat els punts més destacables i la manera en la que es relacionen dins i fora de la organització.

Anàlisi de Riscos:

Un cop coneixem l'empresa hem de procedir a fer un primer anàlisi de riscos als quals es troba exposada. Molts d'aquests riscos venen relacionats amb l'afectació per mitjà d'alguna vulnerabilitat a un actiu que es consideri important. D'altres, en canvi, poden aparèixer com a riscos relacionats amb el propi desenvolupament d'una activitat. La llista d'actius que s'han identificat apareix llistada al annex 1.

Per fer el càlcul sobre els riscos es poden utilitzar diferents fórmules. Nosaltres ens hem decantat per l'establerta a la metodologia MAGERIT.

- Anàlisi de riscos intrínsec

Per aquest càlcul farem servir la següent fórmula, aplicant els valor abans esmentats a les taules:

$$Risc = Valor\ de\ l'actiu \times Vulnerabilitat \times Impacte$$

Per calcular el risc efectiu en cas que fos necessari utilitzaríem:

$$R.Efectiu = R.Intrínsec \times percentatge\ disminució\ vulnerabilitat \times percentatge\ disminució\ impacte$$

A partir d'aquí es construiria una taula amb aquests valors i el resultat de les multiplicacions, i obtindríem per a cada actiu el seu valor anual. En aquest cas hem obviat aquesta taula, ja que ocuparia massa espai i dificultaria la lectura. Per una classificació més neta, es recomana col·locar un codi especific per a cada actiu, i un codi per a cada amenaça. D'aquesta manera la incorporació de les dades a la taula de càlcul serà més senzilla. En el cas d'utilitzar les eines proporcionades per Magerit, els càlculs es fan automàticament un cop introduïts els paràmetres. Per al nostre cas, podem fer servir com a alternativa una fulla de càlcul, el disseny del qual correra a càrrec del responsable de l'àrea informàtica.

Tal i com indiquen les fórmules, hem calculat diferents paràmetres relacionats amb cada actiu. Per saber quin procediment i metodologia hem seguit podem consultar el annex 2, on queden especificades totes les dades.

Un cop coneixem les amenaces que afecten a Hotel XXXX, és hora de veure com es relacionen cadascuna amb els principals actius de l'empresa i quina de les dimensions de la seguretat es veu afectada en cada cas concret. Totes aquestes dades es mostren en taules que han estat confeccionades com a resultat de Anàlisi de Riscos, i figuren adjuntades en el document que conforma el annex 3. De entre les principals conclusions que podem extreure, destaquem el nivell de risc que està disposat a assumir la junta directiva per a Hotel XXXX. Del corresponent Annex 3 obtenim la següent taula.

Nivell de Risc Acceptable i de Risc Residual:

Nivell de Risc = Valor + (Impacte x Probabilitat)

Aplicant la fórmula anterior com a resultat obtindrem un valor numèric. Aquest valor es pot classificar com:

Valor	**Nivell**
9.1 - 10	Extrem
7.1 - 9	Molt alt
4.1 - 7	Alt
2.6 - 4	Baix
0 - 2.5	Molt Baix

En el cas que ens ocupa, la junta directiva ha manifestat que, un cop exposat el cas que ens ocupa, vol implantar les mesures necessàries **per a que tot nivell de risc quedi englobat en els llindars "baix o molt baix"**, que **es consideraran nivells de Risc Acceptable**. La resta de nivells i els seus actius seran objecte de controls per tal de reduir aquest risc fins a valors acceptables. Igualment és aconsellable que el nivell de risc que resti un cop implantats els controls necessaris, anomenat Risc Residual, es trobi en el nivell "molt baix". Si no és així, caldrà revisar si existeix l'opció de millorar el control o implantar-ne d'addicionals.

Resum executiu del AR:

A partir de les dades obtingudes podem sintetitzar alguns resultats i explicar-los de manera resumida. S'han comptabilitzat un total de 19 actius agrupats en 9 àmbits diferents. Tal i com mostra el gràfic 1, veiem que la majoria es concentren en actius de tipus hardware. Això vol dir que les amenaces contra hardware englobaran el gruix dels nostres problemes, ja que aquests representen un 36% dels nostres actius. També podem destacar que no existeixen, per el moment, actius classificats com a "serveis". Això pot ser degut al tipus d'activitat que desenvolupa Hotel XXXX, i sobretot, a la seva mida, on queda patent que no existeixen algunes característiques que en altres casos serien bàsiques. No obstant, deixem la categoria oberta a futures incorporacions, dotant al sistema de classificació de major flexibilitat en futures revisions.

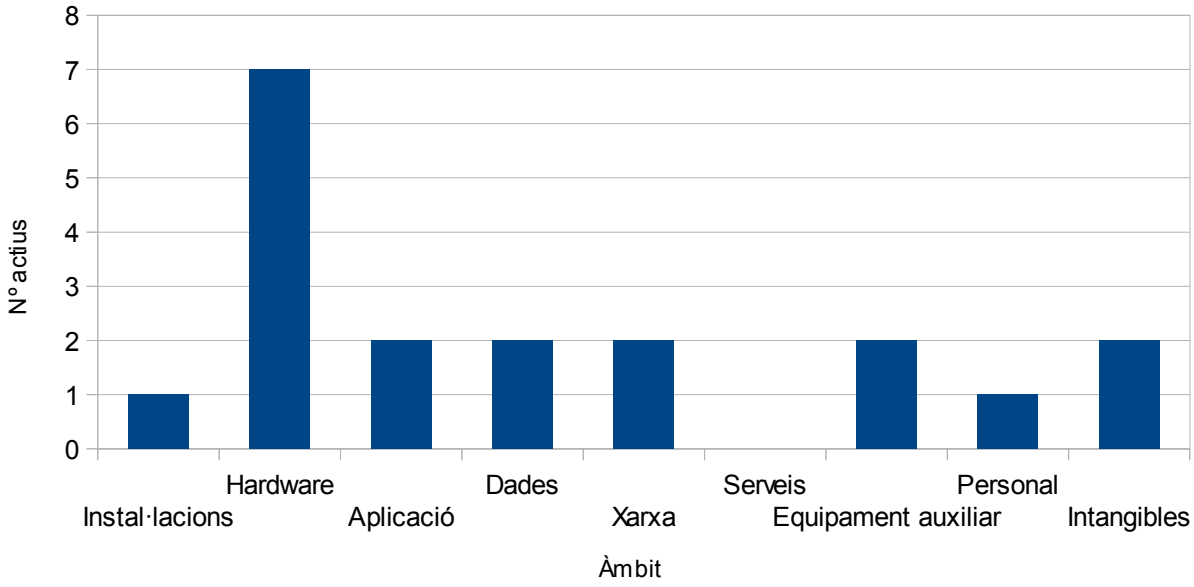


Tabla 1: distribució d'actius segons la seva categoria

Ara, mostrem a la taula 2, quina dimensió de la seguretat és la més important per a cada actiu, i quin percentatge total representa aquesta dimensió. Per referenciar-se a la dimensió concreta de cada actiu podem consulta el annex 3. En aquest gràfic veiem que la disponibilitat és la dimensió que més vegades té el major pes en un actiu, i que seria la que es veuria majorment afectada en cas d'incidència.

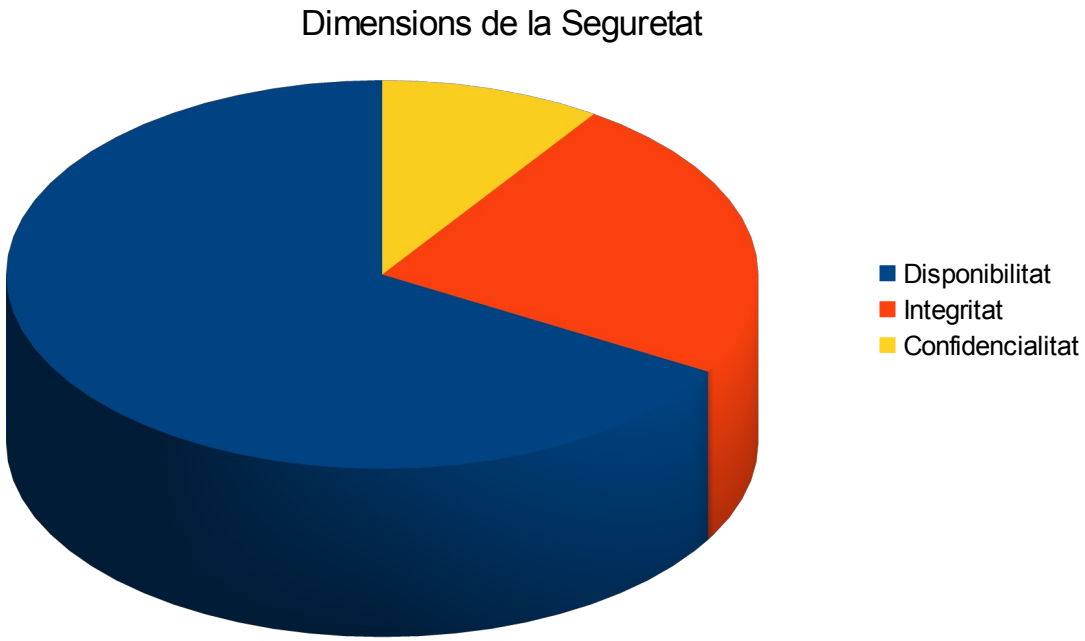


Tabla 2: Percentatge de les dimensions de la seguretat

Lligant els resultats de les dos taules anteriors, entenem que els processos de la informació que es duen a terme a Hotel XXXX estan molt lligats amb els seus actius de hardware, que seran a través dels quals es gestionaran les dades. Per tant, una fallada en la disponibilitat serà especialment important quan es tracti d'un actiu físic que formi part d'aquest grup de maquinari. Aquesta conclusió la tindrem en compte a l'hora de proporcionar plans d'acció per millorar la seguretat de la informació.

No obstant, també és interessant observar en quina freqüència creiem que es poden produir les incidències de seguretat. En el document de AR queda classificat segons la probabilitat de aparició en cinc categories: molt baixa, baixa, mitjana, alta, extrema. Del total de amenaces materialitzables, extraiem la taula 3, en la que veiem quina quantitat d'aquestes pertany a cada grup. Fent aquest procés podrem prioritzar els nostres plans d'acció, orientant els esforços a corregir els grups amb una freqüència d'aparició més elevada.

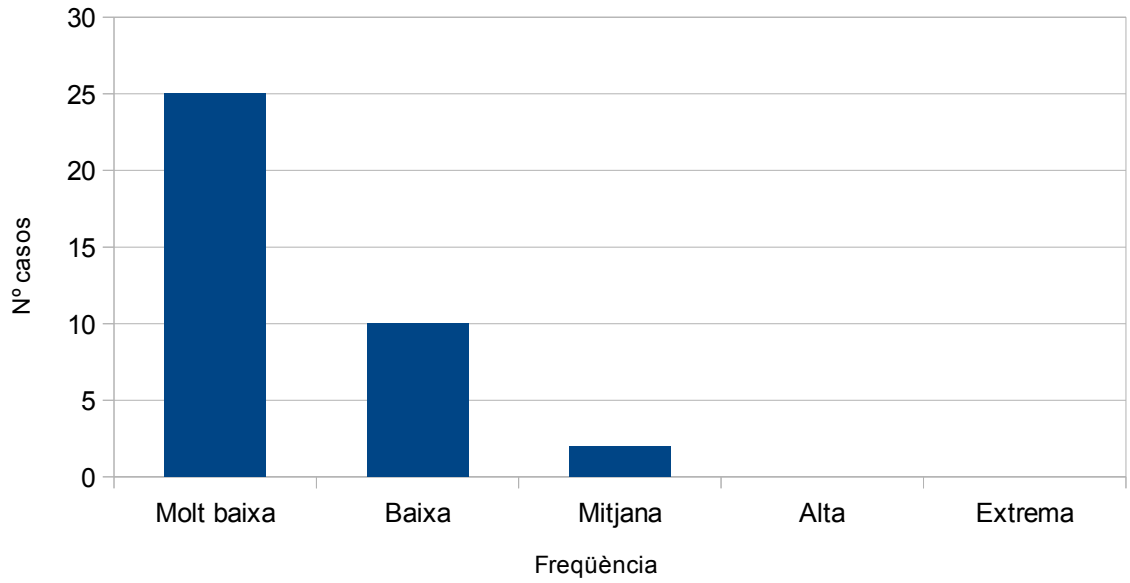


Tabla 3: Freqüència d'aparició de vulnerabilitats

Afortunadament observem que la majoria de vulnerabilitats tenen una freqüència estimada d'aparició molt baixa, i tot i que existeixen algunes amb una probabilitat mitjana, cal veure en profunditat quines són i quins actius queden afectats. El fet de no haver constatat vulnerabilitats amb freqüència alta o extrema és un bon símptoma per a l'empresa.

En quant a la valoració dels actius, s'ha establer una escala de valor entorn a un criteri objectiu: el conjunt d'actius mai superarà els 50.000€

Donat aquest límit, hem xifrat la resta d'actius i classificat segons els seu valor. D'aquesta classificació extraiem la taula 4 i les següents conclusions. Primerament, la majoria d'actius tenen una valoració relativament petita. Aquest fet es positiu davant de l'impacte que pot tenir la pèrdua d'aquest actiu, tot i que cal actuar segons unes fórmules plantejades en el AR.

D'altra banda el grup d'actius de baixa i mitjana valoració ocupen la mateixa posició. Per tant, pot ser convenient centrar l'atenció sobre quins són els actius de mitjana valoració per si cal actuar sobre ells amb prioritat.

Finalment, tenim un únic actiu de valor alt. Concretament es tracta de la imatge corporativa. Tal i com ja havíem estat informats per part de la junta directiva, aquesta imatge es considera un dels actius fonamentals de Hotel XXXX, i a través del qual el creixement del negoci i la seva viabilitat són possibles. Per tant, un dany que afectés a aquest actiu tindria un cost molt elevat per a la organització. Aquest actiu serà sense cap dubte, un dels punts en els quals centrarem els nostres plans d'acció per tal de reduir el risc al que queda exposat.

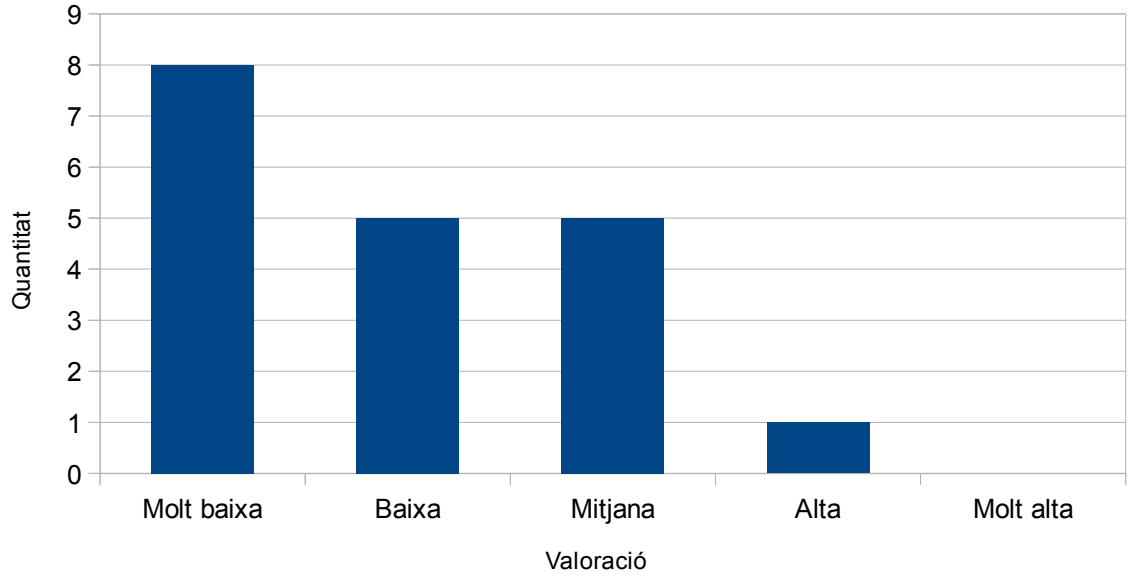


Tabla 4: Valoració d'actius

Nivell de Compliment Actual:

Un cop hem identificat i classificat els actius i les amenaces a les que es trobem exposats, podem procedir a generar la documentació relacionada amb el nivell de compliment actual de Hotel XXXX en relació amb cadascun dels 133 punts de controls establerts a la ISO/IEC 27002:2005.

En el annex 4 trobarem conjuntament el nivell de compliment amb un anàlisi diferencial per a cada control. La nomenclatura ha quedat establerta en el propi document, i per cada punt de control s'identifica si és d'aplicació o no, l'estat o fase en que es troba, i els comentaris relacionats oportuns. D'aquesta manera hem aconseguit agrupar en un mateix document la doble informació, fent-la més accessible i fàcil de consultar. Addicionalment, en el futur ens ajudarà a comparar l'evolució de l'empresa un cop s'hagin dut a terme plans d'acció amb activitats de millora. Per tal d'il·lustrar les conclusions extretes, adjuntem un resum executiu sobre el anàlisi GAP que es troba en el annex 4.

Resum executiu Anàlisi Compliment Actual:

Per conèixer de manera global l'estat actual de la organització en relació a la Seguretat de la Informació, realitzarem un anàlisis diferencial respecte la ISO/IEC 27001 i ISO/IEC 27002. Compararem quins controls s'apliquen adequadament i quins no, a més d'indicar si en falta algun per aplicar-se. Per a fer-ho, esmentarem les clàusules i els controls que afecten, indican el grau de compliment.

- **Política de Seguretat de la Informació**: no existeix aquest document. El control no es compleix.
- **Aspectes organitzatius per a la seguretat**: no existeix.
  - Organització interna: no compleix cap dels controls recomanats al no existir un document on es reflecteixi de manera clara les responsabilitats i els responsables de diferents àrees.
  - Seguretat enfront accessos de terceres parts: cap control implantat. No es té en compte els accessos de terceres parts a informació sensible, ni s'estableixen protocols o pautes a seguir en aquests casos.
- **Classificació i control d'actius**:
  - Responsabilitat dels actius: cap control implantat. Els actius es posen a disposició dels treballadors segons sorgeixi la necessitat, i no s'estableix una documentació on constin els responsables o propietaris d'aquests actius. Qualsevol acord o indicació és merament verbal.
  - Classificació de la informació: sense controls implantats. La informació rellevant no es etiquetada ni marcada, simplement distribuïda segons uns criteris marcats per direcció.
- **Seguretat en recursos humans**:
  - Seguretat abans del contracte: sense control. Al no existir una política de seguretat definida, aquesta no pot ser explicada als treballadors ni a les terceres parts. No existeixen acords de confidencialitat explícits, exceptuant algun contracte per defecte amb terceres parts, però redactada sempre pel proveïdor del servei.
  - Durant el contracte: controls inexistents.
  - Finalització del contracte: controls inexistents, tot i que no són aplicables a tots els treballadors.

- **Seguretat física de l'entorn**:
  - Àrees segures: no existeixen controls ja que no existeixen aquestes àrees.
  - Seguretat dels equips:
    - Protecció d'equips: control no aplicat, els equips estan el llocs accessibles per tothom.
    - Subministre elèctric: control no aplicat, no existeix protecció davant de talls en el subministre.
    - Seguretat en el cablejat: control no aplicat, les instal·lacions són les bàsiques, on el cablejat circula per el lloc "més adequat",
    - Altres controls no aplicats al ser desconeguts.
- **Gestió de comunicacions i operacions**:
  - Responsabilitats d'operacions: sense controls coneguts, les tasques no estan assignades.
  - Gestió de serveis externs: controls inexistents. No es revisa la política ni els acords amb terceres parts. Tampoc el bon funcionament dels contractes establerts.
  - Planificació i acceptació del sistema: no existeixen controls, no es planifiquen la disponibilitat ni capacitat del sistema per garantir el seu funcionament.
  - Protecció contra software maliciós: control implementat a baix nivell. Es disposa de mesures preventives com un antivirus o un programa anti-malware.
  - Gestió de recuperació i copies: sense controls, no existeixen copies ni polítiques que les fomentin i recolzin.
  - Gestió de la seguretat en xarxes: no existeixen controls, la seguretat en xarxa està configurada en nivell predeterminat, inclús a vegades essent inexistent.
  - Serveis de correu electrònic: controls no implantats parcialment, ningú garanteix la integritat de la informació més enllà de les garanties que dona el proveïdor de servei. Únicament es disposa de passarel·les electròniques per a les transaccions en línia que satisfan el control requerit. No existeixen activitats de monitoratge ni de registre de les activitats dutes a terme pels administradors.
- **Control d'accés**:
  - Política de control d'accés: no existeix el control, no existeix aquesta política.
  - Registre d'usuaris: sense control, no hi ha cap registre d'altes i baixes dels usuaris del sistema, en aquest cas, dels empleats o dels clients.
  - Gestió de contrasenyes d'usuaris: sense control. No es disposa d'un procés formal per gestionar les contrasenyes dels empleats a l'ordinador de recepció.
  - La resta de controls no són aplicables o no existeixen.
- **Adquisició, desenvolupament i manteniment de sistemes**: controls no aplicats ja que aquest apartat queda fora de l'abast del projecte. Els equips informàtics no acumulen prou informació com per ser tractats en aquest apartat. Posteriorment, en les revisions que es faran, si que seran inclosos en alguns punts de control.
- **Gestió d'incidents de la seguretat de la informació**: controls no aplicats. No existeix cap document previ que mostri debilitats o reports en forats de seguretat trobats. Les fallades tècniques més fonamentals es reporten verbalment.
- **Gestió de la continuïtat del negoci**: sense controls. No existeix un pla de continuïtat de negoci definit, i per tant, no hi han disponibles guies i pautes a seguir davant de grans imprevistos que pugin aturar el desenvolupament de les tasques bàsiques del negoci.
- **Compliment**:
  - Identificació de la legislació vigent: control implantat a baix nivell. Es coneix la llei vigent, però no es fa incidència en actualitzar-se voluntàriament. Es disposen dels certificats obligatoris que indica la llei.

- Drets de propietat intel·lectual: control implantat parcialment. El nom i el logotip estan registrats.
- Salvaguarda dels registres de l'organització: control no implementat, no s'aplica una política acurada per guardar les dades sensibles i els registres importants.
- Protecció de dades d'informació personal: control mal aplicat. Simplement es correspon correctament amb el relatiu a les càmeres de seguretat.
- Comprovació de la conformitat tècnica: control inexistent. No existeixen comprovacions prèvies.
- Altres controls no són aplicats.

Com podem veure, la gran majoria de controls no s'apliquen en gran part pel seu desconeixement. És per aquest motiu que és ben rebut la iniciativa de la junta directiva de demanar un estudi per elaborar un Pla de Seguretat. Els punts referits com a "no aplicats" estan relacionats amb una sèrie de controls que deriven d'altres anteriors que no existeixen, i per tant, aquests tampoc poden existir.

Documentació:

Tot Pla Director de Seguretat exigeix l'existència de certa documentació imprescindible per dur a terme tasques que poden ser, o molt senzilles, o molt complexes. La documentació que caldrà és:

- **Política de Seguretat:** Normativa interna que ha de conèixer i complir tot el personal afectat per l'abast del SGSI. El contingut de la Política ha de cobrir aspectes relatius a l'accés de la informació, us dels recursos de la Organització, comportament en cas d'incidents de seguretat, etc. (Annex 5)
- **Procediment d'Auditories Internes:** Document que ha d'incloure una planificació de les auditories que es portaran a terme durant la vigència del certificat (un cop s'obtingui), requisits que establiran els auditors interns i es definirà el model d'informe d'auditoria. (Annex 6)
- **Gestió d'indicadors:** És necessari definir indicadors per a mesurar l'eficiència dels controls de seguretat implementats. Igualment és important definir la sistemàtica per a fer les mesures. (Annex 9)
- **Procediment de Revisió per Direcció:** La Direcció de l'Organització ha de revisar anualment les qüestions més importants que han anat passant en relació al Sistema de Gestió de Seguretat de la Informació. Per aquesta revisió, la ISO/IEC 27001 defineix, tant els punts d'entrada, com els punts de sortida que han d'obtenir-se. (Annex 7)
- **Gestió de Rols i Responsabilitats:** El sistema de Gestió de Seguretat de la Informació ha d'estar compost per un equip que s'encarregui de crear, mantenir, supervisar i millorar el Sistema. Aquest equip de treball, conegut habitualment com a Comitè de Seguretat, es composa com a mínim d'una persona del comitè de direcció, d'aquesta manera les decisions que es prenguin podran estar aprovades prèviament per un membre de Direcció. (Annex 8)
- **Metodologia de Anàlisis de Riscos:** Estableix la sistemàtica que s'haurà de seguir per a calcular el risc i ha d'incloure bàsicament la identificació i valoració dels actius, amenaces i vulnerabilitats. (Annex 2)
- **Declaració de Aplicabilitat:** Document que inclou tots els controls de Seguretat establerts a la Organització, amb el detall de la seva aplicabilitat, estat i documentació relacionada. (Annex 4)
- **Objectius Pla Director de Seguretat:** Document en el que s'explica quina finalitat té la implantació d'aquest pla i quins objectius es persegueixen amb la creació del SGSI. Mostra els objectius de negoci de l'empresa i com el Pla Director queden alineats amb aquests. (Annex 10)

Hem pogut constatar que en el moment d'iniciar els nostres estudis, Hotel XXXX no disposava d'aquests documents. Per tal, ha estat de vital importància crear una primera versió que serà presentada a la junta directiva i aprovada, deixant així constància de la seva participació en el procés i de la bona voluntat recolzant la nostra tasca. La Declaració de Aplicabilitat la podem trobar al annex 4. La Metodologia de Anàlisi de Riscos es troba detallada al annex 2. La resta de documents es troben en els corresponents annexes segons s'ha detallat al llistat.

Proposta de Projectes:

Ara que ja coneixem bona part de les particularitats de Hotel XXXX, tant sobre el seu funcionament com sobre les amenaces que l'afecten, podem començar a treballar en planificar un Pla d'Acció que estigui alineat amb els objectius de l'empresa i que ajudin a mitigar els riscos en la seguretat de la informació. El projectes proposats queden adjuntats al annex 11.

Prèviament a la planificació dels projectes, s'ha estudiat quins actius podien patir un atac o ser víctimes d'algun error fortuït o accident, i quin cost es reflectiria en l'empresa. Per aquest motiu s'han plantejat moltes propostes destinades a corregir aquests errors amb una eficàcia superior al 90%, ja que en la majoria de casos era possible trobar solucions així d'eficients. Mirant als dominis de la ISO 27002:2005, trobem el gràfic següent:

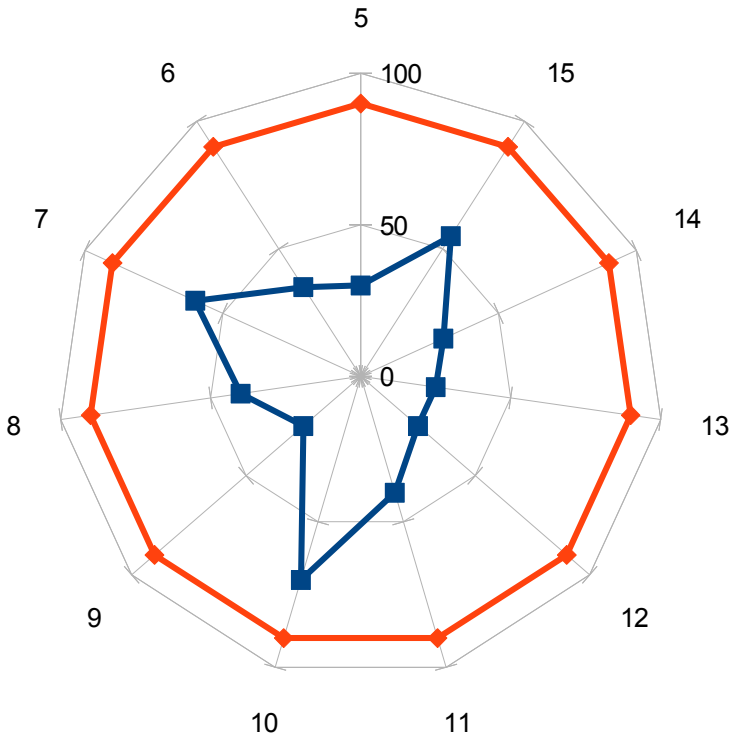


Tabla 5: Compliment dels dominis ISO/IEC 27002:2005

En color taronja se suposa l'estat ideal cap al qual desitgem que la nostra organització es dirigeixi. En canvi, en blau, trobem la realitat en la que es trobem aquests dominis. Observem que només tres dominis superen el 50% de compliment. De tots els possibles programes per solucionar aquesta situació, ens hem centrat en tres grans branques:

- **Documentació:** crear tota la documentació relacionada amb cada domini. Calien molts documents i polítiques d'aplicació que governessin els dominis de la seguretat de la informació. Aquests documents han de servir de guia per a la normalització de cada domini i

els seus respectius punts de control. També entenem com a documentació tot fitxer o text derivat de contractes o acords, que han de ser actualitzats i creats segons estableix la normativa legal vigent.

- **Prevenció i recolzament:** entre les principals amenaces que hem trobat estan la destrucció de la disponibilitat dels actius, sobretot dels que es troben físicament en el recinte. Per aquest motiu es duran a terme varies accions, entre les que destaquen:
  - reacondicionament d'espais per millorar la seguretat física dels actius
  - dotació d'equips i de mitjans de suport als equips actuals per tenir sempre present un pla de contingència davant d'emergències, i reduir el temps de reacció en la nova posada en marxa del sistema

  Amb aquestes dos vies es busca partir de una petita inversió inicial, però que repercuteixi en una gran disminució de la probabilitat de materialització d'una amenaça. En el cas de materialitzar-se, al disposar d'equips d'emergència, es mitiga considerablement les conseqüències.
- **Formació i conscienciació:** aquesta serà una de les etapes que possiblement ens ocupin més temps, però que serà necessària per arribar a un nivell de compliment suficient dels punts de control com per disposar d'un SGSI certificable. Al mateix temps, la formació treballa en paral·lel amb les tasques de prevenció d'incidents.

Altrament s'han proposat projectes que abracen més dominis diferents, però que potser no han estat tan destacables. En qualsevol cas, és interessant veure com aquestes propostes poden millorar la situació de l'empresa amb un cost suficientment baix, i acord amb els pressupostos pactats.

D'entre els aspectes organitzatius que calen abordar per a dur a terme aquestes propostes, a més de l'indicat als propis projectes, podem resumir que necessitarem la ferma voluntat de la junta directiva de realitzar-los. Això significa l'aprovació del pressupost indicat per a cada projecte, i l'acceptació del plaç proposat. A més, en molts casos, caldrà contractar mà d'obra extra, significant que cal trobar aquests treballadors dins dels terminis adients, sense demorar més la seva aplicació.

Altrament necessitem la col·laboració de tot el personal, per tal de que entenguin la importància dels projectes i que és el que significa dur a terme el pla d'acció aprovat. En alguns casos cal la implicació dels treballadors, com per exemple en el cas de oferir el cursos de formació que es comenta als annexos.

Els terminis i calendaris exactes per començar cada projecte serà pactat amb la junta directiva, buscant aquelles dates en les que quedin menys perjudicades les activitats quotidianes.

Quantificació de les millores:

Partint de la base coneguda, tant de problemes com de propostes per a la seva correcció, hem d'avaluar quina serà la millora que això aportarà al nostre sistema. Al annex 12 trobarem l'evolució després d'efectuar un estudi d'auditoria interna per a deixar preparat el sistema davant d'una futura certificació. Allà hi consten les evolucions més destacables, així com les fitxes que recullen els comentaris i les "no conformitats" més importants.

De entre els resultats que queden reflectits, podem comentar i comparar el nivell de compliment dels diferents dominis abans i després d'aplicar els plans d'acció presentats. La següent taula mostra la comparativa expressada en tant per cert.

En color verd considerem els dominis que han assolit l'objectiu plantejat i una millora proporcional als plans d'actuació. Això no vol dir que no siguin considerades com a "No Conformitats Menors". En la majoria de casos caldrà tornar a fer feina per millorar els resultats, però cal tenir en compte que hem partit d'una base molt plana i pràcticament sense cap antecedent ni planificació coneguda.

En groc queden ressaltats els dominis que han millorat, però que encara presenten deficiències.

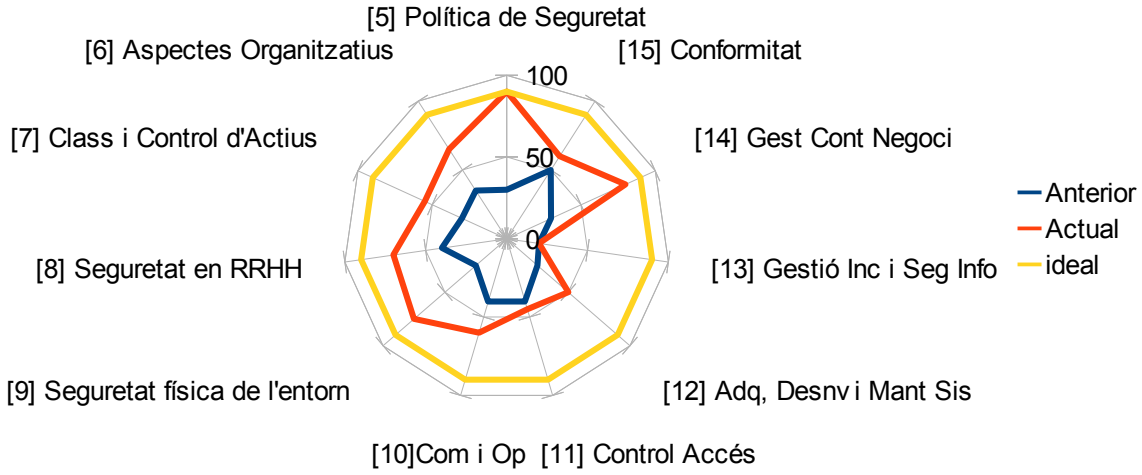
En vermells apareixen aquells seran considerats com No Conformitat Major, i que necessiten encara molt treball per augmentar el nombre de controls conformes.

Domini	% Inicial	% Actual
5	30	90
6	35	65
7	30	55
8	40	70
9	25	75
10	40	60
11	40	45
12	25	50
13	20	20
14	30	80
15	50	60

Com podem veure, gairebé tots els dominis superen el 50%, i tots han crescut. Un dels objectius dels plans d'accions eren fer créixer cada domini. En el diagrama de radar presentat més avall, podem veure la comparativa gràfica entre el abans i el després. Si bé és cert que alguns dominis han crescut fins assolir el nivell desitjat, altres ho han fet molt poc.

La millora quantificable podem xifrar-la en un increment de més del 80% el nombre de controls que s'apropen en un 50% o més a la puntuació desitjada.

La conclusió final és que els plans d'actuació han funcionat correctament sobre aquells dominis als que anaven dirigits, tal i com queda especificat en cada pla en concret. També es cert que s'ha actuat segons uns preferències determinades en el AR.



Després de totes aquestes conclusions i de les que es comenten més detalladament als annexos, podem donar per finalitzar el Pla Director de Seguretat. Tots els documents seran presentats a la junta directiva per explicar els resultats. Aquests documents poden trobar-se en forma d'arxius adjunts i annexos. La presentació que es farà també està inclosa.

Amb els documents generats, i la primera revisió del SGSI efectuant una auditoria interna, deixem el procés PDCA a punt per a tornar a començar la primera fase, i d'aquesta manera entrar en el cicle de millora continua.

Annex 1: Inventari d'Actius

A continuació mostrem una llista dels actius organitzats segons el grup al que pertanyin. Cal destacar equipaments auxiliars, on s'han considerat actius que ajuden en les tasques de la gestió de la informació.

Àmbit	***Actiu***	***Model***	***Ubicació***
Instal·lacions	Cablejat telefònic	Estàndard homologat	Tot edifici

Àmbit	***Actiu***	***Model***	***Ubicació***
Hardware	Ordinador recepció	HP Pro 3500	Recepció
	Ordinador portàtil direcció	Asus K550C	Despatx direcció
	Fax/impressora	Canon MG3250	Recepció
	Lector targetes crèdit	Conceptronic B670	Recepció
	Telefon recepció	Famitel	Recepció
	Telefon mòbil direcció	Samsung i9300	
	Càmera seguretat	Swann H284	Entrada, recepció, menjador

Àmbit	***Actiu***	***Model***	***Ubicació***
Aplicació	Pàgina web		En la xarxa
	Paquet ofimàtica	AOO v3.3.0	Ordinadors

Àmbit	***Actiu***	***Model***	***Ubicació***
Dades	Llibre registre	Travelmate	Recepció
	Llibreta calendari reserves	Papyrus Espiral	Recepció

Àmbit	***Actiu***	***Model***	***Ubicació***
Xarxa	Router wifi	Zyxzel T600	Recepció
	Repetidor wifi	D-link DAP 2310	Un per planta

Àmbit	***Actiu***	***Model***	***Ubicació***
Serveis			

Àmbit	*Actiu*	*Model*	*Ubicació*
Equipament auxiliar	Carpeta factures	Papyrus	Traster darrera recepció
	Caixa forta direcció	Desconegut	Traster

Àmbit	*Actiu*	*Model*	*Ubicació*
Personal	Treballador		Tot l'edifici

Àmbit	*Actiu*
Intangibles	Imatge corporativa
	Confiança dels clients

Entre els actius podem destacar algunes de les seves finalitats i relacions amb els serveis de informació:

- Ordinador Recepció: gestionar comandes en línia, donar suport a clients, consultar dades, navegació web variada, oferir un terminal d'accés a internet als clients que ho sol·licitin i ho cregui oportú la junta directiva, etc. Podem veure que és un terminal amb multitud de funcions, sense segregació de tasques.
- Ordinador Portàtil: és un ordinador d'ús exclusiu pels membres de la junta directiva. Té com a objectiu suplir les carències que pugin sorgir a l'ordinador de recepció. És el terminal des de on la junta realitza contractes amb terceres parts, consulta ordres i reserves, modifica informació sobre la web, i realitza altres tasques pròpies de la direcció.
- Fax/impressora: ubicat a la recepció, són els mitjans físics on arriben moltes confirmacions de reserves per part de terceres parts. A més serveixen per imprimir tota mena de documentació dels clients, com per exemple les seves fitxes. Són una eina important en la gestió de les peticions dels clients.
- Router/repetidors: tenen dos finalitats destacades. D'una banda donar accés a internet tant a la junta directiva com a l'ordinador de recepció. D'altra banda, també han de servir com a punt d'accés per als clients que desitgin establir una connexió amb la xarxa de manera gratuïta. Representa un dels serveis que ofereix Hotel XXXX.
- Telèfon recepció: primera línia de contacte telefònic amb l'hotel. A través d'aquest telefon s'atenen trucades de clients, que poden arribar a concretar reserves i entregar les seves dades mitjançant el canal de veu.
- Cablejat telefònic: es troba distribuït per tot l'edifici, ja que aquest ha estat construït fa més de 50 anys. La seva finalitat és donar servei als actius abans mencionats.
- Telèfon mòbil direcció: es tracta del terminal a través del qual es pot tenir comunicació directa amb algun membre de direcció en cas de que aquests no es trobin al edifici. Al mateix temps pretén ser un equip de suport en cas de fallida de les comunicacions mitjançant el cable telefònic tradicional. En la seva memòria s'hi guarden documents relacionats amb els clients, ja que es té accés a internet i als correus electrònics des de les comptes de l'empresa. També s'hi guarden nombroses dades de caràcter personal i que necessiten ser protegides.
- Lector targetes crèdit: la seva finalitat és realitzar els cobrament telemàtic als clients que

desitgen pagar amb una targeta de crèdit. Es troba al mostrador de recepció i es gestionada per el personal que en aquell moment ocupa la recepció.

- Llibre de registre: es tracta d'un llibre en format físic, tradicional, de paper, on els clients signen el seu registre quan arriben a l'hotel. Hi figuren dades de caràcter personal.
- Llibreta calendari de reserves: llibreta de paper, en la que s'anoten les reserves que fan els clients. Hi figuren els noms, les dates, l'habitació, i poca informació més. No obstant, és un dels elements més importants, ja que serveix com a comprovant per dur una correcte distribució dels clients, i conèixer la ocupació en un moment determinat. No existeixen còpies ni altres dispositius que guardin aquesta informació de manera centralitzada.
- Pàgina web: és l'element a través dels quals Hotel XXXX projecta la seva imatge en el món digital. Hi figuren les dades i les vies per contactar amb l'hotel, i s'hi poden fer reserves i pagar-les. Els clients transferiran les seves dades de caràcter personal a través d'aquesta web, al mateix temps que hi intervindran plataformes segures proporcionades per terceres parts.
- Paquet ofimàtica: conjunt de software dedicat a les tasques d'ofimàtica que podem trobar en qualsevol equip domestic. Es tracta de software lliure per evitar problemes de llicencies i estalviar en costos d'adquisició.
- Carpeta factures: tots els resguards i comprovants de pagament s'emmagatzemen en una carpeta ubicada en una petita habitació que es troba darrera de recepció. Aquesta habitació serveix per allotjar caixes i paquets que arriben de manera momentània. No disposa de un pany de seguretat; simplement una porta amb un pany tradicional. Les factures que es guarden contenen informació rellevant als clients i a la forma de pagament, així com altres dades que els vinculen amb el servei prestat per l'hotel.
- Caixa forta direcció: en la mateixa habitació abans descrita, s'hi amaga una petita caixa forta, en la que es guarden documents o objectes que es puguin considerar de valor. El seu contingut el desconeixem, però ens han assegurat que no hi conté actualment cap element rellevant. Pot servir per guardar la recaptació diària en èpoques de molta afluència de clients.
- Imatge corporativa: és l'actiu a través del qual el client identifica a Hotel XXXX amb un servei prestat, i que impulsa el negoci en tots els mitjans de comunicació dels que es tenen constància. La imatge corporativa té un valor molt alt, ja que és la via a través de la qual es comunica la satisfacció dels clients entre ells, i és un mitjà per atraure a nous i potencials consumidors. No es troba localitzada en un lloc en concret, sinó que forma part de la pròpia empresa.
- Confiança dels clients: ve relacionada amb la imatge corporativa, i és el nivell quantificable de confiança que els clients dipositen sobre Hotel XXXX, ja que creuen que aquests estaran a l'altura de les seves expectatives i sabran satisfer les seves necessitats en tot moment.
- Treballador: considerat treballador qualsevol membre del personal que participi activament en les tasques diàries. Aquestes persones formen part del molts processos diferents, entre els que s'hi troben la gestió de la seguretat de la informació, tot i que en la majoria de casos no són conscients d'això. Altres actius com la imatge corporativa i la confiança dels clients poden resultar afectades en funció de les accions en les que prenen part els treballadors i la manera en la que solucionen els problemes quotidians.

<u>Annex 2:</u> Anàlisi de Riscos

Per dur a terme l'anàlisi de riscos, prendrem la metodologia establerta que coneguda com Magerit, elaborada per el Ministeri d'Administracions Públiques. A continuació presentarem unes taules en les que es mostren els valors que s'han decidit considerar de manera objectiva per al càlcul dels riscos, tenint sempre en compte la dimensió de l'organització tractada i la seva estratègia de negoci. Per aquest motiu, si una valoració excedeix un plantejament coherent i alineat amb la política de l'organització, aquesta serà indicada i desestimada si es creu oportú.

- Procediment de valoració

  El conjunt d'actius que es valorarà no superarà mai el valor de 50.000€

Valoració	Rang	Valor
Molt alta	Valor > 25.000	50.000
Alta	10.000 < valor < 25.000	15.000
Mitjana	2.500 < valor < 10.000	5.000
Baixa	500 < valor < 2.500	1.500
Molt baixa	Valor < 500 €	500€

- Classificació de vulnerabilitats

Estimem que el pitjor cas suposaria que una vulnerabilitat es presentes un cop al dia, representant un valor anual de 365 / 365 = **1**

Vulnerabilitat	Rang	Valor
Freqüència extrema	1 vegada al dia	1
Freqüència alta	1 vegada cada dos setmanes	0,0712
Freqüència mitjana	1 vegada cada 2 mesos	0,0164
Freqüència baixa	1 vegada cada 6 mesos	0,0054
Freqüència molt baixa	1 vegada l'any	0,0027

- Valor impacte

Estimació de quin tant per cent del valor de l'actiu es perdria depenent del tipus d'impacte. En pitjor cas, es perdria el 100% de l'actiu.

Impacte	Valor
Molt alt	100%
Alt	75%
Mitjà	50%
Baix	20%
Molt baix	5%

- Efectivitat del control de seguretat

Valorarem en quin percentatge l'aplicació d'un control reduirà l'aparició del risc sobre el qual protegeix o preveu. Assumirem que mai serà del 100%.

Variació impacte	Valor reducció
Molt alt	90%
Alt	70%
Mitjà	50%
Baix	20%
Molt baix	10%

- Valoració d'actius

Es presenta la relació d'actius declarats, classificats segons la seva topologia, amb el valor assignat corresponent d'acord amb la taula de valoració adjuntada.

Actiu	Valor	Comentaris
Actius físics		
Ordinador recepció	Molt baixa	
Ordinador portàtil direcció	Baixa	
Fax/impressora	Molt baixa	
Lector targetes crèdit	Molt baixa	
Telefon recepció	Baixa	
Telefon mòbil direcció	Baixa	
Router wifi	Molt baixa	
Repetidor wifi	Molt baixa	
Llibre registre	Molt baixa	
Llibreta calendari reserves	Mitjana	Essencial per gestionar les entrades i sortides de clients
Carpeta factures	Molt baixa	
Càmera seguretat	Baixa	
Caixa forta direcció	Mitjana	Desconeixem el contingut
Actius lògics		
Pàgina web	Mitjana	
Paquet ofimàtica	Molt baixa	
Actius de personal		
Treballador	Mitjana	
Actius d'entorn i infraestructura		
Cablejat telefònic	Baixa	Imprescindible per les comunicacions
Actius intangibles		
Imatge corporativa	Alta	
Confiança dels clients	Mitjana	

- Anàlisi de riscos intrínsec

Per aquest càlcul farem servir la següent fórmula, aplicant els valor abans esmentats a les taules:

Risc = Valor de l'actiu x Vulnerabilitat x Impacte

Per calcular el risc efectiu en cas que fos necessari utilitzaríem:

R.Efectiu = R.Intrínsec x percentatge disminució vulnerabilitat x percentatge disminució impacte

A partir d'aquí es construiria una taula amb aquests valors i el resultat de les multiplicacions, i obtindríem per a cada actiu el seu valor anual. En aquest cas hem obviat aquesta taula, ja que ocuparia massa espai i dificultaria la lectura. Per una classificació més neta, es recomana col·locar un codi especific per a cada actiu, i un codi per a cada amenaça. D'aquesta manera la incorporació de les dades a la taula de càlcul serà més senzilla. En el cas d'utilitzar les eines proporcionades per Magerit, els càlculs es fan automàticament un cop introduïts els paràmetres.

Annex 3: Resultats Anàlisi de Riscos

Un cop tenim la metodologia que seguirem per fer el AR, ara podem quantificar els valors de cada actiu i observar quines dimensions de la seguretat intervenen en cadascun d'ells. Els següents documents mostren l'estudi dels actius relacionats amb la gestió de la informació de la nostra empresa, i en tractaran de fer una aproximació del seu valor, tant qualitatiu com quantitatiu, i l'impacte que tindria la seva fallada per a la nostra organització. Tots aquests punts juntament amb d'altres conformen l'Anàlisi de Riscos. Entre les diferents metodologies que podem triar per fer aquest anàlisis, treballarem seguint els passos oferts per la coneguda com MAGERIT juntament amb les accions que ens obliga la ISO/IEC 27001. Per a la justificació dels actius, prendrem els considerats en apartats anteriors.

Valoració dels actius:

Aquesta valoració es farà en funció de tres paràmetres per cada actiu i de manera qualitativa. Aquests paràmetres són "**integritat, disponibilitat i confidencialitat**". Per a cada característica assignarem un valor que es trobarà entre "**molt baix, baix, mitjà, alt, molt alt**", depenent de la importància de la pèrdua de cadascun d'aquests valors. Finalment, ens quedarem amb el valor més alt que resulti de entre les tres propietats esmentades, i serà aquest el valor reflexat a les taules següents. Entre parèntesis trobarem la propietat fonamental i considerada més important per aquell actiu, i la qual dona la nota del valor d'aquest.

Actiu	Valor	Comentaris
Actius hardware		
Ordinador recepció	Molt baixa	(Disponibilitat)
Ordinador portàtil direcció	Mitjà	(Disponibilitat)
Fax/impressora	Baixa	(Disponibilitat)
Lector targetes crèdit	Molt baixa	(Disponibilitat)
Telefon recepció	Baixa	(Disponibilitat)
Telefon mòbil direcció	Mitjà	(Disponibilitat)
Càmera seguretat	Molt baixa	(Disponibilitat)
Actius aplicació		
Pàgina web	Alta	(Disponibilitat)
Paquet ofimàtica	Molt baixa	(Disponibilitat)
Actius de personal		
Treballador	Mitjana	(Disponibilitat)
Actius d'entorn i infraestructura		
Cablejat telefònic	Alta	Imprescindible per les comunicacions (Disponibilitat)

Actius intangibles		
Imatge corporativa	Molt alta	(Integritat)
Confiança dels clients	Alta	(Confidencialitat)
Actius de xarxa		
Router wifi	Mitjà	(Disponibilitat)
Repetidor wifi	Molt baixa	(Disponibilitat)
Actius de dades		
Llibre de registre	Baixa	(Integritat)
Llibreta calendari reserves	Alta	Essencial per gestionar les entrades i sortides de clients (Disponibilitat / Integritat)
Actius d'equipament auxiliar		
Carpeta factures	Molt baixa	(Integritat)
Caixa forta direcció	Mitjana	Desconeixem el contingut (Integritat / Confidencialitat)

Taula de dependències		
Actiu Superior	**Actiu Inferior**	**Comentaris**
Repetidor wifi	Router wifi	Sense en funcionament del router, el repetidor no actua
Lector targetes crèdit	Cablejat telefònic	Necessari per mantenir les comunicacions
Fax / impressora	Cablejat telefònic	

Dimensions de la seguretat:

En aquest apartat crearem una taula resum amb la informació de cada actiu i la seva criticitat relacionada amb cadascuna de les 5 dimensions de la seguretat. Aquestes dimensions són "**A**utenticitat, **C**onfidencialitat, **I**ntegritat, **D**isponibilitat, **T**raçabilitat". Mitjançant aquestes valoracions podrem avaluar l'impacte de la materialització d'una amenaça sobre l'actiu exposat.

En la nostra empresa el significat de cadascuna d'aquestes dimensions és el següent:

- **Autenticitat**: garantia de la identitat dels usuaris que realitzen una acció sobre el procés de la informació.
- **Confidencialitat**: l'accés a la informació sensible o privada està disponible només a les persones autoritzades.
- **Integritat**: la informació i els mètodes de processament són exactes i complets.
- **Disponibilitat**: els usuaris autoritzats poden accedir a la informació quan ho necessitin.
- **Traçabilitat**: possibilitat de reproduir una seqüència d'accions sobre un determinat procés i determinar l'autor.

L'escala per a la valoració que utilitzarem serà com segueix:

VALOR	CRITERI
10	Dany molt greu a la organització
7-9	Dany greu a la organització
4-6	Dany important a la organització
1-3	Dany menor a la organització
0	Dany irrellevant a la organització

Els actius es valoraran segons la seva importància per al procés de la seguretat de la informació com “Molt alta, alta, mitja, baixa, irrellevant”. Tot el conjunt ens permet obtenir la **taula resum** següent:

Valoració dels Actius							
Àmbit	**Actiu**	**Valor**	**Aspectes Crítics**				
			A	**C**	**I**	**D**	**T**
Hardware	Ordinador recepció	BAIXA	1	3	2	3	0
Hardware	Ordinador portàtil direcció	MITJANA	4	6	3	6	1
Hardware	Fax/impressora	BAIXA	1	1	1	3	0
Hardware	Lector targetes crèdit	IRRELLEVANT	1	1	0	2	1
Hardware	Telefon recepció	BAIXA	2	2	1	3	1
Hardware	Telefon mòbil direcció	MITJANA	4	3	1	5	3
Hardware	Càmera seguretat	IRRELLEVANT	3	0	0	3	0
Aplicació	Pàgina web	ALTA	7	7	8	8	3
Aplicació	Paquet ofimàtica	IRRELLEVANT	0	0	0	2	0
Xarxa	Router wifi	MITJANA	2	5	1	4	0
Xarxa	Repetidor wifi	BAIXA	0	1	1	3	0
Dades	Llibre de registre	BAIXA	2	2	2	1	2
Dades	Llibreta calendari reserves	ALTA	8	5	7	8	3
Equipament auxiliar	Carpeta factures	IRRELLEVANT	0	2	3	1	1
Equipament auxiliar	Caixa forta direcció	MITJANA	4	6	5	2	0
Infraestructura	Cablejat telefònic	ALTA	3	7	5	9	0
Personal	Treballador	MITJANA	3	0	0	6	4
Intangibles	Imatge corporativa	MOLT ALTA	10	4	10	8	0
Intangibles	Confiança clients	ALTA	7	6	3	8	0

Anàlisi d'amenaces:

En aquest apartat la nostra intenció és analitzar les diferents amenaces que existeixen, quines vulnerabilitats estan relacionades i exploten, i a quin actiu afecten. Per fer-ho, crearem diverses taules classificatòries amb la informació, i finalment ho agruparem en una taula que relacioni les dades. Serà important classificar les amenaces segons el seu origen, i per aquest motiu, farem servir els criteris de la nomenclatura Magerit:

- Desastres naturals
- D'origen industrial
- Errors o fallides no intencionades
- Atacs intencionats

Al mateix temps, disposarem d'una taula estimatòria de la freqüència d'ocurrència d'aquestes amenaces. La taula resum que sorgirà estarà agrupada segons el tipus d'actiu que analitzem, i sempre seguint el mateix criteri que hem fet servir en apartats anteriors. A continuació exposem les taules que hem comentat:

- **Classificació de vulnerabilitats**

Estimem que el pitjor cas suposaria que una vulnerabilitat es presentes un cop al dia, representant un valor anual de 365 / 365 = **1**

Vulnerabilitat	Rang	Valor	Codi
Freqüència extrema	1 vegada al dia	1	F5
Freqüència alta	1 vegada cada dos setmanes	0,0712	F4
Freqüència mitjana	1 vegada cada 2 mesos	0,0164	F3
Freqüència baixa	1 vegada cada 6 mesos	0,0054	F2
Freqüència molt baixa	1 vegada l'any	0,0027	F1

- **Classificació d'amenaces**

Les agruparem segons el seu origen i els hi assignarem un codi. Degut al tamany de l'empresa no existeixen un conjunt massa gran d'amenaces identificades, i es poden arribar a escapar al nostre anàlisis algunes de molt remotes.

Tipus (Origen)	Amenaça	Codi
Desastre Natural	Incendi	DN1
Desastre Natural	Inundació	DN2
Desastre Natural	Pujada tensió a la xarxa elèctrica	DN3
Origen Industrial	Baixa laboral (personal)	OI1
Origen Industrial	Mal servei ofert	OI2
Error o fallides no intencionades	Avaria	E1
Error o fallides no intencionades	Pèrdua d'un objecte concret	E2
Error o fallides no intencionades	Esborrat accidental	E3
Atacs intencionats	Esborrat informació	A1
Atacs intencionats	Defacement	A2
Atacs intencionats	Atac DdoS	A3
Atacs intencionats	Robatori	A4
Atacs intencionats	Destrucció	A5
Atacs intencionats	Intrusió no autoritzada	A6
Atacs intencionats	Sabotatge	A7
Atacs intencionats	Devaluació d'un valor concret	A8

Amb tota la informació anterior, elaborem una taula per a cada tipus d'actiu amb les amenaces sota les que es troba envoltat. Aquesta taula mostra els actius i les seves dimensions de la seguretat i com aquestes queden compromeses davant d'aquesta incidència.

Actiu	Amenaça	Freqüència	[A]	[C]	[D]	[I]	[T]
Hardware							
Ordinador recepció	DN1	F1			100%		
Ordinador recepció	DN2	F1			100%		
Ordinador recepció	DN3	F1			100%		
Ordinador recepció	E1	F3		50%	100%		
Ordinador recepció	A4	F1	100%	100%	100%		
Ordinador recepció	A7	F1	50%	50%	100%		
Ordinador portàtil direcció	DN1	F1			100%		

Ordinador portàtil direcció	DN2	F1			100%		
Ordinador portàtil direcció	DN3	F1			50%		
Ordinador portàtil direcció	E1	F2		25%	100%		
Ordinador portàtil direcció	A4	F1	100%	100%	100%		
Fax/impressora	E1	F2			100%		
Fax/impressora	A4	F1			100%		
Lector targetes crèdit	E1	F1			100%		
Lector targetes crèdit	A4	F1			100%		
Telefon recepció	A4	F1			100%		
Telefon mòbil direcció	E1	F2			50%		
Telefon mòbil direcció	E2	F2	50%	75%	100%		25%
Telefon mòbil direcció	A4	F1	75%	75%	100%		25%
Càmera seguretat	E1	F1		25%	100%		
Aplicació							
Pàgina web	A2	F1	90%	80%	60%	90%	75%
Pàgina web	A3	F2	25%	25%	80%	10%	75%
Pàgina web	A1	F1	50%		100%	90%	90%
Pàgina web	A6	F3	75%	100%	85%	50%	50%
Paquet ofimàtica	E3	F1			100%	50%	
Xarxa							
Router wifi	E1	F2			100%		
Router wifi	A3				80%	60%	50%
Router wifi	A6	F2	50%	50%	50%		70%
Repetidor wifi	E1				100%		
Dades							
Llibre de registre	E2	F2	40%		30%	60%	50%
Llibre de registre	A5	F1	40%		50%	75%	50%
Llibreta calendari reserves	E2	F1	50%	60%	90%	75%	50%
Llibreta calendari reserves	A5	F1	50%	60%	90%	75%	50%
Equipament auxiliar							
Carpeta factures	E2	F1	20%	30%	50%		40%
Caixa forta direcció	A4	F1	70%	90%	100%		
Infraestructura							
Cablejat telefònic	DN1				100%		
Cablejat telefònic	A5				100%		
Personal							

Treballador	OI1	F2			100%		
Intangibles							
Imatge corporativa	OI2	F1			20%	75%	
Imatge corporativa	A8	F1	70%	80%	50%	75%	
Confiança clients	OI2	F2			20%	75%	

Impacte potencial:

Un cop tenim les dades presentades fins ara, es tracta de determinar quin cost tindrà per a l'empresa la materialització d'alguna de les amenaces. Per aconseguir una estimació quantitativa d'aquest cost, hem avaluat de manera objectiva els possibles valors del actius segons la següent taula:

El conjunt d'actius que es valorarà no superarà mai el valor de 50.000€

Valoració	Rang	Valor
Molt alta	Valor > 25.000	50.000
Alta	10.000 < valor < 25.000	15.000
Mitjana	2.500 < valor < 10.000	5.000
Baixa	500 < valor < 2.500	1.500
Molt baixa	Valor < 500 €	500€

Actiu	Valor	Comentaris
Actius hardware		
Ordinador recepció	Molt baixa	
Ordinador portàtil direcció	Baixa	
Fax/impressora	Molt baixa	
Lector targetes crèdit	Molt baixa	
Telefon recepció	Baixa	
Telefon mòbil direcció	Baixa	
Càmera seguretat	Baixa	
Actius aplicació		
Pàgina web	Mitjana	
Paquet ofimàtica	Molt baixa	
Actius de personal		
Treballador	Mitjana	

Actius d'entorn i infraestructura		
Cablejat telefònic	Baixa	Imprescindible per les comunicacions
Actius intangibles		
Imatge corporativa	Alta	
Confiança dels clients	Mitjana	
Actius de xarxa		
Router wifi	Molt baixa	
Repetidor wifi	Molt baixa	
Actius de dades		
Llibre de registre	Molt baixa	
Llibreta calendari reserves	Mitjana	Essencial per gestionar les entrades i sortides de clients
Actius d'equipament auxiliar		
Carpeta factures	Molt baixa	
Caixa forta direcció	Mitjana	Desconeixem el contingut

Cal notar que aquesta última taula, tot i que s'assembla a la presentada en la valoració dels actius, no respon segons la vinculació d'aquests amb les diferents dimensions de la informació, sinó que ho fa respecte la valoració econòmica i en "xifres" aproximades.

A partir d'aquesta taula podríem seguir tal i com suggereix la metodologia Magerit, on el software que ens proporciona disposa d'una graella per omplir amb les dades anteriors i fer una estimació del cost anual del risc intrínsec per a cada actiu. D'aquesta manera podrem visualitzar en termes econòmics i quantificables aquest nivell de risc intrínsec.

- Anàlisi de riscos intrínsec

Per aquest càlcul farem servir la següent fórmula, aplicant els valor abans esmentats a les taules:

$$Risc = Valor\ de\ l'actiu \times Vulnerabilitat \times Impacte$$

Per calcular el risc efectiu en cas que fos necessari utilitzaríem:

$$R.Efectiu = R.Intrínsec \times percentatge\ disminució\ vulnerabilitat \times percentatge\ disminució\ impacte$$

Nota: El disseny de la taula l'hem obviat donada la seva mida, ja que com és evident, partiríem de les taules anteriors, les quals són prou amplies. No obstant, el càlcul s'efectuaria dintre de les eines proporcionades per Magerit, de manera que els "outputs" també poguessin ser visualitzats de manera més neta i ordenada. En el nostre cas i al tractar-se d'una pràctica, no disposem d'aquesta eina indicada per a professionals del sector, però sempre podríem crear-ne una de similar amb una taula i graelles d'una fulla de càlcul convencional.

Nivell de Risc Acceptable i de Risc Residual:

En aquesta fase haurem de decidir quin llindar de risc es acceptable per a la nostra empresa i a partir de quin punt hem d'actuar per disminuir el risc i que quedi dintre dels paràmetres desitjats.

Nivell de Risc = Valor + (Impacte x Probabilitat)

Com a resultat obtindrem un valor numèric. Aquest valor es pot classificar com:

Valor	**Nivell**
9.1 - 10	Extrem
7.1 - 9	Molt alt
4.1 - 7	Alt
2.6 - 4	Baix
0 - 2.5	Molt Baix

En el cas que ens ocupa, la junta directiva ha manifestat que, un cop exposat el cas que ens ocupa, vol implantar les mesures necessàries per a que tot nivell de risc quedi englobat en els llindars “baix o molt baix”, que es consideraran nivells de Risc Acceptable. La resta de nivells i els seus actius seran objecte de controls per tal de reduir aquest risc fins a valors acceptables. Igualment és aconsellable que el nivell de risc que resti un cop implantats els controls necessaris, anomenat Risc Residual, es trobi en el nivell “molt baix”. Si no és així, caldrà revisar si existeix l'opció de millorar el control o implantar-ne d'addicionals.

<u>Annex 4:</u> Declaració de Aplicabilitat

A continuació llistarem la serie de controls que resulten de la norma ISO/IEC 27001 annex A, i reflectirem si són d'aplicació o no a Hotel XXXX. Per a millorar la nostra declaració d'aplicabilitat, acompanyarem cada control amb un valor de la següent taula, en funció del nivell de maduresa del control:

- Planificat: encara no ha estat implementat
- Iniciat: s'està treballant per implementar-lo
- Implantat sense documentar
- Implantat sense auditar: està documentat, però ha de ser auditat
- Auditat: completament implantat i auditat

Ref	Nom	Aplicabilitat	Comentaris	Maduresa
5	Política Seguretat			
5.1	Política de Seguretat de la Informació			
5.1.1	Doc Política de Seguretat de la Informació	APLICA		Iniciat
5.1.2	Revisió i avaluació	APLICA		Planificat
6	Aspectes organitzatius			
6.1	Organització interna			
6.1.1	Comitè de gestió de la seguretat de la informació	APLICA		Iniciat
6.1.2	Coord de la seguretat de la informació	APLICA		Iniciat
6.1.3	Assig responsabilitats seguretat informació	APLICA		Iniciat
6.1.4	Proc autorització recursos tractament informació	APLICA		Planificat
6.1.5	Acords confidencialitat	APLICA		Implantat sense documentar
6.1.6	Contacte autoritats	APLICA		Planificat
6.1.7	Contacte grups especialitzats	NO APLICA	No existeixen grups relacionats amb sector hosteleria	
6.1.8	Revisió independent de la seg informació	APLICA	Inclourà la certificació del SGSI	Planificat

6.2	Seguretat en els accessos de terceres parts			
6.2.1	Identificació de riscos	APLICA		Iniciat
6.2.2	Requisits seg al tractar amb clients	APLICA		Planificat
6.2.3	Requisits seg contractes outsourcing	APLICA		Implementat sense documentar
7	Classificació i control d'actius			
7.1	Responsabilitat sobre actius			
7.1.1	Inventari actius	APLICA	Existeix una relació d'actius, però no està correctament documentada	Implementat sense documentar
7.1.2	Propietat dels actius	APLICA		Implementat sense documentar
7.1.3	Ús adequat dels actius	APLICA		Iniciat
7.2	Classificació informació			
7.2.1	Guies de classificació	APLICA		Planificat
7.2.2	Marcatge i tractament informació	APLICA		Planificat
8	Seguretat en recursos humans			
8.1	Seguretat abans de la feina			
8.1.1	Inclusió de la seg en les responsabilitats laborals	APLICA		Planificat
8.1.2	Selecció i política de personal	APLICA		Planificat
8.1.3	Acords confidencialitat	APLICA		Implantat sense documentar
8.2	Durant el treball			
8.2.1	Responsabilitat de la gerència	APLICA		Iniciat
8.2.2	Conscienciació, formació i capacitació en seguretat	APLICA	Amb els contractes de confidencialitat són suficients per al tipus de	Iniciat

			feina	
8.2.3	Proces disciplinari	APLICA		Implantat sense documentar
8.3	Finalització treball			
8.3.1	Responsabilitats finalització	NO APLICA	Cobert pels controls 6.1.5 i 8.1.3	
8.2.3	Retorn d'actius	NO APLICA	Els empleats no posseïxen actius fora del recinte	
8.3.3	Revocació drets accés	NO APLICA	Queda fora de la magnitud de l'organització	
9	Seguretat física de l'entorn			
9.1	Àrees segures			
9.1.1	Perímetre de seguretat física	APLICA	Aquestes zones no havien estat determinades	Planificat
9.1.2	Controls físics d'entrada	NO APLICA	No existeixen zones tant concretes de inf sensible	
9.1.3	Seg oficines, despatxos i recursos	APLICA		Planificat
9.1.4	Protecció contra amenaces externes	APLICA		Implantat sense documentar
9.1.5	Treball en àrees segures	NO APLICA	No existeixen	
9.1.6	Accés àrees carrega	NO APLICA	No existeixen	
9.2	Seguretat dels equips			
9.2.1	Instal·lació i protecció equips	APLICA		Iniciat
9.2.2	Subministre elèctric	APLICA	Està previst col·locar SAI's	Planificat
9.2.3	Seguretat cablejat	NO APLICA	Fora de l'abast de la empressa	
9.2.4	Manteniment equips	APLICA		Iniciat
9.2.5	Seg equips fora locals	NO APLICA	No existeixen	
9.2.6	Seg eliminació equips	APLICA		Planificat
9.2.7	Revocació propietat	NO APLICA	No es dona la situació	
10	Gestió comunicacions i operacions			
10.1	Procediments i responsabilitats de operacions			

10.1.1	Documentació i procediments operatius	APLICA		Planificat
10.1.2	Gestió i canvis	APLICA	Aplica però no existeixen màquines prou rellevants i diferenciades	Planificat
10.1.3	Segregació de tasques	NO APLICA	Mida de l'organització massa petita	
10.1.4	Separació de recursos per al desenvolupament i producció	NO APLICA	Queda fora de l'àmbit de l'organització	
10.2	Gestió de serveis externs			
10.2.1	Servei d'entrega	APLICA		Implementat sense documentar
10.2.2	Monitoratge i revisió serveis externs	NO APLICA	Excedeix l'abast de la política de seguretat	
10.2.3	Gestionar canvis pels serveis externs	NO APLICA	Excedeix l'abast de la política de seguretat	
10.3	Planificació i acceptació del sistema			
10.3.1	Planificació de capacitat	NO APLICA	No hi ha risc de sobrecàrrega al sistema	
10.3.2	Acceptació del sistema	NO APLICA	Fora de l'abast	
10.4	Protecció contra software maliciós			
10.4.1	Mesures i controls	APLICA	Aplicat antivirus, firewalls i actualitzacions	Iniciat
10.4.2	Mesures codi mòbil	NO APLICA	No existeix	
10.5	Gestió de recuperació			
10.5.1	Recuperació informació	APLICA		Iniciat
10.6	Gestió seg en xarxes			
10.6.1	Controls de xarxa	APLICA		Implantat sense documentar
10.6.2	Seguretat en serveis de xarxes	NO APLICA	Queda fora de l'ambit de treball de l'organització	
10.7	Utilització dels mitjans de informació			
10.7.1	Gestió de mitjans extractables	NO APLICA	No existeixen aquests medis	
10.7.2	Eliminació dels mitjans	NO APLICA	No existeixen	
10.7.3	Procediments de	APLICA		Planificat

	manipulació de info			
10.7.4	Seg de la documentació de sistemes	NO APLICA	No existeix aquesta informació	
10.8	Intercanvi de informació			
10.8.1	Polítiques i procediments per l'intercanvi de info i software	APLICA	Centrar en correus electrònics i comunicacions bancàries	Implementat sense documentar
10.8.2	Acords d'intercanvi	APLICA		Implementar sense documentar
10.8.3	Mitjans físics en trànsit	NO APLICA	No existeixen	
10.8.4	Seguretat en missatgeria electrònica	APLICA		Implementat sense documentar
10.8.5	Sis informació de negoci	NO APLICA	No existeixen	
10.9	Serveis de correu electrònic			
10.9.1	Comerç electrònic	APLICA		Implementat sense auditar
10.9.2	Transaccions en línia	APLICA		Implementat sense auditar
10.9.3	Info pública disponible	APLICA		Implementat sense auditar
10.10	Monitoratge			
10.10.1	Registre de la auditoria	NO APLICA	No adient a la mida de l'organització	
10.10.2	Monitoratge de l'ús del sistema	NO APLICA	No es té necessitat en els processos existents	
10.10.3	Protecció de les traces	NO APLICA	No existeixen instal·lacions	
10.10.4	Traces d'administració i operació	NO APLICA	Excedeix la mida de l'organització	
10.10.5	Registre de fallades	APLICA		Planificat
10.10.6	Sincronització de rellotges	NO APLICA	No necessari per a les tasques desenvolupades	
11	Control d'accés			
11.1	Requisits de negoci per al control d'accés			
11.1.1	Política de control d'accés	APLICA		Planificat

11.2	Gestió de l'accés dels usuaris			
11.2.1	Registre d'usuaris	APLICA		Implementat sense documentar
11.2.2	Gestió de privilegis	APLICA		Implementat sense documentar
11.2.3	Gestió de contrasenyes d'usuari	NO APLICA	Aquest procés queda reduït a altres apartats donada el petit tamany a gestionar	
11.2.4	Revisió dels drets d'accés d'usuari	NO APLICA	No aplica degut a la mida de l'organització	
11.3	Responsabilitats dels usuaris			
11.3.1	Ús de credencials	APLICA		Implementat sense documentar
11.3.2	Equips d'usuaris desatesos	NO APLICA	No existeixen ni poden existir	
11.3.3	Política de taules i pantalles netes	NO APLICA	No existeix aquesta possibilitat	
11.4	Control d'accés a la xarxa			
11.4.1	Política d'ús dels serveis de xarxa	APLICA		Planificat
11.4.2	Autenticació d'usuaris conexions remotes	NO APLICA	No existeix aquesta opció	
11.4.3	Autenticació de nodes a la xarxa	NO APLICA	No existeix aquesta opció	
11.4.4	Config port en remot	NO APLICA	No existeix aquesta opció	
11.4.5	Segregació de xarxes	NO APLICA	No existeix xarxa a segregar	
11.4.6	Control de connexió a la xarxa	NO APLICA	Queda cobert amb el punt 11.1.1	
11.4.7	Control d'encaminament xarxa	NO APLICA	Mida massa petita per aplicar aquest control	
11.5	Control d'accés al sistema operatiu			
11.5.1	Procediments connexió	APLICA		Planificat
11.5.2	Identificació i autenticació usuaris	NO APLICA	Utilització de comptes compartides	
11.5.3	Sistema de gestió de contrasenyes	NO APLICA	Queda controlat amb altres punts degut a la mida petita	
11.5.4	Ús serveis sistema	NO APLICA	No s'han detectat serveis a	

			restringir el seu ús	
11.5.5	Desconnexió automàtica sessió	APLICA	Mesures per defecte aplicades	Iniciat
11.5.6	Limitació temps connexió	NO APLICA	Contradiu altres necessitats de treball de l'organització	
11.6	Control d'accés a la info i a les aplicacions			
11.6.1	Restricció d'accés info	APLICA		Iniciat
11.6.2	Aïllament sis sensibles	NO APLICA	No existeixen aquests sist	
11.7	Informàtica mòbil i teletreball			
11.7.1	Informàtica mòbil	NO APLICA	No existeix	
11.7.2	Teletreball	NO APLICA	No està disponible l'opció	
12	Adquisició, desenvolupament i manteniment sistemes			
12.1	Requisits seguretat en sistemes de informació			
12.1.1	Anàlisi especificacions requisits	NO APLICA	Està fora de la planificació de l'organització	
12.2	Control processos en aplicacions			
12.2.1	Validació dades entrada	NO APLICA	No hi han dades d'entrada	
12.2.2	Control de processos interns	NO APLICA	No hi han processos interns	
12.2.3	Integritat de missatges	NO APLICA	No hi han aplicacions que ho requereixin	
12.2.4	Validació dades sortida	NO APLICA	No hi han processos	
12.3	Controls criptogràfics			
12.3.1	Política ús controls crip	APLICA		Planificat
12.3.2	Xifratge	NO APLICA	No aplicable als petits processos que existeixen	
12.4	Seguretat fitxers sistema			
12.4.1	Control programari en producció	NO APLICA	No existeix	
12.4.2	Protecció dades de prova	NO APLICA	No es disposen d'aquest tipus de dades	
12.4.3	Control accés codi font	NO APLICA	No es produeix aquest codi	

12.5	Seguretat en el desenvolupament i en el suport			
12.5.1	Procediments de control de canvis	APLICA		Iniciat
12.5.2	Revisió tècnica canvis sistema operatiu	APLICA	Els canvis es proven però no deixen constància	Iniciat
12.5.3	Restricció canvis en paquets de programari	NO APLICA	No s'utilitza programari	
12.5.4	Fuites d'informació a través del codi	NO APLICA	No es desenvolupa programari amb codi font	
12.5.5	Externalització del desenvolupament de programari	NO APLICA	No es demana aquesta funció	
12.6	Gestió vulnerabilitats tècniques			
12.6.1	Control vuln tècniques	APLICA	Pentesting pendent	Planificat
13	Gestió incidències de seguretat de la informació			
13.1	Notificació incidències i debilitats			
13.1.1	Notificació events seg	APLICA		Planificat
13.1.2	Notificació debilitats	APLICA		Planificat
13.2	Gestió incidències i millora			
13.2.1	Identificació responsabilitat i procediments	APLICA		Iniciat
13.2.2	Avaluació incidències	APLICA		Iniciat
13.2.3	recol·lecció evidències	APLICA		Planificat
14	Gestió de continuïtat de negoci			
14.1	Aspectes de la gest de continuïtat de negoci			
14.1.1	Incloure la seg info en el procés de cont negoci	APLICA	Iniciat amb aquesta tasca	Iniciat
14.1.2	Continuïtat negoci i anàlisi impacte	APLICA		Iniciat

14.1.3	Documentació i implantació del pla de continuïtat de negoci	APLICA		Planificat
14.1.4	Marc de planificació	APLICA		Iniciat
14.1.5	Proves, manteniment i reavaluació dels plans	APLICA		Planificat
15	Conformitat			
15.1	Conformitat amb requisits legals			
15.1.1	Identificació legislació	APLICA		Implementat sense documentar
15.1.2	Dret de la propietat intel·lectual	APLICA		Implementat per ser auditat
15.1.3	Control seg registres de l'organització	APLICA		Iniciat
15.1.4	Protecció dades personals	APLICA		Implementat per ser auditat
15.1.5	Evitar mal ús recursos de tractament de la info	APLICA		Implementat sense documentar
15.1.6	Reglamentació controls xifratge	NO APLICA	Queda fora de l'abast dels objectius plantejats	
15.2	Compliment marc normatiu			
15.2.1	Compliment polítiques i normes	APLICA		Planificat
15.2.2	Comprovació conformitat tècnica	APLICA	Es farà mitjançant auditories internes	Planificat
15.3	Auditoria de sistemes			
15.3.1	Controls d'auditoria	APLICA		Planificat
15.3.2	Protecció eines auditoria	NO APLICA	Aquesta responsabilitat queda en mans de l'auditor	

<u>Annex 5:</u> Objectius del Pla Director

El Pla Director de Seguretat que desenvoluparem té diversos objectius. D'una banda vol constatar l'estat actual de la seguretat del sistemes de comunicació definits en l'abast d'aquest pla. Així mateix, pretén mostrar les mancances que existeixin i oferir una guia amb recomanacions i possibles solucions per pal·liar aquestes deficiències.

Les millores en seguretat de la informació proporcionaran una millor imatge corporativa a l'organització, sobretot en un punt concret que està fortament alineat amb els plans de negoci que té la junta directiva. Primerament millorarà la seguretat d'informació que es considera clau, evitant incidències fortuïtes o planejades sobre aquesta. Aquesta seguretat repercutirà en un augment de la confiança per part dels clients, ajudant a l'estratègia de negoci que consisteix en fidelitzar a la clientela.

Addicionalment, aquest estudi pot servir per oferir una primera avaluació de l'estat actual dels punts abans descrits, i en quina mesura serien necessaris uns canvis per adaptar-se a la normativa legal vigent de cara a obtenir les certificacions oficials que pugi requerir la llei en un futur proper.

Finalment cal destacar que les conclusions que s'extrauran serviran per mostrar les correccions més importants i urgents que cal fer, i com aquestes poden significar un estalvi futur en matèria de seguretat de la informació i les comunicacions.

Per dur a terme aquest Pla Director la junta directiva d'Hotel XXXX es compromet a facilitar les tasques que durà a terme el personal responsable, i a posar tot l'interès possible així com els mitjans necessaris que resultin oportuns per dur a terme les mesures correctives proposades, sempre que aquestes siguin proporcionals i adequades amb els plans de negoci de l'organització.

D'aquesta manera queda definit l'**abast** com: tots els mitjans de comunicació de Hotel XXXX, ja siguin digitals o físics, incloent plataformes proporcionades per terceres parts, i tot el seu cicle de vida, d'inici a fi. La seguretat de tots els actius que prenent part en aquestes tasques queda inclosa.

<u>Annex 6:</u> Política de Seguretat

Política de Seguretat

Versió 1.0
Data: dia XX del mes TAL, any YYYY
Document en discussió

Aquest document pretén deixar constància de la implicació que té la junta directiva de Hotel XXXX en elaborar una Política de Seguretat que estableixi les bases per treballar en la creació i implantació d'un Sistema de Gestió de la Seguretat de la Informació. El que la junta entén com Seguretat de la Informació engloba unes característiques que considerem necessàries i vitals per garantir el correcte desenvolupament de la nostra activitat, així com per respondre correctament davant de situacions d'emergència, estiguin o no previstes. La Seguretat de la Informació fa referència a tota informació que passa per les nostres mans i amb la que tenim vinculació, especialment aquella que conté dades que calen protegir o que són d'accés restringit. La informació pot estar guardada en qualsevol medi, ja sigui en paper i de forma tradicional, com en un format digital i de manera remota. La comunicació pot ser igualment digital o simplement una conversació via telefònica, o inclús presencial. El cicle de vida que considerem per el tractament és complet; és a dir, que vetllarem per el seu bon ús des de la seva creació fins que sigui destruïda o eliminada completament, incloent les etapes intermèdies que puguin sorgir.

Els pilars als que fem referència i als quals ha d'ajudar a mantenir i millorar el SGSI conjuntament amb aquesta política de seguretat, són fonamentalment els següents:

- Disponibilitat: la informació rellevant ha d'estar en tot moment disponible, sigui quin sigui el moment en que és requerida. Mai sabem quant podem necessitar consultar un rebut, o simplement, no desitgem que un client no pugui accedir al nostre portal web degut a incidències varies.

- Confidencialitat: la junta directiva és conscient de que la normativa vigent exigeix uns criteris de anonimat i tractament confidencial de informació de caràcter sensible, essent aquest un tipus de informació molt abundant en el nostre àmbit.

- Integritat: volem garantir que la informació que tenim és correcte i no presenta error o pugin faltar dades.

Objectiu: amb la integració d'aquesta política de seguretat en el futur SGSI la junta directiva vol dotar a Hotel XXXX d'un valor afegit com és la seguretat de la informació. D'acord amb els estàndards en base als quals es treballarà, podrem transmetre uns valors als nostres empleats que es reflectiran en la manera de treballar, i que a la seva vegada repercutirà positivament en l'experiència dels nostres clients.

Igualment és objecte i finalitat aconseguir un correcte Pla de Continuïtat de Negoci, el qual sigui una eina a la que pugem recórrer en els moments d'emergència si mai fos necessari.

Aquests valors han de millorar el posicionament del negoci respecte a la competència, ajudant a situar-se entre els hotels més ben valorats i punters del nostre entorn. Tot plegat ajudarà a continuar creixent com a organització, i a entendre millor les necessitats actuals d'un mercat que creix dia a dia.

Compliment legal: l'elaboració d'aquesta política gira entorn als requisits legals vigents. Els més destacables i que s'exposaran en documents de procediments i manuals, són les lleis de *Serveis de La Societat de la Informació i la Comunicació (LSSI)*, i la *Llei Orgànica de Protecció de Dades de Caràcter Personal (LOPD)*. Aquestes lleis toquen de ple l'activitat que es porta a terme a Hotel XXXX i que involucra a tot el seu personal. A més, es pretén certificar el futur SGSI en base a la norma ISO/IEC 27001, la qual vetlla pel compliment de les legalitats vigents aplicables a cada negoci en particular.

Àmbit: aquest document va dirigit a tot treballador de Hotel XXXX, des de la junta directiva fins als treballadors esporàdics de temporada. El seu coneixement és obligatori, així com el seu compliment. La junta directiva mostra explícitament el seu suport amb els recursos que siguin apropiats per aquesta tasca, així com la seva participació en la elaboració, revisió i aprovació del document. Els treballadors que signin contracte amb Hotel XXXX accepten la conformitat en quant a aquesta política així com el seu coneixement i obligació de donar-hi suport en la mesura del possible.

Vigència: es condeix un període de 3 mesos per a la discussió i revisió de la primera versió de la política de seguretat. Un cop aprovada, serà revisada per la junta directiva i el comitè de seguretat com a mínim anualment.

Control i responsabilitats: els membres responsables de revisar i esmenar en futures reunions la política de seguretat són, d'una banda, el comitè de direcció, i d'altra, el comitè de seguretat. El consens entre tots dos comitès donarà lloc a la aprovació d'aquesta política.

Qualsevol incidència detectada per un treballador ha de ser comunicada tan aviat com sigui necessari a l'encarregat o responsable de torn. Les incidències es comunicaran al tècnic de seguretat en el plaç establer segons la topologia del event. El tècnic decidirà sobre si cal actuar immediatament o es tracta d'un fet aïllat. En qualsevol cas, aquest comunicarà, amb un informe pertinent, la situació al comitè de seguretat, el qual exposarà la situació davant de la junta directiva si fos necessari. Totes les incidències seran exposades en les reunions de seguretat que és celebraran en les dates previstes per la junta directiva.

Incompliments: qualsevol acció que representi un incompliment d'aquesta política de seguretat per part d'un treballador de Hotel XXXX representarà motiu per a obrir un expedient sancionador a aquesta persona. Les sancions variaran segons la gravetat de la seva actuació i dels fets que l'hagin motivat. Aquestes valoracions les farà la junta directiva, i aplicarà les sancions previstes al reglament vigent i aprovat en junta.

Distribució: aquesta política serà distribuïda a tot empleat de Hotel XXXX en format físic i digital, quedant sota la seva responsabilitat no re-distribuir-la ni distorsionar-la. A més es guardaran copies al registre de la junta, amb les actes rellevants, i amb els informes tècnics que calguin.

En tal lloc, a data XX, de TAL, any YYYY

Signat, el comitè de direcció

<u>Annex 7:</u> Procediment d'auditories internes

Procediment d'auditories internes

Versió 1.0
Data: dia XX del mes TAL, any YYYY
Document en discussió

Objectiu: establir el plaç en els que es duran a terme les auditories internes i el format que s'exigirà.

Contingut: la junta directiva, en relació amb la seva voluntat de promoure un correcte desenvolupament de la seguretat de la informació i en concret del SGSI del qual hem assumit part de responsabilitat, manifesta que es convocarà una auditoria interna com a mínim una vegada al any. En el cas que els resultats d'aquesta fossin deficients, es procediria a subsanar les deficiències i a convocar una nova auditoria interna. El contingut de l'auditoria ha de ser, com a mínim, el següent:

- Data
- Nom dels auditors
- Abast
- Controls auditats
- Conformitat del SGSI amb la norma
- No-conformitats detectades
- Recomanacions de millora
- Resum comparatiu enfront de l'última auditoria

<u>Annex 8:</u> Procediments de revisió per Direcció

Procediment de revisió

Versió 1.0
Data: dia XX del mes TAL, any YYYY
Document en discussió

Objectiu: establir els processos de revisió interns duts a terme per Direcció.

Contingut: El procediment establert consistirà en dues reunions anuals, separades cada una per 6 mesos de diferencia. En la primera reunió s'avaluaran els objectius aconseguits i es compararan amb els que eren objectius proposats. S'estudiarà els informes entregats pel comitè de seguretat i es faran els anàlisis sobres les lectures dels controls aplicats

En la primera reunió anual es proposarà demanar una auditoria interna. En aquesta reunió es fixaran els punts a demanar en l'auditoria, i els objectius que es persegueixen en base als documents aportats fins el moment.

En la segona reunió anual s'estudiaran les conclusions i resultats de l'auditoria interna, i es fitaran els objectius a complir un cop arribada la següent reunió semestral. Es revisarà el SGSI i es donaran les ordres oportunes per a la seva millora o modificació Es proposaran el desenvolupament de nous sistemes de monitoratge si és necessari.

Aquest cicle es repetirà anualment, i les actes que en constin seran firmades i guardades pel comitè de direcció.

<u>Annex 9:</u> Gestió de Rols i Responsabilitats

A continuació presentem l'organigrama que explica l'estructuració dels responsables del SGSI en relació a l'organització. Aquest document i les seves explicacions han de ser aprovats per la direcció de la empresa.

Comitè de Direcció	
Comitè de Seguretat de la Informació	Responsable de la seguretat de la informació

Resta de treballadors i unitats possibles

Assessoria jurídica	Assegurances	Auditoria/control intern

Com podem veure, l'estructura es pràcticament vertical i molt clara, donat que l'organització té un tamany petit i no són necessaris altres departaments, al menys per el moment. El Comitè de Direcció està format per dos persones. A més porta a terme les funcions pròpies de direcció, pressa de decisions, administració i contractes, RRHH, i altres que no estiguin especificades.

D'altra banda, el Comitè de Seguretat serà l'encarregat d'implantar correctament el SGSI. Per a dotar de validesa la seva pressa de decisions, aquest comitè estarà format per una persona del Comitè de Direcció. Al mateix temps, la persona encarregada responsable de la seguretat de la informació prendrà part d'aquest comitè. Per tant, quedarà estructurat tal com segueix:

Comitè de Seguretat de la Informació	
Persona responsable de la seguretat de la informació	Director de l'organització

<u>Annex 10:</u> Gestió d'indicadors

Per tal d'avaluar i fer unes correctes lectures dels controls aplicats o que seran aplicats, definirem una serie d'indicadors on hi constaran els valors de lectura i el seu funcionament. En un cas ideal podríem col·locar un indicador per control. No obstant, el volum de dades que obtindríem el faria difícil de manegar. En el cas que ens ocupa, esmentarem un exemple dels indicadors més rellevants, i la restà seran explicitats en el document oportú per a tal efecte.

Nom indicador	Control disponibilitat pàgina web
Descripció	Comprova l'estat de la pàgina web
Control de Seguretat	10.9.1 i 10.9.2
Fórmula de mesurament	Nombre errors / Nombre de comprovacions
Unitats de mesura	Comprovacions / comprovacions
Freqüència	2 vegades al dia durant un trimestre
Valor objectiu	0,03
Valor llindar	> 0'05
Responsable mesura	Responsable seguretat de la informació

Nom indicador	Control línia telefònica
Descripció	Comprova l'estat operatiu de la xarxa de telefon i internet
Control de Seguretat	6.1.2 i 6.2.1
Fórmula de mesurament	Dies amb fallada / Dies operativa
Unitats de mesura	Dies
Freqüència	1 cop per dia
Valor objectiu	0,01
Valor llindar	> 0,09
Responsable mesura	Personal de recepció

Nom indicador	Control salut equip informàtic
Descripció	Comprova l'estat en el que es troba un equip informàtic en relació a virus i altre contingut perjudicial trobat
Control de Seguretat	12.5.2 i 12.6.1, 13.1.1 i 13.1.2
Fórmula de mesurament	Nombre dies infectat / Nombre de comprovacions
Unitats de mesura	Comprovacions / comprovacions
Freqüència	1 vegada a la setmana, recompte trimestral
Valor objectiu	0,08
Valor llindar	> 0'16
Responsable mesura	Responsable seguretat de la informació

Nom indicador	Control satisfacció clients
Descripció	Revisa els comentaris aportats pels clients en les webs especialitzades
Control de Seguretat	14.1.5
Fórmula de mesurament	% de comentaris
Unitats de mesura	Feedback negatiu / feedback total
Freqüència	1 vegada al mes
Valor objectiu	0,02
Valor llindar	> 0'05
Responsable mesura	Direcció i responsable de publicitat i imatge

Nom indicador	Control compliment normativa
Descripció	Comprova si existeixen normatives recents no acomplides
Control de Seguretat	15.2.1
Fórmula de mesurament	Nombre d'infraccions total
Unitats de mesura	Nombre infraccions
Freqüència	1 vegada al semestre
Valor objectiu	< 3
Valor llindar	> 5
Responsable mesura	Responsable àrea jurídica

Nom indicador	Control no conformitats auditories
Descripció	Comprova les no conformitats greus trobades en les auditories internes
Control de Seguretat	15.3.1
Fórmula de mesurament	Nombre NC greus total
Unitats de mesura	Comprovacions
Freqüència	1 cop a l'any ha d'existir una audit interna
Valor objectiu	Proper a 0
Valor llindar	> 2
Responsable mesura	Responsable seguretat de la informació

Annex 11: Proposta de Projectes

En aquesta document centrarem la nostra atenció en la proposta de projectes que ajudin a millorar l'estat de la seguretat a la nostra organització. Partirem de la base obtinguda en la fase de Anàlisis de Riscos, de la qual es deduirà la prioritat dels projectes segons l'àmbit que aquests tractin, i en relació amb el nivell de risc actual existent. Tots els projectes proposats han de poder ser quantificables en termes econòmics, tant el projecte en sí mateix com els resultats que es reflectiran en la reducció del risc i del valor d'aquest. A més també hauran de ser mesurables en temps, i obtenir unes dates realistes i assumibles per la organització. Tant el cost com la durada d'un projecte ha de ser proporcional al risc que cal mitigar, i en conseqüència, alineat amb els objectius de negoci del client.

El desenvolupament i propostes quedaran reflectides en documents que presentarem a continuació, i sempre que sigui oportú s'acompanyaran de dades i comparatives per tal d'entendre millor la dimensió de cada proposta. No obstant, com que algunes àrees o matèries poden trobar-se en un estat primerenc, alguns projectes estaran encarats a fomentar una primera implantació, fent èmfasis en aspectes més generals i deixant de banda aspectes més concrets i que formaran part del procés i cicle de millora continua. Per tant, és possible que per tal de mesurar aquestes millores al llarg del temps, o simplement per quantificar l'estat d'implantació del projecte, es suggeriran controls de mesura i verificació.

Propostes:

Títol: Política de Seguretat de la Informació

Àmbit: Política de Seguretat, Control de accessos

Objectiu: documentar una Política de Seguretat de la Informació, revisar-la i aprovar-la en junta directiva, per tal de disposar de les bases i directius que marquin el camí en el qual la empresa vol treballar per assolir els objectius de un correcte SGSI.

Descripció: aquest document serà la constatació de les intencions per part de la direcció de la organització de gestionar la seguretat de la informació, que s'entén per Seguretat de la Informació i quins abast té aquesta. Això ajudarà als treballadors a comprendre les seves responsabilitats en relació a la gestió de la informació i tots els processos relacionats, i al mateix temps s'adequarà a les normatives legals vigents que s'exigeixen a cada empresa en particular. Serà important per als treballadors entendre quines responsabilitats existeixen sobre alguns actius importants per a Hotel XXXX, tant de cara a la pròpia empresa com als clients, i les possibles sancions en les cal evitar incórrer degut a un ús inadequat.

Responsable: comitè de la Seguretat de la Informació

Durada prevista: mig termini. Cal disposar d'una primera versió aprovada d'aquests documents amb urgència. Es considerarà un plaça màxim de 6 mesos per a la seva redacció, revisió i aprovació. Es preveu un control al cap de 3 mesos, per verificar que ha estat redactat i es pot procedir a la seva revisió.

1	2	3	C	4	5	6

Cost estimat: el cost està inclòs en el salari que rebrà el personal que pertany al comitè de la Seguretat de la Informació, ja que aquesta feina forma part de les seves tasques.

Títol: Pentesting pàgina web

Àmbit: Gestió de Comunicacions i Operacions

Objectiu: provar l'actual nivell de seguretat de la pàgina web, el seu disseny, i descobrir millores generals.

Descripció: en el Anàlisis de Riscos hem comprovat que la pàgina web està considerat un dels actius més importants per a Hotel XXXX, tant pel seu contingut com per les vinculacions a altres aspectes en els quals està alineat el creixement de la empresa. No obstant, la freqüència amb la que es produeixen erros o atacs és alta. Per tant, elaborarem un pla per detallar aquests punts, reflectir-los en un informe, i aporta les solucions necessàries. El projecte inclou la revisió del codi font de la pròpia pàgina web, la realització de proves de penetració i modificació del contingut, i la revisió del codi en el casos oportuns. Tot això es durà a terme sense notificar als responsables actuals del servei de hosting, per poder provar en un entorn més "real" aquestes situacions. Es duran a terme dos controls: un en acabar el primer pentesting, on es reculli en un informe les vulnerabilitats detectades, i un altre després de corregir aquestes vulnerabilitats. Es compararan els dos informes per tal de veure el grau de millora obtingut.

Responsable: responsable de la Seguretat de la Informació

Durada prevista: curt plaç. Es preveu que aquestes tasques triguin un màxim de 2 mesos.

1	C	2	C

Cost estimat: inclòs en el sou del responsable com a tasca del seu menester.

Títol: Creació i adequació sala “segura”

Àmbit: Seguretat Física i de l'Entorn, Compliment Legal

Objectiu: disposar d'una sala habilitada per guarda informació sensible sota les condicions establertes per la ISO/IEC 27002

Descripció: l'existència d'actius de cert valor rellevant ubicats en àrees “no segures” o que no disposen de les mesures de prevenció necessàries, eleven el risc de materialització sobre aquests actius de forma considerable. La materialització va lligada a un cost econòmic, i per tant, una opció és treballar per disminuir aquesta probabilitat. L'alternativa més sensata i donada les característiques de Hotel XXXX, és la de construir una zona amb les mesures de seguretat adequades. En particular i per reduir costos, s'aprofitarà una petita habitació ubicada darrera de la zona de “recepció”, que fins ara es feia servir per guardar caixes i paquets sense valor, essent un espai desaprofitat en forma de traster.

Les obres es realitzaran en una única fase. Els protocols a seguir seran aquells orientats a dotar de seguretat l'habitació, ja que en ella s'hi guardaran actius que contenen dades personals. Més concretament l'habitació ha de donar cabuda a elements com:

- caixa forta
- llibre de registre
- llibreta calendari reserves
- documentació relacionada amb plans estratègics
- certificats i altres dades que han de ser físicament a l'edifici en cas de ser requerits
- discos durs on s'emmagatzemen les filmacions de les càmeres de seguretat
- altres

Aquesta habitació ha de contenir com a mínim les següents mesures de seguretat:

- porta d'accés reforçada (no cal que sigui blindada)
- pany amb clau de alta seguretat (clau perforada)
- interior recobert amb pintura i materials ignífugs
- armaris amb pany i clau d'accés
- detector de fums i de foc
- càmera de vigilància gravant l'accés (aprofitarem la que grava a recepció)

Responsable: Junta directiva

Durada prevista: curt termini. Es calcula que les obres de remodelació i condicionament no superaran la durada de 1 mes.

1

Cost estimat: el pressupost previst entre materials i ma d'obra es xifra en 2000€

Títol: Programa de Protecció Activa i Passiva contra intrusions no desitjades

Àmbit: Seguretat Física i de l'Entorn, Control d'Accessos, Compliment Legal

Objectiu: provar l'estat de la seguretat i les seves vulnerabilitats contra accessos no autoritzats al recinte i als equips instal·lats. Millorar aquesta seguretat.

Descripció: hem vist al AARR que existeixen diversos actius, com per exemple els ordinadors de recepció, els telèfons, o carpetes amb informació confidencial, que estan exposats amenaces com robatori o sabotatge. Tot i que el seu impacte per separat es contempla dintre del risc acceptable i assumible, volem evitar que aquests incidents es manifestin de forma repetida i simultània. A més, aquesta seguretat engloba certs aspectes legals que cal considerar.

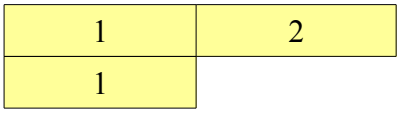
Per dur a terme aquest projecte, es proposa la revisió i la instal·lació si s'escau, de noves càmeres de seguretat dintre del recinte. Adequarem legalment la disposició dels cartells indicadors de "zona videovigilada" amb els drets dels que disposen els usuaris, i els col·locarem en llocs apropiats segons la normativa.

A més es canviaran les portes i els panys que comuniquen diferents estàncies comunes de l'edifici, com menjador-cuina, menjador-recepció, sala de estar-jardí. En cas necessari es col·locaran panys nous amb claus de seguretat adient a l'estància a la que donen accés.

Un altre tipus d'intrusió que volem evitar és l'accés no autoritzat als equips informàtics, ja sigui des de el mateix equip o des de l'exterior. Per tal de millorar aquest aspecte, durem a terme un pla de gestió d'usuaris i contrasenyes nou. Tot el personal disposarà d'un usuari i clau d'accés personal, i l'administració d'aquestes dades i de les seves sessions quedarà registrada en un llibre de o fitxer de "logs". Igualment s'implantaran sistemes de salvaguarda com tallafocs i antivirus a tots els equips, amb una configuració segura duta a terme per el personal informàtic apropiat.

Responsable: junta directiva / responsable informàtic

Durada prevista: les obres de remodelació es calculen en tenir una durada curta de 2 mesos. La configuració i elaboració del pla de gestió d'usuaris i contrasenyes es calcula no superior a 1 mes.



Cost estimat: el valor econòmic acumulat serà sempre inferior a 2500€, ja que s'intentarà utilitzar programari lliure i els serveis del Responsable de la Seguretat de la Informació, sent les despeses més importants les obres de reformes i el material emprat.

Títol: Adquisició d'Equip de Suport

Àmbit: Adquisició, Desenvolupament i Manteniment de Sistemes, Gestió de Continuïtat de Negoci

Objectiu: adquirir l'equip necessari per fer front a events imprevistos i de origen natural que pugin malmetre el correcte desenvolupament de l'activitat diària.

Descripció: un dels aspectes que ha quedat al descobert en el Anàlisis de Riscos és l'exposició dels actius a incidents d'origen natural, com per exemple un tall en el subministrament elèctric. L'objectiu d'aquest projecte és de dotar a Hotel XXXX dels mitjans oportuns per fer front de manera proporcionada a aquests elements.

S'ha decidit que per protegir els equips informàtics "fixes" s'instal·larà un dispositiu SAI que protegeixi davant de les pujades i caigudes de tensió. Igualment és objectiu contractar una nova tarifa de dades per al telèfon mòbil de direcció, de manera que en cas d'interrupció del servei telefònic, puguem fer servir el terminal com a "router" provisional. En l'àmbit de la pàgina web, s'ha decidit buscar i contractar un servei de hosting doble, o que ofereixi aquesta opció, garantint així la total disponibilitat de la pàgina web de Hotel XXXX.

Responsable: junta directiva

Durada prevista: curt termini, no superior a 1 mes.

1

Cost estimat: destinarem un pressupost de 1500€ que agrupa els equips SAI, el servei de hosting, i la tarifa de dades anualment.

Títol: Instal·lació Equips de Còpies de Seguretat

Àmbit: Gestió de Comunicacions i Operacions

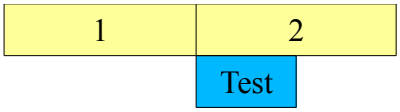
Objectiu: disposar de còpies de seguretat dels arxius relacionats amb la gestió de la informació.

Descripció: entre les diferents amenaces que apareixen al AARR, trobarem l'esborrat accidental o pèrdua de algun actiu que contingui informació. Al mateix temps, podem entendre que un esborrat podria ser ocasionat intencionadament com un acte de sabotatge. Per aquest motiu es durà a terme aquest projecte per la instal·lació d'equips responsables de automatitzar i gestionar les còpies de seguretat que es creguin importants.

Per fer-ho es comprarà un equip que faci la feina de servidor exclusivament per gestionar aquestes còpies. Es preveu l'ús de software lliure per abaratir costos. L'equip estarà connectat en xarxa als equips principals i es durà a terme una política de còpies de seguretat establerta per el responsable de la seguretat de la informació. Aquest servidor disposarà de còpies del codi font de la pàgina web així com d'altres programes que es considerin necessaris.

Responsable: responsable de la Seguretat de la Informació

Durada prevista: curt termini. Adquisició, instal·lació i configuració prevista en un temps inferior a 2 mesos, incloent un període de proves de 2 setmanes.



Cost estimat: 500€ per el servidor.

Títol: Formació del Personal

Àmbit: Seguretat en Recursos Humans, Gestió d'Incidents en la Seguretat de la Informació, Compliment Legal

Objectiu: formar al personal per que puguin dur a terme les seves tasques amb un coneixement profund sobre la matèria que estan treballant, i d'aquesta manera, millorar el servei ofert.

Descripció: una de les amenaces amb la que ens podem trobar és la catalogada com "mal servei ofert". Aquesta amenaça fa referència al servei que presta un treballador davant d'un client o d'una tasca, i com la qualitat d'aquest servei influeix en els resultats finals. Per exemple, si un client no està content amb el tracte rebut, això pot repercutir sobre la "confiança", catalogat com un actiu de important valor. Per tant, la manera de posar solució per aquest problema consisteix en la formació del personal sobre les seves tasques. Igualment les lleis actuals exigeixen disposar de certificats variats, els quals justifiquin la capacitació dels treballadors per dur a terme una tasca. Així dons, la formació també servirà per cobrir els buits que ara existeixen a la organització en quant a cursos oficials.

Per fer-ho es proposa una revisió sobre la legalitat vigent i la normativa actual, i amb el suport de la junta directiva, finançar aquests cursos als treballadors. Un cop acabat el plaç fixat, s'utilitzarà un indicador que mesurarà el nombre de cursos realitzats i el nombre que en resta per fer, aconseguint així una primera aproximació al nostre objectiu.

Responsable: junta directiva / recursos humans (junta directiva) / departament jurídic i legal

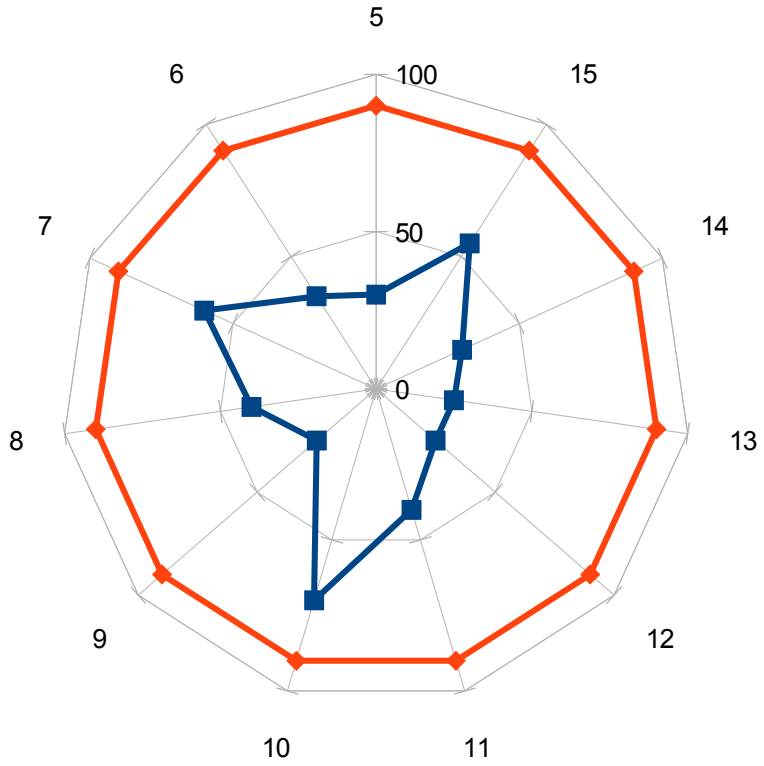
Durada prevista: llarg termini. Sabem que molts cursos són impartits una vegada a l'any, i per tant, per aquesta primera revisió estimarem el temps en 18 mesos.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Cost estimat: es preveu que els cursos pugin costar un promig de 600€ anuals per treballador.

Diagrama de radar:

En aquest diagrama en forma de radar es mostra una comparativa entre l'assoliment del compliment dels diferents dominis de la ISO/IEC 27002, i l'estat actual. De color taronja veiem el nivell a assolir desitjat, mentre que en color blau el nivell actual previ a la implantació i a l'execució dels projectes proposats. Cada aresta està numerada amb el domini específic de la ISO/IEC 27002. Tal i com s'observa, en molts dominis encara queda molt recorregut per fer. Això pot ser degut a que molts punts de control es troben en fase "planificat" o "iniciat", i per tant, encara no han adquirit un grau de maduresa òptim. Un cop s'hagin dut a terme el projectes, podrem comparar l'estat anterior amb el que en resultarà, el qual ha d'aproximar-se al dibuix taronja tant com sigui possible.



Pressupost total:

El pressupost total acumulat es xifra en 7200€ + salari del responsable de Seguretat de la Informació. Si tenim en compte que aquest especialista forma part del grup de treballadors fixes, però que no treballa en exclusiva per a Hotel XXXX, al llarg d'un any s'estima que aportarà factures per valor de 6000€, que seran equivalents a les hores de treball invertides. Per tant, al cap d'un any haurem destinat 13200€ a la posada en marxa de tots els projectes plantejats.

<u>Annex 12:</u> Auditoria de Compliment de la ISO/IEC 27002:2005

En aquesta document i un cop coneixem els actius de la organització i les amenaces a les que estan exposats, és el moment de reflectir el grau de compliment del objectius de control que estableix el estandar ISO/IEC 27002:2005. Per fer aquest informe es consideraran assolits els projectes de millora plantejats en la fase anterior. Els resultats es mostraran en taules on es relacionin els objectius i els punts de control amb el seu grau de maduresa. La metodologia que seguirem consistirà en repassar els documents aportats fins el moment i dels quals es té coneixement, i veure en quin estat es troben respecte als processos que es duen a terme. Altres punts a tenir en compte són:

- Formalització de les pràctiques mitjançant documents escrit o aprovats
- Polítiques de personal
- Sol·licituds tècniques (software, hardware, comunicacions)
- Seguretat física

Per fer l'estimació ens basarem en el Model de Maduresa de la Capacitat (CMM), els valors del qual queden reflectits en la següent taula:

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	L0	Inexistent	Carència completa de qualsevol procés que reconeguem
10%	L1	Inicial / Ad-hoc	L'èxit dels processos es basa la major part en esforç del personal. Els procediments són inexistents o localitzats en àrees molts concretes. No existeixen plantilles
50%	L2	Reproduïble però intuïtiu	Els processos similars es porten a terme de manera similar diferents persones amb la mateixa tasca. Es normalitzen les bones pràctiques en base a l'experiència i el mètode.
90%	L3	Procés definit	La organització sencera participa en el procés. Els processos estan implantats i documentats.
95%	L4	Gestionat i mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos. Es disposa de tecnologia per

			automatitzar el flux de treball.
100%	L5	Optimitzat	Els processos estan sota constant millora. En base a criteris quantitatius es determinen les desviacions.

Per al càlcul de cada objectiu es tindrà en compte els valors obtinguts en cada sub-apartat, i es realitzarà una mitja aritmètica que pot estar arrodonida per facilitat la comprensió. Per ajudar-nos a situar aquests valors, hem cregut oportú incorporar les dades que varen resultar de fer l'anàlisi d'aplicabilitat, i en les que es reflectia l'estat d'aquell control en base a la seva implantació abans de dur a terme el projectes de millora proposats. Tot i que es tracta d'una valoració molt semblant, aquesta no era numèrica, i per tant, ara l'agafarem com a orientativa per acabar de xifrar amb més detall els valors respecte al CMM. Les classificacions possibles venien donades per:

- Planificat: encara no ha estat implementat
- Iniciat: s'està treballant per implementar-lo
- Implantat sense documentar
- Implantat sense auditar: està documentat, però ha de ser auditat
- Auditat: completament implantat i auditat

D'aquesta manera, veurem l'evolució del sistema des de l'estat inicial en que el vam trobar, fins a l'actual. A més ens permetrà comparar aquesta evolució tant punt per punt, com per objectius de manera agrupada en posteriors gràfics que recolliran aquesta informació. Els punts de control que no siguin d'aplicació no es tindran en compte per a fer el càlcul del valor total.

Ref	**Nom**	**Aplicabilitat**	**Comentaris**	**Maduresa (inicial)**	**Maduresa CMM %**
5	Política Seguretat				90%
5.1	Política de Seguretat de la Informació				90%
5.1.1	Doc Política de Seguretat de la Informació	APLICA		Iniciat	90%
5.1.2	Revisió i avaluació	APLICA		Planificat	90%
6	Aspectes organitzatius				65%
6.1	Organització interna				65%
6.1.1	Comitè de gestió de	APLICA		Iniciat	90%

	la seguretat de la informació				
6.1.2	Coord de la seguretat de la informació	APLICA		Iniciat	50%
6.1.3	Assig responsabilitats seguretat informació	APLICA		Iniciat	90%
6.1.4	Proc autorització recursos tractament informació	APLICA		Planificat	50%
6.1.5	Acords confidencialitat	APLICA		Implantat sense documentar	40%
6.1.6	Contacte autoritats	APLICA		Planificat	60%
6.1.7	Contacte grups especialitzats	NO APLICA	No existeixen grups relacionats amb sector hosteleria		
6.1.8	Revisió independent de la seg informació	APLICA	Inclourà la certificació del SGSI	Planificat	70%
6.2	Seguretat en els accessos de terceres parts				60%
6.2.1	Identificació de riscos	APLICA		Iniciat	50%
6.2.2	Requisits seg al tractar amb clients	APLICA		Planificat	70%
6.2.3	Requisits seg contractes outsourcing	APLICA		Implementat sense documentar	60%
7	Classificació i control d'actius				55%
7.1	Responsabilitat sobre actius				90%
7.1.1	Inventari actius	APLICA	Existeix una relació d'actius, però no està correctament documentada	Implementat sense documentar	95%
7.1.2	Propietat dels actius	APLICA		Implementat sense	90%

				documentar	
7.1.3	Ús adequat dels actius	APLICA		Iniciat	90%
7.2	Classificació informació				15%
7.2.1	Guies de classificació	APLICA		Planificat	20%
7.2.2	Marcatge i tractament informació	APLICA		Planificat	10%
8	Seguretat en recursos humans				70%
8.1	Seguretat abans de la feina				85%
8.1.1	Inclusió de la seg en les responsabilitats laborals	APLICA		Planificat	90%
8.1.2	Selecció i política de personal	APLICA		Planificat	90%
8.1.3	Acords confidencialitat	APLICA		Implantat sense documentar	70%
8.2	Durant el treball				55%
8.2.1	Responsabilitat de la gerència	APLICA		Iniciat	40%
8.2.2	Conscienciació, formació i capacitació en seguretat	APLICA	Amb els contractes de confidencialitat són suficients per al tipus de feina	Iniciat	80%
8.2.3	Proces disciplinari	APLICA		Implantat sense documentar	50%
8.3	Finalització treball				
8.3.1	Responsabilitats finalització	NO APLICA	Cobert pels controls 6.1.5 i 8.1.3		
8.2.3	Retorn d'actius	NO APLICA	Els empleats no posseïxen actius fora del recinte		
8.3.3	Revocació drets accés	NO APLICA	Queda fora de la magnitud de l'organització		

9	Seguretat física de l'entorn				75%
9.1	Àrees segures				90%
9.1.1	Perímetre de seguretat física	APLICA	Aquestes zones no havien estat determinades	Planificat	90%
9.1.2	Controls físics d'entrada	NO APLICA	No existeixen zones tant concretes de inf sensible		
9.1.3	Seg oficines, despatxos i recursos	APLICA		Planificat	90%
9.1.4	Protecció contra amenaces externes	APLICA		Implantat sense documentar	90%
9.1.5	Treball en àrees segures	NO APLICA	No existeixen		
9.1.6	Accés àrees carrega	NO APLICA	No existeixen		
9.2	Seguretat dels equips				55%
9.2.1	Instal·lació i protecció equips	APLICA		Iniciat	90%
9.2.2	Subministre elèctric	APLICA	Està previst col·locar SAI's	Planificat	95%
9.2.3	Seguretat cablejat	NO APLICA	Fora de l'abast de la empressa		
9.2.4	Manteniment equips	APLICA		Iniciat	30%
9.2.5	Seg equips fora locals	NO APLICA	No existeixen		
9.2.6	Seg eliminació equips	APLICA		Planificat	10%
9.2.7	Revocació propietat	NO APLICA	No es dona la situació		
10	Gestió comunicacions i operacions				60%
10.1	Procediments i responsabilitats de operacions				35%
10.1.1	Documentació i procediments	APLICA		Planificat	20%

	operatius				
10.1.2	Gestió i canvis	APLICA	Aplica però no existeixen màquines prou rellevants i diferenciades	Planificat	50%
10.1.3	Segregació de tasques	NO APLICA	Mida de l'organització massa petita		
10.1.4	Separació de recursos per al desenvolupament i producció	NO APLICA	Queda fora de l'àmbit de l'organització		
10.2	Gestió de serveis externs				50%
10.2.1	Servei d'entrega	APLICA		Implementat sense documentar	50%
10.2.2	Monitoratge i revisió serveis externs	NO APLICA	Excedeix l'abast de la política de seguretat		
10.2.3	Gestionar canvis pels serveis externs	NO APLICA	Excedeix l'abast de la política de seguretat		
10.3	Planificació i acceptació del sistema				
10.3.1	Planificació de capacitat	NO APLICA	No hi ha risc de sobrecàrrega al sistema		
10.3.2	Acceptació del sistema	NO APLICA	Fora de l'abast		
10.4	Protecció contra software maliciós				70%
10.4.1	Mesures i controls	APLICA	Aplicat antivirus, firewalls i actualitzacions	Iniciat	70%
10.4.2	Mesures codi mòbil	NO APLICA	No existeix		
10.5	Gestió de recuperació				95%
10.5.1	Recuperació informació	APLICA		Iniciat	95%
10.6	Gestió seg en xarxes				90%
10.6.1	Controls de xarxa	APLICA		Implantat sense	90%

				documentar	
10.6.2	Seguretat en serveis de xarxes	NO APLICA	Queda fora de l'ambit de treball de l'organització		
10.7	Utilització dels mitjans de informació				40%
10.7.1	Gestió de mitjans extractables	NO APLICA	No existeixen aquests medis		
10.7.2	Eliminació dels mitjans	NO APLICA	No existeixen		
10.7.3	Procediments de manipulació de info	APLICA		Planificat	40%
10.7.4	Seg de la documentació de sistemes	NO APLICA	No existeix aquesta informació		
10.8	Intercanvi de informació				75%
10.8.1	Polítiques i procediments per l'intercanvi de info i software	APLICA	Centrar en correus electrònics i comunicacions bancàries	Implementat sense documentar	60%
10.8.2	Acords d'intercanvi	APLICA		Implementar sense documentar	80%
10.8.3	Mitjans físics en trànsit	NO APLICA	No existeixen		
10.8.4	Seguretat en missatgeria electrònica	APLICA		Implementat sense documentar	80%
10.8.5	Sis informació de negoci	NO APLICA	No existeixen		
10.9	Serveis de correu electrònic				75%
10.9.1	Comerç electrònic	APLICA		Implementat sense auditar	90%
10.9.2	Transaccions en línia	APLICA		Implementat sense auditar	90%
10.9.3	Info pública disponible	APLICA		Implementat sense auditar	50%
10.10	Monitoratge				20%
10.10.1	Registre de la auditoria	NO APLICA	No adient a la mida de l'organització		

10.10.2	Monitoratge de l'ús del sistema	NO APLICA	No es té necessitat en els processos existents		
10.10.3	Protecció de les traces	NO APLICA	No existeixen instal·lacions		
10.10.4	Traces d'administració i operació	NO APLICA	Excedeix la mida de l'organització		
10.10.5	Registre de fallades	APLICA		Planificat	20%
10.10.6	Sincronització de rellotges	NO APLICA	No necessari per a les tasques desenvolupades		
11	Control d'accés				45%
11.1	Requisits de negoci per al control d'accés				90%
11.1.1	Política de control d'accés	APLICA		Planificat	90%
11.2	Gestió de l'accés dels usuaris				55%
11.2.1	Registre d'usuaris	APLICA		Implementat sense documentar	40%
11.2.2	Gestió de privilegis	APLICA		Implementat sense documentar	70%
11.2.3	Gestió de contrasenyes d'usuari	NO APLICA	Aquest procés queda reduït a altres apartats donada el petit tamany a gestionar		
11.2.4	Revisió dels drets d'accés d'usuari	NO APLICA	No aplica degut a la mida de l'organització		
11.3	Responsabilitats dels usuaris				70%
11.3.1	Ús de credencials	APLICA		Implementat sense documentar	70%
11.3.2	Equips d'usuaris desatesos	NO APLICA	No existeixen ni poden existir		
11.3.3	Política de taules i pantalles netes	NO APLICA	No existeix aquesta possibilitat		
11.4	Control d'accés a la				20%

	xarxa				
11.4.1	Política d'ús dels serveis de xarxa	APLICA		Planificat	20%
11.4.2	Autenticació d'usuaris conexions remotes	NO APLICA	No existeix aquesta opció		
11.4.3	Autenticació de nodes a la xarxa	NO APLICA	No existeix aquesta opció		
11.4.4	Config port en remot	NO APLICA	No existeix aquesta opció		
11.4.5	Segregació de xarxes	NO APLICA	No existeix xarxa a segregar		
11.4.6	Control de connexió a la xarxa	NO APLICA	Queda cobert amb el punt 11.1.1		
11.4.7	Control d'encaminament xarxa	NO APLICA	Mida massa petita per aplicar aquest control		
11.5	Control d'accés al sistema operatiu				15%
11.5.1	Procediments connexió	APLICA		Planificat	10%
11.5.2	Identificació i autenticació usuaris	NO APLICA	Utilització de comptes compartides		
11.5.3	Sistema de gestió de contrasenyes	NO APLICA	Queda controlat amb altres punts degut a la mida petita		
11.5.4	Ús serveis sistema	NO APLICA	No s'han detectat serveis a restringir el seu ús		
11.5.5	Desconnexió automàtica sessió	APLICA	Mesures per defecte aplicades	Iniciat	20%
11.5.6	Limitació temps connexió	NO APLICA	Contradiu altres necessitats de treball de l'organització		
11.6	Control d'accés a la info i a les aplicacions				30%
11.6.1	Restricció d'accés info	APLICA		Iniciat	30%
11.6.2	Aïllament sis sensibles	NO APLICA	No existeixen aquests sist		
11.7	Informàtica mòbil i teletreball				

11.7.1	Informàtica mòbil	NO APLICA	No existeix		
11.7.2	Teletreball	NO APLICA	No està disponible l'opció		
12	Adquisició, desenvolupament i manteniment sistemes				50%
12.1	Requisits seguretat en sistemes de informació				
12.1.1	Anàlisi especificacions requisits	NO APLICA	Està fora de la planificació de l'organització		
12.2	Control processos en aplicacions				
12.2.1	Validació dades entrada	NO APLICA	No hi han dades d'entrada		
12.2.2	Control de processos interns	NO APLICA	No hi han processos interns		
12.2.3	Integritat de missatges	NO APLICA	No hi han aplicacions que ho requereixin		
12.2.4	Validació dades sortida	NO APLICA	No hi han processos		
12.3	Controls criptogràfics				20%
12.3.1	Política ús controls crip	APLICA		Planificat	20%
12.3.2	Xifratge	NO APLICA	No aplicable als petits processos que existeixen		
12.4	Seguretat fitxers sistema				
12.4.1	Control programari en producció	NO APLICA	No existeix		
12.4.2	Protecció dades de prova	NO APLICA	No es disposen d'aquest tipus de dades		
12.4.3	Control accés codi font	NO APLICA	No es produeix aquest codi		
12.5	Seguretat en el desenvolupament i en el suport				45%

12.5.1	Procediments de control de canvis	APLICA		Iniciat	50%
12.5.2	Revisió tècnica canvis sistema operatiu	APLICA	Els canvis es proven però no deixen constància	Iniciat	40%
12.5.3	Restricció canvis en paquets de programari	NO APLICA	No s'utilitza programari		
12.5.4	Fuites d'informació a través del codi	NO APLICA	No es desenvolupa programari amb codi font		
12.5.5	Externalització del desenvolupament de programari	NO APLICA	No es demana aquesta funció		
12.6	Gestió vulnerabilitats tècniques				90%
12.6.1	Control vuln tècniques	APLICA	Pentesting pendent	Planificat	90%
13	Gestió incidències de seguretat de la informació				20%
13.1	Notificació incidències i debilitats				25%
13.1.1	Notificació events seg	APLICA		Planificat	30%
13.1.2	Notificació debilitats	APLICA		Planificat	20%
13.2	Gestió incidències i millora				15%
13.2.1	Identificació responsabilitat i procediments	APLICA		Iniciat	40%
13.2.2	Avaluació incidències	APLICA		Iniciat	10%
13.2.3	recol·lecció evidències	APLICA		Planificat	0%
14	Gestió de continuïtat de negoci				80%

14.1	Aspectes de la gest de continuïtat de negoci				80%
14.1.1	Incloure la seg info en el procés de cont negoci	APLICA	Iniciat amb aquesta tasca	Iniciat	95%
14.1.2	Continuïtat negoci i anàlisi impacte	APLICA		Iniciat	90%
14.1.3	Documentació i implantació del pla de continuïtat de negoci	APLICA		Planificat	90%
14.1.4	Marc de planificació	APLICA		Iniciat	70%
14.1.5	Proves, manteniment i reavaluació dels plans	APLICA		Planificat	60%
15	Conformitat				60%
15.1	Conformitat amb requisits legals				75%
15.1.1	Identificació legislació	APLICA		Implementat sense documentar	80%
15.1.2	Dret de la propietat intel·lectual	APLICA		Implementat per ser auditat	70%
15.1.3	Control seg registres de l'organització	APLICA		Iniciat	90%
15.1.4	Protecció dades personals	APLICA		Implementat per ser auditat	90%
15.1.5	Evitar mal ús recursos de tractament de la info	APLICA		Implementat sense documentar	50%
15.1.6	Reglamentació controls xifratge	NO APLICA	Queda fora de l'abast dels objectius plantejats		
15.2	Compliment marc normatiu				40%
15.2.1	Compliment polítiques i normes	APLICA		Planificat	30%

15.2.2	Comprovació conformitat tècnica	APLICA	Es farà mitjançant auditories internes	Planificat	50%
15.3	Auditoria de sistemes				70%
15.3.1	Controls d'auditoria	APLICA		Planificat	70%
15.3.2	Protecció eines auditoria	NO APLICA	Aquesta responsabilitat queda en mans de l'auditor		

Fitxes de No Conformitats:

Atenent als resultats anteriors i d'acord amb el Model de Maduresa de la Capacitat (CMM), podem desenvolupar les següents fitxes amb les No Conformitats trobades. Les agruparem segons dominis, especificant per a cadascun quin nivell s'ha adquirit en els seus controls. Procedirem segons la classificació:

No Conformitats Majors: (CMM 0 i 1)
No Conformitats Menors: (CMM 2 i 3)
Observacions: (CMM 4 i 5)

Domini	5, Política Seguretat
Punts de control	5.1 (CMM 3)
Valor CMM acumulat	CMM 3
Comentaris	En aquest domini ens trobem amb una no conformitat menor, que bé pot no ser-ho, ja que s'han assolit tots els punts de control amb gran èxit

Domini	6, Aspectes Organitzatius
Punts de control	6.1 (CMM 2), 6.2 (CMM 2)
Valor CMM acumulat	CMM 2
Comentaris	Cal treballar els punts de control iniciats, però sense implementar de manera exhaustiva

Domini	7, Classificació i Control d'Actius
Punts de control	7.1 (CMM 3), 7.2 (CMM 1),
Valor CMM acumulat	CMM 2
Comentaris	Hem caigut en No conformitat degut a que els punts de control de classificació de la informació estan poc madurats, i no s'han ni tans sols iniciat.

Domini	8, Seguretat en Recursos Humans
Punts de control	8.1 (CMM 2), 8.2 (CMM 2)
Valor CMM acumulat	CMM 2
Comentaris	Tornen a faltar assignar responsabilitats en el treball i documentar processos que es duen a terme, com el disciplinari, però no deixen constància en cap registre.

Domini	9, Seguretat Física de l'Entorn
Punts de control	9.1 (CMM 3), 9.2 (CMM 2)
Valor CMM acumulat	CMM 2
Comentaris	En aquests cas tenim una altra No conformitat Menor per la falta de tractament en la seguretat durant el procés d'eliminació d'equips. Cal planificar com fer-ho i documentar-ho. El manteniment dels equips també necessita més atenció per funcionar i millorar sobre els seus resultats.

Domini	10, Gestió Comunicacions i Operacions
Punts de control	10.1 (CMM 2), 10.2 (CMM 2), 10.4 (CMM 2), 10.5 (CMM 4), 10.6 (CMM 3), 10.7 (CMM 2), 10.8 (CMM 2), 10.9 (CMM 2), 10.10 (CMM 1),
Valor CMM acumulat	CMM 2
Comentaris	No Conformitat Menor. Patim massa desigualtat entre punts de control del mateix domini. S'han de revisar especialment el registre de fallades del sistema, no implementat encara. Els procediments de manipulació de la informació tampoc han estat definits.

Domini	11, Control d'Accès
Punts de control	11.1 (CMM 3), 11.2 (CMM 2), 11.3 (CMM 2),11.4 (CMM 1), 11.5 (CMM 1), 11.6 (CMM 1)
Valor CMM acumulat	CMM 1
Comentaris	No Conformitat Major. Obtenim una no conformitat greu derivada del gairebé nul compliment de la majoria de subdominis. Cal revisar a fons aquest domini.

Domini	12, Adquisició, Desenvolupament i Manteniment Sistemes
Punts de control	12.3 (CMM 1), 12.5 (CMM 1), 12.6 (CMM 3)
Valor CMM acumulat	CMM 2
Comentaris	No Conformitat Menor. Tot i aquesta consideració, estem molt a prop de que sigui considerada com a Major. Tots els controls que apliquen excepte el 12.6.1 estan simplement iniciats. Cal tirar endavant tasques en aquest domini.

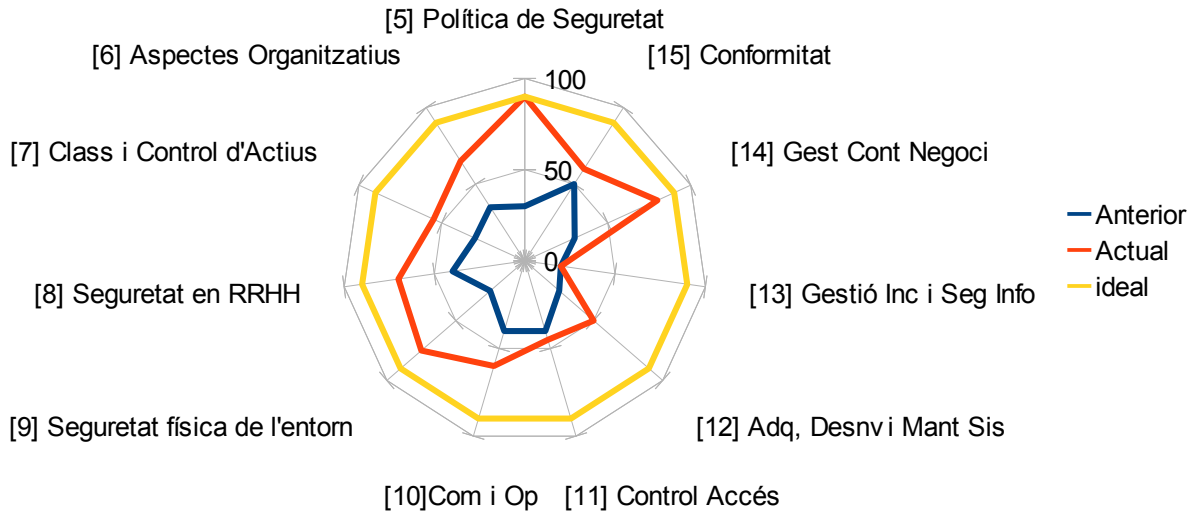
Domini	13, Gestió Incidències Seguretat de la Informació
Punts de control	13.1 (CMM 1), 13.2 (CMM 1)
Valor CMM acumulat	CMM 1
Comentaris	No Conformitat Major. No s'han dut a terme accions en aquest camp. La majoria de punts estan iniciats o planificats, però no existeixen evidències del seu treball.

Domini	14, Gestió de Continuïtat de Negoci
Punts de control	14.1 (CMM 2)
Valor CMM acumulat	CMM 2
Comentaris	No Conformitat Menor. Estem molt a prop d'aconseguir una conformitat. Només cal millorar el punt de proves, manteniment i reavaluació dels plans d'aquest domini.

Domini	15, Conformitat
Punts de control	15.1 (CMM 2)
Valor CMM acumulat	CMM 2
Comentaris	No Conformitat Menor. Cal millorar en el mal ús dels recursos del tractament de la informació i millorar alguns aspectes referents a la propietat intel·lectual com a prioritats.

Resultats:

El següent gràfic en forma de radar mostra l'evolució dels diferents blocs de la norma. Podem comparar entre l'estat inicial, l'actual després d'aplicar reformes i projectes per millorar la gestió de la Seguretat de la Informació, i l'estat ideal al que es desitja arribar. D'aquesta manera podem interpretar el grau de maduresa en el qual actualment ens trobem, i identificar aquells blocs en els que cal millorar i treballar amb més profunditat.



D'aquest diagrama podem extreure diverses conclusions:

- **Els projectes han resultat efectius.** Podem observar com la tendència actual és la de acostar-se al punt ideal. Això significa que el projectes plantejats i que s'han dut a terme han tingut un impacte positiu en la nostra empresa.

- **Existeixen blocs poc treballats.** Això no és sinònim d'error; el que estem observant és que s'ha prioritzat l'actuació sobre àrees concretes en funció del Anàlisis de Riscos. Aquesta metodologia de treball és correcte, però no ens ha de fer perdre de vista l'objectiu final de millora continua i que implica treballar ara en les seccions més desnivellades.

- **La inversió ha estat adequada.** Tot i que pugui semblar precipitada aquesta afirmació, podem deduir del punt anterior que la inversió ha estat proporcional i correcte, alineada amb els objectius de Hotel XXXX. Tenint en compte que els plans i projectes han estat aprovats en junta, i que el pressupost s'ha considerat adient, veiem que aquesta inversió ha tingut efectes positius en les seccions a les que anava destinat. Per tant, es pot dir que hem fet una elecció correcte de projectes i de la estimació del cost d'aquests.

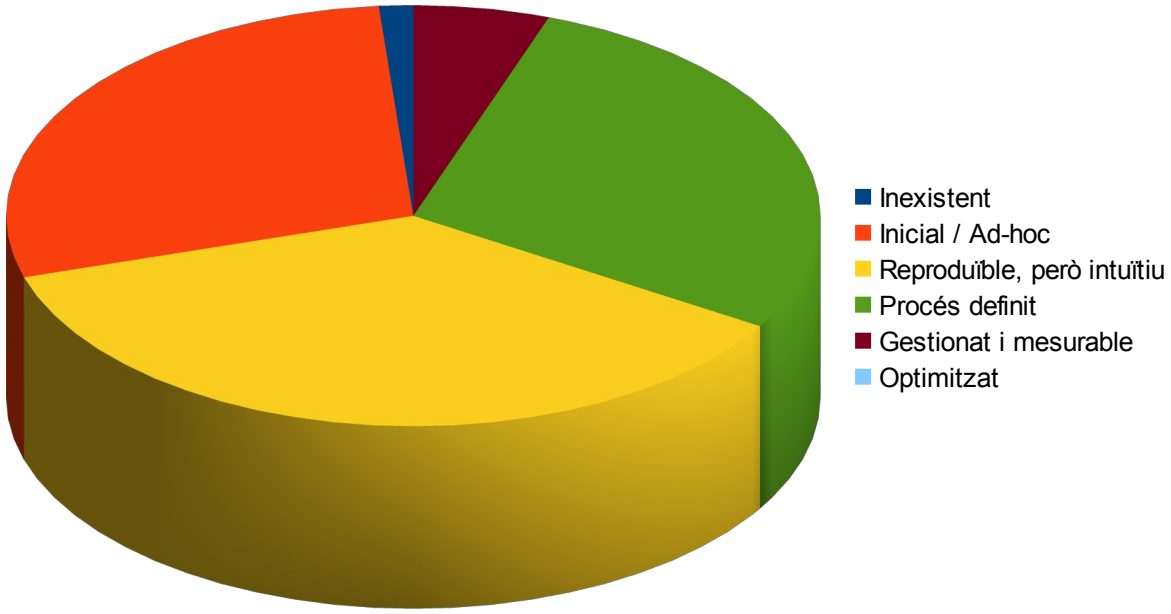
- **S'ha treballat especialment en mesures preventives.** De la taula anterior i d'analitzar el gràfic adjunt, es dedueix que el AR plantejava problemes sobre els actius més importants, i les solucions proposades en molts casos han estat resoltes mitjançant mesures preventives. Per aquest motiu, aquells blocs que necessitaven la implantació d'aquestes mesures són els que han experimentat un gran canvi i millora. D'altra banda, aquelles seccions en les quals el risc no impactava de manera tant directe en un primer moment, no han estat treballades específicament, i només s'han beneficiat de les millores compartides per altres objectius.

- **Hi ha manca de documents i fulls de ruta.** Aquest és un dels problemes que s'extreuen de l'evolució dels blocs en el diagrama. Si parem atenció a aquells blocs que han experimentat un creixement petit i els revisem en la taula anterior, veurem que existeixen molts sub-apartats que necessiten d'una guia o document que indiqui les maneres de procedir. Com que aquests documents no presentaven un interès primordial en relació a les amenaces dels actius (tal i com expliquem en la conclusió anterior) han estat obviats, i en conseqüència, no han rebut una millora per part d'un projecte específic.

- **Accions concretes no retornen un valor general.** Gràcies a la divisió de la norma ISO/IEC 27002:2005 en diferents objectius i punts de control, podem veure que aquelles accions importants però a nivell concret no aconsegueixen la millora proporcional del sistema total. Això vol dir que hem de treballar per millorar cadascun dels objectius, de abaix fins a dalt, fins obtenir el grau de maduresa desitjat. Només en el bloc 5 de Seguretat de la Informació en el qual s'ha treballat cada apartat en concret s'ha aconseguit assolir l'objectiu ideal.

Si avaluem els punts de control, del total de 133 si no tenim en compte els que “no apliquen”, obtenim un total de 74 punts, dels quals podem extreure la següent informació i gràfic:

- Inexistent: 1
- Inicial / Ad-hoc: 21
- Reproduïble, però intuïtiu: 27
- Procés definit: 21
- Gestionat i mesurable: 4
- Optimitzat: 0



Entre les conclusions que podem extreure, la primera que identifiquem és que es tracta d'un gràfic després d'un primer procés de millora del SGSI. Es veu clarament que no existeix cap procés optimitzat degut a la poca maduresa del sistema, i en canvi, encara queda algun control inexistent, que pot ser per diferents motius, alguns explicats anteriorment. De la mateixa manera, la majoria dels objectius estan ubicats en la zona mitja de valoració, indicant una transició cap als estats de gestionat i mesurable i finalment optimitzat. Per tant, podem dir que estem treballant en la direcció correcte.

Una altra conclusió molt important que obtenim de analitzar el conjunt de dades total, és que actualment no disposem de gaires eines per a mesurar i adquirir dades sobre el funcionament dels objectius. Els punts de control relacionats amb les mesures estan poc evolucionats. La organització ha prioritzat la reducció del risc actual i ha descuidat la instal·lació dels elements de mesura oportuns. Això seria dolent si no fos la primera vegada que es dur a terme aquests informes i estudis. El responsable de la gestió del SGSI haurà de prioritzar la instal·lació d'aquests elements en els processos de millora continua que tindran lloc. D'aquesta manera serà possible arribar als estats més madurs de cada bloc.

Conclusions:

Després dels raonaments plantejats podem resumir que la feina feta en anteriors fases ha tingut un èxit considerable que ha ajudat a assolir objectius. No obstant, encara estem lluny de aconseguir un grau de maduresa prou optim i desitjat. Els motius que propicien aquesta desviació han estat les consideracions individuals d'alguns actius molt importants, i la focalització de les tasques en àmbits molt semblants i de manera massa repetitiva, en aquest cas, aportant solucions relacionats amb elements preventius.

El punts més importants que caldrà treballar amb profunditat estan relacionats amb la documentació tècnica i especifica de cada bloc indicat a la ISO/IEC 27002:2005, així com potenciar l'ús de sistemes i mesures per l'adquisició i el tractament de dades que indiquin el grau de funcionament del punts de control existents. Amb la millora d'aquests paràmetres hauríem de poder dur a terme una tasca de millora en la maduresa del sistema prou important com per assolir gran part dels nivells desitjats en un principi. Així mateix, el sistema estarà més a prop de poder afrontar amb garanties una auditoria externa de certificació.