Anàlisi de riscos

PID_00253139

Daniel Cruz Allende
Arsenio Tortajada Gallego
Antonio José Segovia Henares

Universitat Oberta de Catalunya

Daniel Cruz Allende

Enginyer tècnic en Informàtica de Gestió per la Universitat Politècnica de Catalunya. *Chief Operating Officer* a Ackcent Cybersecurity. Consultor del departament de planificació de la seguretat d'esCERT-UPC (Equip de Seguretat per a la Coordinació d'Emergències en Xarxes Telemàtiques de la UPC). Ha impartit cursos i seminaris sobre seguretat informàtica en diverses institucions.

Arsenio Tortajada Gallego

Enginyer Superior en Informàtica per la Universitat Autònoma de Barcelona. Consultor/Auditor de Seguretat de la Informació en diferents organitzacions. Certificat CISA / CDPP / ISO 27001 i ISO 22301 Lead Auditor. Ha impartit cursos i seminaris sobre seguretat informàtica en diferents institucions.

Antonio José Segovia Henares

Enginyer en Informàtica, i Enginyer Tècnic en Informàtica de sistemes per la UOC. Expert en Seguretat de la Informació, *hacker* ètic i professional expert qualificat en el RGPD. Des del 2010, qualificat com a Auditor Líder en ISO 27001, i qualificat també en altres esquemes com ISO 27018, ISO 22301, i ISO 20000, per diverses entitats certificadores. *Blogger* i ponent de *webinars* sobre la Seguretat de la Informació a nivell mundial.

Índex

Introducció

Actualment, hi ha moltes organitzacions que són capaces de dedicar grans recursos a la seva seguretat, i fins i tot inverteixen diners a fer canvis en la seguretat de l'organització. A l'hora de la veritat, si se'ls pregunta per què han gastat aquests recursos a protegir-se d'alguna manera, les seves respostes no demostren que estiguin gaire convençudes que amb aquesta inversió reduiran realment les incidències que tenen.

Això ens informa que les organitzacions fan canvis i inversions en seguretat sense prou convicció. Sorprèn, en canvi, que no estiguin disposades a fer servir recursos a estudiar realment les mancances que té la seva organització.

Si s'analitza quines són les necessitats de l'organització, la inversió posterior en seguretat serà molt més petita i més ajustada a la realitat d'aquesta organització. Aquest procés es fa amb les anomenades *anàlisis de riscos*.

Objectius

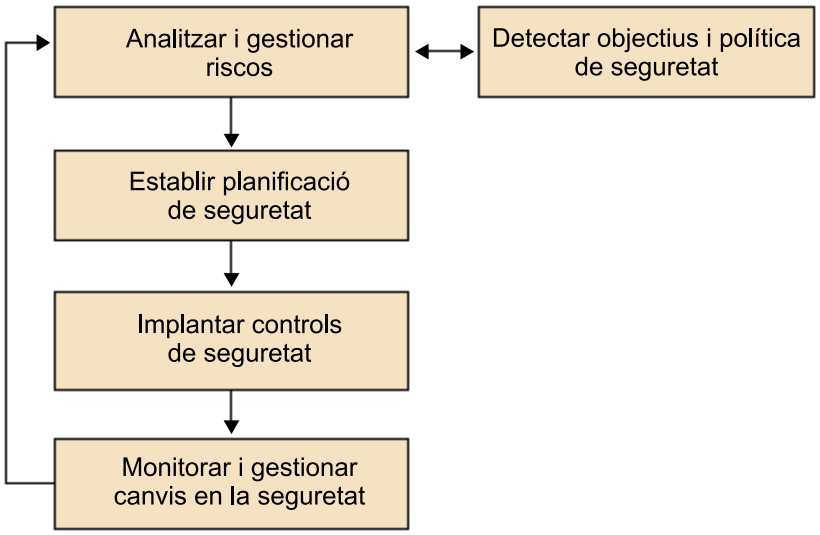
En acabar de treballar els materials d'aquest mòdul, els participants han d'aconseguir els objectius següents:

1. Saber en què consisteix el procés d'anàlisi de riscos.
2. Conèixer les diferents metodologies d'anàlisi de riscos.
3. Identificar els principis en què es basen les diferents metodologies d'anàlisi de riscos.
4. Ser capaços de dur a terme una anàlisi exhaustiva de riscos aplicant alguna de les metodologies presentades.

1. Cicle de vida de la seguretat

Quan es parla de la seguretat de la informació cal tenir en compte que es tracta d'un dels processos que es duen a terme en una organització. Es tracta, a més, d'un procés viu, en actualització i renovació constants, ja que si això no és així no s'aconsegueixen els resultats esperats.

El gràfic següent mostra quin és el cicle de vida correcte de la seguretat de la informació:



En aquest gràfic s'observen les diferents etapes per les quals s'ha de passar quan es parla de seguretat de la informació.

La primera fase, i la més important, correspon a l'**anàlisi de riscos**, que ens serveix per a descobrir quines necessitats de seguretat té l'organització després de detectar quins són els nostres forats en seguretat i també les amenaces a què estem exposats.

Aquesta primera fase ha d'estar sempre molt relacionada amb els **objectius de l'organització**; és a dir, la seguretat que nosaltres creem ha d'estar sempre encaminada al fet que es puguin complir els objectius que té fixats la nostra organització. Una mesura de seguretat no ha de constituir mai un obstacle per a dur a terme les activitats pròpies de l'organització.

Dins d'aquesta primera fase també hi ha la **gestió de riscos**, que consisteix a saber triar la millor solució de seguretat per a afrontar els riscos a què està exposada l'organització i que alhora permetin complir els objectius d'aquesta organització.

Una vegada ja tenim clar quins perills ens esperen i com ens n'hem de protegir, es passa a la segona fase, coneguda com a **planificació de la seguretat**, que correspon al procés de priorització de les diferents mesures de seguretat que s'ha detectat com a necessàries per a millorar la seguretat de l'organització. Sempre s'han de mirar de minimitzar, en primer lloc, els riscos més grans i, en segon lloc, la resta. Mai a l'inrevés.

La tercera fase correspon pròpiament a la implantació de les diferents mesures que hem decidit adoptar, tant si són procedimentals com organitzacionals o tècniques. En aquest punt sabem què hem de fer per a protegir-nos de les situacions a què estem exposats.

El problema radica en el fet que, una vegada tenim implantades les mesures de seguretat, no ens podem aturar aquí i pensar que, sense fer res més, estarem ben segurs durant un temps il·limitat. És precisament al contrari: a partir d'aquest moment s'ha d'entrar en la fase de **monitoratge** i de **gestió de canvis de la seguretat**, que consisteix a disposar de mecanismes que ens aportin evidències que les mesures de seguretat que hem implantat eviten les incidències de seguretat que preteníem eludir. Així mateix, si es detecta algun canvi per a millorar la seguretat, també s'ha d'analitzar.

Tant si s'ha detectat amb aquest monitoratge que les incidències de seguretat es continuen produint com si s'ha de fer algun canvi en alguna de les mesures, s'ha d'entrar en la primera de les fases, és a dir, s'ha de tornar a fer l'anàlisi de riscos, perquè aquest canvi no provoqui problemes de seguretat.

S'ha de fer un procés constant de renovació i actualització de les mesures de seguretat d'una organització, tenint com a punt de partida l'anàlisi de riscos, alineat amb els objectius de l'organització.

Exemple

Imaginem-nos que una organització que ha arribat a la conclusió que necessita un antivirus per a evitar les possibles infeccions dels sistemes informàtics decideix implantar-lo, però, una vegada ho ha fet, deixa de banda l'actualització perquè considera que amb la instal·lació de l'antivirus ja n'hi ha prou per a evitar les incidències de seguretat. Amb el pas del temps, l'aparició de virus nous i la falta d'actualitzacions del sistema antivirus fan que l'organització no disposi d'un sistema antivirus realment operatiu; de fet, és com si no el tingués instal·lat. En resum, no s'ha de passar per alt el punt de monitoratge i actualització de totes les mesures de seguretat que té una organització.

2. Anàlisi de riscos

Com s'ha comentat més amunt, l'anàlisi de riscos correspon a la primera fase que ha de fer una organització per a millorar la seva seguretat.

Una anàlisi de riscos correspon, des del punt de vista de la seguretat, al procés d'identificació d'aquests riscos: en determina la magnitud i n'identifica les àrees que requereixen mesures de protecció.

Anàlisi de riscos

Una anàlisi de riscos equival a fer una fotografia d'una organització, des del punt de vista de la seguretat, que mostri els aspectes que amb més probabilitat poden provocar una incidència de seguretat.

Cal destacar que un procés d'anàlisi de riscos dóna com a resultat una informació i no una mesura de seguretat com a tal; és a dir, el procés en si no evitarà que l'organització tingui incidències de seguretat, sinó que permetrà identificar els perills a què està exposada. Això vol dir que, si tenim ben identificats els perills, a l'organització li serà més fàcil protegir-se de les situacions que representen un risc més gran.

De fet, una anàlisi de riscos ens permet respondre a les tres grans preguntes sobre la seguretat de la informació en una organització per a fer, més endavant, una anàlisi i estar en disposició de prendre decisions basant-nos en situacions concretes. Les tres preguntes són les següents:

- Què cal protegir? S'identifiquen els elements que ha de mirar d'assegurar l'organització.

- De què o de qui ens hem de protegir, i per què? S'identifiquen els perills que poden afectar l'organització i el motiu pel qual es pot produir una incidència.

- Com ens volem protegir? Després d'una anàlisi exhaustiva, s'opta per la millor protecció perquè els perills no s'arribin a materialitzar.

Analitzar les preguntes fonamentals

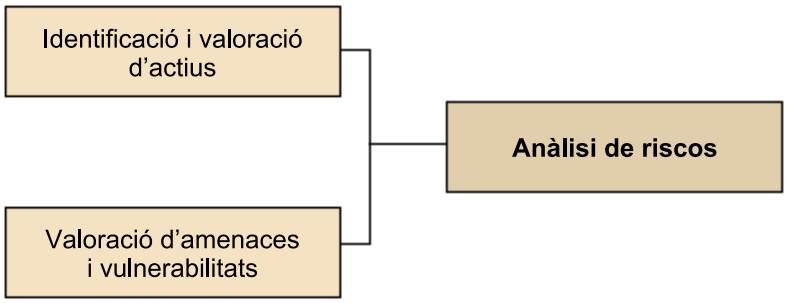
Si una organització no fa el procés d'aturar-se a analitzar aquestes preguntes fonamentals, no es podrà justificar la instal·lació d'una determinada mesura de seguretat ni es tindran les evidències necessàries per a fer-ho. I aquest és l'avantatge principal i la utilitat més bona de fer una anàlisi de riscos: detectar totes les situacions que s'han de protegir per a mirar d'evitar les incidències de seguretat.

2.1. Procés d'anàlisi de riscos

Actualment, hi ha diferents metodologies vàlides per a fer una anàlisi de riscos. Cadascuna d'aquestes metodologies té una sèrie de característiques pròpies, però bàsicament es fonamenten totes en els mateixos processos i, encara que amb matisos, treballen sobre els mateixos elements:

- Actius: elements que s'han de protegir.
- Amenaces: situacions de què s'han de protegir els actius.
- Vulnerabilitats: aspectes que faciliten la materialització de les amenaces.

El risc consisteix en la relació d'aquests tres elements. Combinant-los entre si s'obté els diferents tipus de riscos a què està exposada una organització:



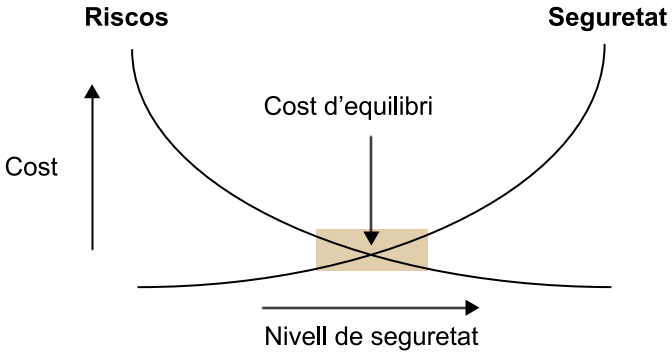
Una vegada fet aquest procés d'anàlisi de riscos es duu a terme la fase següent, que és l'última, això és, la gestió de riscos, en la qual es decideixen les mesures de protecció que s'han d'implantar per a evitar que els riscos detectats arribin a afectar l'organització, i tot plegat invertint tants pocs recursos com es pugui.

Aquest procés de gestió de riscos ha d'equilibrar el cost de protecció i el cost d'exposició d'una organització.

- Cost de protecció: cost que comporta a l'organització protegir-se d'una situació detectada prèviament.
- Cost d'exposició: cost que representaria que s'arribés a donar la situació analitzada i l'organització no tingués protecció.

El punt a què s'ha d'arribar és al de trobar el cost d'equilibri; és a dir, no s'ha de gastar més del que representaria recuperar-se de la situació analitzada.

És llavors quan s'ha de determinar l'anomenat **llindar de risc**, que és el punt a partir del qual s'ha de reduir tot risc almenys fins a situar-se en el punt justament inferior al marcat per cada organització.



I en aquesta fase de gestió de risc s'ha de triar entre alguna de les opcions següents:

- **Acceptar-lo**. Aquesta decisió consisteix en el fet que l'organització ha detectat que està exposada a un risc important que s'ha de reduir per sota del llindar de risc marcat. Per a fer-ho, hi ha d'invertir una sèrie de recursos, però la protecció enfront del risc detectat representa un cost tan elevat, i la probabilitat que arribi a passar és tan improbable, que no resulta possible la inversió per a protegir-se davant aquesta situació. La decisió és que l'organització treballi acceptant que està exposada al risc i, si es produeix una incidència, improvisar-hi una resposta.

Esperar un terratrèmol

Imaginem-nos que una organització detecta que està exposada al risc de tenir un terratrèmol i que el fet que aquesta situació arribi a passar representa un risc superior al llindar de risc determinat per aquesta organització. Ara bé, el cost de "disposar d'un segon edifici" és massa costós tenint present la probabilitat que arribi a passar. Davant aquesta situació, l'organització decideix acceptar aquest risc i continua treballant de la mateixa manera.

- **Assignar-lo a tercers**. Correspon a la situació en què una organització determina que té algun risc per sobre del seu llindar de risc. A més, considera que no el pot assumir, per la gravetat del risc, però que alhora no el pot reduir, sia perquè no té la capacitat de fer-ho o perquè no té els recursos necessaris. En aquests casos, es decideix contractar un tercer que sí que té aquesta capacitat de reduir i gestionar el risc de tal manera que quedi per sota del llindar de risc.

Assignació de riscos a tercers

Els exemples més habituals són els de contractació de pòlisses d'assegurança o els de contractació de terceres organitzacions perquè gestionin alguna determinada àrea que per defecte ha de gestionar l'organització mateixa; per exemple, les empreses especialitzades a gestionar la xarxa d'una organització.

- **Reduir-los o evitar-los.** Correspon a la situació en què una organització ha detectat un risc elevat, per sobre del seu llindar de risc, i decideix implantar algun control de seguretat per a reduir-lo, almenys fins a situar-lo per sota del llindar de risc determinat.

Sens dubte, l'ideal és sempre mirar d'evitar o reduir un risc, ja que implica que l'organització mateixa controla i disposa de les mesures de seguretat adequades que li permeten mirar d'evitar aquests riscos.

3. Anàlisi de riscos. Justificació i estudi

Ja sabem que una anàlisi de riscos ha de ser la primera tasca, i la principal, que ha de fer una organització quan es planteja millorar en qualsevol aspecte la seguretat de la informació.

3.1. Per què cal fer-la?

Els motius pels quals s'ha de fer una anàlisi de riscos són els següents:

- Permet identificar els riscos a què està exposada l'organització des del punt de vista de la seguretat i que poden afectar el desenvolupament de les activitats de negoci de l'organització.

- Permet a l'organització fer una selecció de les mesures de seguretat que s'hi han d'implantar, molt més ajustada a les necessitats d'aquesta organització.

- Permet fer i elaborar els plans de contingències d'una organització. Això vol dir que una anàlisi de risc ens presentarà les situacions que poden provocar una incidència de seguretat i que, alhora, no es poden reduir implantant les mesures de seguretat. Per tant, ha de servir de base per a elaborar els plans de contingències.

- Les organitzacions que tinguin previst implantar les diferents normatives de seguretat (ISO 27001) i crear un sistema de gestió de la seguretat de la informació (SGSI), amb la intenció d'aconseguir certificar-lo, han de tenir una anàlisi de riscos, que és l'autèntic punt de partida de tot el procés de certificació.

El sistema de gestió de la seguretat de la informació correspon al procés d'implantació d'una sèrie de mesures indicades en les normatives i bones pràctiques de seguretat de la informació.

3.2. Tipus d'anàlisi

Depenent dels objectius que es pretén aconseguir i de l'enfocament que es té a l'hora de fer una anàlisi de risc, es poden fer dos tipus diferents de processos d'anàlisi de riscos:

- **Anàlisi de riscos intrínsecs**. És l'estudi que es fa sense tenir en consideració les mesures de seguretat que ja hi ha implantades en una organització. Aquest procés dóna com a resultat un risc intrínsec.

- **Anàlisi de riscos residual**. És l'estudi que es fa tenint en consideració les mesures de seguretat que ja té implantades l'organització. Com a resultat d'aquest procés s'obté un risc real.

La decisió de fer una anàlisi de riscos intrínsecs o una de residual depèn de si una organització pretén analitzar si la inversió que ha fet en seguretat ha estat la correcta o si, en canvi, el que pretén és estudiar la situació real en què es troba. El més habitual és fer l'anàlisi de riscos residual, perquè si una organització ja té unes mesures de seguretat implantades i pretén millorar la seva seguretat ha de preveure aquestes solucions tenint en compte la situació actual en què es troba, ja que encara que la inversió no hagi estat la correcta no la podrà recuperar.

De totes maneres, tenint en compte que hi ha diferents metodologies per a fer anàlisis de riscos, és possible que el nom que posin a cadascuna d'aquestes metodologies sigui diferent, encara que l'essència sigui la mateixa:

- Hi ha un estudi que reflecteix la situació inicial o sense mesures de seguretat.
- Hi ha un estudi que reflecteix els riscos i les mesures de protecció que s'han d'implantar.

Independentment de la metodologia que s'utilitzi, tal com s'ha comentat, el resultat de totes les anàlisis és el mateix, ja que totes es fonamenten en els mateixos elements.

3.3. Elements de l'anàlisi

Totes les anàlisis de riscos es fonamenten en els mateixos elements i, encara que hi hagi diferents metodologies, en totes es tenen en consideració els mateixos aspectes i han de donar resultats similars independentment de la manera d'expressar-ho.

Els elements que es tenen en consideració en els processos d'anàlisi de riscos són els següents:

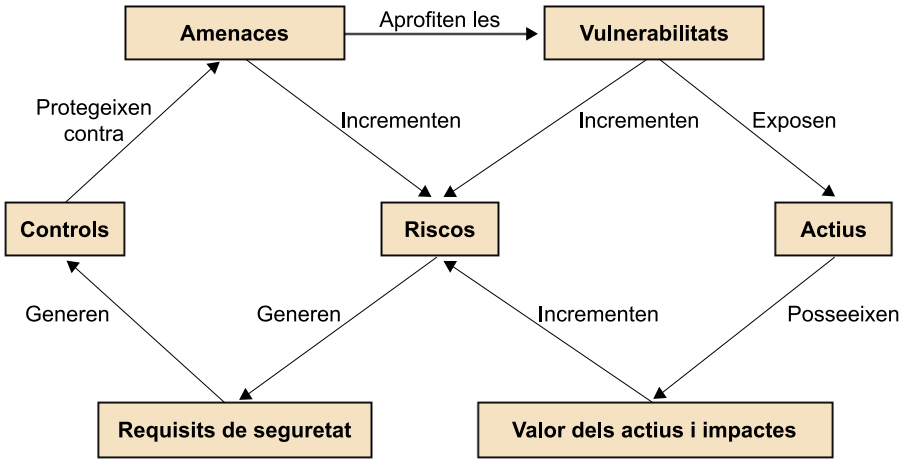
- **Actius**: són tots els elements que té l'organització i que s'analitzen durant el procés. Cal destacar que per a *actiu* s'entén tot element que requereix l'organització per a fer les activitats de negoci que li són pròpies.

- **Amenaces**: són totes les situacions que poden arribar a passar en una organització i que poden danyar els actius, i provocar, doncs, que aquests actius no funcionin correctament o que no es puguin utilitzar de la manera correcta per a dur a terme l'activitat de negoci de l'organització.

- **Vulnerabilitats**: són les diferents debilitats que presenten els actius identificats anteriorment i que són aprofitats per les amenaces per a provocar un dany.

- **Impactes**: són les conseqüències que es produeixen en l'organització quan una amenaça aprofita una vulnerabilitat per a danyar un actiu.

Tots aquests elements són la base per a qualsevol anàlisi de riscos, i s'hi fonamenta tot l'estudi. A partir d'aquests elements, s'estimen els riscos a què està exposada l'organització i que més endavant s'hauran de tractar en el procés de gestió dels riscos. De fet, dins de tot procés d'anàlisi i gestió de riscos es creen una sèrie de relacions:



El gràfic mostra les relacions que es creen quan es parla de seguretat de la informació i quan es pretén minimitzar els **riscos** a què està exposada una organització.

Cal tenir en compte que una organització està exposada a una sèrie d'**amenaces** que són les causants dels riscos i alhora dels danys possibles. Les amenaces aprofiten les **vulnerabilitats** per a danyar els actius; de fet, si no hi ha vulnerabilitats, les amenaces no poden danyar una organització. Aquestes amenaces exposen els **actius** i són aquests actius els que tenen realment **valor** per a una organització, és a dir, que són els elements que necessita una organització per a desenvolupar les seves activitats.

Tant les amenaces com les vulnerabilitats i el mateix valor dels actius fan que els riscos augmentin de manera que les organitzacions s'hagin de plantejar mesures de protecció.

Aquests riscos són els que generen **requisits de seguretat**. Al seu torn, aquests requisits acaben generant **controls** de seguretat, que són finalment els que s'implanten en les organitzacions per a reduir els riscos. Aquests controls miren de protegir les empreses contra les amenaces enumerades més amunt.

El gràfic que acabem de presentar mostra que totes les metodologies d'anàlisi de riscos, independentment de la que s'ha utilitzat, es regeixen per les relacions anteriors.

4. Metodologies

Actualment, hi ha diverses metodologies al mercat. Totes ofereixen resultats similars si s'apliquen d'una manera correcta a les mateixes organitzacions. Les diferències entre unes i altres radiquen en la manera en què presenten els resultats.

Podeu accedir a un conjunt de metodologies a l'enllaç següent:

https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra- methods.

4.1. Magerit

Aquesta metodologia la va elaborar el Ministeri d'Administracions Públiques (MAP) amb la finalitat d'ajudar totes les administracions públiques de l'Estat espanyol a millorar diversos aspectes. Més endavant s'ha aplicat a qualsevol organització (https://administracionelectronica.gob.es/ctt/magerit).

Aquesta metodologia es pot aplicar a qualsevol organització, independentment que sigui a l'Estat espanyol o en un altre país. Alhora, aquesta metodologia ha desenvolupat una eina que ajuda a aplicar-la.

Amb el pas del temps s'han desenvolupat diferents versions, i es presenta a l'octubre de 2012 la tercera versió.

Com a suport a aquesta metodologia, hi ha les eines d'entorn d'anàlisi de riscos (EAR), que suporten l'anàlisi i la gestió de riscos d'un sistema d'informació seguint la metodologia Magerit (metodologia d'anàlisi i gestió de riscos dels sistemes d'informació) i està desenvolupada i finançada parcialment pel CCN (https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html).

Aquesta metodologia té com a característica fonamental que els riscos que es plantegen per a una organització s'expressen en valors econòmics directament, cosa que té un avantatge i un inconvenient:

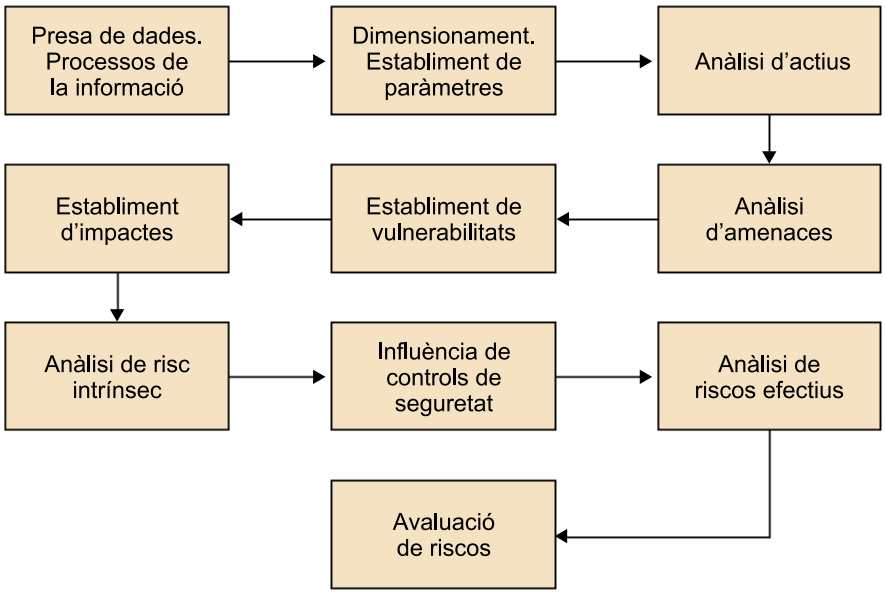
- L'aspecte positiu d'aquesta metodologia és que el resultat s'expressa en valors econòmics. Això fa que les decisions que s'han de prendre i que ha de validar la direcció estan fonamentades i són fàcilment defensables.

- En canvi, el fet d'haver de traduir de manera directa totes les valoracions en valors econòmics fa que l'aplicació d'aquesta metodologia sigui realment costosa.

4.1.1. Fases de Magerit

Aquesta metodologia, com s'ha comentat, té una eina –encara que no és imprescindible– que permet l'aplicació de Magerit d'una manera directa.

Magerit segueix un procés fins a arribar a elaborar i identificar tots els riscos d'una organització. Les fases són les següents:



Presa de dades i processos d'informació

En aquesta primera fase –la més important de tota la metodologia–, s'ha de definir l'abast que s'ha d'estudiar o analitzar, ja que, depenent d'aquest abast, el procés és més o menys costós. Com més abast, més gran és el nombre de riscos analitzables.

Un altre factor que s'ha de tenir en compte és que, en aquesta primera fase, s'han d'analitzar els processos que duu a terme l'organització, ja que els riscos que s'han d'estudiar són els que poden interferir en els processos crítics. No s'ha de passar per alt que l'objectiu de tota seguretat és sempre garantir que els processos propis de l'organització es puguin fer de la millor manera possible.

Hi ha amenaces que no provocaran interferències en les activitats de l'organització i que no s'han d'analitzar, ja que protegir-se contra aquestes amenaces no té sentit, perquè no l'afectaran mai.

En aquesta primera fase també cal tenir present un factor importantíssim: la granularitat.

La **granularitat** té a veure amb la definició de les unitats que es pretén analitzar. Vol dir que s'ha de determinar el nivell de detall a què es vol arribar. Com més detall (baix nivell), més elements s'han d'analitzar i més costós és l'anàlisi de riscos.

Establiment de paràmetres

La segona fase és la més important en la metodologia Magerit. Consisteix a establir paràmetres que s'utilitzaran durant tot el procés d'anàlisi de riscos.

S'ha de tenir present que els paràmetres que s'identifiquin en aquesta fase s'han d'utilitzar durant tot el procés d'anàlisi de riscos i que si això no es compleix els resultats que s'obtindran no es podran comparar, de manera que el resultat no mostrarà els riscos reals d'una organització.

Els paràmetres que s'han d'identificar són els següents:

- Valor dels actius.
- Vulnerabilitat.
- Impacte.
- Efectivitat del control de seguretat.

Vegem-los detalladament:

- **Valor dels actius**. Aquest paràmetre té l'objectiu d'assignar una valoració econòmica a tots els actius d'una organització que es pretenen analitzar.
  Els actius que s'han d'analitzar són els que requereix l'organització per a dur a terme els processos que són propis d'aquesta organització.
  Quan es tracta d'assignar valoracions econòmiques als actius, no solament en cal tenir present el valor de compra, sinó també el valor segons la importància que té per a la tasca que s'utilitza.
  Per a dur a terme la valoració s'han d'establir diferents grups d'actius segons el valor que tenen. A cadascun d'aquests rangs s'hi assigna un valor estimat que és el que s'utilitzarà per a tots els actius la valoració econòmica dels quals es correspongui amb aquest rang de valors.
  Cada organització ha de dictaminar quins són els rangs de valors que pretén utilitzar durant l'estudi. No és recomanable establir més de cinc rangs, ja que com més se n'estableixin més complicada serà l'assignació de cada actiu al nivell adequat.
  A l'hora d'assignar una valoració a cada actiu s'ha de tenir en consideració el següent:

- El **valor de reposició** és el valor que té per a l'organització reposar aquest actiu en cas que es perdi o que no es pugui utilitzar.

- El **valor de configuració** és el temps que es necessita des que s'adquireix el nou actiu fins que es configura o es posa a punt perquè es pugui utilitzar per a la funció que desenvolupava l'anterior actiu.

- El **valor d'ús de l'actiu** és el valor que perd l'organització durant el temps que no pot utilitzar aquest actiu per a la funció que desenvolupa.

- El **valor de pèrdua d'oportunitat** és el valor que perd potencialment l'organització pel fet de no poder disposar d'aquest actiu durant un temps.

Valor d'un portàtil

Imaginem-nos que es mira d'analitzar el valor que té un portàtil per a dues organitzacions diferents. L'una únicament utilitza aquest equip per a fer presentacions. En canvi, l'altra utilitza aquest equip (que té el mateix preu al mercat) com a servidor o com a repositori d'informació. A l'hora de fer-ne l'estimació, el valor del portàtil per a la segona organització és superior, encara que el preu de l'equip sigui el mateix per a totes dues.

Procediment de valoració

Valoració	Rang	Valor
Molt alta	valor > 200.000 €	300.000 €
Alta	100.000 € < valor > 200.000 €	150.000 €
Mitjana	50.000 € < valor > 100.000 €	75.000 €
Baixa	10.000 € < valor > 50.000 €	30.000 €
Molt baixa	valor < 10.000 €	10.000 €

En aquest exemple s'ha de considerar que, durant el procés d'anàlisi de riscos, el valor màxim de tots els actius que s'han d'analitzar, independentment del valor definitiu que tinguin, és de 300.000 €.

- **Vulnerabilitat**. Per a Magerit, les vulnerabilitats s'entenen com una freqüència d'ocurrència d'una amenaça; és a dir, la freqüència amb què una organització pot tenir una amenaça en concret.
  Aquesta freqüència d'ocurrència, o vulnerabilitat, també es plasma en una escala de valors (no es recomana més de cinc nivells) que s'han d'utilitzar per a tot l'estudi.
  Una vegada hem determinat l'escala de valors que utilitzarem durant l'anàlisi de riscos, cal traduir aquestes vulnerabilitats a nombres, per a treballar-hi. Aquesta valoració numèrica es fa amb estimacions anuals, és a dir, assignant un nombre de vegades per any:

Vulnerabilitat

Són forats que té l'organització des del punt de vista de la seguretat de la informació.

Vulnerabilitat = freqüència estimada / dies de l'any

Classificació de la vulnerabilitat

Vulnerabilitat	Rang	Valor
Freqüència extrema	1 vegada al dia	1
Freqüència alta	1 vegada cada 2 setmanes	26/365 = 0,071233
Freqüència mitjana	1 vegada cada 2 mesos	6/365 = 0,016438
Freqüència baixa	1 vegada cada 6 mesos	2/365 = 0,005479
Freqüència molt baixa	1 vegada l'any	1/365 = 0,002739

Suposició: l'any té 52 setmanes

En aquest exemple, l'organització ha estimat que, en el pitjor dels casos (a allò que serà més vulnerable, o amb més freqüència), la situació es donarà una vegada al dia. Això, extrapolat a l'any, representa el 100% de vulnerabilitat:

vulnerabilitat = 365 / 365 = 1

El segon cas representa el que s'estima que passarà una vegada cada dues setmanes, que representa unes 27 vegades a l'any i en resulta un valor de 0,071. I d'aquesta manera s'extreuen la resta de valors.

Cal afegir que, a l'hora d'elaborar l'anàlisi de riscos, el més correcte no és pensar en els conceptes *una vegada a l'any* o *una vegada al mes*, sinó si una situació, en virtut de les característiques de l'organització, té una freqüència d'ocurrència extrema, alta, mitjana, baixa o molt baixa, i a partir d'aquesta classificació treballar amb la numeració que s'ha extret per a aquest nivell de vulnerabilitat.

Ha de quedar clar que no es pot anar modificant els valors durant l'estudi, sinó que s'han de mantenir d'aquesta manera per a tots els actius i per a totes les amenaces que s'han d'analitzar. Si es canvia les escales a la meitat de l'estudi, els resultats no seran adequats i no es podran comparar.

- **Impactes**. Per a Magerit, s'entén per **impacte** el tant per cent del valor de l'actiu que es perd en cas que hi hagi una incidència sobre aquest actiu.
  Per a fer aquesta anàlisi *a priori*, també s'ha de fer una estimació per rang d'impactes; és a dir, cal pensar en els diferents nivells d'impacte que es vol utilitzar, i a partir d'aquí assignar el percentatge de valor que s'estima que es pot perdre en cada cas.

Impacte

És la conseqüència del fet que una amenaça, aprofitant una vulnerabilitat, danyi un actiu.

Valoració dels impactes

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

En aquest exemple s'estima que, en cas que hi hagi la incidència amb l'impacte més gran possible, s'arribarà a perdre el 100% del valor d'aquest actiu; en cas que l'impacte sigui alt (però sense arribar a ser el més alt), es perdrà el 75% del valor de l'actiu, i així per a cadascun dels nivells establerts.

- **Efectivitat del control de seguretat**. Aquest paràmetre consisteix a veure la influència que tindran les mesures de protecció davant els riscos que detectem, és a dir, a pensar en la manera com ens poden reduir el risc detectat les diferents mesures de seguretat que implantem.
  A l'hora de reduir un risc, cal tenir en compte que les mesures de seguretat tenen dues maneres d'actuar-hi en contra: o bé redueixen la vulnerabilitat (la freqüència d'ocurrència), o bé redueixen l'impacte que provoca aquest risc.
  Per a aquest paràmetre, també s'ha de fer una classificació de nivells vàlida per a tot l'estudi.

Classificació de nivells

Variació impacte/vulnerabilitat	Valor
Molt alt	95%
Alt	75%
Mitjà	50%
Baix	30%
Molt baix	10%

Segons la taula, l'organització estima que, en cas d'utilitzar la millor mesura de seguretat per a un determinat risc, aquesta mesura l'ajudarà a reduir el risc inicial en un 95%, i així per a cadascun dels nivells que ha establert.

Una vegada més cal destacar que tots aquests paràmetres són els que s'han d'**utilitzar durant tota l'anàlisi de riscos**. No es poden anar modificant depenent de l'actiu que s'analitza o de l'amenaça que afecti.

Anàlisi d'actius

Aquesta fase de l'estudi consisteix a identificar els actius que té l'organització i que necessita per a dur a terme les seves activitats. En aquesta fase és molt important haver deixat identificat clarament l'abast de l'anàlisi de riscos, ja que solament s'ha d'analitzar els actius que hi ha dins d'aquest abast.

Cal recordar que és important tenir clar el nivell de granularitat a què es vol arribar, ja que com més baix sigui més gran serà la llista d'actius analitzables.

Quan es parla d'actius analizables cal pensar en els tipus d'actius següents:

- **Actius físics**. Són tots els actius de tipus *maquinari* que s'utilitzen en l'organització: ordinadors, servidors, portàtils, PDA, telèfons mòbils, impressores, etc.

- **Actius lògics**. Són tots els elements de *programari* que s'utilitzen: sistemes operatius, aplicacions pròpies, paquets tancats de mercat, processos *batch*, etc.

- **Actius de personal**. Són les persones, des del punt de vista de rols o perfils que intervenen en el desenvolupament de les activitats de l'organització: responsable de seguretat, administrador de la xarxa, personal d'administració, secretaris, usuaris, etc.

- **Actius d'entorn i infraestructura**. Són tots els elements que té l'organització i que necessita perquè la resta funcioni correctament. Són, per exemple, els sistemes d'aire condicionat o el cablejat de dades i de corrent elèctric.

- **Actius intangibles**. Són els elements que no té directament l'organització però que són importants per a ella, com ara la imatge corporativa, la credibilitat, la confiança dels clients, o el saber fer o *know how*.

S'han de classificar segons els valors que s'han establert prèviament com a paràmetres, de manera que cal recordar que s'ha de tenir en compte el següent:

- Valor de reposició.
- Valor de configuració o posada al punt.
- Valor d'ús de l'actiu.
- Valor de pèrdua d'oportunitat.

Anàlisi d'amenaces

Les **amenaces** són les situacions que es poden arribar a donar en una organització i que desembocarien en un problema de seguretat.

Convé tenir present que les amenaces depenen molt de l'organització, i també de les característiques d'aquesta organització, en el sentit que cal analitzar les amenaces que afectaran els actius que té una organització en concret.

Diversitat d'amenaces

Les amenaces que pot tenir una multinacional no tenen res a veure amb les que pot tenir una pime. Alhora, una organització que es dedica al comerç electrònic no està sotmesa tampoc a les mateixes amenaces que una empresa que es dedica a fabricar qualsevol producte i que ni tan sols té connexió a Internet.

Magerit classifica les amenaces que poden afectar una organització en quatre grans grups, i dins de cadascun d'aquests grups identifica amenaces més concretes, que són les que s'han de preveure:

- **Accidents**. Són les situacions no provocades voluntàriament que sovint no es poden evitar, sinó que passen per efectes naturals. Dins d'aquesta categoria d'accidents n'hi ha de diferents tipus, com ara:
  - Accident físic (inundació, incendi, terratrèmol, explosió, etc.).
  - Avaria.
  - Interrupció dels serveis essencials (talls en el subministrament elèctric, en les telecomunicacions, etc.).
  - Accidents mecànics o electromagnètics (xoc, caiguda, radiació, etc.).
- **Errors**. Són les situacions que són comeses de manera involuntària pel desenvolupament mateix de les activitats diàries de l'organització, sia per desconeixement o per distracció del personal d'aquesta organització o de tercers que són contractats per l'organització mateixa. Entre aquestes situacions esmentem les següents:
  - Errors en la utilització dels sistemes, provocats per un mal ús.
  - Errors en el disseny conceptual de les aplicacions.
  - Errors en el desenvolupament de les aplicacions.
  - Errors d'actualització o aplicació de pegats als sistemes o aplicacions.
  - Errors en el monitoratge.

  - Errors de compatibilitat entre aplicacions.

  - Errors inesperats (virus, cavalls de Troia, etc.).

- **Amenaces intencionals presencials**. Són les provocades pel personal mateix de l'organització de manera voluntària quan fan accions que saben que provoquen un dany, tant des del punt de vista físic com del lògic. Entre aquestes amenaces esmentem les següents:
  - Accés físic no autoritzat, sia amb destrucció de la informació o amb substracció.

  - Accés lògic no autoritzat, intercepció passiva de la informació o substracció o alteració de la informació en trànsit.

  - Indisponibilitat de recursos, tant si són humans (baixes, vacances, abandonament, malaltia, etc.) com tècnics (bloqueig de sistema, per exemple).

  - Filtració de dades a terceres organitzacions, tant si són dades personals (LOPD) com tècniques.

- **Amenaces intencionals remotes**. Amenaces provocades per terceres persones, és a dir, per persones alienes a l'organització i que aconsegueixen danyar-la. Entre aquestes amenaces esmentem les següents:
  - Accés lògic no autoritzat. Accés d'un tercer no autoritzat, que explota una vulnerabilitat del sistema per utilitzar-la en benefici propi.

  - Suplantació de l'origen. Intercepció d'una comunicació escoltant o falsejant les dades intercanviades.

  - Cucs. Virus que utilitzen les capacitats de servidors i clients per a propagar-se per Internet.

  - Denegació de servei, sia contra l'amplada de banda (consumir tota l'amplada de banda de la màquina que es vol atacar) o contra els recursos del sistema (consumir tota la memòria i els recursos de la màquina utilitzada per a oferir un servei).

Com s'observa, tots els perills que imaginem es poden englobar en algun dels tipus d'amenaces que hem analitzat. La metodologia Magerit ofereix una llista de tot un seguit d'amenaces corresponents a cadascun d'aquests nivells, llista que es pot utilitzar per a fer les anàlisis de riscos independentment de la metodologia que es faci servir.

Establiment de les vulnerabilitats

Recordem que per *vulnerabilitats* s'entén els forats que tenim en la nostra seguretat i que permeten que una amenaça pugui danyar un actiu. És important tenir clar que, sense vulnerabilitat, l'amenaça no pot danyar els nostres actius i també que les vulnerabilitats per si mateixes no provoquen danys, sinó que aquests danys els provoquen sempre les amenaces.

En Magerit, malgrat que no és necessari fer una llista de les vulnerabilitats, sí que ho és tenir-les en compte per a estimar la freqüència d'ocurrència d'una determinada amenaça sobre un actiu.

Risc d'incendi

Imaginem-nos que analitzem el risc d'una organització de tenir un incendi en el servidor que hi ha en una sala (centre de processament de dades o CPD) que té un sistema d'extinció automàtica d'incendis per gas haló, i també detectors de fums i detectors de temperatura. La freqüència d'ocurrència, és a dir, la vulnerabilitat que té davant l'amenaça d'incendi, és més petita que si no disposa d'aquests elements.

Aquesta anàlisi s'ha de fer a l'hora d'identificar les vulnerabilitats de Magerit.

Valoració d'impactes

Els impactes es defineixen com les conseqüències que provoca en l'organització el fet que una certa amenaça, aprofitant una determinada vulnerabilitat, afecti un actiu.

A l'hora d'analitzar els impactes s'han de tenir en consideració els aspectes següents:

- El resultat de l'agressió d'una amenaça sobre un actiu.

- L'efecte sobre cada actiu per a agrupar els impactes en cadena segons la relació d'actius.

Incendi d'un servidor

En analitzar l'impacte de l'incendi d'un servidor, cal tenir en compte que l'incendi no solament afecta la disponibilitat de l'equip, sinó també la informació que conté aquest equip, encara que no sigui l'actiu mateix el que s'analitza.

- El valor econòmic representatiu de les pèrdues produïdes en cada actiu.

- Les pèrdues quantitatives o qualitatives.

Anàlisi de riscos intrínsecs

A partir d'aquest punt, i amb els valors que hàgim identificat per a cada situació, ja es pot fer l'estudi dels riscos actuals a què està sotmesa una organització.

Per a aquest estudi, únicament és necessari fer una multiplicació dels valors que hem indicat fins ara:

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

Per a Magerit, l'estudi de la situació actual és l'anàlisi de riscos intrínsecs, és a dir, l'anàlisi de la situació en què es troba l'organització en el moment de l'estudi encara que ja tingui implantades mesures de seguretat.

Recordem que definim **riscos intrínsecs** com els riscos a què estem exposats sense tenir en compte les mesures de seguretat que implantem. En el cas de Magerit, s'entén per **intrínseca** la situació en què ens trobem tenint en consideració tots els elements que té l'organització.

Influència dels controls de seguretat

Una vegada tenim identificats els riscos actuals a què està exposada l'organització, s'entra en la fase de **gestió de riscos**, que consisteix a mirar d'escollir la millor solució de seguretat que ens permeti reduir-los.

Per a fer-ho, hi ha dos tipus fonamentals de controls de seguretat:

- **Preventius**. Són les mesures de seguretat que redueixen les vulnerabilitats (la freqüència d'ocurrència).

  $$\text{Nova vulnerabilitat} = \text{Vulnerabilitat} \times \text{Percentatge de disminució de vulnerabilitat}$$

- **Correctius**. Són les mesures de seguretat que redueixen l'impacte de les amenaces.

  $$\text{Nou impacte} = \text{Impacte} \times \text{Percentatge de disminució d'impacte}$$

Exemples de controls de seguretat

Com a exemples de cadascun d'aquests dos tipus de controls de seguretat tenim els següents:

- Un tallafoc. Com a mesura preventiva, el que fa és reduir la freqüència d'ocurrència d'intrusions a la nostra xarxa. En cas, però, que s'arribi a produir una intrusió, no pot fer res per a reduir els danys que provocaria.

- Una còpia de seguretat. El que fa és reduir l'impacte que provocaria una pèrdua d'informació. En canvi, no redueix la possibilitat que algú pugui esborrar la informació de l'organització.

Per a reduir cadascun dels riscos que hem identificat en la nostra organització, és necessari buscar les solucions de seguretat que hi ha al mercat, tant si són preventives com curatives.

Anàlisi de riscos efectius

És el resultat d'estudiar com es reduirien els riscos amb cadascuna de les mesures de protecció (controls de seguretat) que hem identificat; és a dir, s'ha de calcular el risc definitiu, que dóna com a resultat el risc efectiu que tindrà l'organització per a cadascuna de les amenaces identificades.

En resum, l'estudi és el següent:

- Risc intrínsec
  Valor actiu × Vulnerabilitat × Impacte

- Risc efectiu
  Valor efectiu × Nova vulnerabilitat × Nou impacte = Valor actiu × (Vulnerabilitat × Percentatge de disminució de vulnerabilitat) × (Impacte × Percentatge de disminució d'impacte) = Risc intrínsec × Percentatge de disminució de vulnerabilitat × Percentatge de disminució d'impacte

Gestió de riscos

Aquesta última fase consisteix en la presa de decisions de l'organització sobre les mesures de seguretat que ha d'escollir entre la llista de controls de seguretat que li permeten reduir els riscos.

Llindar de riscos

És el punt en què una organització considera que els riscos a què està exposada no són acceptables.

Aquí cal tenir en compte que les organitzacions han de pretendre disminuir tots els riscos que han detectat fins a situar-los per sota de l'anomenat *llindar de riscos*, que en cada organització és diferent o pot ser diferent.

A l'hora de gestionar els riscos, s'han d'escollir les mesures de seguretat que permetin reduir els riscos intrínsecs de l'organització fins a situar-los per sota del llindar de riscos amb un cost més petit per a l'organització.

Recordem que, a l'hora de gestionar els riscos en una organització, es poden prendre tres decisions:

- Reduir-los.
- Transferir-los.
- Acceptar-los.

Pla d'acció

És un document en què es descriu les conclusions de l'anàlisi de riscos i les mesures que durà a terme l'organització per reduir-los.

A l'hora de gestionar riscos s'ha d'elaborar un **pla d'acció**, que ha de contenir la informació següent:

- Establir prioritats. Consisteix a designar els riscos que s'han de reduir en primer lloc perquè són els més elevats per a l'organització.

- Plantejar l'anàlisi de cost-benefici. Consisteix a estudiar, per a cadascuna de les mesures que es poden implantar, quin cost comporta a l'organització i en quin percentatge redueix els riscos detectats.

- Seleccionar controls definitius. Una vegada analitzat el cost-benefici de tots els controls, cal seleccionar definitivament els que ha d'implantar l'organització per a reduir els riscos fins a situar-los per sota del seu llindar de risc.

- Assignar responsabilitats. Consisteix a assignar els responsables dins de l'organització de dur a terme la implantació dels controls. És important tenir identificades aquestes persones ja que, si no, hi ha el perill que les decisions que es prenguin no s'acabin implantant.

- Implantar controls. Consisteix a implantar els controls de seguretat designats. Cal tenir en compte que els controls que s'implanten no han de ser forçosament tècnics, sinó que poden ser controls organitzatius o procedimentals.

Exemple de Magerit

Malgrat que, com s'ha comentat, Magerit aporta una eina per a fer aquests processos d'anàlisi de riscos, es pot fer sense necessitat d'aquesta eina, encara que pot ser laboriós.

Imaginem-nos una organització que té una sèrie d'actius i que fa l'anàlisi de riscos utilitzant Magerit. El resultat seria una cosa semblant a la que s'exposa a continuació.

Resum. Vulnerabilitat/impacte i risc intrínsec 22.502

					4		5		6		
			Personal de desenvolupament de programari i maquinari		PC de desenvolupament		PC de maquinari		PC d'entorn de proves		Any
			EN-003		SI-001		SI-002		SI-003		
Nombre	**Codi**	**Nom**	50.000		10.000		10.000		2.500		
1	A1-001	Incendi en oficines			0,003*	50%**	0,003	50%	0,003	50%	
					13,70		13,70		3,42		30,82
3	A2-001	Avaria de maquinari			0,005	50%	0,005	50%	0,005	50%	
					27,40		27,40		6,85		61,65
5	P1-002	Accés físic a oficines			0,003	5%	0,003	5%	0,003	5%	
					1,37		1,37		0,34		3,08
6	P2-001	Accés lògic intern als sistemes			0,005	50%	0,005	50%	0,005	50%	
					27,40		27,40		6,85		61,65
8	P5-002	No hi ha disponibilitat de personal	0,003	50%							
			68,48								68,48
Risc intrínsec anual per actiu			68,48 €		69,87 €		69,87 €		17,46 €		225,68

* Vulnerabilitat; per al càlcul, utilitzar el valor amb sis decimals, és a dir, 0,002739.
** Impacte.

En aquest estudi, el primer que s'ha fet és identificar els actius de l'organització, que són en una llista a la fila superior. Abans, s'ha identificat i establert els paràmetres que s'utilitzaran durant tot l'estudi.

Després, s'ha valorat aquests actius, prenent com a base el paràmetre que s'ha marcat. Potser, el grup dels PC de desenvolupament té un valor superior al dels PC de maquinari (entorns diferents dins de l'organització), però no prou per a saltar a un altre rang de valors dins dels paràmetres que ha establert l'organització.

A continuació, s'han buscat les amenaces que poden arribar a afectar els actius anteriors i se n'ha fet una llista a la columna de l'esquerra.

El pas següent consisteix a identificar les vulnerabilitats que hi ha entre cada amenaça i cadascun dels actius anteriors (correspon al valor que apareix primer en cada amenaça per a cada actiu).

Una vegada acabat aquest pas, s'estima l'impacte que provocarà aquesta amenaça en l'organització en cas que arribi a passar, i s'introdueix en la casella que hi ha a la dreta de la de vulnerabilitat.

Finalment, es multiplica els tres valors i obtenim el risc (és el valor que hi ha a la casella inferior per a cada encreuament d'actiu i amenaça) que té cada actiu. Aquest resultat és el valor anual, ja que les vulnerabilitats estan expressades en nombre de vegades d'ocurrència per any.

Quan ja tenim identificats aquests riscos, es fa la suma de tots plegats tant en horitzontal (risc a què s'està exposat per cada amenaça) com en vertical (riscos que té cadascun dels actius de l'organització).

A partir d'aquest moment, ja tenim els riscos intrínsecs, i s'ha de determinar el llindar de risc que marca l'organització i analitzar, per a cadascuna de les situacions anteriors, especialment o prioritàriament les que ultrapassen aquest llindar de risc, quins controls de seguretat permetran reduir aquests riscos, quant menys per sota del llindar se situaran i, entre totes les solucions possibles, seleccionar la que redueix el risc en un percentatge més gran amb un cost més petit per a l'organització.

Conclusions de Magerit

Com hem vist, la metodologia Magerit té com a gran virtut que els resultats que s'ofereixen estan expressats econòmicament. Això té com a avantatge que és fàcilment defensable davant la direcció, ja que la direcció és qui ha d'acceptar i assumir els riscos a què està exposada l'organització i qui ha de gastar uns recursos determinats per a reduir aquests riscos.

En canvi, el principal inconvenient que té és que tractar els actius prenent com a base la valoració econòmica fa que el mètode sigui més costós, ja que fer l'estimació econòmica de determinats actius és laboriós.

4.2. NIST 800-30

Aquesta metodologia és americana, està desenvolupada pel NIST (National Institute for Standards and Technology) i té l'avantatge que les valoracions que es fan no són econòmiques, sinó que són més qualitatives. Atès que és una metodologia americana, només està disponible en anglès.

Els passos dels que es compon aquesta metodologia són similars als d'altres metodologies, i hi ha guies que es poden utilitzar com a suport per a la seva execució. Un exemple és NIST 800-37.

Podreu trobar tant NIST 800-30 com NIST 800-37 a l'enllaç següent: https://csrc.nist.gov/publications/sp800.

4.3. CRAMM

Aquesta metodologia és britànica i la característica principal que té és l'ús de valoracions numèriques per a calcular els riscos a què està exposada una organització.

Els valors que es requereixen per a aplicar CRAMM són els següents:

- **Valoracions dels actius**. Enteses com el valor que té aquest actiu dins de l'abast que s'estudia.

- **Estimació de les probabilitats**. Entesa com la probabilitat que una amenaça, aprofitant una vulnerabilitat, danyi un determinat actiu.

- **Estimació dels impactes**. Entesa com les conseqüències que tindrà per a l'organització el fet que una amenaça aprofiti una vulnerabilitat per a danyar un actiu.

Les valoracions que s'han d'assignar en utilitzar CRAMM solen ser d'1 a 5. El valor d'1 és l'actiu amb menys valor, o la probabilitat més baixa que una determinada amenaça afecti l'organització, o l'impacte més petit que es pot provocar en una organització.

De la mateixa manera, el valor de 5 és l'actiu que té el màxim valor per a l'organització, o la probabilitat més elevada que arribi a passar una incidència, o l'impacte més gran que pugui provocar.

Per a calcular el risc a què està exposat un actiu davant aquestes amenaces i les vulnerabilitats que té, l'única cosa necessària és sumar aquests tres valors.

valor + probabilitat + impacte

Arran d'aquestes possibilitats, el rang de valors per a identificar els riscos va des del més petit, que és de 3, fins al més gran, que equival a 15.

El quadre resultant d'aquests riscos és el següent:

Probabilitat	1					2					3					4					5				
Impacte / Valor	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
1	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
2	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12
3	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13
4	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14
5	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15

De 3 a 7	No cal control
De 8 a 10	Control recomanat
D'11 a 15	Control obligatori

Segons aquest gràfic, el que s'ha d'assignar és el llindar de riscos per a cada organització. En aquest cas, l'organització ha estimat que els riscos inacceptables, i per tant els que obligatòriament necessiten implantar una mesura de seguretat, són els valors que hi ha entre l'11 i el 15 (tots dos inclosos). Després, en un segon nivell, vénen els controls recomanables, és a dir, els que, una vegada l'organització ha reduït tots els riscos anteriors, ha de mirar d'implantar si és que té recursos per a fer-ho. Són els riscos que hi ha entre el valor 8 i el 10. Finalment, queden els riscos menors, que com a tals no requereixen protecció, ja que és possible que la protecció mateixa sigui més costosa que el risc en si (de 3 a 7).

En aquest sentit, ha de quedar molt clar que l'acció prioritària de la gestió dels riscos és reduir els que hi ha per sobre del llindar de riscos i que la secundària, si és possible, és reduir els menys amenaçadors. No és lògic que es redueixi un risc de segon nivell si encara queden riscos inacceptables per contrarestar.

4.3.1. Valoracions de CRAMM

Aquesta metodologia té com a gran avantatge el fet que és fàcil d'aplicar, ja que no entra en valoracions econòmiques com Magerit, la qual cosa fa que sigui més senzill assignar valors als actius. Alhora, identifica dins dels diferents nivells dels riscos la priorització de cadascun d'aquests riscos, cosa que també permet Magerit però en canvi no NIST.

L'inconvenient és que els resultats que s'expressen estan indicats en nombres, cosa que no reflecteix realment la dimensió del risc a què està exposada una organització, ja que, en comparació de Magerit, parlar d'un risc de 12 no és el mateix que parlar d'un risc de 23.000 €. Per això, aquesta metodologia porta associat un segon procés que consisteix a traduir aquests riscos a unes valoracions econòmiques, de manera que siguin defensables davant la direcció.

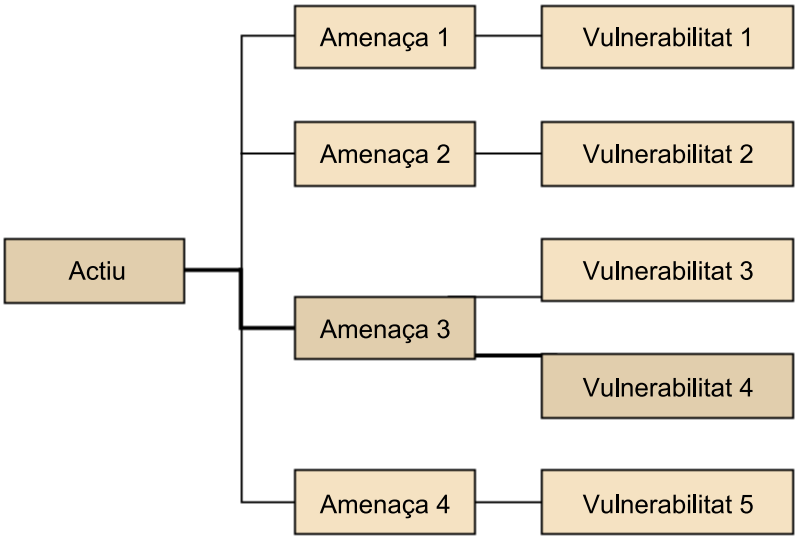
4.4. Octave

Aquesta metodologia és britànica, igual que CRAMM, però té una manera de representar els riscos a què està exposada una organització ben diferent de les anteriors.

Octave requereix entrar en un procés iteratiu de revisió per mirar d'obtenir una reducció de tots els riscos a què està exposada una organització.

La metodologia s'acaba traduint en la construcció d'un arbre de riscos en què queda marcat quin és el camí més crític davant el qual ha d'actuar primer l'organització. Una vegada s'aconsegueix reduir aquest risc, és necessari que es repeteixi l'estudi per a tornar a trobar el camí crític següent, i així successivament fins a reduir tots aquests riscos.

El resultat acaba essent el següent:



Després d'aplicar aquesta metodologia, Octave ens indica la primera actuació que ha de dur a terme una organització si vol reduir els riscos a què està sotmesa. No és que la resta de riscos no siguin importants: simplement indica que hi ha una determinada combinació que és la que té un risc més elevat.

4.4.1. Conclusions d'Octave

Aquesta metodologia té com a aspecte positiu que és necessari centrar-se a analitzar totes les situacions amb el detall que requereixen altres metodologies. En canvi, té com a gran inconvenient que s'ha de completar un cicle de revisió de l'anàlisi per a acabar d'identificar tots els riscos que en cada ocasió són els més crítics.

5. Normatives

Relacionat amb la gestió de riscos, cal destacar l'existència de diferents estàndards internacionals que aporten directrius de com realitzar una anàlisi de riscos alineada als estàndards de seguretat de la informació, que són els següents:

- **ISO 27005**. La norma ISO 27005 conté **diferents recomanacions i directrius generals** per a la gestió de risc en sistemes de gestió de seguretat de la informació. És compatible amb els conceptes generals especificats en la norma ISO 27001 i es troba dissenyada com a suport per a aplicar de forma satisfactòria un SGSI basat en l'enfocament de gestió de risc. No obstant això, la versió actual de l'ISO 27005 (del 2011), no està alineada amb l'actual ISO 27001:2013.

- **ISO 31000**. L'ISO 31000 estableix els principis, el marc i un procés per a la gestió de qualsevol tipus de risc en una forma transparent, sistemàtica i fiable en qualsevol àmbit o context (entenent risc com la incertesa en l'assoliment dels objectius). A més, permet que totes les empreses puguin comparar el seu sistema de gestió de riscos amb un únic punt de referència reconegut internacionalment.

Activitats

L'empresa en què treballeu, Serveis, SL, ha decidit posar en marxa un sistema d'informació que oferirà serveis d'allotjament amb explotació o *hosting* i d'allotjament sense explotació o *housing* als seus clients, ja que són serveis que se sol·liciten sovint. S'ha pensat a donar un servei 7 × 24:

- **Personal**:
  - Responsable de projecte
  - **3 + 3 operadors** (entre setmana: 3 torns diaris; en cap de setmana: 3 persones, distribuïdes segons la seva conveniència)
  - **2 becaris** (suport)

- **Equipament**:
  - 4 estacions de treball
  - 1 servidor que conté 1 servidor de DNS, 1 servidor de bases de dades (MySQL), 1 servidor web (Apache), 1 impressora i 1 servidor d'aplicacions (Tomcat)
  - 1 aire condicionat

Tot està inclòs dins de la xarxa corporativa com un segment o uns segments de xarxa més. La direcció vol avaluar si és viable el projecte amb el pressupost de què disposa, fent una anàlisi de riscos realista. A més, vol evitar el possible robatori d'informació.

- Analitzeu els riscos intrínsecs d'aquest sistema i proposeu-hi solucions.
- Analitzeu els riscos residuals després d'aplicar les contramesures proposades en l'anàlisi de riscos intrínsecs.

(L'exercici s'ha de fer triant una de les metodologies que s'han explicat en el mòdul. S'han de justificar i explicar les solucions triades, i també les conclusions obtingudes.)