PROJECTE 1
DOCUMENTACIÓ ESTRATÈGICA, GESTIÓ DEL RISC I CONTINUÏTAT DEL NEGOCI

Curs: PQTM 19. Tècnic/a en Ciberseguretat

Ivan Ricart Borges iricartb@uoc.edu

ÍNDEX

1. ANÀLISI I GESTIÓ DELS RISCOS

1.1. INTRODUCCIÓ

A finals del segle XX degut a que la presència dels riscos informàtics dintre de les organitzacions són cada cop més freqüents, el seu estudi es comença a valorar amb gran importància. Un bon estudi que contempli els actius de l'organització, les vulnerabilitats i les amenaces, proporcionarà una eina molt important per l'organització per anticipar-se a la materialització d'aquestes en el futur. Per protegir les vulnerabilitats dels actius de les amenaces mitjançant controls o salvaguardes es necessari un cost inicial, temps i dedicació, però hem de dir que el seu benefici pot ser incalculable a curt o llarg termini, i que per tant, tota organització que vulgui protegir els seus actius hauria de contemplar.

1.2. DETERMINAR L'ABAST DEL PROJECTE

Abans de començar amb l'anàlisi de riscos, s'ha de definir l'abast del projecte per proporcionar una idea general sobre els punts que es desitgen controlar, per tant, s'estudiaran aquells punts que es consideren importants pel correcte funcionament de la universitat, com per exemple, els serveis interns (telefonia, internet, ensenyament en línia, correu electrònic i fitxers en xarxa), les aplicacions, els equips, les comunicacions, l'equipament auxiliar i el personal.

1.3. ETAPA D'ANÀLISI DE RISCOS

Podríem definir la etapa d'anàlisi de riscos com el primer pas a seguir en la seguretat informàtica, el mateix que busca establir la probabilitat d'ocurrència dels riscos i l'impacte de les seves conseqüències, qualificant-les i avaluant-les amb el fi d'obtindre informació per establir el nivell de risc i les accions que s'implementaran.

S'estudien tots els controls de seguretat, tant físics com tècnics d'una empresa amb la finalitat de protegir l'ambient informàtic, d'aquesta manera s'obté una visió mes pròxima de la realitat sobre l'estat actual de seguretat de l'organització. Es responsabilitat dels actors de seguretat que treballen en l'organització, realitzar l'anàlisi de riscos amb els responsables de cada àrea, ells són coneixedors dels riscos els quals estan exposats i que per tant poden ajudar a mitigar-los. Finalment podem dir que l'anàlisi de riscos ajuda als gerents a tindre una previsió de la inversió necessària a realitzar per implementar el nivell de seguretat desitjat.

Degut a la seva complexitat i la brevetat de temps que tenim, en aquest estudi **no avaluarem** numèricament els impactes, i per tant el nivell de risc que pot ocasionar, però si que identificarem els actius, els avaluarem, identificarem les amenaces, la freqüència d'ocurrència i la degradació i finalment els controls a establir per mitigar el nivell de risc de l'organització.

1.3.1. IDENTIFICACIÓ DELS ACTIUS

Un actiu es tot allò que representa un valor dintre de l'organització (la informació es pot considerar l'actiu principal més important), necessiten de protecció per assegurar les operacions del negoci i la continuïtat de la empresa. La identificació correcta dels actius permet identificar les amenaces i escollir els controls o salvaguardes necessaris per protegir-los.
Dintre de la universitat hem considerat com a mètode d'estudi els actius especificats en l'apartat de l'abast i que es mostraran a continuació.

1.3.1.1. [IS] SERVEIS INTERNS

Com a serveis interns que presta la universitat, podem citar els següents:

- [IS_TEL]: Telefonia IP
- [IS_INT]: Internet
- [IS_MDL]: Sistema d'ensenyament en línia (Moodle)
- [IS_MAI]: Correu electrònic (Extern)
- [IS_FS]: Fitxers en xarxa

1.3.1.2. [SW] APLICACIONS

Com a principals aplicacions, podem citar les següents:

- [SW_OS]: Sistemes operatius
- [SW_OFM]: Ofimàtica
- [SW_AV]: Antivirus
- [SW_OTR]: Altres

1.3.1.3. [HW] EQUIPS

Com a equips informàtics, podem citar els següents:

- [HW_SRV_VOIP]: Servidors VoIP
- [HW_SRV_AD]: Servidors AD
- [HW_SRV_WEB]: Servidors WEB
- [HW_SRV_SQL]: Servidors SQL
- [HW_SRV_FS]: Servidors FS
- [HW_SRV_BKP]: Servidors BKP
- [HW_SRV_OTR]: Altres servidors (DNS, DHCP, SQUID, WSUS ...)
- [HW_FRW]: Firewalls

- [HW_RTR]: Routers
- [HW_PC]: Computadores d'escriptori
- [HW_PRN]: Serveis d'impressió

1.3.1.4. [COM] COMUNICACIONS

Com a mitjà de transport de la informació, podem citar els següents:

- [COM_TEL]: Telefonia IP
- [COM_LAN]: Xarxa LAN
- [COM_WFI]: Xarxa WIFI
- [COM_INT]: Xarxa Internet

1.3.1.5. [AUX] EQUIPS AUXILIARS

Com a equips auxiliars, podem citar els següents:

- [AUX_SAI]: Alimentació ininterrompuda
- [AUX_CBL]: Cablejat
- [AUX_SEC]: Sistemes de vigilància
- [AUX_OTR]: Altres

1.3.1.6. [EMP] PERSONAL

Com a personal involucrat en aquesta investigació, podem citar els següents:

- [EMP_MNG]: Encarregats en la gestió
- [EMP_TCH]: Encarregats en l'ensenyament

1.3.2. VALORACIÓ DELS ACTIUS

Una vegada s'han identificats els actius que es volen protegir, posteriorment s'han de valorar segons el seu grau d'importància, tenint en compte com a dimensions a avaluar, la disponibilitat, la integritat, la confidencialitat, la autenticitat i la traçabilitat.

La valoració pot ser quantitativa (escala amb una quantitat numèrica) o bé qualitativa (escala de nivells), com per exemple: nivell baix, nivell mitjà, nivell alt o bé el rang numèric de 0 a 10.

La valoració ha de ser la més objectiva possible, s'hauria de comptar amb la involucració de totes les àrees de l'organització per a que ens proporcionin un resultat coherent i que s'apropi el màxim possible a la realitat.

Per indicar el nivell d'importància dels actius dintre de l'organització, hem fet ús d'una escala de

quantitats numèriques, on el rang de valors, es comprèn del 0 al 10, cal mencionar que la eina **PILAR** es un bon referent per realitzar aquest estudi.

NIVELL	CRITERI
10	Crític
9	Molt Alt (+)
8	Molt Alt (-)
7	Alt (+)
6	Alt (-)
5	Mitjà (+)
4	Mitjà
3	Mitjà (-)
2	Baix (+)
1	Baix (-)
0	Despreciable

Eina PILAR v7.3.1

Com hem comentat anteriorment, de cada actiu avaluarem, sempre i quan aquest sigui rellevant, la disponibilitat, la integritat, la confidencialitat, la autenticitat i la traçabilitat.

[D]	Disponibilitat	La disponibilitat és l'assegurament de que els usuaris autoritzats tenen accés, quant ho necessitin, a la informació i als actius associats. La disponibilitat d'un sistema implica que, tant el hardware, com el software, es mantinguin funcionant correctament, eficaçment i que sigui capaç de recuperar-se davant d'una fallida.
[I]	Integritat	La integritat significa que la informació no hagi sigut esborrada, copiada o modificada, durant el seu trajecte d'origen cap a destí.
[C]	Confidencialitat	Es pot definir la confidencialitat, com la privacitat o el secret de guardar la informació, degut això, un requisit indispensable és que només aquelles persones autoritzades puguin accedir a la informació.
[A]	Autenticitat	La autenticitat fa referència als mecanismes de seguretat dels equips que utilitzem per comunicar-nos, permitent-nos verificar si l'origen de les dades és el correcte, qui ens ho va enviar i quant van ser enviats i rebuts.

[T] Traçabilitat	La traçabilitat és la capacitat de reproduir l'historial d'un producte per poder localitzar ràpidament l'origen dels problemes.

ACTIUS	DIMENSIONS				
	[D]	[I]	[C]	[A]	[T]
[IS] Serveis Interns					
[IS_TEL] Telefonia IP	7			7	7
[IS_INT] Internet	8			8	8
[IS_MDL] Sistema d'ensenyament en línia (Moodle)	9	9	9	9	9
[IS_MAI] Correu electrònic (Extern)	8	8	8	8	8
[IS_FS] Fitxers en xarxa	7	7	7	7	7
[SW] Aplicacions					
[SW_OS] Sistemes operatius					8
[SW_OFI] Ofimàtica					7
[SW_AV] Antivirus					7
[SW_OTR] Altres					4
[HW] Equips					
[HW_SRV_VOIP] Servidors VoIP	7	7	7	7	7
[HW_SRV_AD] Servidors AD	8	8	8	8	8
[HW_SRV_WEB] Servidors WEB	9	9	9	9	9
[HW_SRV_SQL] Servidors SQL	9	9	9	9	9
[HW_SRV_BKP] Servidors BKP	8	8	8	8	8
[HW_SRV_OTR] Altres servidors	7	7	7	7	7
[HW_FRW] Firewalls					8
[HW_RTR] Routers					8
[HW_PC] Computadores d'escriptori					7
[HP_PRN] Serveis d'impressió					6
[COM] Comunicacions					
[COM_TEL] Telefonia IP		7	7		
[COM_LAN] Xarxa LAN					7
[COM_WFI] Xarxa WIFI					7
[COM_INT] Xarxa Internet		8	8		
[AUX] Equips auxiliars					
[AUX_SAI] Alimentació ininterrompuda	7				
[AUX_CBL] Cablejat	7				
[AUX_SEC] Sistemes de vigilància	7				
[AUX_OTR] Altres	6				
[EMP] Personal					

[EMP_MNG] Encarregats en la gestió		8	
[EMP_TCH] Encarregats en l'ensenyament		8	

1.3.3. DETERMINACIÓ DE LES AMENACES

Una amenaça es un perjudici potencial provocat per un incident desitjat o no desitjat, la seva materialització depèn de la existència d'una vulnerabilitat, la qual un cop efectuada, podria provocar un problema important (disponibilitat, integritat, confidencialitat o autenticitat) sobre l'actiu.

Segons la eina **PILAR** v7.3.1 estandarditzada per MAGERIT, les amenaces es classifiquen en cinc grups:

- [N] Desastres Naturals
- [I] D'origen Industrial
- [E] Errors i falles no intencionades
- [A] Atacs intencionats
- [PR] Riscos de privacitat

1.3.4. IDENTIFICACIÓ DE LES AMENACES

En el següent llistat es mostren les amenaces identificades amb un cert grau d'importància o probabilitat d'ocurrència, per cada un dels actius.

ACTIUS	AMENACES
[IS] Serveis Interns	
[IS_TEL] Telefonia IP	[I.5] Avaria d'origen físic o lògic [E.2] Errors del administrador del sistema / de la seguretat [E.20] Vulnerabilitats en els programes (software) [E.21] Errors de manteniment / actualització de programes (software) [A.24] Denegació del servei
[IS_INT] Internet	[A.7] Ús no previst
[IS_MDL] Ensenyament en línia	[I.5] Avaria d'origen físic o lògic [E.20] Vulnerabilitats en els programes (software) [E.21] Errors de manteniment / actualització de programes (software) [A.24] Denegació del servei
[IS_MAI] Correu electrònic	[E.4] Errors de configuració

[IS_FS] Fitxers en xarxa	[I.5] Avaria d'origen físic o lògic [E.19] Fugues d'informació [E.20] Vulnerabilitats en els programes (software) [E.21] Errors de manteniment / actualització de programes (software) [A.24] Denegació del servei
[SW] Aplicacions	
[SW_OS] Sistemes operatius	[E.1] Errors dels usuaris [E.8] Difusió de software perillós [E.20] Vulnerabilitats en els programes (software) [E.21] Errors de manteniment / actualització de programes (software) [Parcial, organització amb actualitzacions centralitzades, principalment sistemes Windows] [A.7] Ús no previst
[SW_OFI] Ofimàtica	[E.1] Errors dels usuaris [E.20] Vulnerabilitats en els programes (software) [E.21] Errors de manteniment / actualització de programes (software) [A.8] Difusió de software perillós
[SW_AV] Antivirus	[E.20] Vulnerabilitats en els programes (software) [E.21] Errors de manteniment / actualització de programes (software)
[SW_OTR] Altres	[E.8] Difusió de software perillós [E.20] Vulnerabilitats en els programes (software) [E.21] Errors de manteniment / actualització de programes (software)
[HW] Equips	
[HW_SRV_VOIP] Servidors VoIP [HW_SRV_AD] Servidors AD [HW_SRV_WEB] Servidors WEB [HW_SRV_SQL] Servidors SQL [HW_SRV_BKP] Servidors BKP [HW_SRV_OTR] Altres servidors	[N.1] Focs [N.2] Danys per aigua [N.*] Desastres naturals [I.3] Contaminació mediambiental [I.5] Avaria d'origen físic o lògic [I.7] Condicions inadequades de temperatura o humitat [E.2] Errors del administrador del sistema / de la seguretat. [E.23] Errors de manteniment / actualització d'equips (hardware) [A.11] Accés no autoritzat

[HW_FRW] Firewalls	[N.1] Focs
[HW_RTR] Routers	[N.2] Danys per aigua
	[N.*] Desastres naturals
	[I.3] Contaminació mediambiental
	[I.5] Avaria d'origen físic o lògic
	[I.7] Condicions inadequades de temperatura o humitat
	[E.2] Errors del administrador del sistema / de la seguretat
	[A.11] Accés no autoritzat
[HW_PC] Computadores d'escriptori	[N.1] Focs
	[N.2] Danys per aigua
	[N.*] Desastres naturals
	[I.*] Desastres industrials
	[I.5] Avaria d'origen físic o lògic
	[I.7] Condicions inadequades de temperatura o humitat
	[E.23] Errors de manteniment / actualització d'equips (hardware)
	[E.24] Caiguda del sistema per esgotament dels recursos
	[A.7] Ús no previst
	[A.25] Robatori d'equips
[HP_PRN] Serveis d'impressió	[I.5] Avaria d'origen físic o lògic
	[I.7] Condicions inadequades de temperatura o humitat
	[E.23] Errors de manteniment / actualització d'equips (hardware)
[COM] Comunicacions	
[COM_TEL] Telefonia IP	[I.8] Fallida de serveis de comunicacions
	[E.9] Errors de [re-]encaminament
	[E.10] Errors de seqüència
	[E.15] Alteració de la informació
	[E.19] Fugues d'informació
	[A.7] Ús no previst
	[A.9] [Re-]encaminament de missatges
	[A.10] Alteració de seqüència
	[A.12] Anàlisi del tràfic
	[A.14] Intercepció de la informació
[COM_LAN] Xarxa LAN	[I.8] Fallida de serveis de comunicacions
[COM_WFI] Xarxa WIFI	
[COM_INT] Xarxa Internet	

[AUX] Equips auxiliars	
[AUX_SAI] Alim. ininterrompuda	[I.3] Contaminació mediambiental
[AUX_CBL] Cablejat	[I.3] Contaminació mediambiental
[AUX_SEC] Sistemes de vigilància	[I.7] Condicions inadequades de temperatura o humitat
	[E.23] Errors de manteniment / actualització d'equips (hardware)
[AUX_OTR] Altres	[I.3] Contaminació mediambiental
[EMP] Personal	
[EMP_MNG] Enc. en la gestió	[E.28.1] Malaltia
[EMP_TCH] Enc. en l'ensenyament	[A.29] Extorsió
	[A.30] Enginyeria social (engany)

1.3.5. VALORACIÓ DE LES AMENACES

En la valoració de les amenaces s'equilibren totes les possibles amenaces que puguin afectar en alguna de les dimensions de valoració d'un actiu. Per a fer una valoració més exacta es necessari estimar la freqüència d'ocurrència i el percentatge de degradació.

FREQÜÈNCIA D'OCURRÈNCIA	
CS	Casi Segur
MA	Molt Alt
P	Possible
PP	Poc Probable
MB	Segles
MR	Molt Rara
0	

Eina PILAR v7.3.1

PERCENTATGE DE DEGRADACIÓ	
MA	Molt Alt
A	Alt
M	Mitjà
B	Baix
MB	Molt Baix
0	

Eina PILAR v7.3.1

ACTIUS	AMENACES	FREQ.	[D]	[I]	[C]	[A]	[T]
[IS] Serveis Interns							
[IS_TEL] Telefonia IP	[I.5]	P	A	-	-	-	-
	[E.2]	P	M	M	M	-	-
	[E.20]	P	B	M	M	-	-
	[E.21]	P	B	B	M	-	-
	[A.24]	PP	MA	-	-	-	-
[IS_INT] Internet	[A.7]	P	M	M	M	-	-
[IS_MDL] Ensenyament en línia	[I.5]	P	A	-	-	-	-
	[E.20]	P	B	M	M	-	-
	[E.21]	P	B	B	M	-	-
	[A.24]	PP	MA	-	-	-	-
[IS_MAI] Correu electrònic	[E.4]	MR	A	-	-	-	-
[IS_FS] Fitxers en xarxa	[I.5]	P	A	-	-	-	-
	[E.20]	P	B	M	M	-	-
	[E.21]	P	B	B	M	-	-
	[E.19]	P	-	-	M	-	-
	[A.24]	PP	MA	-	-	-	-
[SW] Aplicacions							
[SW_OS] Sistemes operatius	[E.1]	PP	M	M	M	-	-
	[E.8]	PP	B	B	B	-	-
	[E.20]	MA	B	M	M	-	-
	[E.21]	PP	M	B	-	-	-
	[A.7]	P	B	B	B		-
[SW_OFI] Ofimàtica	[E.1]	P	M	M	M	-	-
	[E.20]	P	M	M	M	-	-
	[E.21]	PP	M	B	-	-	-
	[A.8]	PP	B	B	B	-	-
[SW_AV] Antivirus	[E.20]	P	M	M	M	-	-
	[E.21]	P	M	M	-	-	-
[SW_OTR] Altres	[E.8]	PP	B	B	B	-	-
	[E.20]	PP	B	B	B	-	-
	[E.21]	PP	M	M	-	-	-
[HW] Equips							
[HW_SRV_VOIP] Servidors VoIP	[N.1]	PP	A	-	-	-	-
[HW_SRV_AD] Servidors AD	[N.2]	PP	A	-	-	-	-
[HW_SRV_WEB] Servidors WEB	[N.*]	PP	A	-	-	-	-

[HW_SRV_SQL] Servidors SQL	[I.3]	PP	A	-	-	-	-
[HW_SRV_BKP] Servidors BKP	[I.5]	P	A	-	-	-	-
[HW_SRV_OTR] Altres servidors	[I.7]	P	MA	-	-	-	-
	[E.2]	P	M	M	M	-	-
	[E.23]	P	M	-	-	-	-
	[A.11]	PP	-	A	A	-	-
[HW_FRW] Firewalls	[N.1]	PP	A	-	-	-	-
[HW_RTR] Routers	[N.2]	PP	A	-	-	-	-
	[N.*]	PP	A	-	-	-	-
	[I.3]	PP	A	-	-	-	-
	[I.5]	P	M	-	-	-	-
	[I.7]	P	M	-	-	-	-
	[E.2]	P	M	M	M	-	-
	[A.11]	PP	-	B	B	-	-
[HW_PC] Computadores d'escriptori	[N.1]	PP	A	-	-	-	-
	[N.2]	PP	A	-	-	-	-
	[N.*]	PP	A	-	-	-	-
	[I.*]	PP	A	-	-	-	-
	[I.5]	P	M	-	-	-	-
	[I.7]	PP	M	-	-	-	-
	[E.23]	P	M	-	-	-	-
	[E.24]	P	M	-	-	-	-
	[A.7]	P	M	B	M	-	-
	[A.25]	PP	M	-	-	-	-
[HP_PRN] Serveis d'impressió	[I.5]	P	M	-	-	-	-
	[I.7]	P	M	-	-	-	-
	[E.23]	P	M	-	-	-	-
[COM] Comunicacions							
[COM_TEL] Telefonia IP	[I.8]	PP	M	-	-	-	-
	[E.9]	P	-	-	M	-	-
	[E.10]	P	-	M	-	-	-
	[E.15]	P	-	A	-	-	-
	[E.19]	P	-	-	M	-	-
	[A.7]	P	-	M	M	-	-
	[A.9]	P	-	-	M	-	-
	[A.10]	P	-	M	-	-	-
	[A.12]	P	-	-	A	-	-

	[A.14]	P	-	-	A	-	-
[COM_LAN] Xarxa LAN	[I.8]	P	B	-	-	-	-
[COM_WFI] Xarxa WIFI	[I.8]	P	M	-	-	-	-
[COM_INT] Xarxa Internet	[I.8]	P	A	-	-	-	-
[AUX] Equips auxiliars							
[AUX_SAI] Alim. ininterrompuda	[I.3]	PP	M	-	-	-	-
[AUX_CBL] Cablejat	[I.3]	PP	A	-	-	-	-
	[I.7]	P	M	-	-	-	-
	[E.23]	P	M	-	-	-	-
[AUX_SEC] Sistemes de vigilància	[I.3]	PP	M	-	-	-	-
	[I.7]	P	M	-	-	-	-
[AUX_OTR] Altres	[I.3]	P	M	-	-	-	-
[EMP] Personal							
[EMP_MNG] Enc. en la gestió	[E.28.1]	P	M	M	M	-	-
	[A.29]	PP	M	M	M	-	-
	[A.30]	P	M	M	M	-	-
[EMP_TCH] Enc. en l'ensenyament	[E.28.1]	PP	M	M	M	-	-
	[A.29]	PP	M	M	M	-	-
	[A.30]	P	M	M	M	-	-

1.3.6. IDENTIFICACIÓ DE LES SALVAGUARDES O CONTROLS

Les salvaguardes es defineixen com aquells procediments o mecanismes tecnològics que redueixen el risc, es a dir, la materialització d'una amenaça cap a una vulnerabilitat. En aquesta secció s'identificaran les salvaguardes efectives per l'organització per mitigar el risc.

ACTIUS	AMENACES	SALVAGUARDES
[IS] Serveis Interns		
[IS_TEL] Telefonia IP	[I.5] [E.2] [E.20] [E.21] [A.24]	[S.SC] S'apliquen perfils de seguretat [SW.CM.3] Es fa un seguiment permanent de les actualitzacions [SW.CM.4] Avaluació del impacte i del risc residual després de l'actualització. [SW.CM.a] Control de versions de tota actualització de software [SW.CM.e] Es prova anteriorment en un equip que no està en producció

		[S.cont.1] Protecció a atacs de denegació de servei (DoS)
La telefonia IP és el servei amb més mancances de seguretat dintre de l'organització, s'han d'aplicar perfils de seguretat degut a que el software que gestiona la centraleta IP utilitza comptes d'usuari estàndards, usuaris administratius de personal que actualment no hi treballa, permisos d'usuari assignats de forma incorrecta, etc. També s'ha de controlar i fer seguiment de les actualitzacions de software, d'aquesta manera reduirem el risc d'explotació de noves vulnerabilitats i finalment intentar reduir el risc de que es produeixi un atac de denegació de servei.		
[IS_INT] Internet	[A.7]	[PDS.www.3] Eina de control de continguts amb filtres actualitzats [Actualitzar els filtres dels servidors SQUID]
L'internet és un servei bastant controlat dintre de l'organització, la universitat fa ús de servidors Nagios per controlar els terminals i la intranet en general, d'aquesta manera pot analitzar el tràfic, les accions que duen a cap els usuaris i així posteriorment introduir mesures de seguretat en el cas de que aquestes siguin sospitoses, també fa ús de servidors SQUID per millorar la experiència de navegació, es a dir, el seu rendiment i a més a més poder filtrar els continguts per assegurar una navegació segura. El problema principal radica en que aquests filtratges no estan actualitzats i existeix el risc de poder accedir a pàgines web fraudulentes.		
[IS_MDL] Ensenyament en línia	[I.5] [E.20] [E.21] [A.24]	[SW.CM.3] Es fa un seguiment permanent de les actualitzacions [SW.CM.4] Avaluació del impacte i del risc residual després de l'actualització. [SW.CM.a] Control de versions de tota actualització de software [SW.CM.e] Es prova anteriorment en un equip que no està en producció [S.cont.1] Protecció a atacs de denegació de servei (DoS)
El servei d'ensenyament en línia, en aquest cas el Moodle, és un dels serveis més importants que proporciona la universitat, el desenvolupament és extern però la obligació de mantindre'l actualitzat recau sobre el personal de manteniment d'aplicacions informàtiques, és necessari estar al corrent de les últimes versions per conèixer les seves millores i les possibles correccions d'errors de seguretat. Hem de pensar que aquest servei és visible fora de l'organització, així els docents poden estar al corrent de les tasques a realitzar i poder consultar el material, però alhora, això comporta un gran risc degut a que qualsevol persona, sigui o no alumnat, pot intentar explotar la existència d'alguna vulnerabilitat del servidor web o bé del software Moodle.		
[IS_MAI] Correu electrònic (Extern)	[E.4]	[SW.CM.h.1] Es documenten totes les

		modificacions [SW.CM.h.2] S'actualitza la documentació del sistema
El correu electrònic també és un servei molt important per l'organització, és el principal mecanisme de comunicació, cal dir que no existeixen servidors propis de correu electrònic, però això no obliga a estar exempt de responsabilitat de gestionar la seva seguretat, degut això, és responsabilitat del personal encarregat de l'administració de sistemes, documentar totes les accions necessàries de configuració per garantir el seu correcte funcionament (registres DNS, filtres SPAM, etc.).		
[IS_FS] Fitxers en xarxa	[I.5] [E.19] [E.20] [E.21] [A.24]	[SW.CM.3] Es fa un seguiment permanent de les actualitzacions [SW.CM.4] Avaluació del impacte i del risc residual després de l'actualització. [SW.CM.a] Control de versions de tota actualització de software [SW.CM.e] Es prova anteriorment en un equip que no està en producció [PS.AT] Formació i conscienciació [S.cont.1] Protecció a atacs de denegació de servei (DoS)
El servei de fitxers és una eina important per gestionar l'organització, per exemple, per compartir informació entre departaments, entre d'altres, però com aquest emmagatzema informació privada, pot existir conscient o inconscientment el risc de fuga d'informació, degut això, s'han d'impartir cursos de formació i conscienciació, per donar una visió més amplia del tractament d'aquestes dades i la conscienciació sobre les conseqüències derivades del seu incompliment.		
[SW] Aplicacions		
[SW_OS] Sistemes operatius	[I.5] [E.1] [E.8] [E.20] [E.21] [A.7]	[S.SC] S'apliquen perfils de seguretat [SW.SC.1] Es redueixen les opcions a les mínimes necessàries [SW.CM.3] Es fa un seguiment permanent de les actualitzacions [SW.CM.4] Avaluació del impacte i del risc residual després de l'actualització [SW.CM.a] Control de versions de tota actualització de software [SW.CM.e] Es prova anteriorment en un equip que no està en producció
En l'organització s'utilitzen servidors Linux però les estacions de treball són majoritàriament Windows,		

les actualitzacions d'aquestes últimes estan centralitzades mitjançant servidors WSUS, però encara així s'han de valorar les actualitzacions del servidors de forma manual, es interessant que els sistemes operatius de les estacions de treball utilitzin les opcions mínimes necessàries, d'aquesta manera el seu rendiment serà major i el nombre de vulnerabilitats pot decréixer de forma considerable degut a que s'utilitzen els serveis mínims.		
[SW_OFI] Ofimàtica	[E.1] [E.20] [E.21] [A.8]	[S.SC] S'apliquen perfils de seguretat [SW.SC.1] Es redueixen les opcions a les mínimes necessàries [Evitar Macros] [SW.CM.3] Es fa un seguiment permanent de les actualitzacions [SW.CM.a] Control de versions de tota actualització de software
La ofimàtica és una eina indispensable per l'alumnat, el professorat i els empleats de gestió, per evitar possibles problemes ha d'estar correctament actualitzada, a més a més, de forma anàloga al punt anterior, és interessant utilitzar les opcions mínimes necessàries per defecte, per evitar la execució de macros o altres tipus de funcionalitats que poden ser perilloses.		
[SW_AV] Antivirus	[E.20] [E.21]	[SW.CM.3] Es fa un seguiment permanent de les actualitzacions. [SW.CM.a] Control de versions de tota actualització de software
Es interessant tindre els antivirus actualitzats, el nivell de perillositat avui en dia és molt alt, els mètodes de difusió dels virus són molt variats i la inexperiència o la bona voluntat dels usuaris provoquen que aquests compleixin la seva finalitat, a més a més, seria interessant contemplar eines de Antirandsom, ja que ha guanyat molta popularitat aquests darrers anys i els seus efectes poden ser devastadors.		
[SW_OTR] Altres	[E.8] [E.20] [E.21]	[SW.CM.3] Es fa un seguiment permanent de les actualitzacions [SW.CM.a] Control de versions de tota actualització de software
Les altres eines software també es important que estiguin actualitzades, normalment les últimes versions són les més protegides però també s'ha de valorar si són les més estables.		
[HW] Equips		
[HW_SRV_VOIP] Servidors VoIP [HW_SRV_AD] Servidors AD [HW_SRV_WEB] Servidors WEB [HW_SRV_SQL] Servidors SQL [HW_SRV_BKP] Servidors BKP	[N.1] [N.2] [N.*] [I.3] [I.5]	[L.6.2.c] Es disposa d'un sistema automàtic de detecció d'incendis [L.6.3.4] Es disposa d'un sistema de detecció d'inundacions [L.6.4] Protecció davant accidents naturals i

[HW_SRV_OTR] Altres servidors	[I.7] [E.2] [E.23] [A.11]	industrials [L.6.5] Protecció davant la contaminació mediambiental [HW.CM.3] Es segueixen les recomanacions del fabricant o proveïdor [HW.CM.4] Es fa un seguiment permanent d'actualitzacions [PPS.8] Control de claus, combinacions o dispositius de seguretat
Els servidors estan localitzats en sales independents, refrigerats correctament i amb alimentació ininterrompuda, però encara així, no estan exempts de les amenaces de tipus natural, com el foc, l'aigua, terratrèmols, etc. Actualment per accedir a les sales de servidors s'utilitzen claus físiques, seria interessant contemplar la possibilitat d'introduir mecanismes de control d'accés biomètrics, d'aquesta manera reduiríem, per exemple, el risc de duplicitat de claus.		
[HW_FRW] Firewalls [HW_RTR] Routers	[N.1] [N.2] [N.*] [I.3] [I.5] [I.7] [E.2] [A.11]	[L.6.2.c] Es disposa d'un sistema automàtic de detecció d'incendis [L.6.3.4] Es disposa d'un sistema de detecció d'inundacions [L.6.4] Protecció davant accidents naturals i industrials [L.6.5] Protecció davant la contaminació mediambiental [PPS.8] Control de claus, combinacions o dispositius de seguretat
Els firewalls i els routers són elements complexes e indispensables pel correcte funcionament d'una organització, estan exposats als riscos comentats anteriorment, de forma anàloga al punt anterior, aquests s'haurien de protegir de les amenaces naturals i dels accessos no autoritzats.		
[HW_PC] Computadores d'escriptori	[N.1] [N.2] [N.*] [I.*] [I.5] [I.7] [E.23] [E.24] [A.7]	[L.6.2.c] Es disposa d'un sistema automàtic de detecció d'incendis [L.6.3.4] Es disposa d'un sistema de detecció d'inundacions [L.6.4] Protecció davant accidents naturals i industrials [L.6.5] Protecció davant la contaminació mediambiental [HW.CM.3] Es segueixen les recomanacions del

	[A.25]	fabricant o proveïdor [HW.CM.4] Es fa un seguiment permanent d'actualitzacions [PPE.3] Els elements fàcils d'emportar s'encadenen
Les computadores d'escriptori també estan exposats als riscos comentats anteriorment, però a més a més cal contemplar el risc de que en les sales públiques poden produir-se robatoris, degut això es important contemplar mesures per evitar manipulacions i encadenar-los.		
[HP_PRN] Serveis d'impressió	[I.5] [I.7] [E.23]	[HW.CM.3] Es segueixen les recomanacions del fabricant o proveïdor [HW.CM.4] Es fa un seguiment permanent d'actualitzacions
Els serveis d'impressió també estan exposats als riscos anteriors, però actualment no es volen contemplar perquè són elements fàcilment substituïbles. Cal seguir les recomanacions del fabricant quan es necessita manipular el dispositiu (tòners, kits, etc.).		
[COM] Comunicacions		
[COM_TEL] Telefonia IP	[I.8] [E.9] [E.10] [E.15] [E.19] [A.7] [A.9] [A.10] [A.12] [A.14]	[COM.cont.7] Es realitzen copies de seguretat de la configuració (backup) [COM.cont.a.1] Es disposa de connexió redundant (mitjançant doble targeta de xarxa) dels dispositius crítics [COM.cont.a.3] Redundància dels enllaços amb repartiment de càrrega [COM.SC] S'apliquen perfils de seguretat [COM.SC.2] S'eliminen o modifiquen els usuaris estàndards [COM.SC.3] S'eliminen o modifiquen els usuaris administratius estàndards [COM.SC.4] Només els administradors de seguretat autoritzats poden modificar les configuracions [COM.SC.5] Els serveis activats es configuren de forma segura
Anteriorment s'ha comentat que la telefonia IP presenta mancances de seguretat, degut això s'han d'aplicar perfils de seguretat per mitigar els riscos d'errors de reencaminament, de seqüència, d'alteració de la informació, etc. Per garantir la seva disponibilitat es interessant realitzar copies de seguretat de les configuracions, disposar de connexions redundants, etc.		

[COM_LAN] Xarxa LAN [COM_WFI] Xarxa WIFI [COM_INT] Xarxa Internet	[I.8]	[COM.cont.7] Es realitzen copies de seguretat de la configuració (backup) [COM.cont.a.1] Es disposa de connexió redundant (mitjançant doble targeta de xarxa) dels dispositius crítics [COM.cont.a.3] Redundància dels enllaços amb repartiment de càrrega
Per garantir la disponibilitat de les diferents xarxes, de forma anàloga al punt anterior, es necessari realitzar copies de seguretat de les configuracions, disposar de connexions redundants, repartiment de càrrega per evitar una sobrecàrrega, etc.		
[AUX] Equips auxiliars		
[AUX_SAI] Alim. ininterrompuda	[I.3]	[L.6.5] Protecció davant la contaminació mediambiental
[AUX_CBL] Cablejat [AUX_SEC] Sistemes de vigilància	[I.3] [I.7] [E.23]	[L.6.5] Protecció davant la contaminació mediambiental [AUX.wires.4] Tots els elements de cablejat estan etiquetats
[AUX_OTR] Altres	[I.3]	[L.6.5] Protecció davant la contaminació mediambiental
Aquests elements estan exposats a diferents tipus de contaminació, degut això s'han de buscar mecanismes de protecció. Es important comentar que el cablejat ha d'estar degudament etiquetat, davant d'una avaria es pot reduir significativament el temps de resolució si en un principi es coneix la funcionalitat d'aquell cable.		
[EMP] Personal		
[EMP_MNG] Enc. en la gestió [EMP_TCH] Enc. en l'ensenyament	[E.28.1] [A.29] [A.30]	[PS.8] Procediments de prevenció i reacció [PS.8.3] davant extorsions [PS.8.4] davant atacs de enginyeria social
Es important la formació i la conscienciació del personal davant extorsions i atacs d'enginyeria social, aquests últims són molt efectius degut a que s'aprofita de la inexperiència o la bona voluntat de la persona, per tant, es necessari estar alerta, ser conscient i detectar-ho en el moment adequat.		

2. CONTINUÏTAT DEL NEGOCI

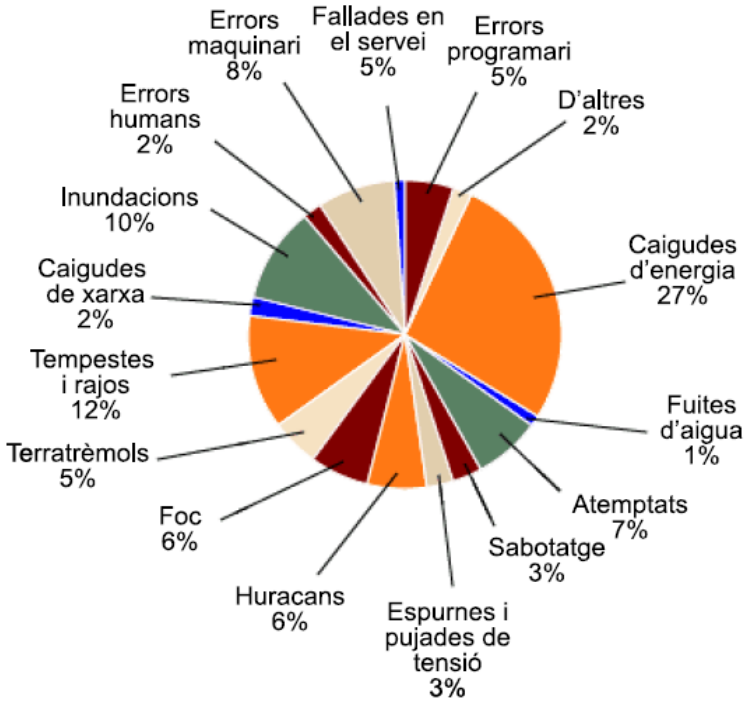
2.1. INTRODUCCIÓ

La continuïtat del negoci és un concepte que pertany a una disciplina superior anomenada "Administració de continuïtat de negocis" (BCM) i que compren tant el pla per la recuperació de desastres (DRP), de naturalesa típicament tecnològica, com el pla pel restabliment del negoci, que normalment s'enfoca en els processos crítics del mateix. La recuperació de desastres és la capacitat per respondre a una interrupció dels serveis tecnològics mitjançant la implementació d'un pla per restablir les funcions crítiques de l'organització.

Aquest pla és la resposta prevista per l'organització per fer front a aquelles situacions de risc que li poden afectar de forma crítica, es a dir, impedint la operació tecnològica que suporta els processos de negoci més importants. No importa la dimensió de la empresa o els costos de les mesures de seguretat implantades, tota organització necessita d'un pla de recuperació de desastres o d'un de continuïtat del negoci, ja que més tard o més d'hora s'enfrontarà amb una incidència de seguretat o algun esdeveniment que detingui les seves operacions.

Primerament s'ha de realitzar un anàlisi del impacte al negocio (BIA), aquest és bàsicament un informe que mostra el cost ocasionat per la interrupció dels processos crítics del negoci, posteriorment l'organització haurà de classificar els processos de negoci segons el seu grau d'importància i establir prioritats de recuperació en ordre seqüencial.

A continuació podem observar les circumstàncies que justifiquen la necessitat de disposar d'un pla de continuïtat de negoci.



2.2. ESTRUCTURA DEL PLA DE CONTINUÏTAT DE NEGOCI

El pla de continuïtat de negoci es compon mitjançant una estructura on es determina l'abast del projecte, la situació que cal controlar, el llistat de procediments a seguir, el disparament d'alarma, el pla de resposta, el pla de suport, el pla de recuperació, el pla d'anàlisi i millora i els plans de prova. En el nostre projecte farem referència a aquells punts que creiem que són més significatius.

2.2.1. DETERMINAR L'ABAST DEL PROJECTE

Determinar l'abast del projecte és important per proporcionar una idea general sobre aquells punts que es consideren crítics per la continuïtat del negoci i que per tant, en cas de produir-se una fallida, poden provocar un impacte molt negatiu sobre l'organització. En la universitat, com podrem observar en el següent punt, el servei intern d'ensenyament en línia és considera l'actiu més crític degut al seu grau d'afectació i la sensibilitat de les dades que gestiona, per tant, l'abast del projecte es centrarà en aquest i en proporcionar mecanismes per garantir la seva disponibilitat.

2.2.2. SITUACIÓ QUE S'HA DE CONTROLAR

Com ja s'ha comentat anteriorment, la universitat proporciona diferents tipus de actius o serveis, alguns d'ells enfocats més cap al personal de gestió i d'altres cap al professorat i l'alumnat. Podem considerar com a crítics o vitals aquells actius o serveis que sense la seva disponibilitat poden crear una problemàtica important pel desenvolupament normal de l'activitat, per tant hem de valorar la transcendència i el grau d'afectació que poden provocar cada un d'ells en cas de fallida.

ACTIUS	GRAU D'IMPORTÀNCIA	TEMPS DE RESPOSTA
[IS] Serveis Interns		
[IS_TEL] Telefonia IP	ALTA	< 48h
[IS_INT] Internet	MOLT ALTA	< 24h
[IS_MDL] Ensenyament en línia	CRÍTICA	< 6h
[IS_MAI] Correu electrònic	MOLT ALTA	< 24h
[IS_FS] Fitxers en xarxa	ALTA	< 48h
[SW] Aplicacions		
[SW_OS] Sistemes operatius	ALTA	
[SW_OFI] Ofimàtica	MITJÀ / ALTA	
[SW_AV] Antivirus	BAIXA / MITJÀ	

[SW_OTR] Altres	SENSE ESPECIFICAR
[HW] Equips	
[HW_SRV_*] Servidors	ALTA / MOLT ALTA / CRÍTICA
[HW_FRW] Firewalls	MOLT ALTA
[HW_RTR] Routers	
[HW_PC] Computadores d'escriptori	MITJÀ / ALTA
[HP_PRN] Serveis d'impressió	BAIXA
[COM] Comunicacions	
[COM_TEL] Telefonia IP	ALTA
[COM_LAN] Xarxa LAN	MOLT ALTA
[COM_WFI] Xarxa WIFI	
[COM_INT] Xarxa Internet	
[AUX] Equips auxiliars	
[AUX_SAI] Alim. ininterrompuda	MITJÀ / ALTA
[AUX_CBL] Cablejat	BAIXA / MITJÀ / ALTA / MOLT ALTA / CRÍTICA
[AUX_SEC] Sistemes de vigilància	
[AUX_OTR] Altres	SENSE ESPECIFICAR

Com podem observar en la taula anterior, el servei d'ensenyament en línia és considerat el servei més crític, degut a la diversificació del seu grau d'afectació, la seva manca de disponibilitat pot afectar tan a empleats de l'ensenyament com a l'alumnat, a més a més, la informació que gestiona és de vital importància perquè els alumnes puguin seguir els cursos, els seus materials, les tasques a realitzar, les avaluacions, etc. Per assegurar la disponibilitat d'aquest, hem de proporcionar mecanismes de control sobre els servidors que el gestionen o bé les comunicacions, degut a que la fallida d'un simple cable (sense cap tipus de mecanisme de redundància) podria provocar la caiguda del servei.

L'estudi dels riscos sobre aquest servei es de vital importància perquè l'organització estigui assabentada dels causants que poden provocar algun tipus d'interrupció, per tant, és necessari identificar les seves possibles amenaces (veure punt 1.3.4).

ACTIUS	AMENACES
[IS] Serveis Interns	
[IS_MDL] Ensenyament en línia	[I.5] Avaria d'origen físic o lògic [E.20] Vulnerabilitats en els programes (software) [E.21] Errors de manteniment / actualització de programes (software)

	[A.24] Denegació del servei
[HW] Equips	
[HW_SRV_WEB] Servidors WEB	[N.1] Focs
[HW_SRV_SQL] Servidors SQL	[N.2] Danys per aigua
	[N.*] Desastres naturals
	[I.3] Contaminació mediambiental
	[I.5] Avaria d'origen físic o lògic
	[I.7] Condicions inadequades de temperatura o humitat
	[E.2] Errors del administrador del sistema / de la seguretat.
	[E.23] Errors de manteniment / actualització d'equips (hardware)
	[A.11] Accés no autoritzat

2.2.3. GESTIÓ DE LA CONTINUÏTAT

La gestió de continuïtat no s'implanta quan succeeix un desastre, sinó que fa referència a totes aquelles activitats que es duen a cap diàriament per mantindre el servei i facilitar la seva recuperació. En aquest cas, la organització fa ús d'alimentació ininterrompuda per garantir la continuïtat dels serveis en cas de pèrdua d'electricitat, realitza copies de seguretat de forma diària de les bases de dades, fitxers en xarxa, servidors i configuracions per facilitar la seva recuperació, en referència al servei d'ensenyament en línia, aquest s'actualitza de forma periòdica revisant la existència de noves versions, el procès d'actualització es documenta i es realitzen les proves pertinents en altres equips, els servidors utilitzen targetes de xarxa alternatives per balancejar la carga i per garantir el seu funcionament en cas de fallida, també cal dir que la organització fa ús d'una estratègia "**hot site**" amb abocament sincronitzat (les dades dels centres estan totalment sincronitzades), per poder garantir la seva disponibilitat en cas de produir-se una catàstrofe i que per tant la seva recuperació es pugui dur a terme amb un temps de resposta adequat.

2.2.4. DISPARAMENT D'ALARMA

El disparament d'alarma de contingència és el moment a partir del qual s'ha de començar a executar el pla de continuïtat de negoci, tenint en compte que el temps màxim de resposta per restablir el servei d'ensenyament en línia és de sis hores i que el temps d'execució del pla és de quatre hores implica que el temps de disparament d'alarma no haurà de superar les dues hores.

2.2.5. PLA DE RESPOSTA

Podem definir el pla de resposta com el conjunt d'accions que es fan immediatament després del disparament de l'alarma de contingència. A continuació farem una breu descripció de les accions a seguir un cop materialitzades algunes d'aquestes amenaces sobre l'actiu més crític de l'organització, en aquest cas, l'ensenyament en línia.

AMENACES	ACCIONS PER A ELIMINAR L'AMENAÇA
[E.20] Vulnerabilitats en els programes	- Identificar la vulnerabilitat - Identificar l'agent que l'ha explotat (virus, usuari, etc.) - Eliminar l'agent (antivirus, tallar la comunicació, etc.) - Solucionar la vulnerabilitat (configuracions, actualitzacions) - Documentar la solució
Els virus o els usuaris malintencionats són clarament una amenaça quan tenen la intenció d'explotar les vulnerabilitats dels programaris o recursos, algunes poden provocar la denegació del servei (DoS), degut això, per mitigar la amenaça es necessari fer ús d'antivirus o d'altres elements per tallar la comunicació entre l'usuari i el servidor atacat. Es necessari identificar la vulnerabilitat i aplicar mecanismes per solucionar-la, així s'evitarà la reproducció de la explotació de la vulnerabilitat.	
[N.1] Focs	- Identificar l'agent causant (aparells elèctrics, estufes, instal·lació elèctrica, etc.) - Utilitzar extintors manuals, trucar als bombers, etc.
Els incendis poden tindre diferents tipus d'origen, normalment el seu origen està ubicat en aparells elèctrics que no funcionen correctament, en estufes, etc. En aquests casos, generalment es detecten amb certa rapidesa, però existeix un altre tipus d'incendi bastant habitual, que s'origina per una falla en el sistema elèctric de l'edifici, en aquests casos, quan es detecta, normalment, l'incendi és gran i difícilment el podrem controlar amb extintors manuals, per tant, haurem d'avisar als bombers.	
[N.2] Danys per aigua	- Identificar l'agent causant (juntes, desaigües, radiadors, fenomen natural, etc.) - Utilitzar les claus de pas, trucar als bombers, etc.
Entre les inundacions, s'han de distingir entre les localitzades en el interior de l'edifici, degudes a problemes estructurals o d'instal·lacions i les externes de l'edifici, que provenen d'un fenomen natural o d'un problema de tubàries generals d'aigua. Les inundacions localitzades en el interior de l'edifici, estan provocades per goteres procedents dels sostres, desaigües que es trenquen, radiadors en que els tubs perden, etc. Els motius son diversos, però sempre tenen que veure en que l'edifici no es troba en condicions, en cas contrari, les inundacions localitzades en el exterior de l'edifici poden ser conseqüència d'un fenomen natural com el desbordament d'un riu o pluges torrencials, o bé la ruptura d'una tubària general d'aigua, generalment es necessita la intervenció dels bombers.	

2.2.6. PLA DE SUPORT

Podem definir el pla de suport com el conjunt d'accions que s'han de desenvolupar per a oferir el servei que ha quedat afectat. Com hem comentat anteriorment, la organització fa ús d'una estratègia "hot site" amb abocament sincronitzat, per tant, de forma resumida les accions a desenvolupar per a oferir el servei d'ensenyament en línia es mostren a continuació:

ACCIONS PER A OFERIR EL SERVEI
- Comprovar el funcionament dels serveis WEB i SQL del "hot site"
- Comprovar que les dades estiguin sincronitzades
- Configurar físicament aquells aspectes que afectin la posada en marxa del "hot site"
- Configurar lògicament aquells aspectes que afectin la posada en marxa del "hot site"
La posada en marxa del "hot site" no hauria de ser una tasca molt complicada, hem de pensar que fa ús d'un abocament sincronitzat i que per tant, les dades estaran totalment actualitzades en el moment abans de la producció de la contingència. Actualitzar els apuntadors dels registres DNS és una de les tasques importants a realitzar que s'ha de dur a terme per la posada en marxa del servei.

2.2.7. PLA DE RECUPERACIÓ

El pla de recuperació consisteix en el conjunt d'accions que s'han de dur a terme per a retornar a la situació inicial. És a dir, el pla de continuïtat de negoci no s'acaba quan l'organització ha aconseguit oferir el servei dins dels nivells establerts, sinó quan és capaç de tornar al punt en què es trobava just abans que es produís la contingència.

GRAU D'AFECTACIÓ	ACCIONS PER A LA RECUPERACIÓ
Els servidors físicament **no han quedat afectats**. Vulnerabilitats en els programes, actualitzacions de programes, denegació del servei, etc.	- En segons quins casos, fer ús de les copies de seguretat dels servidors - Comprovar el funcionament dels sistemes operatius - Comprovar el funcionament dels serveis WEB i SQL - Comprovar que les dades estiguin sincronitzades - Configurar lògicament aquells aspectes que afectin a la posada en marxa - Configurar físicament els aspectes inicials del "hot site"
Els servidors físicament han quedat **parcialment afectats**, la seva recuperació pot ser possible dintre del temps establert, en el cas d'avaria d'un element físic (targetes de xarxa, targetes gràfiques, etc.)	- En cas de danys per aigua (no gaire intensos), assecar tots els components electrònics afectats - Identificar els elements físics afectats que no es poden reparar i reposar-los - En segons quins casos, fer ús de les copies de seguretat

s'ha de valorar la seva possible reposició. Focs, danys per aigua, desastres naturals, actualització d'equips, avaria física, etc.	dels servidors - Comprovar el funcionament dels sistemes operatius - Comprovar el funcionament dels serveis WEB i SQL - Comprovar que les dades estiguin sincronitzades - Configurar lògicament aquells aspectes que afectin a la posada en marxa - Configurar físicament els aspectes inicials del “hot site”
Els servidors físicament **han quedat totalment afectats**, la seva recuperació no pot ser possible dintre del temps establert. Focs, danys per aigua, desastres naturals, avaria física, etc.	- Identificar els elements físics afectats, aïllar-los i documentar els fets per a la asseguradora - Comprar nous equips amb les mateixes característiques - Fer ús de les copies de seguretat dels servidors - Comprovar el funcionament dels sistemes operatius - Comprovar el funcionament dels serveis WEB i SQL - Comprovar que les dades estiguin sincronitzades - Configurar lògicament aquells aspectes que afectin a la posada en marxa - Configurar físicament els aspectes inicials del “hot site”

Com podem observar en la taula anterior, les accions a realitzar per tornar al punt anterior a la contingència depèn directament sobre el grau d'afectació, com major sigui el grau d'afectació major seran el nombre d'accions a prendre, per tant, és molt important comptar amb un pla de suport per donar disponibilitat als serveis afectats mentre es desenvolupa aquest pla.

3. OPINIÓ PERSONAL

La realització d'aquest treball m'ha permès veure que la seguretat de la informació és una tasca molt complexa, per protegir correctament una organització és necessita molt de temps, pressupost, coneixements e interacció constant amb tots els responsables de l'organització. S'ha d'estudiar el escenari actual, tindre present en tot moment els objectius de l'organització, identificar els actius i valorar-los, identificar les amenaces que poden afectar a aquests actius i estudiar els graus d'afectació i ocurrència, estudiar els impactes i els riscos, establir mecanismes de control o salvaguardes per mitigar o reduir el risc, usar indicadors per controlar la efectivitat d'aquests salvaguardes, documentar totes les accions realitzades, per aprendre constantment i evolucionar cap a un sistema cada cop més segur, etc. Cal dir que la eina **PILAR** és una eina tremendament complicada, conté una gran quantitat d'informació i et permet plasmar digitalment els passos descrits anteriorment fent ús de l'Esquema Nacional de Seguretat. El estudi de la continuïtat de negoci també és un aspecte molt important a tindre en compte, la seva correcta implantació permet que la organització estigui preparada per actuar correctament sobre la ocurrència d'esdeveniments inesperats o no previstos, minimitzant d'aquesta forma el impacte de l'amenaça i garantint els serveis crítics mitjançant mecanismes de replicació. Crec que tota organització que interactuí amb informació sensible o bé que no es pugui permetre la interrupció dels serveis, ha d'estudiar la manera de garantir la seva disponibilitat, tenint en compte sempre, el marge de pressupost de l'organització.

4. FONTS D'INFORMACIÓ

Recursos

Recurs - Tema 2. Implantació d'un sistema de gestió de la seguretat de la informació (SGSI).
PID_00253137.pdf

Recurs - Tema 3. Plans de continuïtat de negoci. Capítol 2.
PID_00253138.pdf

Esquema Nacional de Seguretat

Pàgina oficial - Informació genèrica del Esquema Nacional de Seguretat (ENS).
https://administracionelectronica.gob.es

PILAR

PILAR - Eina d'Anàlisi de Riscos basada en la metodologia MAGERIT.
https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html

Protocols d'actuació

Diputació de Barcelona - Protocols d'actuació en cas de desastre en els arxius.
https://www1.diba.cat/llibreria/pdf/37953.pdf