Plans de continuïtat de negoci

PID_00253138

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

L'objectiu de totes les organitzacions, des del punt de vista de la seguretat de la informació, és mirar de reduir els riscos i evitar les possibles incidències de seguretat. Per a això disposem, com a normatives de referència, de la família ISO 27000, concretament la ISO/IEC 27005: gestió de riscos de la seguretat de la informació; d'altra banda, destaquem la ISO 31000: gestió de riscos, principis i guies (aquest estàndard és similar a la ISO 27005, però enfocat a qualsevol tipus de risc, no només a riscos de seguretat de la informació). Ara bé, cal tenir en compte que sempre es pot arribar a donar alguna situació impossible de protegir o d'evitar.

Per a fer front a aquestes situacions, les organitzacions necessiten crear plans de continuïtat de negoci, que tenen com a finalitat evitar que les activitats de negoci quedin interrompudes.

Depenent de l'organització, la interrupció de l'activitat de negoci pot comportar un autèntic caos, i traduir-se així en pèrdues econòmiques elevadíssimes. Per això, els plans de continuïtat de negoci són fonamentals quan parlem de seguretat de l'organització.

A més, hem de ser conscients que no es podrà aconseguir mai la seguretat total. Per això, convé disposar de plans de continuïtat de negoci. I és que, com se sol dir:

> "L'únic sistema que és realment segur és un d'apagat i desconnectat de la Xarxa, tancat en una caixa forta folrada de titani, enterrat en un búnquer, envoltat de gas nerviós i custodiat per guardes armats i molt ben pagats. Fins i tot llavors, no donaria la vida per això..."
>
> Gene Spafford
> Director de Computer Operations, Audit, and Security Technology (COAST), Universitat de Purdue

Per més que les organitzacions pretenguin evitar els problemes de seguretat, s'ha de tenir clar que les mesures que adoptin o bé poden fallar o bé són insuficients davant totes les amenaces que hi ha.

L'objectiu de la seguretat de la informació és evitar que les activitats pròpies de l'organització no quedin interrompudes per cap circumstància.

Per aquest motiu, els plans de continuïtat de negoci són imprescindibles, independentment de la grandària de l'organització: a més de les inversions que aquesta organització ha fet en mesures de seguretat, necessita tenir establert un pla de continuïtat.

Aquests plans de continuïtat de negoci no solament tenen l'objectiu de mirar d'evitar les interrupcions en l'activitat de negoci, sinó que també intenten minimitzar el temps d'inactivitat en cas que finalment es produeixin aquestes interrupcions.

Com a normatives de referència pel que fa a la continuïtat de negoci, trobem les següents:

- ISO 22301. Gestió de la continuïtat de negoci

- ISO 27031. Guia de continuïtat de negoci referent a tecnologies de la informació i comunicacions

Podem resumir el que hem dit fins ara destacant que els plans de continuïtat de negoci equivalen a **què s'ha de fer en cas que tota la resta falli**.

Objectius

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

1. Saber què és un pla de continuïtat de negoci i quins són els objectius que té respecte a la seguretat de la informació de les organitzacions.

2. Identificar les fases dels plans de continuïtat de negoci i la manera d'implantar-les.

3. Ser capaços d'assignar les accions determinades en el pla de continuïtat de negoci a les persones que configuren l'equip de seguretat de la informació de l'organització.

4. Conèixer l'estructura i el contingut del document del pla de continuïtat.

1. Plans de continuïtat de negoci

Els plans de continuïtat de negoci fan front a situacions que no solen passar. Ara bé, qualsevol organització hi ha d'estar preparada, ja que es poden donar en qualsevol moment. De fet, cada vegada són més freqüents, com es demostra en els exemples següents:

(20-08-04) Un fallo eléctrico paraliza el sistema informático de Barajas e interrumpe la facturación

Decenas de personas han tenido que esperar tiempo de más tras los mostradores de facturación del aeropuerto de Barajas a primera hora de este viernes después de que un corte en el suministro eléctrico, producido a las 8.10 horas a causa de una subida de tensión, haya interrumpido durante veinte minutos el sistema informático. El fallo eléctrico afectó, principalmente, al servicio de transporte de equipajes, lo que hizo que el aeropuerto tuviera que detener la facturación de maletas. Los retrasos no han llegado a afectar la hora de salida de los vuelos.

El incendio en una subestación eléctrica de Unión Fenosa deja a oscuras Madrid

La ciudad poco a poco vuelve a la normalidad.

Un incendio en uno de los transformadores de la subestación eléctrica de la compañía Unión Fenosa en Méndez Álvaro ha dejado sin luz esta tarde a más de 80.000 clientes de varias zonas de Madrid y ha provocado que la subestación de Iberdrola de la calle Ayala dejara de funcionar durante media hora, privando de luz a otros 15.000 vecinos del distrito de Salamanca.

Un incendio en una subestación eléctrica deja sin luz a miles de madrileños

ELMUNDO.ES | AGENCIAS

MADRID - Un incendio desatado en una subestación eléctrica de Unión Fenosa en las inmediaciones de **Méndez Álvaro (barrio del sur de Madrid)** ha dejado sin luz a varios distritos de la capital. Según la compañía eléctrica, el apagón ha afectado a 250.000 clientes.

Usuarios de Retiro, Chamberí, Centro, Puente de Vallecas, Ciudad Lineal-Ventas, Moratalaz, Salamanca, Arganzuela, Pacífico y Vicálvaro se han quedado sin luz a media tarde. Hasta el momento, cerca de 22.000 clientes continúan a oscuras.

Colapsadas las operaciones de Iberia en todo el mundo por un incendio en Madrid

Los técnicos trabajan en la reparación del sistema informático, afectado por las llamas mientras que los vuelos sufren retrasos de una hora. Este es el segundo fallo que sufren sus servicios informáticos en una semana

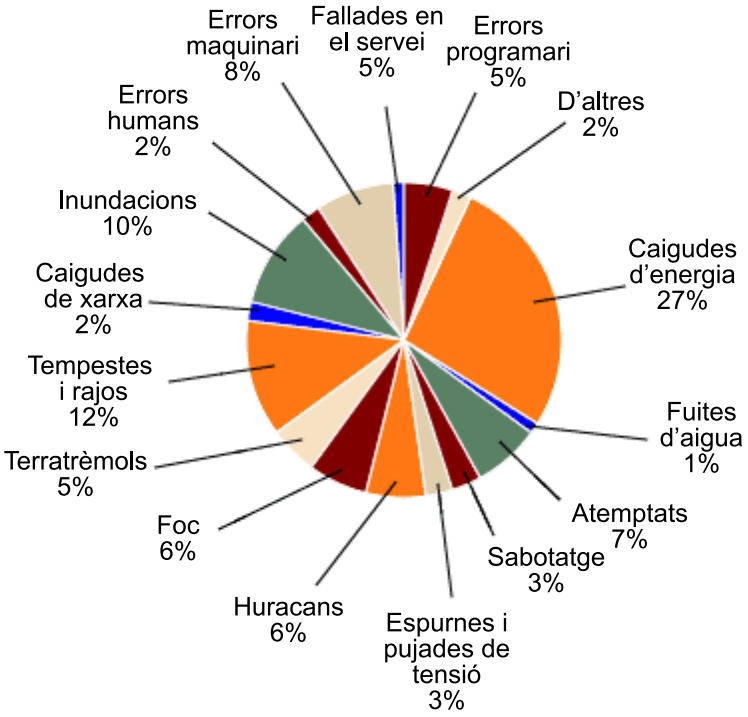
Iberia ha cancelado hasta las 18:00 horas un total de nueve vuelos y continúa registrando un retraso medio en sus vuelos de entre media hora y hora y cuarto en todos los aeropuertos en los que opera, como consecuencia del **incendio declarado a las 10. 00 horas de hoy en sus sistemas informáticos centrales** localizados en el Polígono de la Muñoza (Madrid), informaron a Europa Press fuentes de la aerolínea. Como consecuencia del incendio, **las operaciones de facturación, embarque y entrega de equipajes se están realizando a mano en todos los aeropuertos donde la compañía opera en España y en el resto del mundo.** Aunque el fuego ha sido controlado, Iberia augura «un día complicado» para volar.

Com es veu, aquestes situacions es donen. I no solament es donen, sinó que a més tenen conseqüències importants per a l'organització: fins i tot en poden provocar el tancament.

Un pla de continuïtat de negoci pretén evitar, per tots els mitjans, la interrupció de les activitats de l'organització.

Els plans de continuïtat de negoci es defineixen per a **quan** falla el sistema, no per **si** falla.

Circumstàncies que justifiquen la necessitat de disposar d'un pla de continuïtat de negoci



L'anàlisi de la imatge ens mostra que les situacions són molt diverses i, en molts casos, no depenen de les organitzacions mateixes i no es poden evitar amb les mesures de seguretat, cosa que no vol dir que no puguin provocar pèrdues importants.

2. Enfocaments en els plans de continuïtat de negoci

Per a evitar la possible confusió terminològica, definirem una sèrie de conceptes que se solen usar com a sinònims encara que no ho siguin.

- **Disaster recovery planning (DRP)**. El DRP és una estratègia planificada en fases, l'objectiu de la qual és recuperar tots els serveis relacionats amb les tecnologies de la informació i la comunicació i els recursos que els conformen, tan de pressa com es pugui, a partir d'un esdeveniment que ocasiona una interrupció important en el funcionament d'aquests serveis.

- **Business resumption planning (BRP)**. L'objectiu del BRP és mirar de reprendre tots i cadascun dels processos de negoci que té l'organització que han quedat afectats per una fallada o incidència en les diferents aplicacions IT que els conformen.

- **Continuity of operations planning (CoOP)**. L'objectiu del CoOP és mirar de recuperar les funcions estratègiques d'una organització que s'exerceixen en les seves instal·lacions corporatives.

- **Contingency planning (CP)**. L'objectiu del CP és mirar de recuperar els serveis i recursos de les TIC després d'un desastre que provoca una interrupció important en el funcionament d'aquests serveis i recursos.

- **Emergency response planning (ERP)**. Aquests plans miren de protegir els treballadors, el públic, el medi ambient i la resta d'actius de l'organització davant una situació de desastre.

- **Pla de continuïtat de negoci (PCN)**. El PCN és un conjunt format per plans d'actuació, plans financers, plans de comunicació, plans de contingències, etc., destinats a "mitigar l'impacte" provocat per la concreció de determinats riscos sobre la informació i els processos de negoci d'una companyia.

El PCN és un element estratègic global. En aquest sentit, se substancia en *N* plans de contingència d'àrees de negoci i en *N* plans de contingència de les infraestructures en què es recolza el negoci, entre les quals hi ha els sistemes d'informació i comunicacions.

Aquests PCN tenen l'objectiu de donar resposta de manera ràpida i àgil a les situacions que les mesures de seguretat que ha implantat l'organització no han pogut evitar.

Aquesta resposta de l'organització és la prevista davant les situacions de riscos que afecten d'una manera crítica el servei que cal protegir. En aquest sentit, és fonamental, per a cada organització, determinar el temps crític de recuperació i aconseguir tant que aquest temps sigui tan curt com es pugui com que la incidència tingui tan poc impacte com sigui possible.

El primer que cal fer és implantar tots els controls que s'han detallat al llarg de l'assignatura; és a dir, els que es presenten en la normativa ISO 27002 i més concretament la ISO 22301 específica per a la continuïtat de negoci. Després, com una nova mesura de seguretat que ha de tenir una organització, es dissenya i s'implanta el pla de continuïtat de negoci perquè, si arriba a passar un desastre, s'executi aquest pla i es puguin recuperar els processos de negoci tan aviat com sigui possible.

Característiques d'un pla de continuïtat de negoci

- Es troba en un procés de millora contínua de la gestió de riscos de l'organització.
- Ha d'estar completament orientat a recuperar els processos de negoci crítics per a l'organització.
- Ha d'estar dissenyat per a integrar-se amb la resta d'elements de seguretat de l'organització.
- Ha de servir per a automatitzar un conjunt de tasques de manera que s'eviti haver de planificar-les en moments de crisi.

3. Pla de continuïtat de negoci

Els plans de continuïtat de negoci persegueixen els objectius següents:

- **Mantenir el nivell de servei** en els límits que ha definit la companyia. Es pretén que les activitats de l'organització es puguin oferir sempre dins d'uns mínims, de manera que es pugui considerar que l'activitat no està interrompuda.

Nota

El pla de continuïtat de negoci no solament ha de recuperar els serveis, sinó que els ha de recuperar, com a mínim, amb el nivell de servei marcat per l'organització mateixa. Si el pla de continuïtat de negoci no pot aconseguir aquest nivell, hem de considerar que no és l'adequat per a aquesta organització.

- **Establir un període de recuperació mínim** per a garantir la continuïtat del negoci. Cada organització ha de marcar el temps que considera que pot sobreviure sense oferir les seves activitats; és a dir, ha de marcar els temps d'inactivitat dels seus actius.

- **Recuperar la situació inicial dels serveis i processos**. És a dir, mirar de restablir l'organització a l'estat en què es trobava abans que passés la contingència.

- **Analitzar el resultat de l'aplicació del pla de contingències i els motius de la fallada** per a optimitzar les accions. Durant l'execució d'aquests plans, es genera una sèrie d'evidències perquè es puguin analitzar i per a detectar i identificar el motiu que ha provocat la necessitat d'executar aquests plans.

Aquests plans de continuïtat de negoci estan basats en un altre dels elements fonamentals des del punt de vista de la seguretat: l'**anàlisi de riscos**.

Anàlisi de riscos

L'anàlisi de riscos permet identificar situacions que poden provocar alguna incidència de seguretat en una organització. Alhora, durant la gestió d'aquests riscos, es defineix la manera com cada organització s'ha de protegir, o com pretén fer-ho, dels riscos analitzats prèviament.

En cas que es detectin situacions de risc que no es poden controlar implantant alguna mesura de seguretat, per exemple, perquè el cost d'aquest control és elevat tenint en consideració la probabilitat que la incidència passi, aquestes situacions passen a controlar-se per mitjà dels plans de continuïtat de negoci.

Els plans de continuïtat de negoci estan relacionats íntimament amb l'anàlisi de riscos, ja que sense aquests riscos l'organització no sabria davant quines situacions s'han d'executar aquests plans.

3.1. Elements dels plans de continuïtat de negoci

Identifiquem quatre elements fonamentals en els plans de continuïtat de negoci en les organitzacions.

3.1.1. Definició de les situacions crítiques

Consisteix en el procés d'identificació dels riscos analitzats, riscos que poden afectar l'organització i que no es poden evitar implantant diferents mesures de seguretat. Aquestes situacions són les que surten reflectides en els plans de continuïtat de negoci i les que ha d'evitar l'organització.

Com a resultat d'això s'obté el següent:

- **Actius crítics**. Són els actius que queden afectats per aquests riscos. Aquest procés es basa en l'anàlisi de riscos. Recordem la relació "actius – amenaces – vulnerabilitats = riscos".

- **Processos de treball**. Es tracta de relacionar o identificar quins processos de negoci de l'organització poden quedar afectats per les amenaces que danyin els actius de l'organització.

3.1.2. Assignació de responsabilitats

Una vegada tenim identificats els riscos que provoquen la necessitat de tenir plans de contingències, s'ha de passar a assignar responsabilitats. Com a resultat d'això s'obté el següent:

- **Un comitè d'emergència**. Aquest comitè és l'encarregat d'actuar en cas que s'arribi a produir la situació d'emergència. Té la responsabilitat de fer que es recuperi el servei en els temps que ha establert l'organització.

- **Uns responsables dels plans**. Són les persones, dins del comitè d'emergència, responsables de cadascun dels plans de contingència que formen el pla de continuïtat de negoci d'una organització. Aquests responsables tenen l'obligació de mantenir actualitzats els plans i de verificar que aquests plans permeten la recuperació davant determinades situacions.

3.1.3. Definició de les accions de resposta

Consisteix a determinar davant quines situacions s'ha d'executar cadascun dels plans de contingència que conformen els plans de continuïtat de negoci.

Com a resultat d'això s'obté el següent:

- **Indicadors de disparament**. Són els punts que marquen el moment exacte en què s'ha de començar a executar el pla.

- **Seqüència d'accions**. S'indiquen totes i cadascuna de les accions que s'han de dur a terme des del moment en què es comença a executar el pla fins que s'arriba a la recuperació de la contingència i es torna a l'estat inicial.

- **Registres**. Són les evidències que queden de l'execució de totes i cadascuna de les accions detallades anteriorment.

3.1.4. Manteniment

Es tracta de mantenir tant els plans de continuïtat de negoci com els plans de contingència que els formen. Com a resultat d'això s'obté el següent:

- **Dades de prova i disparament**. Després de l'execució d'un pla, s'analitzen tots els registres de les accions que s'han dut a terme per a extreure'n conclusions.

- **Propostes de millora**. Una vegada analitzats els registres, es pot proposar millores per a optimitzar els plans establerts.

Els plans de continuïtat de negoci han de respondre a les diferents situacions de risc definides i recollir totes les accions que s'han de dur a terme des del moment en què es detecta la contingència fins que l'organització torna a les seves condicions de funcionament.

Perquè el pla de continuïtat de negoci sigui efectiu, és important:

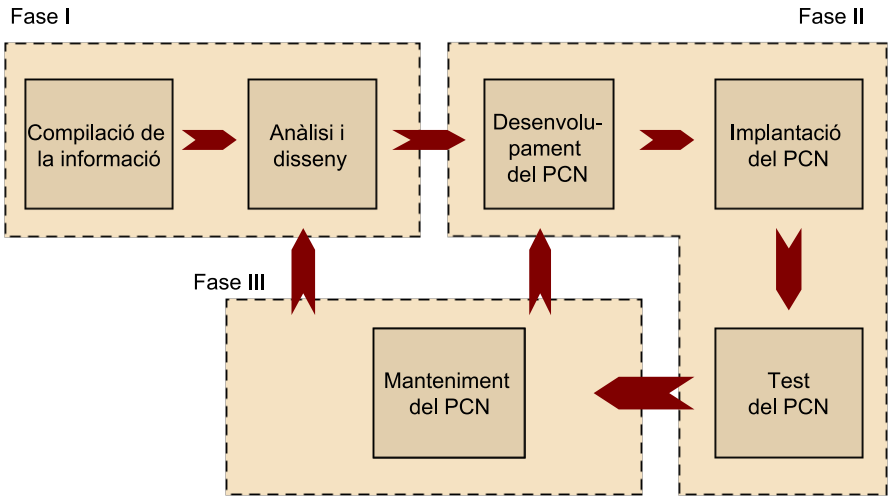
- Detectar els recursos necessaris.
- Definir la disponibilitat, el manteniment i l'operativitat dels recursos.
- Establir clarament el moment de disparament.
- Assignar un responsable als plans de contingències específics.
- Assignar responsabilitats per a cada acció definida.
- Establir un procés de revisió una vegada recuperada la situació.

4. Fases dels plans de continuïtat de negoci

Els plans de continuïtat de negoci són processos cíclics que requereixen una actualització constant, ja que han de reflectir la situació real de l'organització a cada moment.

En la imatge representem les fases dels plans de continuïtat de negoci, seguint el cicle de Deming:

Aquest cicle de Deming per a la continuïtat de negoci, es pot traslladar a tres fases:



4.1. Fase I

La primera fase en la creació dels plans de continuïtat de negoci consisteix a recopilar la informació necessària que permeti elaborar els plans per a cadascun dels escenaris de riscos davant els quals cal protegir-se.

Nota

Aquesta fase és la més important amb vista al resultat final i també es pot considerar com la més complicada, ja que és a partir dels resultats de l'anàlisi quan es desenvolupen els plans de continuïtat de negoci finals.

Una vegada es té tota la informació sobre els riscos davant els quals cal protegir-se, es dissenya el pla de continuïtat de negoci; és a dir, es planteja com es vol protegir l'organització davant aquestes situacions.

En aquesta fase, a més, s'analitza quant està disposada a invertir l'organització (en temps i diners) per a recuperar-se dels desastres.

Aquesta primera fase consta dels processos que analitzem tot seguit:

- Gestió de riscos.

- *Business impact analysis*.
- Desenvolupament d'estratègies del pla de continuïtat de negoci.

4.1.1. Gestió de riscos

Els plans de continuïtat de negoci, com ja hem comentat, estan relacionats íntimament amb l'anàlisi de riscos i la gestió de riscos: es tracta d'identificar els riscos a què està exposada l'organització i buscar la manera de minimitzar-los.

Recordeu

Els plans de continuïtat de negoci no s'han de considerar amb unes mesures de seguretat a les quals es pot recórrer en cas de necessitat, sinó que es tracta de l'últim recurs que té l'organització davant una situació de risc que s'ha concretat.

En primer lloc, s'han de gestionar de la millor manera possible els riscos detectats, i les situacions per sota del llindar de riscos de l'organització que no es poden controlar s'han de tractar mitjançant els plans de continuïtat de negoci.

Per tant, els plans de continuïtat de negoci han de ser completament personalitzats per a cada organització, ja que cadascuna està exposada a uns riscos diferents.

4.1.2. *Business impact analysis* (BIA)

Aquest és el procés més important i l'eix sobre el qual gira tot el pla de continuïtat de negoci. El BIA consisteix a identificar els processos relacionats amb la missió de l'organització i a analitzar amb molt detall els impactes en la gestió comercial del negoci que pot tenir una interrupció d'aquests processos com a resultat d'un desastre.

Procedimentalment, el BIA consisteix a fer una sèrie d'entrevistes amb representants de diferents perfils dins d'una organització, per a obtenir la informació que permeti identificar els processos crítics de l'organització i les conseqüències econòmiques que pot provocar interrompre'ls.

Nota

El BIA es fa com a procés i en cap cas es tracta d'analitzar les conseqüències que té el dany en un determinat actiu, sinó en tot el procés.

Quan es fan les entrevistes, s'ha de tenir en compte que tothom considera que les seves funcions són les més importants. Per tant, cal ser capaç d'allunyar-se de l'organització per a tenir una visió més global que ajudi a corregir els biaixos de la informació obtinguda.

Correcció de biaixos

Hi ha diferents tècniques que ajuden a ajustar els resultats de les entrevistes a la realitat; una d'aquestes tècniques consisteix a fer entrevistes encreuades: preguntar sobre una mateixa tasca a diferents perfils.

Els resultats de les entrevistes s'analitzen per a obtenir la visió global que requereix aquesta fase i es presenten a la direcció de l'organització. No hem de passar per alt que l'objectiu final d'aquesta fase és identificar les conseqüències econòmiques de la interrupció dels processos clau del negoci.

El BIA s'acaba quan s'ha aconseguit indicar d'una manera clara, i amb valors econòmics, una jerarquia de processos que cal protegir en cas que es produeixi un desastre.

En aquest sentit, hi ha quatre grans tipus de processos que es poden identificar a l'hora de fer el BIA:

- Processos crítics. Processos la interrupció dels quals comporta unes conseqüències econòmiques que no pot assumir l'organització, pels quals no s'ha pogut identificar cap procés alternatiu que permeti executar aquestes funcions amb el nivell mínim de servei.

- Processos vitals. Processos amb una tolerància més gran a les fallades que no pas els crítics. Per a aquests processos s'ha identificat un procés alternatiu que permet mantenir l'activitat durant un període curt. El cost de la interrupció d'aquests processos el pot assumir l'organització sempre que no excedeixi d'un nombre reduït de dies.

- Processos sensibles. Les funcions que desenvolupen aquests processos les poden assumir processos alternatius durant un període relativament llarg. Per a executar-los, però, es requereix contractar personal extra. Malgrat això, es pot considerar que el cost d'implantar el procés alternatiu (inclosa la contractació de personal extra) comporta un cost mitjà per a l'organització.

- Processos no crítics. Les funcions que desenvolupen aquests processos les poden assumir processos alternatius durant un període relativament llarg amb un cost nul, o relativament baix, per a l'organització.

La realització de les entrevistes

Quan ens plantegem fer les entrevistes, no hem de passar per alt que les duem a terme per identificar els aspectes següents:

- Nivell de servei que s'ha de mantenir en l'organització en qualsevol circumstància. Aquest aspecte és important en els processos de negoci que es desenvolupen de cara al públic (el client final), ja que si s'incompleixen en poden derivar unes conseqüències econòmiques relatives a l'incompliment dels contractes que es tenen signats.
  Recordem que els plans de continuïtat de negoci han d'assegurar, almenys, el nivell mínim de servei que ha establert l'organització en cada procés.

- Temps màxim d'inactivitat de cada procés que es pot permetre l'organització. Aquest temps mínim s'estableix valorant la pèrdua econòmica que pot assumir l'organització com a conseqüència de la interrupció d'aquest procés. La reducció del temps d'inactivitat provoca un augment

exponencial en el cost econòmic del pla de continuïtat de negoci: com més gran és el temps d'inactivitat que es pot permetre un procés, menys costós és el pla de continuïtat de negoci, i al revés.

Tot pla de continuïtat de negoci ha d'estar enfocat a no superar els temps d'inactivitat màxims identificats, el *recovery time objective* (RTO).

- Processos alternatius. El fet de disposar de processos alternatius per a portar a terme un procés, sempre que el nivell de servei no caigui per sota del mínim identificat, permet reduir bastant el cost dels plans de continuïtat de negoci.

Processos alternatius

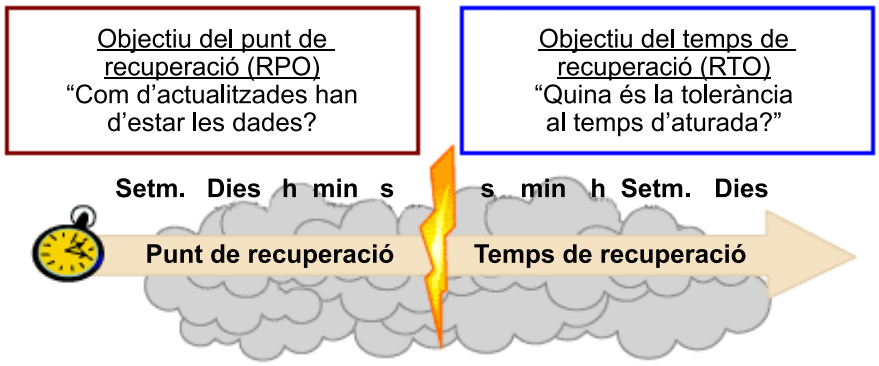
Un procés alternatiu és dur a terme determinades accions (en format paper, per exemple), en cas que el sistema informàtic quedi afectat.

- Primeres dades que permeten tornar a oferir el servei. Identificar si per a recuperar el procés que ha quedat afectat cal disposar de la informació que es tenia just abans que passés la incidència, o si, en canvi, es pot utilitzar la informació anterior (fins a quin moment: una hora, un dia, dos dies, etc.). Es tracta de determinar el que es coneix com a *recovery point objective* (RPO).

4.1.3. Desenvolupament de l'estratègia del pla de continuïtat de negoci

Aquesta subfase consisteix a estudiar les diferents estratègies que poden permetre recuperar els diferents processos identificats en el BIA tan de pressa com sigui possible i amb la inversió més petita que es pugui.

A l'hora de plantejar les diferents estratègies, s'han de tenir presents, sobretot, dos dels aspectes bàsics identificats mitjançant el BIA: temps màxim d'inactivitat assumible (RTO) i informació necessària per a recuperar els processos (RPO):



Les diferents estratègies són les següents:

- ***Cold site***. Aquesta estratègia consisteix a disposar d'un segon emplaçament, identificat i contractat prèviament, perquè, en cas de necessitat, l'organització hi pugui desplaçar l'execució d'alguns processos (o tots).
  Aquest segon emplaçament conté tan sols les instal·lacions bàsiques (cablejat, sistemes d'aire condicionat, etc.), i en cap cas es preveu la necessitat de disposar dels equips informàtics comprats. A tot estirar, es pot disposar de contractes de servei amb els proveïdors dels equips perquè els subministrin en un determinat temps.
  Si s'opta per una solució de *cold site*, s'ha de tenir en compte que comporta adquirir els equips nous, configurar-los i traslladar la informació (i el personal, si escau) com a passos previs a aixecar el servei i treballar amb els equips nous en l'emplaçament nou.

- ***Warm site***. Aquesta estratègia consisteix a disposar d'un segon emplaçament, identificat i contractat prèviament, i dels equips, almenys d'una part, considerats com els més importants per a dur a terme aquest procés. A més, els equips de què es disposi en aquest segon emplaçament han d'estar configurats parcialment (configuracions de xarxa, i equips de xarxa i perifèrics, per exemple) perquè en el moment de la contingència no s'hagi de partir de zero.
  Els *warm sites* estan destinats, principalment, a recuperar processos que poden estar un temps, generalment breu, inactius.
  Respecte dels *cold sites*, els *warm sites* comporten menys temps a l'hora d'adquirir i configurar equips (ja es té el més bàsic) i, per tant, permeten aixecar el servei en un període més curt.

- ***Hot site***. Aquesta estratègia és, des del punt de vista de la seguretat, la millor de totes perquè minimitza el temps d'inactivitat d'un procés, però alhora és la que requereix una inversió més gran, perquè comporta disposar de tots els equips comprats actualitzats i configurats per a utilitzar-los de manera automàtica o en poques hores. També necessita disposar de personal amb coneixements i documentació ajustats i que reflecteixi la situació real de l'organització.
  Pel cost elevat que té, aquesta estratègia està destinada a processos molt crítics que no poden estar inactius gaire temps, de manera que, generalment, no es pot buidar la informació en el moment de la contingència: un *hot site* requereix estar sincronitzat contínuament. En aquest sentit, es pot optar per un dels dos sistemes següents:
  – Abocament sincronitzat: qualsevol modificació que es faci en la informació que s'utilitza en producció es duu a terme de manera instantània en el segon centre, amb el que això comporta pel que fa a amplada de banda i als equips necessaris.

  – Abocament asíncron: els centres es configuren perquè de manera periòdica, i a tot estirar al llarg de vint-i-quatre hores, es faci un abocament complet de la informació en producció al centre alternatiu. D'aquesta

manera, en cas de desastre, es disposa de la informació de fa un dia com a màxim, i en moltes organitzacions n'hi ha prou per a aixecar el procés.

Tenim dues solucions més, a l'hora de plantejar-nos crear un segon centre alternatiu:

- Llocs mòbils. Remolcs dedicats a emplaçar equips i sistemes. Solen contenir servidors, estacions de treball, equips de comunicacions, enllaços via satèl·lit, etc. Els llocs mòbils, malgrat que no són gaire comuns, poden ser útils davant desastres que afectin una àmplia zona geogràfica.

- Acords recíprocs. Dues empreses o més acorden proveir-se mútuament d'instal·lacions en cas d'emergència. Es reserven espais i, en cas de desastre, només cal transportar els equips i connectar-los a la xarxa de l'empresa "receptora".

Aquestes solucions tenen l'avantatge que el cost que tenen és inferior a la contractació d'un *site* (sia *hot*, *warm* o *cold*) a una empresa especialitzada en aquesta mena de serveis, però presenta alguns inconvenients: aquests acords no solen obligar les parts a complir-los (no són empreses dedicades a aquesta mena de serveis) i també hi pot haver algun problema d'incompatibilitats entre configuracions.

Conclusions

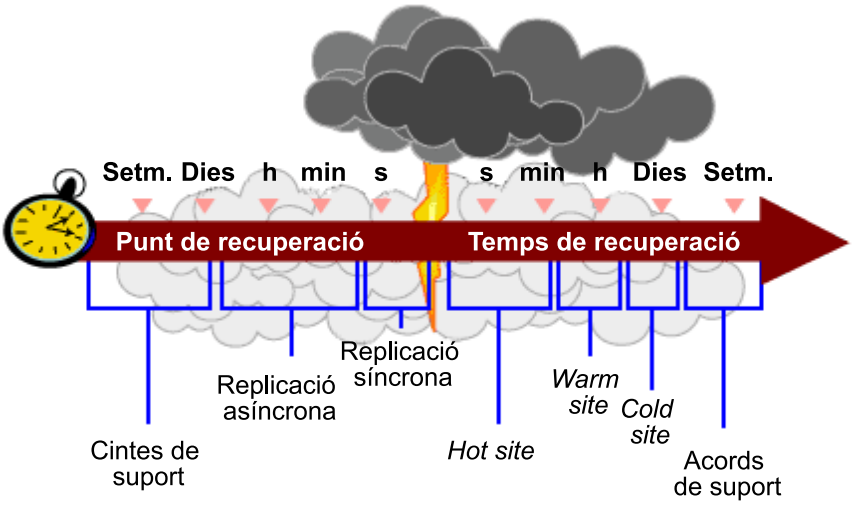
A l'hora de seleccionar una de les estratègies anteriors, cal tenir present que totes presenten uns costos elevats i que és més recomanable trobar processos manuals alternatius que no pas haver de triar una solució més restrictiva.

Si s'opta per contractar un segon emplaçament, s'ha de trobar a prou distància perquè no l'afecti una situació de risc en l'organització. En general, es recomana cinc quilòmetres com a mínim, però, com totes les mesures de seguretat, aquesta distància depèn dels riscos a què estigui exposada l'organització.

En qualsevol de les solucions, a l'hora de seleccionar l'estratègia que cal seguir, s'ha de considerar que no solament es tracta d'un cost d'adquisició de nous equips, sistemes i instal·lacions, sinó que també hi ha un cost important relatiu al manteniment que requereixen aquests equips, sistemes i instal·lacions.

A partir del plantejament de les diferents opcions o estratègies, s'ha de triar la que permet a l'organització complir els seus RTO i RPO amb el nivell de servei marcat sempre amb la mínima inversió possible.

A continuació mostrem gràficament les combinacions més habituals amb vista als plans de continuïtat, prenent com a base les estratègies possibles, segons els temps d'RTO i d'RPO:



4.2. Fase II

Una vegada dissenyat el pla, es desenvolupa, és a dir, es defineixen les diferents accions que s'han de dur a terme per a la recuperació. Alhora, en aquesta fase s'indica, amb tota mena de detalls, les accions que s'han de fer per a recuperar la normalitat.

Una vegada s'ha detallat aquest pla, s'implanta, és a dir, es compren equips, es designen emplaçaments i personal i s'aconsegueixen la resta dels recursos que es requereixin per a executar els plans dissenyats i desenvolupats dins dels temps màxims d'inactivitat que pot assumir l'organització.

I, com tot control d'una organització (els plans de còpies de seguretat o *backups*, per exemple), han de ser provats abans que calgui posar-los en pràctica. S'han de fer les proves pertinents en aquesta fase.

4.3. Fase III

Consisteix a millorar els plans després d'haver dut a terme les proves. Per a fer-ho, s'han d'utilitzar les evidències i els registres que aquestes proves han generat.

L'objectiu d'aquestes millores és reduir el temps de recuperació dels escenaris de riscos identificats.

5. Estructura dels plans de continuïtat de negoci

Com hem dit durant aquest mòdul, els plans de continuïtat de negoci no deixen de ser una sèrie d'accions que s'han de dur a terme en cas que passi una determinada incidència de seguretat que les mateixes mesures de seguretat que té implantades l'organització no pot evitar o contrarestar.

Ha de quedar clar, però, que, igual que l'anàlisi de riscos o la política de seguretat, aquests controls no són més que documents que s'han d'aplicar més endavant en una organització. Si no es fa aquesta implantació, aquests controls queden com un document que no es podrà utilitzar ni aplicar quan faci falta.

Quan es parla del document del pla de continuïtat de negoci, s'ha de considerar l'aspecte fonamental següent:

Cada pla de continuïtat de negoci és diferent del d'una altra organització, ja que no hi ha cap organització que tingui les mateixes necessitats.

En aquest sentit, a l'hora de redactar i crear el pla de continuïtat s'ha de tenir molt clar l'objectiu que s'hi persegueix, que no és altre que aconseguir que la interrupció del negoci sigui mínima si es donen algunes situacions.

Aquest control de seguretat del negoci és el que fa que sigui necessari que el pla sigui completament personalitzat, ja que cada organització té les seves característiques i, a més, té els seus propis recursos per a aconseguir oferir els seus serveis.

Una vegada desenvolupat, el pla de continuïtat presenta una estructura semblant a aquesta:

- Objectiu.
- Abast.
- Descripció de la situació que cal controlar:
  - Riscos que s'han de controlar.
  - Actius que hi intervenen.
  - Nivell de servei exigit.
  - Temps per a cada resposta: temps total de reacció.
  - Recursos necessaris en cadascun dels plans. Disponibilitat i operativitat.
- Llista de procediments concrets i dels responsables d'aquests procediments.
- Disparament d'alarma.
- Pla de resposta.
- Pla de suport.
- Pla de recuperació.
- Pla d'anàlisi i millora.
- Plans de prova.

Aquesta estructura, si és completa, serà aplicable en una organització en cas de necessitat. A continuació es detallen quins aspectes cal que quedin reflectits en cadascun d'aquests punts.

5.1. Objectiu

Aquest primer punt consisteix a explicar el que es pretén aconseguir creant i implantant el pla de continuïtat de negoci, de manera que, quan un treballador de l'organització hagi accedit a aquest document, sàpiga i tingui clar què és el que justifica haver creat el pla.

Exemple de definició de l'objectiu

L'objectiu d'un pla de continuïtat de negoci es pot expressar de la manera següent:

"Com és sabut, la nostra organització té una informació molt sensible i les activitats que fem amb aquesta informació són fonamentals perquè funcioni correctament. La direcció, per tant, ha desenvolupat aquests plans de continuïtat de negoci amb la intenció d'evitar

que aquestes activitats bàsiques s'interrompin per la irrupció d'algun fet que no es pugui controlar amb les mesures de seguretat que hi ha implantades."

La idea és que tots els treballadors, fins i tot sense ser experts en seguretat, entenguin la funció d'aquests plans de continuïtat.

5.2. Abast

És fonamental que l'execució del pla se centri en l'abast definit.

L'abast d'un pla de continuïtat de negoci pot arribar a incloure tota una organització o, per contra, es pot limitar a una part o a uns determinats processos dins de l'organització, els que es considerin més crítics.

En l'elaboració de l'abast, s'ha de concretar clarament, en els plans de continuïtat de negoci, els serveis que es pretenen garantir, i també les localitzacions. També s'ha de definir el personal que es veurà involucrat en l'execució d'aquests plans.

Definició de l'abast per a una empresa

Imaginem-nos que una organització té uns quants centres distribuïts al llarg de tota la geografia espanyola. Els plans de continuïtat de negoci poden fer referència únicament a una determinada seu, de manera que l'abast és el següent:

- Les activitats de negoci que es desenvolupin en aquesta seu.
- El personal que hi treballa.
- Els actius que hi ha a la seu.

5.3. Descripció de la situació que s'ha de controlar

És en aquest punt on es reflecteix la relació que hi ha entre l'anàlisi de riscos i el pla de continuïtat de negoci: les situacions que s'han de identificades són aquelles en què el risc pugui implicar la parada del negoci.

A més, prenent com a base aquests riscos que es pretenen evitar, es poden determinar altres elements fonamentals per a elaborar més endavant el pla de contingències.

Combinant l'anàlisi de riscos i el BIA obtenim el detall dels processos prioritaris per a l'organització i davant quines situacions cal que s'executin els plans.

En aquesta fase també s'elabora la llista d'actius que s'han de tenir en compte en l'execució del pla de continuïtat. En definir l'abast d'aquest pla, es poden determinar quins actius hi queden dins i també es pot saber com queda afectat cadascun d'aquests actius per les diferents amenaces que provoquen riscos elevats.

Des del punt de vista de la funcionalitat de l'organització, en aquest punt es determina quins són els nivells mínims que es volen mantenir quan aquesta organització elabori o executi el pla de continuïtat.

Els temps de resposta, els que determinen el temps que l'organització pot estar sense executar els seus processos, són fonamentals. Una vegada es té clar els temps de resposta volguts, es pot fer una estimació dels recursos que faran falta per a executar els plans i, concretament, els recursos que faran falta per a cadascuna de les fases en què es divideix el pla de continuïtat: pla de resposta, pla de suport i pla de recuperació.

5.4. Llista de procediments concrets i dels responsables d'aquests procediments

Aquest punt el conforma la llista de procediments que cal conèixer, i als quals es farà referència més endavant, per a recuperar-se de les contingències marcades.

Alhora, cal que s'hagin designat els responsables de cadascun dels procediments que s'han identificat com a necessaris. Aquests responsables són els encarregats d'actualitzar aquests procediments, no per necessitats del pla sinó per la mateixa operativa de l'organització.

Procediment de còpies de seguretat

És molt habitual que una organització, per a executar el seu pla, necessiti disposar del procediment de còpies de seguretat, ja que durant alguna de les fases del pla de continuïtat de negoci es requereix recuperar la informació d'algun dels suports d'aquestes còpies de seguretat que té l'organització.

5.5. Disparament d'alarma

Aquest punt és fonamental per a l'èxit del pla de continuïtat.

S'anomena **disparament d'alarma** el moment a partir del qual s'ha de començar a executar el pla de continuïtat de negoci.

És important que s'hagi identificat clarament el responsable de fer l'avís que s'ha d'entrar en contingència i que s'han d'executar les accions pertinents. No és aconsellable que no s'hagi definit aquesta persona ni els moments a partir dels quals s'ha de començar a executar el pla. D'aquesta manera s'eviten situacions interpretables.

S'ha de saber que el moment de disparament depèn de cada organització, ja que, a l'hora de la veritat, cadascuna té un temps de resposta determinat. Com més breu és aquest temps, abans ha de saltar el moment de disparament.

El temps màxim del moment de disparament és el que, sumat al temps establert per a executar el pla de continuïtat de negoci, és igual al temps màxim de resposta que ha definit l'organització.

Exemple

Imaginem-nos que tenim aquestes dades:

- Temps màxim de resposta: sis hores.
- Temps d'execució del pla: quatre hores.

El temps de disparament d'alarma ha de ser com a màxim de dues hores des de la parada de les activitats de negoci.

5.6. Pla de resposta

En aquest punt es defineix les accions que s'han de dur a terme per a executar el pla. Cadascuna de les accions que es considera que s'han de fer, ha de tenir associada un responsable, que és l'encarregat d'executar-les.

Aquest conjunt d'accions es divideix en tres fases diferents:

- Pla de resposta.
- Pla de suport.
- Pla de recuperació.

El pla de resposta consisteix en el conjunt d'accions que es fan immediatament després del disparament de l'alarma de contingència.

Convé determinar les accions següents:

- **Accions per a protegir les persones**. Són el conjunt d'accions destinades a protegir les persones, per sobre de la resta dels actius. Aquestes accions, en molts casos, impliquen diferents plans d'emergència.

- **Accions per a tallar la situació de risc: control de les amenaces**. Aquest conjunt d'accions va encaminat a reduir o eliminar l'amenaça que ha provocat l'execució del pla. Per exemple, l'extinció d'un incendi.

- **Accions per a protegir els actius**. Aquestes accions van encaminades a salvar els actius que no han quedat afectats per aquesta amenaça.

- **Accions de notificació pública**. Aquestes accions consisteixen en les comunicacions que ha de fer l'organització a organitzacions externes per a notificar la situació que s'ha provocat. Aquestes accions de vegades són sinceres i de vegades miren d'amagar la situació per què passa l'organització. S'ha de notificar l'estat de la situació als mitjans de comunicació (en cas que sigui necessari), als proveïdors, als clients, als socis, etc. En definitiva, a tothom qui estigui involucrat en el procés de negoci que s'hi hagi vist afectat.

- **Registre de les accions que es duen a terme**. Cal que cadascuna de les accions que es duen a terme quedin registrades per a analitzar-les més endavant.

El pla de resposta consisteix en les primeres accions que s'han de fer quan l'organització detecta una contingència i que van encaminades a minimitzar-ne l'impacte.

5.7. Pla de suport

És el conjunt d'accions que s'han de desenvolupar per a oferir el servei que ha quedat afectat. Sempre es pretén mantenir el servei dins dels nivells que ha requerit l'organització.

Convé determinar els elements següents:

- **Recursos necessaris per a mantenir l'operació**. Es detecta quins recursos o actius són necessaris per a executar aquestes accions.

Recurs de recuperació d'informació

Un exemple de recurs és la màquina de còpia de seguretat que té l'organització i que és en un altre edifici.

- **Manteniment dels recursos**. S'estableix les operacions que s'han de dur a terme amb els recursos detectats anteriorment perquè siguin operatius tal com ho era el que que ha quedat afectat per la contingència.

- **Activació de les diferents accions**. Es fixa el moment en què s'ha d'activar cadascuna de les accions que s'han dissenyat. S'ha d'haver identificat la persona que s'encarrega de l'activació.

- **Identificació del personal implicat**. S'identifica el personal implicat en l'execució d'aquestes accions. S'ha d'avisar les persones que es requereix que participin en aquests plans.

- **Registre de les accions dutes a terme: inici, desenvolupament i resultats**. Cal que cadascuna de les accions que es duguin a terme quedin registrades per a analitzar-les més endavant.

5.8. 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.

Cal mirar de seguir aquests passos:

- **Restitució d'actius, subministraments, entorn**. Consisteix a tornar a recuperar els actius que van quedar danyats per la contingència. Cal tenir en compte que, moltes vegades, els recursos que ofereix el servei en estat de contingència són de característiques inferiors a les habituals. Són recursos que només s'utilitzen de manera puntual i durant un temps d'excepció.

- **Arrencada dels sistemes, serveis, etc**. Una vegada s'han comprat o recuperat els actius principals s'han d'arrencar, i s'ha de comprovar si funcionen correctament. Aquest és el pas en què es fan les migracions de dades i les configuracions dels actius per a oferir els serveis.

- **Proves per a comprovar els sistemes restaurats**. Cal fer proves, una vegada s'han configurat els actius, per a estar segurs que aquests actius no produiran errors en el moment en què tornin a assumir l'execució dels processos de negoci.

- **Posada en operació**. En el moment en què totes les proves han constatat que els actius funcionen correctament es porta a terme l'activitat amb aquests recursos nous.

- **Retirada dels plans de suport**. Quan els recursos nous estan funcionant, es retiren els actius de contingència i es guarden en la forma en què estaven abans de la incidència per a utilitzar-los en altres situacions d'emergència.

- **Registre de les accions fetes i dels resultats**. Cal que cadascuna de les accions que es duen a terme constin en registres i que aquests registres es puguin recollir per a analitzar-los més endavant.

Acabat el procés, l'organització es troba, per fi, en el mateix estat d'abans que passés la contingència. Això comporta també que, en cas que torni a passar aquesta contingència, pot tornar a executar aquests plans amb la seguretat que es disposa dels actius necessaris perquè el servei no quedi interromput.

5.9. Pla d'anàlisi i millora

Una vegada acabades les accions, s'han de recollir tots i cadascun dels registres que s'han generat en les diverses fases del pla de continuïtat de negoci. Després, s'analitzen per a detectar les possibles fallades que s'han produït durant aquestes execucions.

Aquest pla d'anàlisi té l'objectiu d'elaborar procediments de millora d'aquests plans, de manera que es redueixi el temps en què es duen a terme les diferents accions. Els registres que s'analitzen són els següents:

- Dades sobre la situació d'emergència: causes, durada, dany produït.

- Dades sobre el desenvolupament i l'adequació dels plans de resposta, suport i restauració. Són registres presos durant el desenvolupament dels plans.

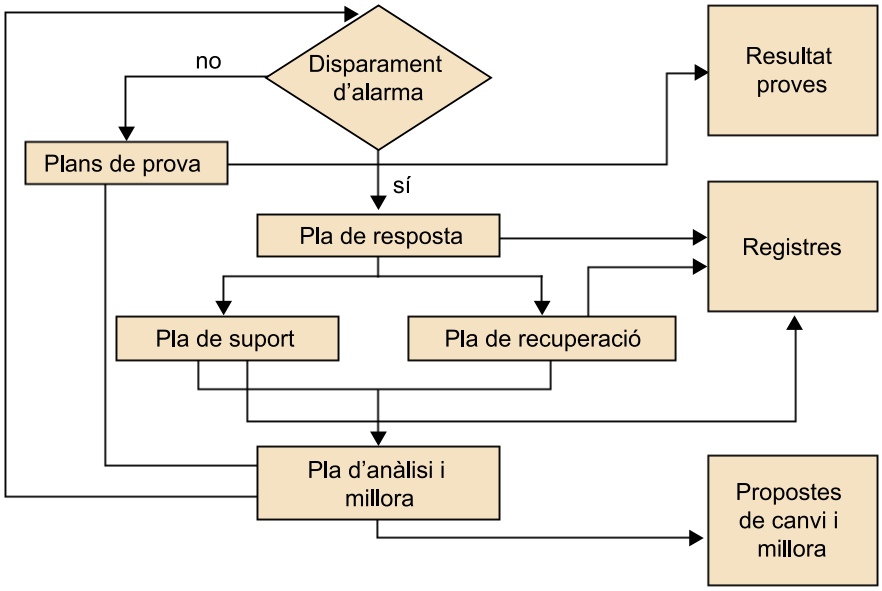
A partir d'aquestes dades, s'elabora un informe perquè el comitè d'emergència, que és l'equip que té la responsabilitat dels plans de continuïtat de negoci, hi proposi millores.

5.10. Plans de prova

No n'hi ha prou de tenir ben descrites les accions que s'han de dur a terme en cas que s'arribi a produir una determinada contingència, sinó que també cal provar-les per a estar segurs que amb aquests plans es poden aconseguir els objectius que ha marcat la direcció.

Aquestes proves han d'estar planificades, perquè moltes vegades poden provocar interferències amb les activitats de negoci de l'organització. Malgrat això, s'han de fer de la manera més real possible per a assegurar-se que, en cas de necessitat, es pot fer ús d'aquests plans de continuïtat amb la tranquil·litat que s'evitarà la interrupció de l'activitat de l'organització per un temps superior del que ha previst la direcció.

5.11. Resum de les relacions entre les fases



6. Conclusions

Els plans de continuïtat de negoci són fonamentals per a assegurar la informació, que és el que pretén l'organització implantant les mesures de seguretat.

En aquests plans han de quedar detallades totes i cadascuna de les accions que s'han de dur a terme per a recuperar-se de determinades situacions, i també l'ordre en què s'han d'anar fent.

Aquestes accions tenen identificades clarament les persones que les han de dur a terme per a evitar que, en el moment de necessitat, s'hagi de decidir qui és la persona encarregada de fer-les.

És fonamental que els plans de continuïtat de negoci estiguin actualitzats i que reflecteixin sempre la situació real de l'organització, ja que, en cas contrari, no és segur que aquesta situació es pugui recuperar dins dels temps establerts.

La progressió en el temps d'aquests plans de continuïtat és la següent: