Continuïtat de negoci. Anàlisi de riscos i d'impacte

Pla de Qualificació en Tecnologia Mòbil

Organitza: CIFO · SOC Servei d'Ocupació de Catalunya · Generalitat de Catalunya · Unió Europea Fons Social Europeu L'FSE inverteix en el teu futur

Imparteix: UOC Universitat Oberta de Catalunya

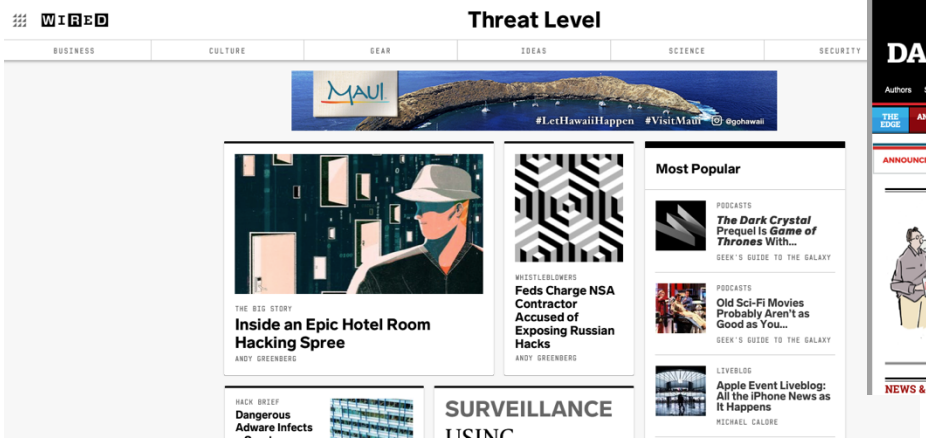
Col·labora: MOBILE WORLD CAPITAL BARCELONA

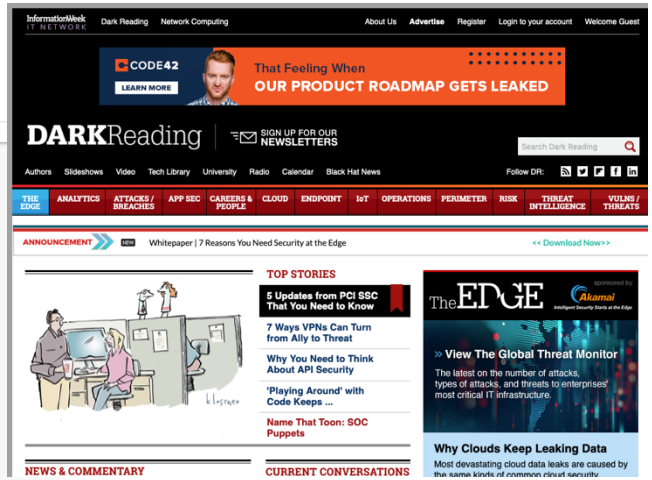
Contingut

- Riscos i continuïtat de negoci
- Virtualització
- Còpies de seguretat
- Estacions de treball
- Plans de continuïtat de negoci

Riscos i continuïtat de negoci

- El coneixement de la tecnologia de la seguretat facilita l'anàlisi dels riscos que posen en perill la continuïtat de negoci.
- Cal tenir coneixements tècnics, però també estar al dia perquè la ciberseguretat requereix una actualització constant:
  - Nous atacs, noves mesures de protecció.
  - Bases de coneixement sobre vulnerabilitats, atacs de dia zero, etc.





Riscos i continuïtat de negoci

- Quan coneixem l'organització (a nivell de processos, a nivell de tecnologia utilitzada), podem fer una anàlisi de riscos i proposar un pla de continuïtat de negoci.
- Quan realitzem auditories de seguretat, de forma similar, podem fer una anàlisi de riscos sobre els sistemes d'informació i la tecnologia de xarxa, servidors, etc. Podem incloure, igualment, a les persones (per valorar si fan bé les coses)

Riscos i continuïtat de negoci

Quins riscos hi pot haver?

- Atacs d'interrupció, es destrueix o queda no disponible un recurs del sistema.
- Atacs d'intercepció, contra la confidencialitat en el qual un element no autoritzat aconsegueix l'accés a un recurs.
- Atacs de modificació.
- Atacs de fabricació, per exemple, afegir un nou usuari al sistema de forma fraudulenta.

Riscos i continuïtat de negoci

- Atacs provinents de persones
  - Atacs passius, on l'atacant observa/escolta amb la finalitat d'aconseguir informació confidencial.
  - Atacs actius
    - Suplantació d'usuaris.
    - Reactuació, per exemple intentar repetir diverses vegades l'ingrés a un compte bancari.
    - Degradació fraudulenta del servei, evitant el funcionament normal dels recursos.
    - Modificació de missatges interceptats i reenviar-los al destinatari.

Riscos i continuïtat de negoci

- Circumstàncies físiques
  - Caigudes d'energia
  - Pujades de tensió
  - Inundacions i fuites d'aigua
  - Incendis
  - Caigudes de la xarxa
  - Tempestes i llamps
  - ...

Riscos i continuïtat de negoci

- Qui pot fer l'atac?
  - Personal de la mateixa organització, penseu que a vegades no són "atacs" pròpiament, sinó accidents provocats pel desconeixement i/o inexpertesa del personal.
  - Antics treballadors.
  - Hackers.

Què passa si llencem a la brossa papers amb contrasenyes?
Què passa si ens fem passar per un tècnic i demanem contrasenyes als treballadors?

Riscos i continuïtat de negoci

- Problemes derivats d'atacs informàtics externs
  - Les IP públiques s'analitzen per cercar vulnerabilitats i punts d'entrada.
- Problemes derivats de fallades físiques
  - Una estació de treball amb la font d'alimentació espatllada
  - Problemes en el disc dur que impedeixen treballar amb normalitat o arrencar l'estació de treball
  - Problemes en les comunicacions externes
    - Operadora de backup?
    - Sistema de backup?
    - Òbviament dependrà de la pèrdua que suposi la materialització del risc.

Riscos i continuïtat de negoci

- Problemes derivats del canvi
  - Nou programari i noves versions
  - Aparició de bugs

Riscos i continuïtat de negoci

- Sovint la materialització d'amenaces implica delictes informàtics
- Delictes contra la intimitat
  - Intercepció de comunicacions, espionatge
  - Obrir correus electrònics d'altres, utilitzar altres bústies
- Frau informàtic
  - Manipulació de maquinari i programari per a cometre actes il·lícits
- Delictes de danys
  - D'equips, d'eliminació de dades
- Delictes contra la propietat industrial i intel·lectual
- Delicte de revelació de secrets

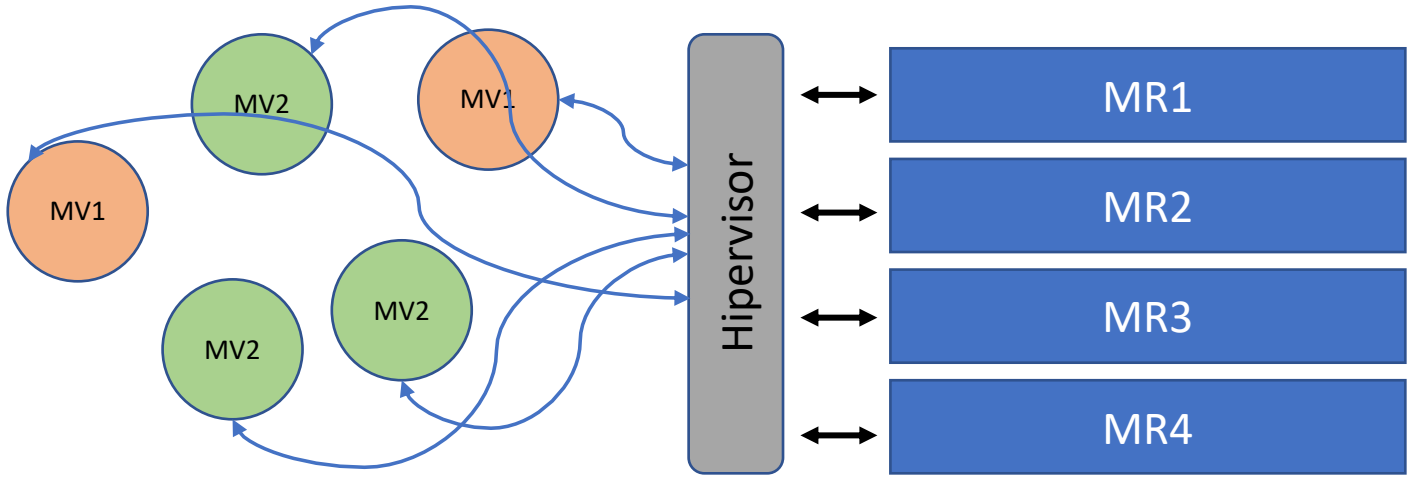
Delegació de bústies, missatges de vacances...

Contingut

- Riscos i continuïtat de negoci
- **Virtualització**
- Còpies de seguretat
- Estacions de treball
- Plans de continuïtat de negoci

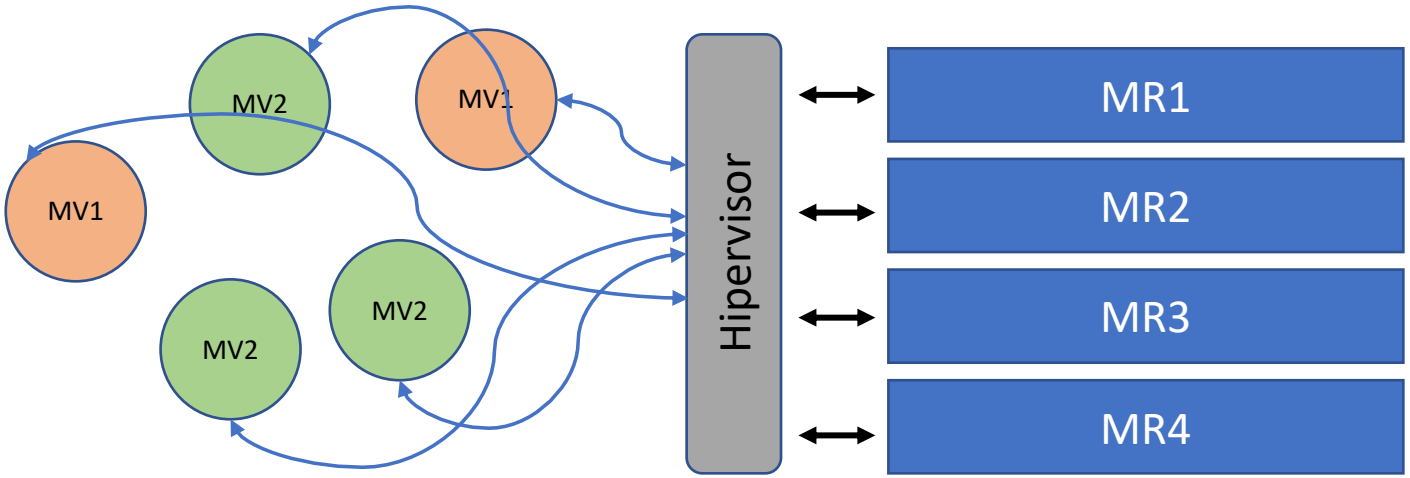
Virtualització

- La virtualització permet representar recursos de maquinari mitjançant programari.
- Típicament es virtualitza un sistema operatiu que funcionarà sobre dispositius virtuals (CPU, memòria, disc, xarxa...), la **màquina virtual (MV).**



Virtualització

- Les MV es poden clonar fàcilment, es poden activar/desactivar en funció de les necessitats de servei, o per restaurar servidors en casos de problemes.



Virtualització

- Podríem definir tres tipus de virtualització:
  - Virtualització en una màquina d'escriptori, per exemple, utilitzant VirtualBox: per tenir diferents sistemes "convivint" en una màquina física.
  - Virtualització sobre un rack de servidors físics, utilitzant eines com ara VMWare, Microsoft Hyper-V o KVM.
  - Aquests servidors poden estar en les instal·lacions de l'organització (**on premise**) o bé en empreses de hosting.
  - En els darrers anys aquests serveis de màquines virtuals s'ofereixen com a serveis a núvol (PaaS, platform as a service), per part de Microsotf (Azure), Amazon (AWS) i Google (Google Cloud)

Virtualització

- Vmware ESXi
  - Hipervisor que inclou un sistema operatiu, és a dir que no s'instal·la sobre un servidor que necessita sistema operatiu (de tipus 1).
  - vCenter és el programari de monitorització que permet:
    - transferir MV entre servidors inclús mentre estan funcionant
    - serveis de disponibilitat, reiniciant màquines o instal·lant-ne de noves en cas de fallada.

Virtualització

- Virtualització i continuïtat de negoci
  - Disminueix la possibilitat que es materialitzin amenaces de seguretat contra els servidors.
  - Servidors on premise:
    - Espai tancat i controlat (qui pot accedir, qui ha accedir i quan)
    - Control de temperatura i humitat
    - Detecció d'incendis, extinció d'incendis
    - Manteniment de hardware, reparacions
    - Obsolescència del hardware
    - Poca flexibilitat d'adaptació al canvi
  - El núvol, una bona opció? Què passa si cau la xarxa?

Contingut

- Riscos i continuïtat de negoci
- Virtualització
- **Còpies de seguretat**
- Estacions de treball
- Plans de continuïtat de negoci

Còpies de seguretat

- Permeten minimitzar l'impacte de la pèrdua de dades.
- Cal definir de què es fa còpia de seguretat
  - Bases de dades, màquines virtuals, etc.
  - Dades de les persones de l'organització, que siguin a les seves carpetes d'usuari.
- Minimitzar els problemes als servidors
  - Sistemes RAID
- Processos de còpia de seguretat, quan s'han de fer?

Còpies de seguretat

- Còpies de seguretat diàries, cap a servidors de disc intermediaris.
- Còpies de seguretat cap a cinta, ideal pels magatzems de dades.
- Còpies externes!
- En organitzacions de seus distribuïdes, còpies mirall en diferents seus.

Contingut

- Riscos i continuïtat de negoci
- Virtualització
- Còpies de seguretat
- **Estacions de treball**
- Plans de continuïtat de negoci

Estacions de treball

- La gestió i manteniment generen molta feina al personal d'informàtica de les organitzacions.
- Per tal de minimitzar problemes davant la materialització d'amenaces, convé minimitzar el temps de restitució de les estacions de treball:
  - Màquines de backup, maquinari idèntic?
  - Imatges de sistemes operatius + programari
  - Estacions de treball congelades
  - Peces de recanvi
- Programari anti-virus degudament actualitzat
  - Actualitzacions des d'un servidor local, a la nit o de manera aleatòria (interrupció del servei?)

Contingut

- Riscos i continuïtat de negoci
- Virtualització
- Còpies de seguretat
- Estacions de treball
- **Plans de continuïtat de negoci**

Plans de continuïtat de negoci

- Des del punt de vista de la seguretat de la informació, l'objectiu de totes les organitzacions és mirar de reduir els riscos i evitar les possibles incidències de seguretat.

Què s'ha de fer quan tota la resta falla?

- Hi ha normatives de referència
  - ISO 27005: gestió de riscos de la seguretat de la informació
  - ISO 31000: gestió de riscos, principis i guies (similar a l'anterior, però enfocat a qualsevol tipus de risc).

Plans de continuïtat de negoci

- Sempre es pot donar alguna situació impossible de protegir o d'evitar, per això les organitzacions necessiten crear plans de continuïtat de negoci.
- Les mesures adoptades o bé poden fallar o bé són insuficients.
- Depenent de l'organització, la interrupció de l'activitat de negoci pot comportar un autèntic caos, i traduir-se així en pèrdues econòmiques elevadíssimes.
- Normatives de referència en la continuïtat de negoci:
  - ISO 22301: Gestió de la continuïtat de negoci
  - ISO 27031: Guia de continuïtat de negoci referent a tecnologies de la informació i comunicacions.

Plans de continuïtat de negoci

- Diferents “noms” pels plans de continuïtat de negoci
  - ***Disaster recovery planning***, estratègia planificada en fases amb l’objectiu de recuperar tots els serveis relacionats amb les TIC.
  - ***Businnes resumption planning***, estratègia de reprendre els processos de negoci aturats a causa de problemes amb les TIC.
  - ***Continuity of operations planning***, estratègia de reprendre les funcions estratègiques d’una organització.
  - ***Contingency planning***, recuperar els serveis i recursos TIC.
  - ***Emergency response planning***, protecció dels 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)**, 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.

Plans de continuïtat de negoci

- Característiques dels PCN
  - Es troba en un procés de millora contínua de la gestió de riscos de l'organització
  - Ja 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.

Plans de continuïtat de negoci

- Objectius dels PCN:
  - Mantenir el nivell de servei en els límits que ha definit la companyia, de manera que es pugui considerar que l'activitat no està interrompuda.
  - Establir un període de recuperació mínim per a garantir la continuïtat del negoci.
  - 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.

Plans de continuïtat de negoci

- Els PCN estan basats en un altre dels elements fonamentals des del punt de vista de la seguretat: **l'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.

Plans de continuïtat de negoci

- Elements dels plans de continuïtat de negoci:
  - **1. Definició de les situacions crítiques**
    - Identificar els riscos analitzats, riscos que poden afectar l'organització i que no es poden evitar implantant diferents mesures de seguretat. 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.
      - **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.

Plans de continuïtat de negoci

- Elements dels plans de continuïtat de negoci:
  - **2. Assignació de responsabilitats**
    - **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.
    - **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.

Plans de continuïtat de negoci

- Elements dels plans de continuïtat de negoci:
  - **3. Definició de les accions de resposta**
    - **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.

Plans de continuïtat de negoci

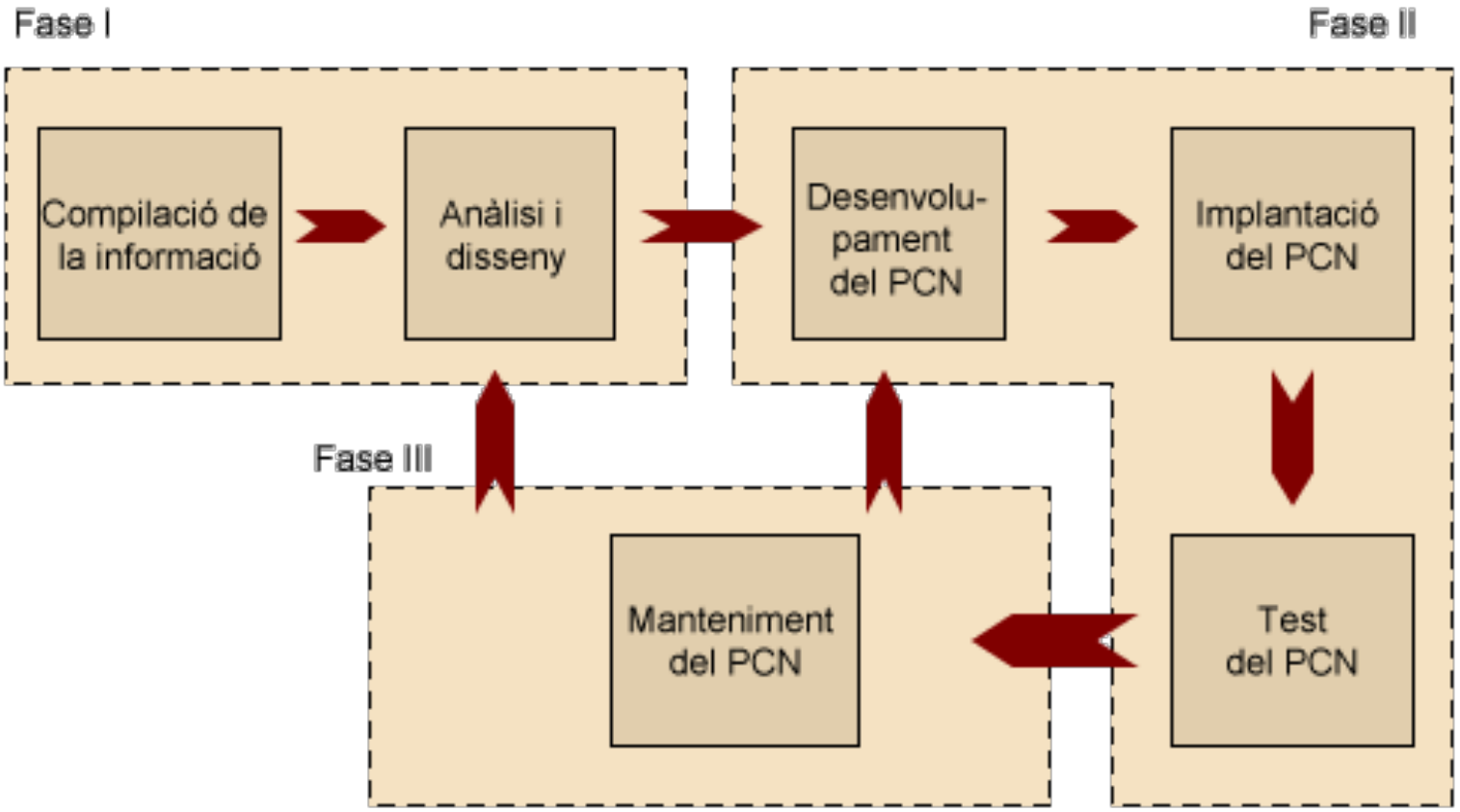
- Elements dels plans de continuïtat de negoci:
  - **4. Manteniment**
    - Es tracta de mantenir tant els plans de continuïtat de negoci com els plans de contingència que els formen. Com a resultat d'això s'obté el següent:
      - **Dades de prova i disparament.** Després de l'execució d'un pla, s'analitzen 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.

Plans de continuïtat de negoci

- 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.

Plans de continuïtat de negoci

- Fases (cicle de Deming)



Plans de continuïtat de negoci

- **Fase I**
  - Aquesta fase és la més important amb vista al resultat final i també es pot considerar com la més complicada.
  - S'analitza quant està disposada a invertir l'organització (en temps i diners) per a recuperar-se dels desastres.
  - Processos:
    - **Gestió de riscos.** Identificar els riscos a què està exposada l'organització.
    - ***Business impact analysis*.**
    - Desenvolupament d'estratègies del pla de continuïtat de negoci.

Plans de continuïtat de negoci

- **Fase I**
  - ***Business impact analysis*.**
    - 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. S'ha de tenir en compte que tothom considera que les seves funcions són les més importants.
    - 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. L'objectiu final d'aquesta fase és identificar les conseqüències econòmiques de la interrupció dels processos clau del negoci.

Plans de continuïtat de negoci

- **Fase I**
  - ***Business impact analysis*.** Classificació dels processos
    - **Processos crítics.** Processos la interrupció dels quals comporta unes conseqüències econòmiques que no pot assumir l'organització.
    - **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. Comporta un cost mitjà per a l'organització i possiblement, contractar persones.
    - **Processos no crítics**

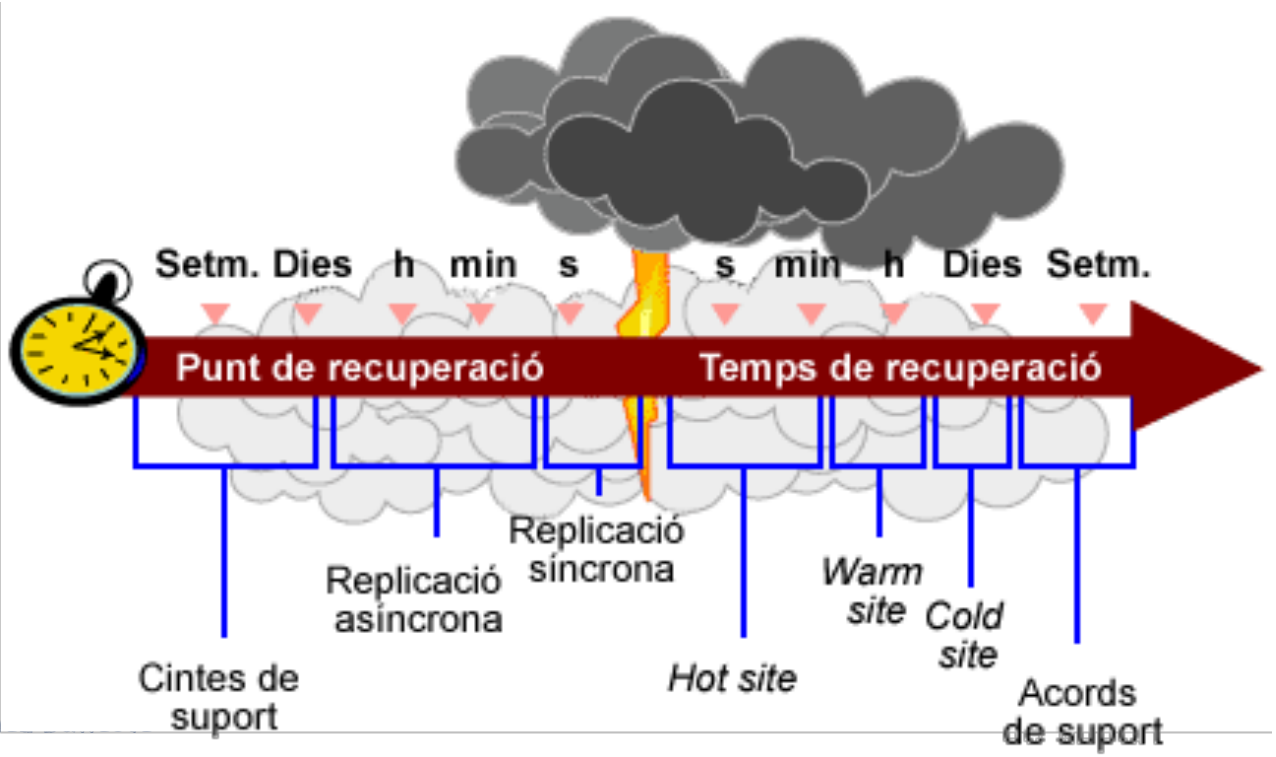
Plans de continuïtat de negoci

- **Fase I**
  - ***Business impact analysis*.** Què cal identificar en les entrevistes?
    - Nivell de servei que s'ha de mantenir en l'organització en qualsevol circumstància.
    - Temps màxim d'inactivitat.
    - Existència de processos alternatius (per exemple en paper).
    - Com sabem que s'haurà arribat al *recovery point objective.*

Plans de continuïtat de negoci

- **Fase I**
  - Desenvolupament d'estratègies del pla de continuïtat de negoci

Cold site, warm site, hot site. Aquest darrer per a infraestructures crítiques/processos crítics o vitals, pràcticament una rèplica dels recursos físics originals, ni que sigui de dimensions més reduïdes.



Plans de continuïtat de negoci

- **Fase II**
  - Es defineixen les diferents accions que s'han de dur a terme per a la recuperació.
  - S'indica, amb tota mena de detalls, les accions que s'han de fer per a recuperar la normalitat.
  - Es compren equips, es designen emplaçaments i personal i s'aconsegueixen la resta dels recursos que es requereixin per a executar els plans.
  - Han de ser provats abans que calgui posar-los en pràctica.

Plans de continuïtat de negoci

- **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.

Plans de continuïtat de negoci

- **Estructura del PCN (document)**

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.

Plans de continuïtat de negoci

- **Descripció de la situació que s'ha de controlar**
  - 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.
  - 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.
  - Els temps de resposta, els que determinen el temps que l'organització pot estar sense executar els seus processos, són fonamentals.
  - Estimació dels 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.

Plans de continuïtat de negoci

- **Llista de procediments concrets i dels responsables**
  - 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.
- **Disparament d'alarma**
  - 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.

Plans de continuïtat de negoci

- **Pla de resposta**
  - 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:
    - **Accions per a protegir les persones.**
    - **Accions per a tallar la situació de risc:** control de les amenaces. Per exemple, l'extinció d'un incendi o la desconnexió d'un router.
    - **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** a organitzacions externes i, si escau, als mitjans de comunicació, 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.

Plans de continuïtat de negoci

- **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.
    - **Recursos necessaris per a mantenir l'operació.** Es detecta quins recursos o actius són necessaris per a executar aquestes accions.
    - **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:** moments i reponsables.
    - **Identificació del personal implicat.**
    - **Registre de les accions** que es duen a terme.

Plans de continuïtat de negoci

- **Pla de recuperació**
  - Consisteix en el conjunt d'accions que s'han de dur a terme per a retornar a la situació inicial.
  - El PCN 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.
  - Elements del pla de recuperació:
    - Restitució d'actius. Arrencada dels sistemes i serveis. Proves per a comprovar els sistemes restaurats. Posada en operació. Retirada dels plans de suport. Registre de les accions fetes i dels resultats :-)

Plans de continuïtat de negoci

- **Pla d'anàlisi i millora**
  - S'han recollit dades per analitzar per poder millorar el PCN.
- **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.