ISACA®
Trust in, and value from, information systems
Barcelona Chapter

Assegurar la continuïtat de la meva activitat en cas de desastre

Joan Barceló i Xavier Rubiralta

Índex

- Introducció: confidencialitat, integritat i DISPONIBILITAT
- Business Impact Analysis (què és important)
- Recovery Time Option (temps que es pot estar aturat)
- Recovery Point Option (dades que es poden perdre)
- Backups: tipus: full, incremental i diferencial
- Backups: ubicacions possibles
- Alternative sites: duplicació, hot sites, cold sites, acords recíprocs
- Referent: ISO 22301 Gestió de la Continuïtat de Negoci
- Diferències entre BCP i DRP
- Desenvolupament d'un BCP: estratègia, equip, documentació, proves, actualització, etc
- Comunicació en cas de desastre: interna, i a les autoritats i mitjans de comunicació

Introducció : confidencialitat, integritat i DISPONIBILITAT

- Confidencialitat
- Integritat
- Disponibilitat

Introducció : confidencialitat, integritat i DISPONIBILITAT

- Disponibilitat

Business Impact Analysis (què és important)

- Un anàlisis d'impacte al negoci (BIA) és una eina per estimar l'afectació que podria patir una organització com a resultat de la ocurrència d'un incident o desastre

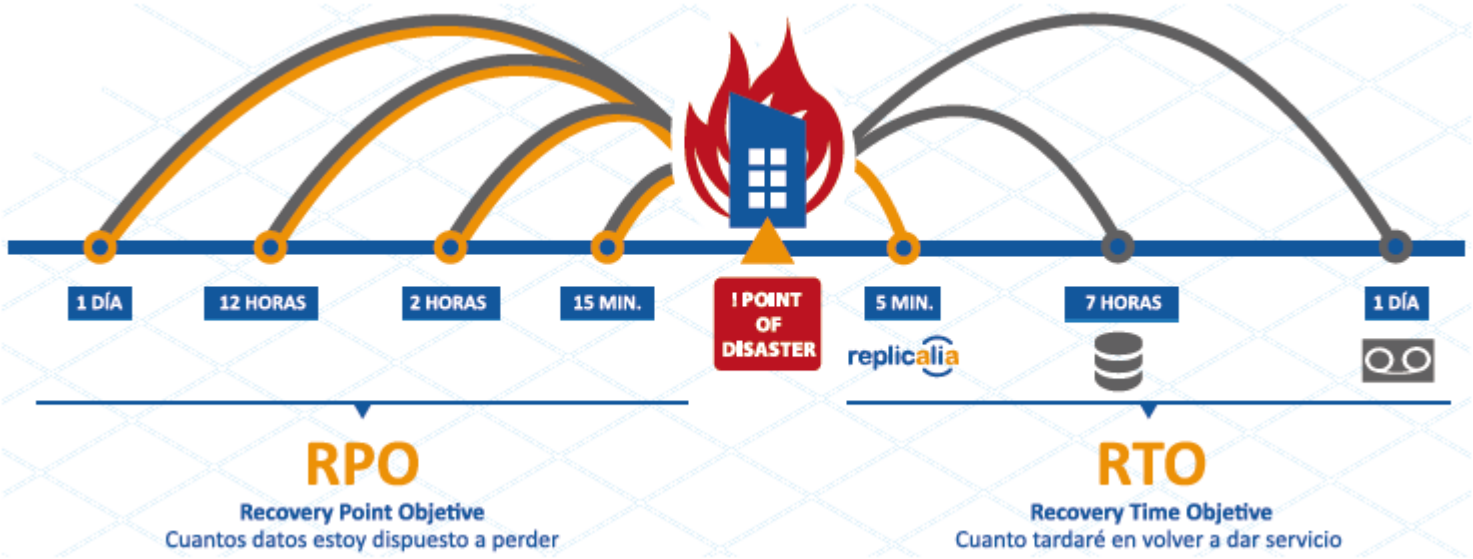
- Objectius:
  - Identificar processos crítics
  - Estimar el recursos necessaris
  - Definir RTO i RPO
  - Prioritzar

- Beneficis:
  - Ajuda a preparar un DRP i un BCP

Recovery Time Option (temps que es pot estar aturat)

- RTO Temps que es tarda en tornar al servei

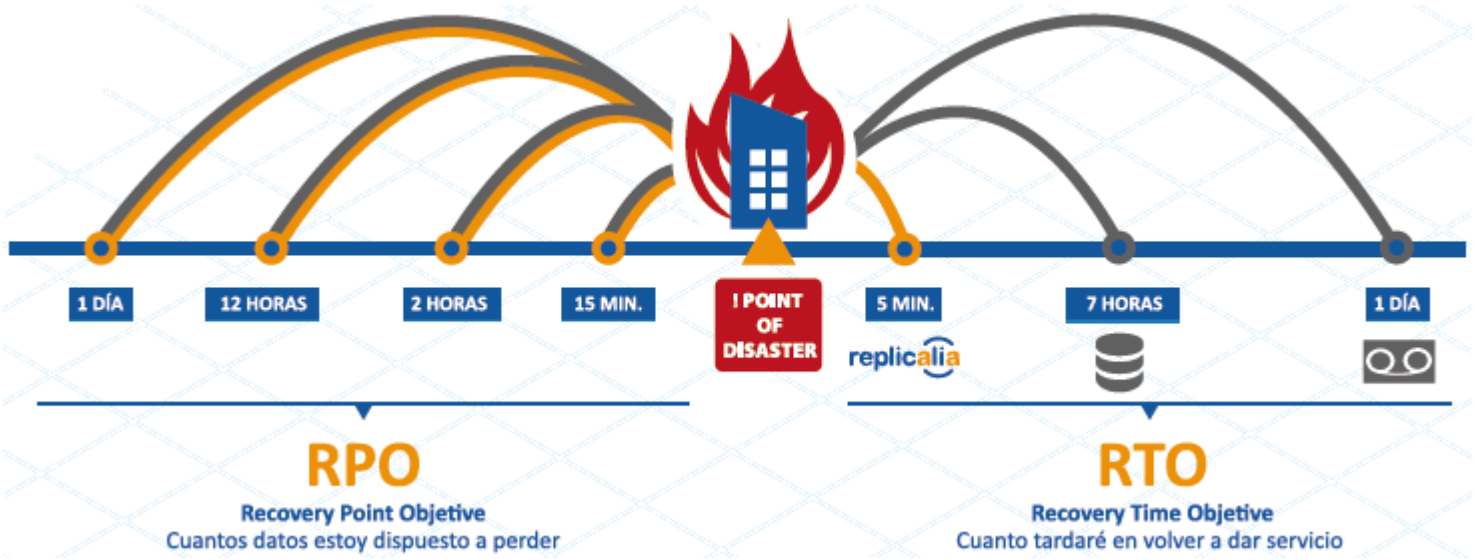
- Definir:
  - Màxim temps sense activitat tolerable
  - Interrupció màxima tolerable per processos



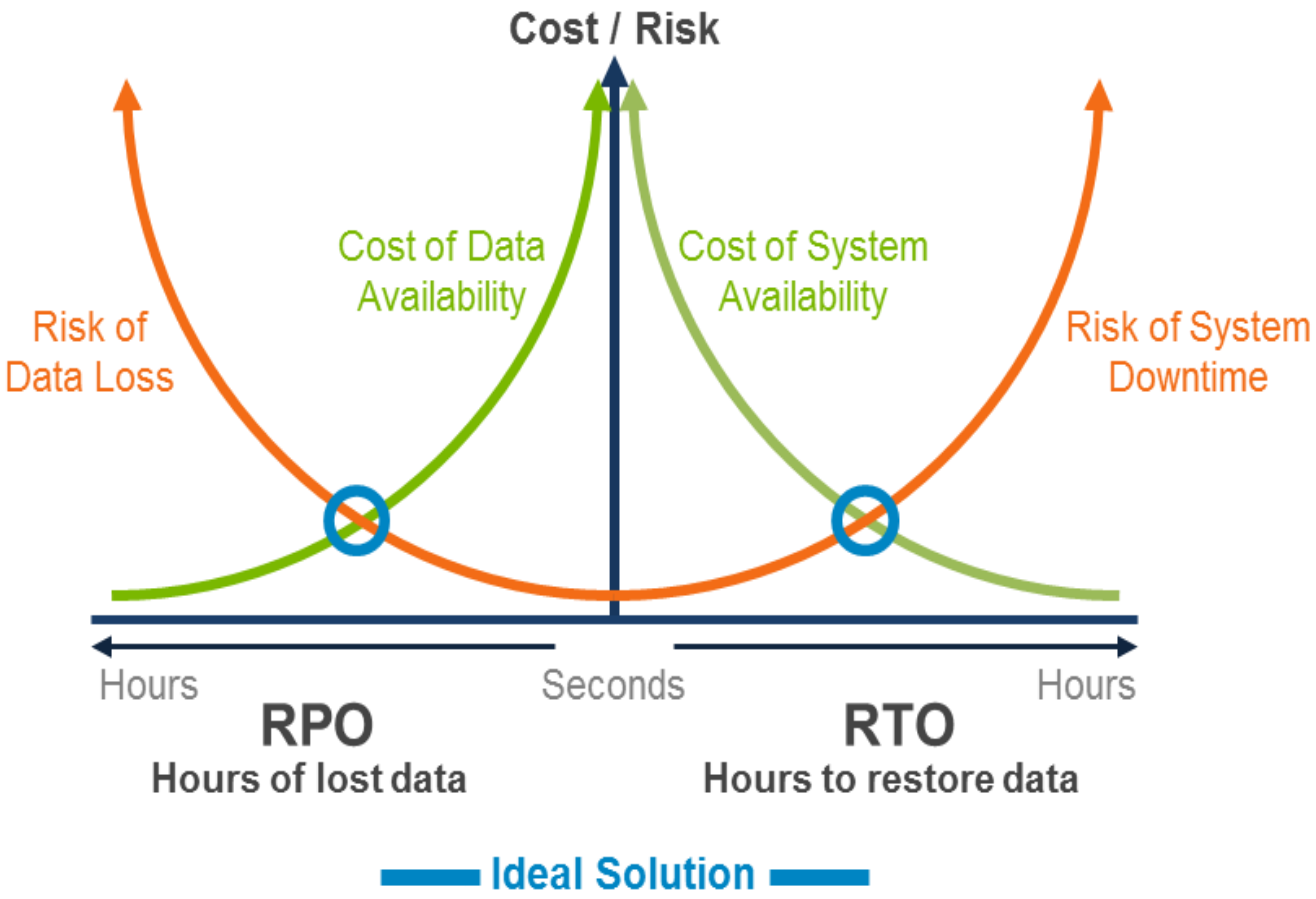
Recovery Point Option (dades que es poden perdre)

- RPO capacitat de recuperar dades en un punt anterior

- Definir:
  - Quantes dades podem perdre (en el temps)



Quines dades podem perdre, en quant temps i a quin cost?



Backups – còpia de seguretat

- Una bona còpia de seguretat ha de:

  - Ser automàtica
  - Guardar diferents versions dels fitxers
  - Copiar les dades a distint suports i localitzacions
  - Disposar d’alertes que indiquen qualsevol error

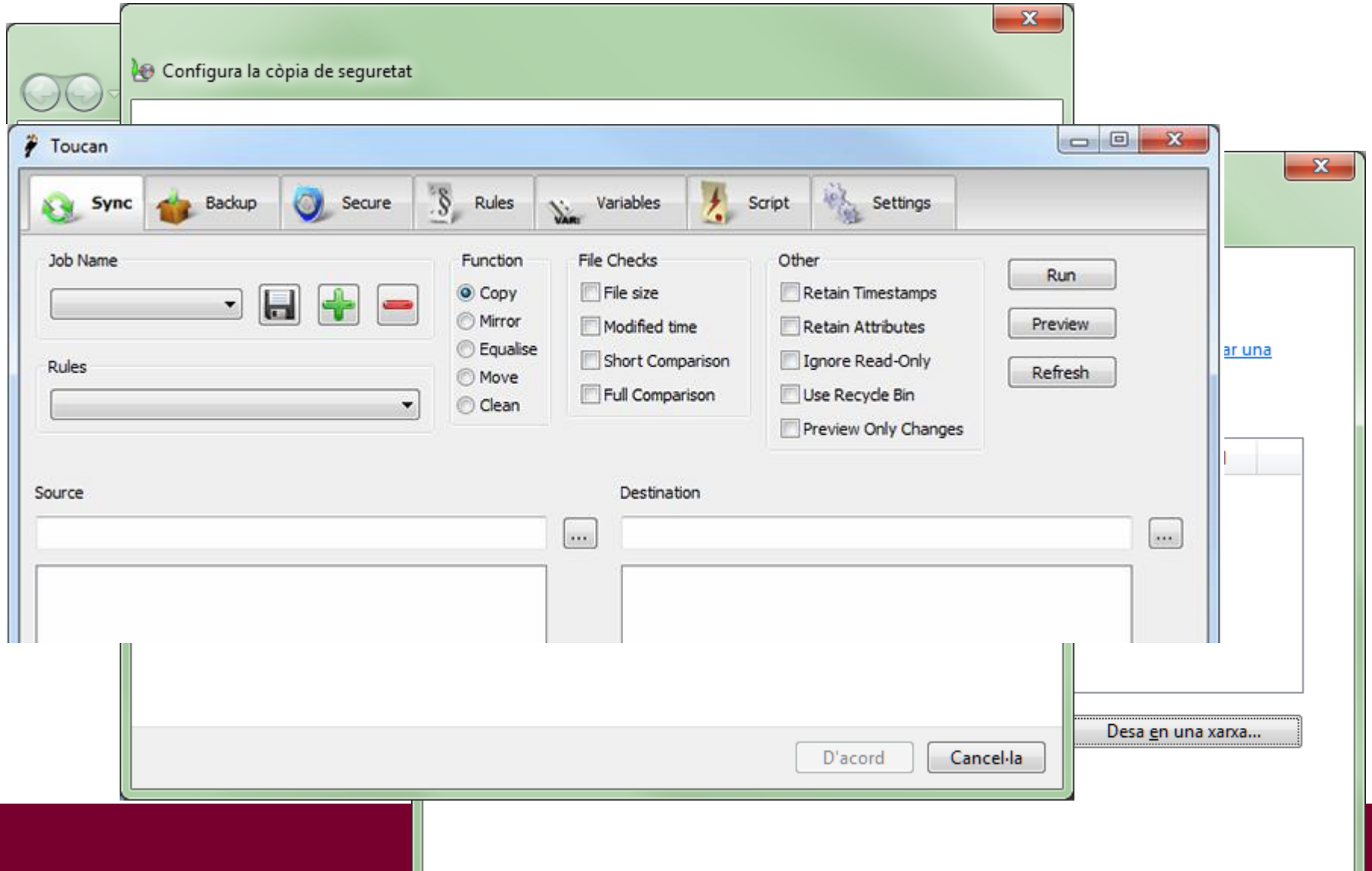
Backups tipus: full, incremental i diferencial

- Complerta
- Incremental, la més ràpida
- Diferencial

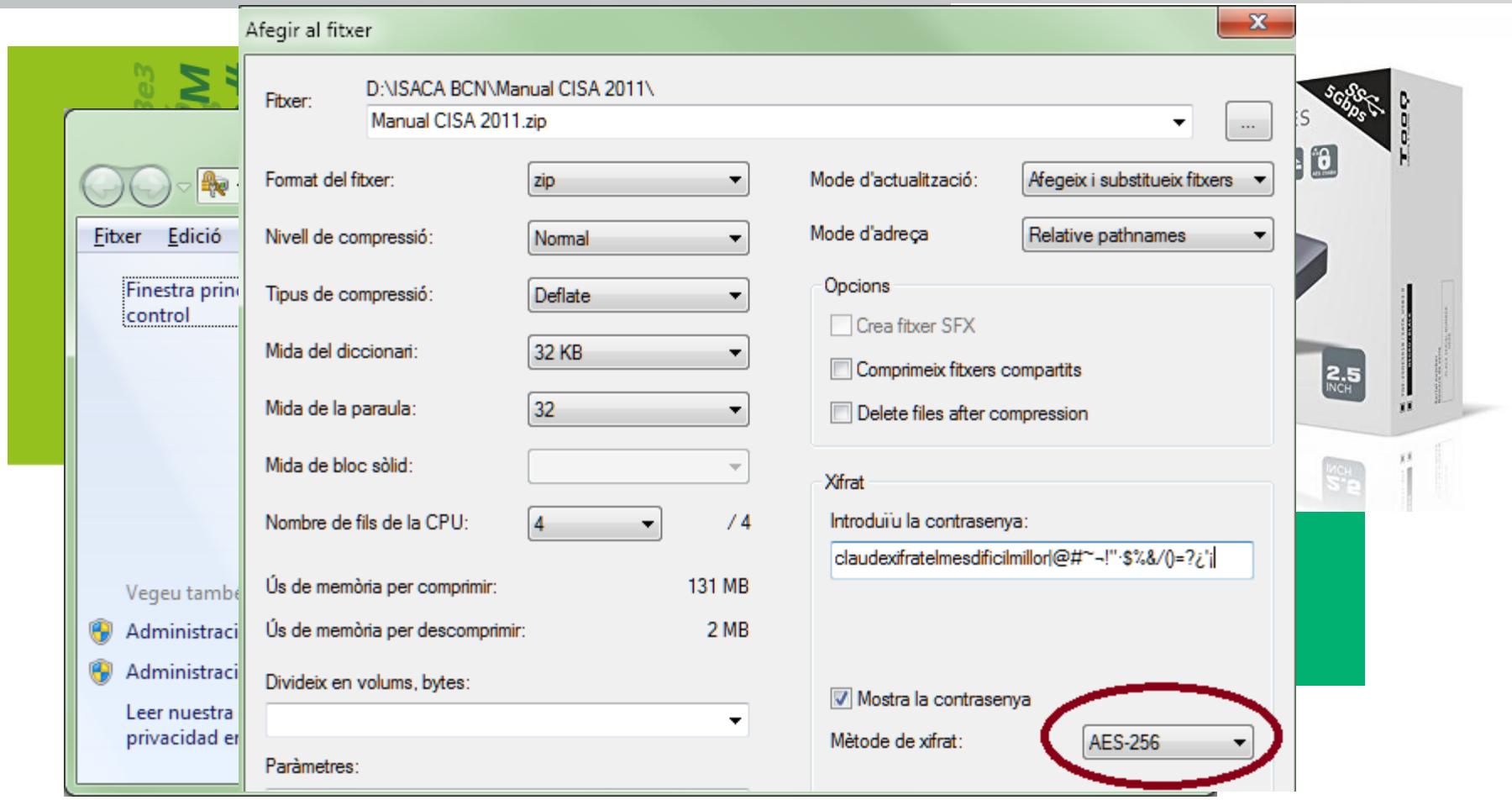
- I com ... Xifrat o en clar?

- Eines a windows
  - Backup and restore, permet copiar a HD intern, extern o xarxa
  - Però hi ha més vida ...

Backups, com fer-ho?



Backups xifrao o sense xifrar



Backups: ubicacions possibles

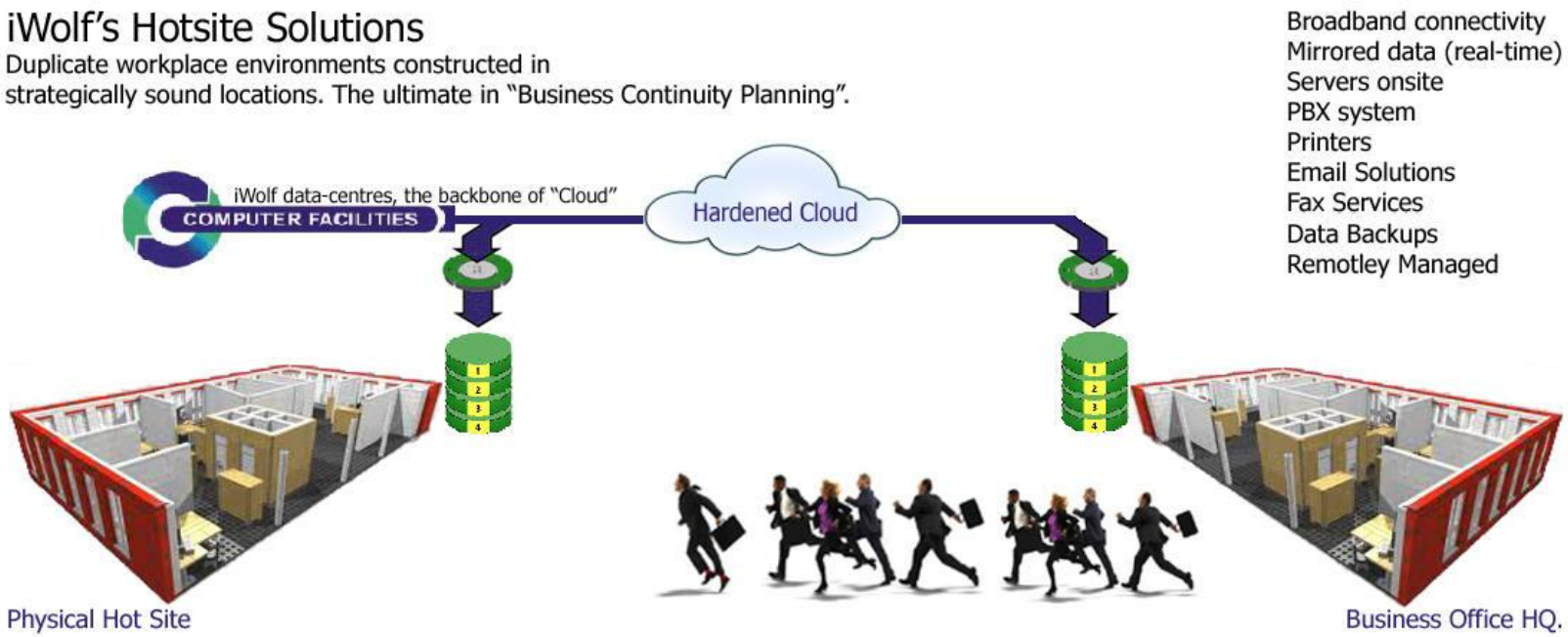
- Regla de les 3 còpies
  - Una al lloc de treball
  - Una a un lloc diferent (xifrada)
  - La tercera al núvol, preferentment xifrada (obligatori si te dades personals)

Backups: ubicacions possibles

- Reviseu que teniu !

Alternative sites: duplicació, hot sites, cold sites, acords recíprocs

- Alternative sites: duplicació, hot sites, cold sites, acords recíprocs



Referent: ISO 22301 Gestió de la Continuïtat de Negoci

- **UNE-ES ISO 22301:2015 Protecció i seguretat dels ciutadans. Sistema de Gestió de la Continuïtat de Negoci. Especificacions**

- La ISO 22301 és la norma internacional que utilitzant el cicle de millora contínua (PDCA) defineix els requisits per a la planificació, la implantació, l'operació, el seguiment, la prova, el manteniment i la millora d'un Sistema de Gestió de Continuïtat de Negoci documentat. És certificable.

- Altres normes relacionades: la ISO 31000 Gestió del risc, principis i directrius, la ISO 27001 de Sistemes de Gestió de la Seguretat de la Informació i la ISO 20000 del Sistema de Gestió de Serveis de Tecnologies de la Informació. Les dues últimes són certificables.

- NIST SP 800-34 Contingency Planning Guide for Federal Information Systems

Referent: ISO 22301 Gestió de la Continuïtat de Negoci

- **Contingut de la ISO 22301**

- Introducció
- Objectiu i camp d'aplicació
- Altres normes
- Termes i definicions
- Context de l'organització (necessitats i expectatives, i abast)
- Lideratge (compromís de la direcció, política i responsabilitats)
- Planificació (objectios, plans i accions)
- Suport (recursos, conscienciació i capacitació, i documentació)
- Operació (planificació, anàlisi d'impacte en el negoci, estratègia, implantació i proves)
- Avaluació del rendiment (supervisió, auditoría i revisió direcció)
- Millora (correccions i millora contínua)

Diferències entre BCP i DRP

El pla de continuïtat de negoci (BCP) és un pla que ha de permetre a una organització a recuperar-se i restaurar les seves funcions crítiques parcial o totalment interrompudes, en un temps predeterminat després d'una interrupció no esperada. En altres paraules, és com l'organització es prepara per a futurs incidents que la puguin posar en perill.

El pla de recuperació davant de desastres (DRP) és el procés de recuperació que inclou les dades, el hardware i el software crític, per tal que un negoci pugui restablir les seves operacions en cas d'un desastre natural o causat per persones. També s'hi haurien d'incloure problemes derivats de la pèrdua inesperada de personal clau.

Diferències entre BCP i DRP

ISACA
Trust in, and value from, information systems
Barcelona Chapter

BCP I DRP s'utilitzen freqüentment de forma indistinta i per tant la diferència entre ambdós termes està desdibuixada. Des d'un punt de vista pràctic s'hi poden veure diferències..

BCP fa referència a com una empresa/entitat s'organitza per tal de poder continuar amb la seva activitat (de negoci) en cas d'un desastre.

DRP fa referència a com la funció de Tecnologia de la Informació s'organitza per a recuperar l'activitat en cas de desastre.

En qualsevol cas la tecnologia, encara que important, és només una part del procés de assegurar la continuïtat del negoci. Són importants persones, comunicació, documentació, organització, responsabilitats, etc.

Desenvolupament d'un BCP: estratègia, equip, documentació, proves, actualització, etc

A l'estratègia d'un BCP cal considerar:

- Implicació i visió de la direcció
- Participació de les unitats de negoci i de TI
- Donat el cost, caldrà aplicar-ho al que és crític, en funció de l'anàlisi d'impacte fet, dels requeriments establerts (RTO i RPO) i de les opcions tecnològiques disponibles
- Estudiar suport extern davant la complexitat en la confecció del pla (consultoria)
- Estudiar solucions pròpies i de tercers en la implementació (sistemes alternatius)
- Establir la estratègia de persones implicades, dinàmica de proves i procés d'actualització
- El BCP ha de ser eficaç i eficient quan sigui necessari

Desenvolupament d'un BCP: estratègia, equip, documentació, proves, actualització, etc

Referent a l'equip humà d'un BCP cal considerar:

- Àrees implicades: direcció, negoci, TI, legal, comunicació, RRHH, empreses externes, etc
- Persones implicades tant en la redacció del BCP i com en l'activació del BCP en cas de desastre
- Autoritat/s per a activar el BCP i prendre decisions
- Equip que comprengui tots els rols i funcions per executar el BCP
- Substituts de les persones clau
- Mecanismes de comunicació i convocatòria de l'equip
- Procediment per ubicar les persones en el seu lloc
- Rol, funcions i responsabilitats ben definits
- Interlocutors amb empreses i entitats externes
- Contemplar dificultats d'assistència de les persones

Desenvolupament d'un BCP: estratègia, equip, documentació, proves, actualització, etc

ISACA
Trust in, and value from, information systems
Barcelona Chapter

Referent a la documentació d'un BCP cal considerar:

- Tota documentació necessària ha d'estar disponible a les persones quan executin el BCP
- Pot no haver-hi connectivitat i per tant accés a documentació remota
- En cas de paper, assegurar que està en el lloc on cal
- Contemplar el cas d'ubicacions diferents
- No descuidar la confidencialitat especialment abans d'activar el BCP
- Si la informació no està actualitzada ocasionarà problemes
- Contemplar el cas d'accés per part de tercers
- Ha d'estar redactada en un registre intel·ligible pels executors del BCP (tècnics, de negoci, externs, etc)

Desenvolupament d'un BCP: estratègia, equip, documentació, proves, actualització, etc

ISACA
Trust in, and value from, information systems
Barcelona Chapter

Referent a les proves d'un BCP cal considerar:

- Rigor de les proves: des d'una lectura del BCP, una prova simulada, una prova parcial o una prova total de la mateixa magnitud que un incident real
- Escalat de proves avaluant el risc que la prova afecti el servei en producció
- Un pla que no s'ha provat prou bé és molt probable que no sigui efectiu quan es necessiti
- D'una prova cal esperar que apareguin punts de millora i fins i tot errors a modificar en el pla
- La prova té un cost i encara més si s'ha contractat serveis externs
- La prova es pot fer "avisant" als que l'han d'executar o "sense avisar"

Desenvolupament d'un BCP: estratègia, equip, documentació, proves, actualització, etc

ISACA
Trust in, and value from, information systems
Barcelona Chapter

Referent a l'actualització d'un BCP cal considerar:

- Els processos de negoci estan en constant evolució
- Els sistemes informàtics estan en constant evolució
- Un sistema no es podrà recuperar seguint un BCP que correspon a una versió antiga i no operativa (obsolet)
- No tots els canvis en processos i sistemes han d'afectar al BCP, ja que el BCP compren només el que és crític
- Però si els canvis l'afecten, s'haurà de canviar el BCP i hi haurà d'haver les proves corresponents
- A priori cal esperar que d'una prova se'n derivin actualitzacions del BCP
- S'han d'actualitzar totes les còpies del BCP
- Les persones implicades hauran d'assabentar-se de les actualitzacions, i també terceres parts

Comunicació en cas de desastre: interna, i a les autoritats i mitjans de comunicació

Referent a la comunicació interna en cas de desastre cal considerar:

- S'ha de poder contactar amb totes les persones implicades en l'execució del BCP, i també els substituts
- És probable que els canals de comunicació habituals no funcionin, n'hi ha d'haver d'alternatius (telefonia)
- Les persones del BCP es poden trobar fora del lloc de treball, i amb dificultats per comunicar-se i per anar al lloc des d'on s'ha d'executar el BCP
- La comunicació ha d'adreçar-se només als interessats i no a altres persones
- Es comunicarà amb les persones a mesura que siguin necessaris per a participar en l'execució del BCP
- També caldrà informar a la resta d'empleats del que sigui oportú

Comunicació en cas de desastre: interna, i a les autoritats i mitjans de comunicació

Referent a la comunicació amb les autoritats en cas de desastre cal considerar:

- Quan un incident és greu el més important són les vides humanes. En aquest sentit probablement caldrà comunicar-ho a les autoritats i a serveis d'emergència
- S'han de conèixer els interlocutors i els canals de comunicació amb les autoritats
- Un BCP pot afectar a la població local
- En el cas d'infraestructures crítiques cal seguir el que marca la llei i normatives aplicables (Llei 8/2011)
- En molts casos caldrà seguir les indicacions de les autoritats per exemple en evacuacions o confinament
- Amb les autoritats hi haurà de parlar qui estigui nomenat per fer-ho, no qualsevol empleat

Comunicació en cas de desastre: interna, i a les autoritats i mitjans de comunicació

Referent a la comunicació amb els mitjans de comunicació en cas de desastre cal considerar:

- És un punt crític, s'ha de ser molt curós amb el que es transmet
- No dir res o faltar a la veritat és igual de perjudicial
- Només hi podrà parlar qui estigui nomenat i analitzant molt bé el que es diu
- Ningú més podrà respondre trucades dels mitjans de comunicació
- Cal tenir molt presents les xarxes socials i els seus riscos de descontrol i generar alarma social
- Evitar filtracions de familiars, coneguts, empreses subcontractades, etc
- La reputació de la companyia pot veure's perjudicada

ISACA®
Trust in, and value from, information systems
Barcelona Chapter

Moltes gràcies

xavier.rubiralta@isacabcn.org

joan.barcelo@isacabcn.org