

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 1 / 15



Llicència Creative Commons:
Reconeixement – No Comercial – Compartir Igual 2.5.

Sou lliure de copiar, distribuir i comunicar públicament l'obra, així com de fer-ne obres derivades, **en les següents condicions:**


Reconeixement. Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el licenciadador.

No comercial. No podeu utilitzar aquesta obra per a finalitats comercials.

Compartir amb la mateixa llicència. Si altereu o transformeu aquesta obra, o en genereu obres derivades, només podeu distribuir l'obra generada amb una llicència idèntica a aquesta.


- Quan reutilitzeu o distribuïu l'obra, heu de deixar ben clar els termes de la llicència de l'obra.
- Alguna d'aquestes condicions pot no aplicar-se si obteniu el permís del titular dels drets d'autor.

Podeu trobar el text legal de la llicència a: [Creative Commons Attribution-NonCommercial-ShareAlike 2.5 License](https://creativecommons.org/licenses/by-nc-sa/2.5/)

ÍNDEX

1.	OBJECTIU I MOTIVACIÓ.....	2
2.	ÀMBIT I VIGÈNCIA	4
3.	COMPLIMENT LEGAL I ESTÀNDARDS RECONEGUTS.....	4
4.	DESCRIPCIÓ	5
5.	CONTROL	11
6.	PENALITZACIONS.....	11
7.	DIVULGACIÓ	11
8.	REVISIÓ	11
9.	GLOSSARI DE TERMES	11
10.	DOCUMENTACIÓ REFERENCIADA.....	13
11.	PARAULES CLAU	13
12.	ANNEX A – MODEL DE POLÍTICA DE LA GESTIÓ DE LA CONTINUÏTAT	14

Versió	Redactat / revisat per	Aprobat per	Data aprovació	Data publicació
1.0	CTTI – QSRaP	Comitè Direcció CTTI	21/2/2011	6/6/2011

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 2 / 15

1. OBJECTIU I MOTIVACIÓ

La creixent necessitat de disposar dels serveis i dels processos de forma continuada i sense interrupcions està sent el detonant per considerar els plans de continuïtat de negoci com una eina indispensable dins de qualsevol organització. Els **incidents** recents (11-S a Nova York o l'incendi de la Torre Windsor a Madrid) han posat de manifest la importància que té per a tothom la disponibilitat dels serveis i processos més crítics. En aquests mateixos termes, la disponibilitat de serveis i infraestructures crítiques de la Generalitat de Catalunya es converteix en un objectiu prioritari per garantir els serveis al ciutadà.

S'ha de tenir present que una interrupció prolongada dels processos crítics podria tenir unes conseqüències molt negatives per al país i podria posar en **risc** el subministrament dels serveis bàsics per als ciutadans de Catalunya. A títol d'exemple:

- Algú es planteja que un servei d'emergències no funcioni durant hores perquè ha marxat la llum?
- Algú es planteja que un hospital no pugui donar servei perquè la xarxa informàtica no funciona?
- Quan de temps un empleat públic pot desenvolupar la seva feina sense correu electrònic o telèfon, o sense poder accedir als sistemes d'informació perquè han deixat de funcionar?
- Quan de temps pot funcionar de forma normal un jutjat sense cap sistema d'informació?
- Quan de temps un ciutadà està disposat a esperar que la pàgina web de tràmits no estigui operativa?
- Què passa si tots els treballadors d'un departament/organisme es posen malalts? Com es dona el servei?
- Què passa si els treballadors d'un departament/organisme no poden accedir al seu lloc de treball (per una nevada, per una vaga, etc.)?
- Què passa si la xarxa de comunicacions dels serveis d'emergència no funciona?
- Què passa si no es poden dispensar medicaments a les farmàcies mitjançant a la recepta electrònica?


Per aquest motiu, en el marc normatiu de la seguretat de la informació, la Generalitat de Catalunya a través del Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) estableix els requeriments en matèria de **continuïtat de negoci** per garantir que davant d'un **incident** es puguin reprendre les **activitats crítiques** en els nivells establerts fins a què puguin ser restaurades a la situació normal.

Conceptualment, es defineix la **continuïtat de negoci** com la capacitat estratègica i tàctica d'una organització per planificar i respondre als **incidents** i interrupcions del negoci i/o servei amb l'objectiu de continuar la prestació del servei a un nivell acceptable predefinit. La **continuïtat de negoci** no té un enfocament exclusivament tecnològic, sinó que contempla tots els mecanismes per protegir les persones, els processos, les àrees de treball, les xarxes de comunicacions (veu i dades), els sistemes d'informació, etc. necessaris per assolir els objectius esmentats.

Per implementar i mantenir la **Continuïtat de Negoci** en una organització, s'utilitza un model de **gestió de la continuïtat de negoci** (GCN) que contempla diferents fases –detallades més endavant– per aconseguir l'objectiu de mantenir funcionant els processos crítics de negoci en l'hipotètic cas d'ocurrència d'un desastre, disposant de respostes efectives i provades per a restaurar la provisió del negoci i/o servei en el mínim temps possible.

La GCN contempla entre d'altres les següents activitats:

- Obtindre el compromís formal de la Direcció per a la seva implantació.
- Aprovació i difusió de la política de **continuïtat de negoci**.
- Anàlisi dels **processos** de l'organització i identificació dels que són crítics.
- **Anàlisi de riscos** respecte la disponibilitat dels **recursos** que suporten els processos crítics.
- Proposta d'estratègies de continuïtat per assolir els requeriments del negoci i/o servei.

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 3 / 15

- Planificació i direcció de les situacions de crisi.
- Recuperació de la tecnologia.
- Recuperació del negoci i/o servei en un lloc alternatiu.
- Formació, proves i manteniment de forma contínua de la GCN.

Per facilitar una correcta implementació de la GCN a la Generalitat de Catalunya, el CTTI ha desenvolupat la metodologia GCNCAT de *gestió de la continuïtat de negoci* que defineix com s'implanta la GCN en totes les seves fases i que s'alinea completament amb els objectius de la Política de Seguretat de la Generalitat de Catalunya.

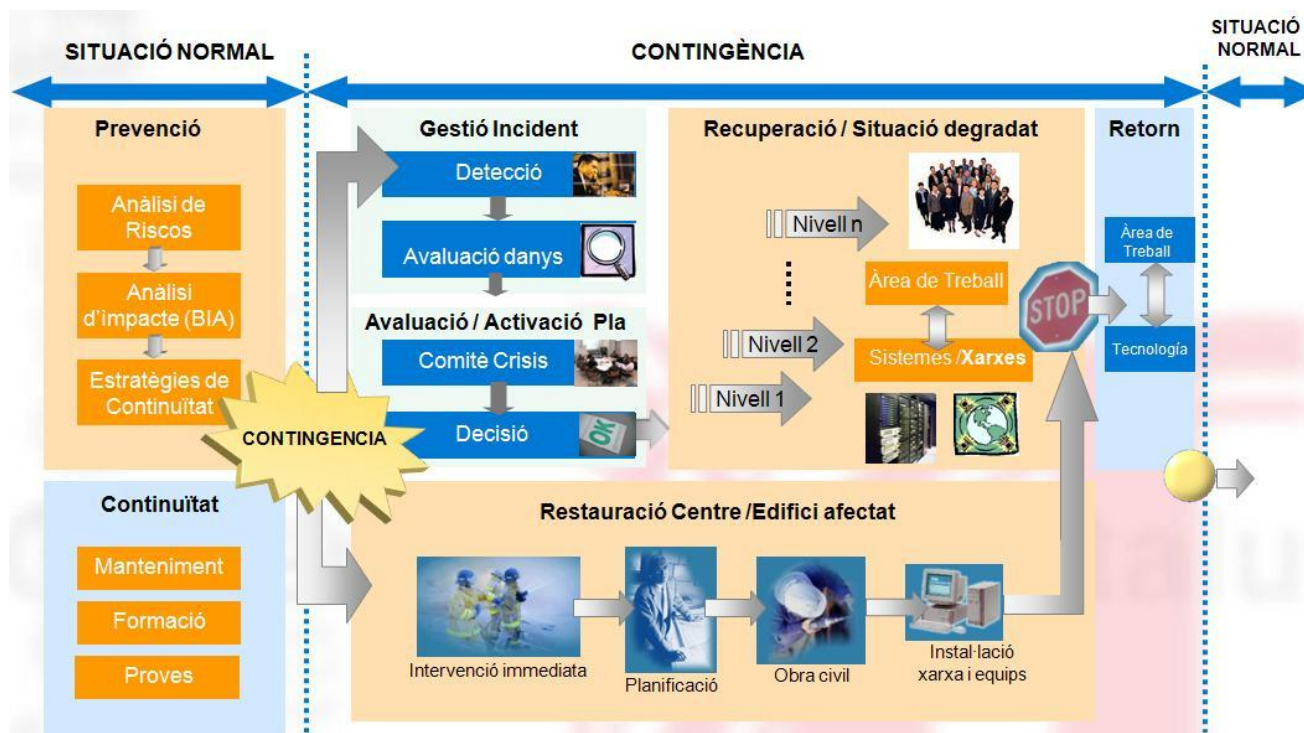
El propòsit d'aquesta guia és recollir els requeriments per a la implementació de la GCN. Està recolzada per la metodologia indicada anteriorment que amplia i desenvolupa els punts recollits en aquesta guia contemplant:


- El detall de cadascuna de les fases.
- Metodologia d'anàlisi (**impacte**, riscos, etc.).
- Formularis per a la presa de dades.
- Plantilles dels lliurables de les diferents fases.

Tant la present guia com la metodologia estan alineades amb els estàndards de seguretat i disponibilitat de la informació més reconeguts a nivell internacional.

En el següent gràfic es mostra de forma esquemàtica les diferents fases que contempla la GCN en els dos principals estats:

- En situació normal: Analitzar, definir, implementar i mantenir la GCN.
- En situació de contingència: Gestió de l'*incident*, presa de decisions, procediments de recuperació i retorn.



 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 4 / 15

2. ÀMBIT I VIGÈNCIA

La guia va dirigida a:

- Responsables de la implementació de la *gestió de la continuïtat de negoci*.
- Personal amb responsabilitat sobre la construcció, evolució, manteniment i operació dels sistemes d'informació i les infraestructures.
- Responsables de negoci i/o servei (directors de serveis o càrrecs superiors) que proporcionaran el suport, criteris i valoracions per a realitzar l'anàlisi i prendre decisions respecte la implantació de la GCN.
- Personal col·laborador (ja sigui del propi departament / ens o bé d'una empresa externa) en la implementació de la GCN.

És d'aplicació a tots els processos de la Generalitat i, conseqüentment, a tots els *recursos* (sistemes d'informació, infraestructures, persones, ubicacions, etc.) que els suporten.


Aquesta guia és d'obligat compliment per part de tot el personal del CTTI responsable d'elaborar Plans de Continuïtat de Negoci, i es recomana el seu ús també en els **Àmbits** de la Generalitat de Catalunya sense presència CTTI.

Entrarà en vigor el dia 1/3/2011 i romandrà vigent fins a la publicació d'una nova versió.

3. COMPLIMENT LEGAL I ESTÀNDARDS RECONEGUTS

La present metodologia proporciona cobertura a aspectes recollits en els següents estàndards o requeriments legals:

- ISO 27002:2005 – *Codi de bones pràctiques per a la gestió de la seguretat de la informació* - Domini 14 (Gestió de la Continuïtat de Negoci)
- BS 25999-2:2007: *Gestió de la Continuïtat de Negoci – Part 1*
- BS25777:2008 *Gestió de la continuïtat de la informació i tecnologia de comunicacions – Codi de bones pràctiques*
- *Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica (ENS) - Reial decret 3/2010*
 - 4.5 Continuïtat del servei

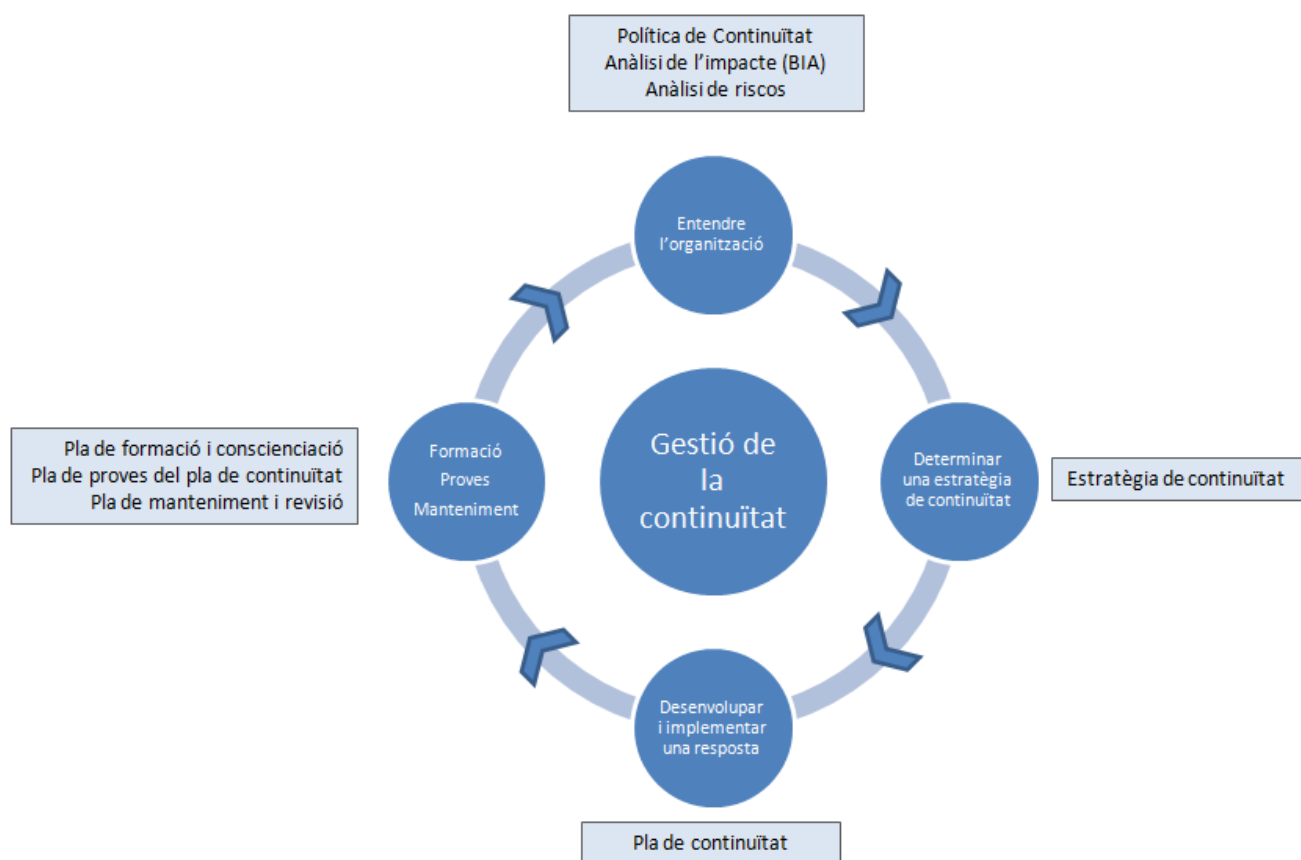
 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 5 / 15

4. DESCRIPCIÓ

4.1. Conceptes preliminars

4.1.1 Fases d'implantació i lliurables de la GCN

La GCN està basada en un enfocament de millora contínua com es mostra en el següent esquema, on es recullen les fases del cicle. Per a cada fase, s'informa dels lliurables que es generen.



En els controls de la guia, es detallen els requeriments per a cadascuna de les fases.

4.1.2 Rols principals en la GCN


A continuació es descriuen els rols principals involucrats en la GCN:

Gestor d'Incidents: Figura que lidera i coordina la fase de gestió de l'incident. És l'encarregat de notificar al gestor de continuïtat per a determinar si és necessari activar el *pla de continuïtat*.

Gestor de Continuitat: És la figura encarregada de liderar la implantació de la GCN així com l'execució del *pla de continuïtat de negoci* (PCN) davant d'una situació de contingència.

Comitè de Crisi: Equip que, liderat pel gestor de continuïtat, analitza la situació per decidir si s'activa alguna part del *pla de continuïtat*.

Direcció: Autoritza les decisions que adopta el comitè de crisi davant de l'activació, per exemple, d'un *pla de continuïtat*.

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 6 / 15

Àrees de suport: Àrees que poden informar o executar accions a petició del comitè de crisi o del gestor de continuïtat. En són exemples *recursos* humans, compres, assessoria jurídica, etc.

Responsable de continuïtat del CTTI: Assessora les diferents implementacions de la GCN que es realitzen a la Generalitat de Catalunya.

4.2. Activitats per al desenvolupament de la GCN

4.2.1 Obtenir el compromís de la Direcció

Com a requeriment previ per a l'inici de la implementació de la GCN, cal que per part de la Direcció del departament / ens es defineixi l'abast, es formalitzi el compromís a assignar els *recursos* humans, materials i econòmics necessaris, així com a donar suport i promoure la conscienciació de la cultura de la continuïtat al departament / ens, amb l'objectiu de garantir-ne l'èxit de la implantació.

C1. La Direcció ha de signar la política de continuïtat. Aquesta ha de contemplar com a mínim:

- a) Compromís de la Direcció en la implantació de la GCN.
- b) Definició de l'abast de la GCN en el departament / ens.
- c) Assignació de *recursos* humans, econòmics i materials necessaris.
- d) Promoció de la formació i conscienciació en matèria de continuïtat.
- e) Manteniment de tota la informació generada en la GCN.

En l'annex A d'aquesta guia s'inclou un model de política de continuïtat.

Si el departament / ens ja disposa d'una política de seguretat de la informació vigent i aprovada, es revisarà per a garantir que contempla els requeriments de continuïtat indicats.

4.2.2 Anàlisi d'impacte en el negoci


Es tracta del pas inicial de treball en el qual es realitza una anàlisi dels diferents processos de negoci i/o servei. L'anàlisi es realitza mitjançant entrevistes i qüestionaris a interlocutors de negoci amb l'objectiu de determinar la criticitat dels processos i determinar l'*impacte* que produiria una indisponibilitat dels mateixos en el negoci i/o servei.

C2. Es realitza una anàlisi inicial per identificar els processos de negoci i/o servei del departament / ens i els *recursos* (persones, equips, xarxes, etc.) que els hi donen suport.

C3. S'han de realitzar entrevistes als responsables dels processos de negoci i/o servei a analitzar amb l'objectiu de disposar de la valoració des del punt de vista del negoci. Es poden utilitzar els qüestionaris de la metodologia GCNCAT com a suport a la presa de dades.

C4. Com a resultat de l'anàlisi, s'elabora l'informe d'anàlisi d'*impacte* en el negoci (**BIA**) amb els següents continguts com a mínim:

- a) Definició dels processos de negoci i els *recursos* que els hi donen suport.
- b) Interrelacions i dependències entre els processos.
- c) Identificació del temps màxim d'indisponibilitat per procés (**RTO**). Aquest determinarà el temps màxim en el què ha de ser recuperat el procés i/o servei després d'una interrupció.
- d) Identificació del temps d'indisponibilitat a partir del qual el negoci i/o servei ja no es pot recuperar derivat de les greus conseqüències que provocaria per al departament / ens (**MTPD**). Aquest temps sempre serà superior al **RTO**.
- e) Identificació del volum de dades que es tolera perdre davant d'una interrupció per procés (**RPO**).

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 7 / 15

- f) Requeriments mínims necessaris quant als *recursos* per a reprendre els processos després d'una interrupció i el temps que es pot treballar en situació **degradada** fins a recuperar els nivells normals d'operació.
- g) Identificació dels processos crítics. Es defineix com a procés crític el que no pot estar aturat més de 24 hores.

C5. L'informe *BIA* ha de ser aprovat per la Direcció del departament / ens.

4.2.3 Anàlisi de riscos

A partir de la identificació realitzada en el *BIA*, es realitza una *anàlisi de riscos* (AR) quant a la disponibilitat per als *recursos* que formen part dels processos identificats com a crítics. L'objectiu és ajudar a entendre al departament / ens els *riscos* als que estan sotmesos els actius que participen en els processos crítics.


Per exemple: si es detecta que l'execució d'un procés crític per al negoci passa pel funcionament d'un servidor que no està **redundat**, aquesta anàlisi haurà de proposar l'alta disponibilitat d'aquest servidor per evitar una pèrdua de servei en cas de fallar l'equip.

- C6. S'elabora l'informe d'*anàlisi de riscos* que afecten a la disponibilitat dels *recursos* que donen suport als processos identificats com a crítics.
- C7. Conjuntament amb l'AR, s'elabora una proposta de pla d'acció per a resoldre o mitigar les debilitats o *riscos* detectats. El pla d'acció ha de contenir tant la correcció de situacions de *risc* detectades com millores que puguin augmentar la **resiliència** i donar solucions de contingència al departament / ens.
- C8. La proposta de pla d'acció ha de ser analitzada per la Direcció del departament / ens i aprovada, gestionant els *riscos* (acceptar, transmetre, assegurar, etc.) que es descarti resoldre o mitigar prèvia justificació.

4.2.4 Estratègies de continuïtat

Per poder garantir la recuperació dels processos i/o serveis en els terminis identificats en la fase d'anàlisi, cal desenvolupar i implementar **estratègies de continuïtat** que permetin alinear el departament / ens als requeriments definits.

- C9. És indispensable disposar dels requeriments de continuïtat per part del client (*RTO*, *RPO*) per poder iniciar la definició de les *estratègies de continuïtat* i el muntatge de la infraestructura tecnològica. Per aquest motiu, en la fase PD0 de la metodologia **ESPRIT** s'ha de contemplar l'anàlisi dels requeriments de continuïtat.
- C10. S'elabora un informe d'*estratègies de continuïtat* per als processos crítics, que analitza la situació actual i realitza propostes d'*estratègies* per assolir els requeriments que s'han identificat en el *BIA*.
- C11. Les *estratègies* han de contemplar els següents elements:
 - a) Processos alternatius: mecanismes o procediments alternatius que existeixin o que es puguin implementar per a poder prestar el servei.
 - b) Persones: cobertura dels requeriments de les persones identificades com a crítiques.
 - c) Informació: garantir que es pot donar compliment al *RPO* identificat en l'anàlisi.
 - d) Sistemes d'informació i comunicacions: disposar de sistemes en un lloc alternatiu, possibilitat de recuperar sistemes en un temps determinat, etc.
 - e) Instal·lacions: tant les àrees de treball (oficines, seus, etc.) com centres de processament de dades on reprendre els processos després d'una contingència.

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 8 / 15

C12.L'informe d'*estratègies* ha de ser analitzat per la Direcció per decidir les que millor s'adaptin per cost / benefici als requeriments de recuperació marcats pel negoci.

4.2.5 Pla de continuïtat

Contempla la definició dels procediments organitzatius per poder fer front a una situació de contingència no planificada, permetent executar de forma estructurada una resposta per reprendre els processos i/o serveis crítics en els temps determinats en la fase d'anàlisi.

El *pla de continuïtat de negoci* (PCN) es divideix en les següents fases:

- Gestió de l'*incident*: Fer front a la contingència i realitzar els primers passos per a analitzar-la i mitigar-la.
- Avaluació i invocació del pla: Constitució del comitè de crisi liderat pel gestor de continuïtat de negoci. El comitè ha d'analitzar la situació i decidir quin dels procediments de continuïtat activa en funció de la contingència. La decisió ha de ser aprovada per part de la Direcció.
- Procediments de resposta, recuperació i retorn si escau:
 - Recuperació de l'àrea de treball alternativa: Permetre la recuperació de les instal·lacions del lloc de treball en una ubicació alternativa. Contempla el trasllat de les persones.
 - Gestió del personal: Procediments per permetre que el personal identificat com a crític en els diferents processos estigui operatiu (personal de substitució).
 - Recuperació tecnològica: Procediments de recuperació dels *recursos* tecnològics per permetre la represa de l'activitat.
 - Procediment de retorn: Permetre la restauració de les activitats en la seva ubicació inicial, una vegada solucionades les contingències.

C13.Els plans de continuïtat han d'identificar clarament els responsables assignats a cada rol que intervé en les diferents etapes del mateix, així com la forma de contacte (telèfon – fix i mòbil – i correu electrònic).

C14.El gestor de continuïtat de negoci és la figura que ha de liderar i coordinar l'execució de les diferents fases del pla, des del moment en què és notificat pel gestor d'incidents.

C15.S'ha de definir el model de comunicació interna dins l'organització i amb terceres parts (premsa, personal extern, proveïdors, etc.) garantint que hi hagi un únic interlocutor autoritzat a difondre o facilitar informació relacionada amb la situació de contingència.


C16.Durant l'execució de les diferents fases del PCN s'ha de registrar informació sobre l'*incident* i les mesures o decisions preses.

C17.S'han de documentar les possibles incidències que es detectin durant l'execució dels procediments recuperació o retorn, així com qualsevol canvi que es realitzi sobre les infraestructures.

4.2.5.1 Gestió d'incidents

C18.S'ha de definir un procediment de gestió d'*incidents* que contempli com a mínim:

- a) Anàlisi de la incidència (determinar l'àmbit d'afectació).
- b) Definició de la figura del gestor d'incidents.

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 9 / 15

- c) Verificació dels temps previstos de resolució de la incidència amb el *RTO* identificat per als diferents processos de negoci.

C19.El Gestor d'Incidents ha de notificar al Gestor de Continuitat la situació quan aquesta no pugui ser resolta en uns temps menors que els que defineix el *RTO* o bé la criticitat de l'incident així ho determini.

Quan el departament / ens ja disposi d'un procediment de gestió d'incidents definit i operatiu, caldrà incorporar la part d'invocació de la fase d'*avaluació i invocació del pla de continuïtat*.

4.2.5.2 Avaluació i invocació del pla

- C20.El *pla de continuïtat* ha de contemplar en la fase d'avaluació com a mínim les següents accions:
- Convocatòria del comitè de crisi per part del gestor de continuïtat, definint on i com es reunirà.
 - Anàlisi de la situació per part del comitè de crisi.
 - Identificació dels escenaris possibles de recuperació definits i provats.
 - Determinació del procediment de continuïtat a activar.
 - Notificació i aprovació –si escau– de la decisió d'activar el pla per part de Direcció.

4.2.5.3 Procediments d'activació de l'àrea de treball alternativa

- C21.Els procediments d'activació de l'àrea de treball alternativa cal que contempli com a mínim:
- Muntatge i activació de l'àrea de treball alternativa amb els equipaments necessaris.
 - Trasllat dels empleats crítics.
 - Validació del correcte funcionament dels processos una vegada recuperada l'àrea de treball alternativa.

4.2.5.4 Procediments de gestió del personal

- C22.Els procediments de gestió del personal mínim per a garantir el funcionament dels processos crítics cal que almenys contemplin:
- Identificació del personal de substitució.
 - Mecanismes de localització i activació del personal de substitució.

4.2.5.5 Procediments tecnològics de recuperació


- C23.Els procediments tecnològics de recuperació dels sistemes d'informació i comunicacions (veu i dades) han de contenir com a mínim:
- Detall operatiu per a l'execució dels procediments de recuperació.
 - Responsables de l'execució de les diferents tasques.
 - Validació de la correcta execució (integritat de dades).

4.2.5.6 Retorn a la situació de normalitat

Una vegada s'hagi restablert la situació en les instal·lacions principals tant de treball com de processament de dades, cal aplicar els procediments de retorn per així reprendre l'execució dels processos a la forma habitual.

C24.El retorn a la situació de normalitat s'ha de realitzar una vegada el comitè de crisi hagi validat que s'ha resolt la situació que ha originat la contingència i s'ha obtingut l'aprovació de la Direcció.

- C25.Els procediments de retorn a l'àrea de treball original han de contenir com a mínim:
- Notificació als empleats de la represa dels processos a les instal·lacions habituals.

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 10 / 15

- b) Validació del correcte funcionament dels processos una vegada recuperada l'àrea de treball habitual.

C26. Els procediments tecnològics de retorn dels sistemes d'informació i comunicacions (veu i dades) han de contenir com a mínim:

- Detall operatiu per a l'execució dels procediments.
- Responsables de l'execució de les diferents tasques.
- Validació de la correcta execució dels procediments de retorn (integritat de dades).

4.2.6 Formació i conscienciació

Per garantir l'èxit de la GCN, és imprescindible realitzar formació i conscienciació a tot el personal del departament / ens, i de forma especial al personal involucrat directament en la gestió de la continuïtat.

C27. La documentació generada del PCN ha d'estar accessible per al personal involucrat en la GCN i en un lloc alternatiu. L'accés ha d'estar restringit només a personal autoritzat.

C28. S'han de realitzar tasques de conscienciació a tot el personal per transmetre la cultura de la GCN a tot el departament / ens. Per exemple:

- Comunicats a tot el personal.
- Divulgació en butlletins interns o taulell d'anuncis.

C29. S'han de realitzar diverses sessions de formació adaptades al personal involucrat en la GCN del departament / ens.

- Formació bàsica de *continuitat de negoci*, dirigida a àrees de suport al PCN (compres, jurídic, etc.).
- Formació avançada del *pla de continuïtat* als empleats involucrats directament en el PCN.

4.2.7 Proves

Igualment, per a garantir l'efectivitat i completesa del PCN, cal que es facin diferents proves per a validar-ne la correcta definició i implementació.

C30. Per a validar la correcta definició i operació del PCN, s'han d'executar diferents tipus de proves, essent necessàries com a mínim les següents:


- Proves de despatx: Execució sobre paper de les diferents etapes del PCN amb la participació de tots els rols involucrats.
- Proves unitàries: Recuperació d'equips o sistemes puntuals i de les dades que suporten.
- Proves de comunicacions: Activació de comunicacions alternatives.
- Proves de l'àrea de treball alternativa: Activació de l'àrea de treball alternativa.
- Prova global que permeti provar una situació de contingència total.

En el cas de la prova global, caldrà traslladar els *riscos* a la Direcció del departament / ens per a decidir la viabilitat de la seva execució amb l'objectiu d'evitar qualsevol possible *impacte* en el servei.

C31. Prèviament a l'execució de les proves, cal definir el pla de la prova detallant les accions que es portaran a terme i el personal involucrat en la mateixa.

C32. Les proves han d'estar auditades per una tercera part externa al departament / ens per garantir-ne la supervisió mentre s'executen, validant que es compleix el guió de la prova definit prèviament.

C33. Les proves s'han de realitzar almenys una vegada en finalitzar la fase de definició del PCN i posteriorment cada vegada que es realitzi una revisió dels documents del mateix. Com a mínim cal realitzar una prova anualment.

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 11 / 15

4.2.8 Manteniment

Per disposar sempre dels plans de continuïtat adaptats al departament / ens, cal realitzar-ne el manteniment per garantir que la informació que contenen s'adapta als canvis que es produeixen. S'aconsella introduir la GCN en el procediment de gestió del canvi del departament / ens, sempre que aquest estigui definit.

C34.S'ha de disposar d'un pla de manteniment que garanteixi que davant de canvis al departament / ens (de personal, tecnològics, d'instal·lacions o de negoci / servei) es realitzi una revisió de la documentació associada a la GCN. Com a mínim cal realitzar una revisió anualment.

C35.El pla de manteniment ha de garantir que una vegada efectuada la revisió, es distribueixin de nou els documents a tot el personal involucrat en el PCN. En funció dels canvis, caldrà realitzar noves sessions de formació per garantir que el personal té la formació necessària davant dels canvis realitzats.

5. CONTROL

El responsable de continuïtat de l'àrea de QSRaP del CTTI –o en qui delegui– vetllarà per tal que s'apliquin els controls descrits en la present guia. El control es realitzarà de manera continuada al llarg de tot el projecte.

En el cas que no s'apliquin alguns dels controls d'aquesta guia, caldrà justificar i documentar aquestes excepcions. Les excepcions hauran de ser validades pel responsable de continuïtat de l'àrea de QSRaP del CTTI.

6. PENALITZACIONS

En cas d'incompliment per part dels proveïdors s'aplicaran les penalitzacions recollides en el contracte de prestació de servei.

7. DIVULGACIÓ

L'àrea de Qualitat, Seguretat i Relació amb Proveïdors vetllarà per tal que aquesta guia estigui disponible i es mantingui actualitzada en el catàleg d'estàndards de la Intranet del CTTI.

8. REVISIÓ


Aquesta guia es revisarà anualment.

9. GLOSSARI DE TERMES

Activitats crítiques: Accions que s'han de realitzar per lliurar els **productes i serveis** fonamentals que permetin a una organització complir els seus objectius més importants i subjectes al compliment dels terminis.

Àmbit: Fa referència a qualsevol departament, organisme o ens adscrit a la Generalitat de Catalunya.

Anàlisi de riscos: Procés sistemàtic per a estimar la magnitud dels riscos a què està exposada una organització.

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 12 / 15

BIA – Business Impact Analysis (Anàlisi d'impacte de negoci): Identificació dels processos de negoci crítics i l'impacte en cas d'indisponibilitat.

Capacitat de reacció (resiliència): Capacitat d'una organització de resistir els efectes d'un incident.

Continuïtat de negoci: Capacitat estratègica i tàctica de l'organització de planificar i respondre a incidents i interrupcions de negoci per continuar les operacions crítiques a un nivell acceptable predefinit.

Degradat: Execució d'una activitat amb un volum de *recursos* inferior als habituals.

Estratègia de continuïtat de negoci: Opció de l'organització que proporciona recuperació i continuïtat davant un desastre, un incident important o una interrupció de negoci.

Gestió de continuïtat de negoci (GCN): Procés de gestió holística que identifica amenaces potencials per a l'organització i l'impacte en les operacions de negoci, a més de proporcionar un marc per incrementar la capacitat de reacció per donar resposta a incidents amb l'objectiu de salvaguardar els interessos dels seus grups d'interès, imatge i activitats de creació de valor.

Gestió de riscos: Selecció i implantació de solucions per a conèixer, prevenir, impedir, reduir o controlar els riscos identificats.

Impacte: Pèrdues quantitatives i qualitatives derivades de l'activitat d'una amenaça sobre una vulnerabilitat.

Incident: Situació inesperada amb conseqüències negatives per el negoci, que pot donar lloc a una interrupció, pèrdua, emergència o crisi.

Metodologia ESPRIT: Es tracta de la metodologia per a l'execució i seguiment de Projectes d'Informàtica i Telecomunicacions a la Generalitat de Catalunya.

MTPD (Maximum Tolerable Period of Disruption): Temps màxim que pot estar un procés o servei aturat sense comportar un impacte greu que provoqui danys irreversibles a l'organització.

Pla de continuïtat de negoci (PCN): Conjunt de procediments i informació actualitzada que serveix com a guia d'actuació en cas de produir-se un incident amb l'objectiu de seguir processant les activitats crítiques de negoci a un nivell acceptable predefinit.

Procés: Conjunt d'activitats relacionades, o que interactuen, que transformen elements d'entrada en resultats. Són exemples de processos: atenció de trucades, producció de documents, elaboració de la nòmina, tramitació electrònica.

Productes i serveis: Resultats beneficiosos proporcionats per una organització als seus clients, destinataris o grups d'interès.


Recursos: Tots els actius, personal, aptituds, informació, tecnologia, locals i subministres que té una organització disponibles per al seu ús, per a operar i complir els seus objectius.

Redundància: Inclusió d'elements suplementaris en un sistema o circuit per a pal·liar la fallada de l'element normal i assegurar així la continuïtat d'una funció vital.

Resiliència (capacitat de reacció): Capacitat d'una organització de resistir els efectes d'un incident.

Risc: Estimació del grau d'exposició a què una amenaça es materialitzi sobre un o més actius provocant danys o perjudicis a l'organització.

RPO (Recovery Point Objective): Punt (temps) des d'on cal recuperar la informació després d'un incident. El volum de dades que l'organització tolera perdre en el moment en què es produeix una contingència.

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 13 / 15

RTO (Recovery Time Objective): Temps “acceptable” de parada dels sistemes des del moment d'interrupció fins que les infraestructures crítiques tornen a funcionar (serà menor que el *MTPD*).

Serveis TIC Centrals: Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya, gestionats pel Centre de Telecomunicacions i Tecnologies de la Informació (CTTI).

10.DOCUMENTACIÓ REFERENCIADA

- GCNCAT-100901-v2.0 Metodologia de Gestió de la Continuitat (GCNCAT).
- GE-POL01-01 Política de seguretat de la informació de la Generalitat de Catalunya.


11.PARAULES CLAU

Continuïtat, Gestió de la Continuitat, *BIA*, Pla de continuïtat, Formació, Conscienciació, Estàndard, Metodologia, Procés de negoci, Sistemes d'informació, Estratègia, Impacte, Risc, Gestor de Continuitat, Desastre.

12.HISTÒRIC DEL DOCUMENT

Versió 1.0

Versió inicial del document


 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA	GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI	
	N. versió: 1.0	Pàg. 14 / 15

13.ANNEX A – MODEL DE POLÍTICA DE LA GESTIÓ DE LA CONTINUÏTAT

La creixent necessitat de disposar dels serveis i dels processos de forma continuada i sense interrupcions ha estat el detonant per considerar el pla de continuïtat de negoci com una eina indispensable per a garantir [el procés de negoci o servei]. La interrupció total o parcial de [el procés de negoci o servei] com a conseqüència d'una contingència (desastre natural, no accés als sistemes d'informació, indisponibilitat de les persones, oficines de treball no accessibles pel personal, no servei per part dels proveïdors, etc.) podria tenir un impacte significatiu en el servei prestat al ciutadà.

Per a preparar l'organització i tenir capacitat per recuperar-se enfront d'aquest tipus de situacions, la Direcció considera necessària la implantació de la Gestió de la Continuïtat de Negoci (GCN), definint les següents directrius:

1. La Gestió de la Continuïtat és responsabilitat de la Direcció amb el suport de les àrees de negoci, tecnologia i altres grups rellevants (compres, assessoria jurídica, seguretat,...), garantint els recursos econòmics, humans i materials per a poder portar-la a terme.
2. L'abast de la GCN contempla [definir la part, servei o procés en la què s'implantarà la GCN].
3. Les directrius establertes en aquesta política apliquen a tots els grups d'interès (proveïdors, serveis externalitzats...) i el personal del [departament / ens] i estableix el marc organitzatiu per la GCN.
4. El compliment d'aquesta política és necessari per a garantir-ne l'efectivitat. Totes les àrees del [departament/ens] han d'adherir-s'hi i donar-ne compliment en les diferents parts que els hi apliqui.
5. Per a garantir l'èxit del compliment de la política, és necessari que tot el personal del [departament/ens] rebi la formació i conscienciació adequada respecte la GCN i segons el nivell de participació en la GCN.
6. La Direcció nomenarà representants amb la deguda experiència i formació per a què formin part de l'equip de continuïtat i designa al Gestor de Continuïtat del Negoci com a responsable de la implantació i posada en pràctica de la GCN.
7. La implantació de la GCN s'efectuarà seguint la normativa i metodologia definida en l'àmbit de la Generalitat de Catalunya.
8. La protecció, seguretat, salut i benestar del personal que pugui veure's involucrat en una situació de contingència serà la primera premissa i objectiu prioritari a tenir en compte en els plans de continuïtat. [fer referència als plans d'evacuació si existeixen en el departament / ens].

 Centre de Telecomunicacions i Tecnologies de la Informació	GUIA		GE-GUI50-01
	GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI		
	N. versió: 1.0		Pàg. 15 / 15

9. L'equip de continuïtat definirà i mantindrà actualitzats els plans de comunicació adients, tant per personal intern com extern (premsa, proveïdors, etc...).
10. L'equip de continuïtat garantirà que els processos crítics poden ser recuperats en els temps que s'han definit en l'anàlisi realitzat amb les àrees de negoci.
11. La GCN contempla un procés de revisió, actualització, millora i proves com a mínim de forma anual o davant de canvis en el [departament/ens]. L'objectiu és permetre que davant d'una contingència els procediments de resposta siguin els adequats a les necessitats del negoci.
12. El Gestor de Continuïtat del Negoci avaluarà l'alineament del [departament/ens] vers aquesta política per a reportar-ho a la Direcció. Addicionalment, es realitzaran auditories internes de forma periòdica per a assegurar-ne el compliment.
13. Tots els responsables de la planificació de nous projectes inclouran en la planificació i pressupost d'aquests els nivells requerits de *resiliència* i impacte en el marc de la GCN.

Organització del [departament/ens]

La Direcció