ÍNDEX

RESUM 2
1. OBJECTIU I MOTIVACIÓ 3
2. ÀMBIT I VIGÈNCIA 3
3. COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT 3
4. DESCRIPCIÓ 4
5. CONTROL 7
6. PENALITZACIONS 7
7. DIVULGACIÓ 7
8. REVISIÓ 7
9. GLOSSARI DE TERMES 7
10. DOCUMENTACIÓ REFERENCIADA 8
11. PARAULES CLAU 8
12. HISTÒRIC DEL DOCUMENT 8

Versió	Redactat / revisat per	Aprovat per	Data aprovació	Data publicació
1.0.	CTTI – Qualitat, Seguretat i Relació amb Proveïdors	Comitè de Direcció del CTTI	23/12/2008	5/1/2009
2.0	CTTI – Qualitat, Seguretat i Relació amb Proveïdors	CTTI – Qualitat, Seguretat i Relació amb Proveïdors	1/3/2011	1/6/2011

Centre de Telecomunicacions i Tecnologies de la Informació
Estàndard aprovat
2011.05.30
09:46:21 +02'00'

RESPONSABLE DEL DOCUMENT: Silvia Garre (CTTI - Qualitat, Seguretat i Relació amb Proveïdors)

RESUM

1. Objectiu: Establir el conjunt de mesures i controls per garantir la definició, implementació, gestió i recuperació de les còpies de seguretat dels diferents sistemes d'informació de la Generalitat de Catalunya.

2. Àmbit: Aquesta guia és d'aplicació a tots els sistemes d'informació de la Generalitat de Catalunya. Va dirigida a tots els responsables de la gestió de les còpies de seguretat, així com als responsables dels serveis i/o aplicacions.

4. Descripció:

- Anàlisi del requeriments del servei i/o aplicació
- Realització de les còpies
- Recuperació de la informació
- Procediments
- Proves
- Gestió de suports
- Seguretat física
- Continuïtat
- Traçabilitat
- Incidències
- Compliment legal

1. OBJECTIU I MOTIVACIÓ

La informació és un actiu molt important per a la Generalitat de Catalunya. Per aquest motiu, cal garantir que aquesta informació es pugui recuperar en cas de pèrdua total o parcial de la mateixa.

Un dels mecanismes de protecció de la informació, és realitzar una còpia, que serà utilitzada en cas de necessitat per a restaurar la informació en el punt que permeti que un servei o sistema pugui tornar a estar operatiu.

En funció de com es realitza la còpia, existeixen diferents tipus de còpies de seguretat:

- *Totals*: Es realitza una còpia completa de tota la informació d'un servei o sistema.
- *Diferencials*: Es realitza una còpia de totes les dades que s'hagin modificat des de l'última còpia total.
- *Incrementals*: Es realitza una còpia de la informació que s'ha modificat respecte l'última còpia.

A l'hora de realitzar les còpies de seguretat, cal realitzar còpia tant de la informació com dels sistemes que la gestionen. El fet de disposar d'una còpia de les dades, sense possibilitat de recuperar un sistema, fa que aquestes puguin no estar disponibles.

És important analitzar els requeriments que presenta un servei i/o aplicació, per a determinar quin és el sistema de còpia que garanteix cobrir les necessitats de restauració en cas d'alguna incidència.

Un altre aspecte que cal tenir en compte, és el compliment de la legislació vigent quant al tractament de la informació:

- La Llei Orgànica 15/1999, de 13 de desembre de Protecció de Dades de Caràcter Personal (LOPD), i més concretament el reglament que la desenvolupa, el Reial Decret 1720/2007 de 21 de desembre, on s'especifiquen alguns requeriments específics relatius a la realització de còpies i la gestió dels suport que les conserven.
- El Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'administració electrònica.
- Altres requeriments legals que puguin afectar a les dades i a la seva conservació.

Per tot això, l'objectiu d'aquesta guia és definir els requeriments per a la definició, implementació i gestió de les còpies de seguretat dels diferents sistemes d'informació de la Generalitat de Catalunya.

No entra en l'objectiu d'aquesta guia abordar aspectes de la continuïtat del servei i/o aplicació. Aquest àmbit, serà cobert per altres estàndards, que podran fer referència a aquesta guia quant a la gestió de les còpies de seguretat.

2. ÀMBIT I VIGÈNCIA

Aquesta guia és d'aplicació per a tots els sistemes d'informació de la Generalitat de Catalunya. Va dirigida a tots els responsables de la gestió de les còpies de seguretat, així com als responsables dels serveis i/o aplicacions.

Entrarà en vigor el dia 1/3/2011.

Aquesta guia romandrà vigent fins la propera versió aprovada de la mateixa.

3. COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT

La present guia proporciona cobertura a aspectes recollits en els següents controls de la ISO/IEC 27002:2005:

- 9.1.2 Controls d'accés físic
- 9.1.4 Protecció contra amenaces externes i ambientals
- 9.2.7 Sortida de propietats
- 10.5.1 Còpies de seguretat de la informació

- 10.7.2 Retirada dels suports
- 10.7.3 Procediments de maneig de la informació
- 10.8.3 Transport de suports
- 10.10.3 Protecció de la informació dels registres
- 15.1.1 Identificació de la legislació aplicable
- 15.1.4 Protecció de les dades de caràcter personal i de la privacitat de les persones

4. DESCRIPCIÓ

Anàlisi dels requeriments del servei i/o aplicació

N1. El contingut, periodicitat, tipus (total, parcial, incremental) i retenció de les còpies de seguretat estarà alineada amb els requeriments del servei i/o aplicació del qual se'n realitza la còpia d'informació. Caldrà tenir en compte els requeriments de *RTO* / *RPO* identificats a l'hora de definir les còpies de seguretat.

N2. Junt amb el responsable de l'aplicació, caldrà classificar el tipus de tractament de la informació, segons estableix la *Guia de classificació dels tractaments d'informació*, amb l'objectiu d'identificar quines són les mesures de seguretat a aplicar en relació a las còpies de seguretat. També caldrà determinar si les dades estan sotmeses a alguna altra legislació vigent, per tal de garantir-ne el compliment.

N3. L'anàlisi es realitzarà per als diferents entorns (producció, preproducció, integració, etc.) del servei i/o aplicació. Per a nous serveis i/o aplicacions aquesta anàlisi es farà en la fase de definició inicial.

Realització de les còpies

N4. Caldrà realitzar còpia de seguretat de les dades, aplicacions i sistema operatiu de tots els actius que conformen el servei i/o aplicació, incloent tant els entorns productius com no productius així com dels elements de xarxa que siguin particulars per aquest entorn.

N5. Si en un entorn existeixen diferents actius amb una configuració idèntica, inclòs el maquinari, serà suficient realitzar còpia de les aplicacions i la de sistema d'un sol actiu.

N6. Pel cas dels entorns no productius, podran existir diferents plans de còpies de seguretat amb un període de retenció menor que les dels entorns productius, prèvia aprovació del responsable del servei i/o aplicacions.

N7. Les còpies es realitzaran per xarxes dedicades diferents de la xarxa de producció. Caldrà aplicar les mesures de protecció especificades en la *Norma de mesures de seguretat en el Nus Corporatiu TIC de la Generalitat*.

N8. Les còpies de seguretat es realitzaran dintre d'una finestra de temps que serà aprovada pel responsable del servei i/o aplicació així com pels responsables d'altres serveis i/o aplicacions que comparteixin la mateixa infraestructura (electrònica de xarxa, infraestructura, etc.). El responsable analitzarà la franja de temps on l'entorn té menys càrrega per poder determinar l'esmentada finestra, preferiblement fora de l'horari laboral.

N9. Per als entorns productius, i sempre que tècnicament sigui possible, les còpies s'hauran de poder realitzar sense necessitat d'aturar el servei i/o aplicació (còpia en calent).

N10. Per als entorns no productius es podran consensuar amb el responsable del servei i/o aplicació finestres d'aturada per a permetre la realització de les còpies de seguretat.

N11. Si la informació a copiar ha de ser xifrada, caldrà que el xifrat utilitzat sigui un estàndard reconegut i no un xifrat propietari de cap programari. Es recomana l'ús de l'estàndard AES amb claus de 256 bits.

Recuperació de la informació

N12. Només les persones autoritzades pel responsable del servei i/o aplicació podran sol·licitar operacions de restauració de les còpies.

N13. Caldrà implantar mecanismes d'autorització i validació de la identitat dels peticionaris de restauracions de còpies.

Procediments

El responsable de la gestió de les còpies de seguretat haurà de definir els següents procediments:

N14. Caldrà definir procediments de còpia i recuperació de dades, que contemplin les accions i passos necessaris per a l'execució dels processos.

N15. Caldrà definir procediments de monitoratge de l'execució de les còpies per a garantir que se'n revisi el resultat i en cas d'error es tracti com a incidència, desencadenant les accions oportunes de resolució.

N16. Els procediments de recuperació hauran de garantir la reconstrucció en l'estat en què estaven les dades en el moment de realitzar-se l'última còpia de les dades. Caldrà que contemplin la recuperació de les dades tant a nivell de fitxer com de sistema.

N17. Caldrà realitzar una revisió dels procediments de forma regular per assegurar la seva efectivitat i que es completen en els temps especificats (RTO).

N18. Caldrà definir procediments per a la gestió de suports, que en contemplin la seva manipulació i emmagatzemament.

N19. Caldrà disposar d'un procediment d'eliminació d'informació dels suports, en cas que aquests siguin reutilitzats. Caldrà donar compliment a la *Guia eliminació segura informació en la reutilització o destrucció de suports.*

N20. Caldrà disposar d'un procediment de destrucció de suports, en cas que aquests siguin rebutjats (baixa del servei i/o aplicació, funcionament incorrecte d'un suport, etc.). Caldrà donar compliment a la *Guia eliminació segura informació en la reutilització o destrucció de suports.*

Proves

N21. Caldrà realitzar proves periòdiques de recuperació de dades de cada servei i/o aplicació com a mínim 1 cop l'any (recomanable dos cops l'any), i sempre que es produeixi un canvi en la infraestructura del servei i/o aplicació.

N22. Les proves hauran de permetre tant la comprovació dels suports que contenen les còpies com la restauració d'un sistema per complet o de forma parcial.

N23. Per considerar les proves vàlides és necessari que s'alternin de forma aleatòria els jocs de suports, sistemes sobre el que realitzar la restauració i dades parcials o totals restaurades.

N24. En el cas de recuperació per causa d'un incident real, es podrà considerar com a prova de recuperació.

N25. Caldrà activar mecanismes tecnològics de comprovació d'integritat per a verificar que a nivell de suport les còpies s'han realitzat sense errors.

Gestió de suports

N26. Caldrà garantir que els suports utilitzats per a emmagatzemar les còpies de seguretat són d'ús exclusiu per a la Generalitat de Catalunya.

N27. Existirà un inventari detallat de tots els suports.

N28. Existirà una nomenclatura comuna per a la identificació de tots els suports.

N29. Tots els suports estaran identificats de manera que permeti identificar la informació que contenen. S'evitarà que la identificació sigui de forma directa i es pugui deduir el contingut del suport, especialment si hi ha dades crítiques quant a confidencialitat o privadesa.

N30. Quan la gestió dels suports estigui confiada a una tercera empresa, caldrà que es formalitzin els contractes d'encarregat de tractament autoritzats pel CTTI que permetin garantir la disponibilitat, confidencialitat i integritat de les còpies, així com els procediments d'entrega i recepció de còpies i el protocol a seguir en cas d'emergència.

N31. Serà necessari implementar un registre d'entrada i sortida de suports.

N32. Caldrà respectar el temps de vida dels suports indicat pel fabricant i definir un pla de rotació dels mateixos que en garanteixi la fiabilitat i el bon funcionament.

Seguretat física

N33. Les còpies de seguretat que s'hagin de conservar de forma permanent o transitòria (a l'espera del seu enviament a una altra ubicació), s'hauran de guardar de forma segura, preferiblement fora del CPD o sala on s'ubiquin els equips, bé en un armari ignífug, bé en una sala d'emmagatzemament de suports, que compleixin amb les condicions ambientals necessàries (control d'humitat, inundacions, fum, extinció,...) i les condicions d'accés físic, que garanteixi només l'accés del personal autoritzat.

Continuïtat

N34. Hi ha d'haver una còpia de seguretat disponible en una ubicació que no estigui sotmesa als mateixos riscos que l'edifici on s'ubiquen els sistemes d'informació.

N35. Caldrà definir un pla de continuïtat per al sistema de gestió de còpies de seguretat, que garanteixi la operativitat del servei de còpies per a sistemes considerats com a crítics.

Traçabilitat

N36. Serà necessari disposar d'un registre de les activitats de còpia, restauració i destrucció, que reculli com a mínim la data, hora, la persona que l'executa i el resultat de l'operació.

N37. Caldrà guardar un registre de les proves de recuperació que es realitzin.

Incidències

N38. Si es produeix alguna incidència en la gestió de les còpies de seguretat, caldrà que es notifiqui al responsable del servei i/o aplicació i s'informi de les accions portades a terme per a la seva resolució.

N39. Tota incidència ha de ser degudament registrada i documentada.

Compliment legal

N40. Quan la informació a copiar contingui dades de caràcter personal, caldrà donar compliment als requeriments de seguretat indicats en el *Reglament de la LOPD*.

N41. Pels serveis i/o aplicacions que gestionin informació subjecta a compliment legal (judicial, financera, sanitària, etc.), el responsable del servei i/o aplicació ha de concretar les necessitats específiques de les còpies de seguretat.

Recomanacions

R1. Es recomana realitzar almenys una còpia una vegada l'any amb el servei aturat.

R2. Quan els temps de restauració establerts siguin molt curts, pot ser recomanable disposar addicionalment de còpies en una ubicació propera a la ubicació dels sistemes.

5. CONTROL

Per a l'àmbit dels *Serveis TIC Centrals*, el control del compliment d'aquesta guia es realitzarà mitjançant auditories periòdiques segons s'estableix en el Pla d'auditories de seguretat del CTTI. Per altres àmbits, es recomana realitzar auditories cada 6 mesos.

En el cas que no s'apliqui algun dels controls d'aquesta guia, caldrà justificar i documentar aquestes excepcions. Per a l'àmbit dels *Serveis TIC Centrals*, cada excepció a un control haurà de ser validada prèviament per l'Oficina de Seguretat i autoritzada per Qualitat, Seguretat i Relació amb Proveïdors del CTTI.

Caldrà mantenir un registre on quedin recollides totes les excepcions, a disposició de les auditories.

6. PENALITZACIONS

En cas d'incompliment de l'empresa contractista aplicaran les penalitzacions recollides en el contracte de la prestació del servei.

Si l'incompliment és per part de personal intern de la Generalitat de Catalunya pot determinar, si s'escau, l'aplicació del règim disciplinari corresponent.

7. DIVULGACIÓ

L'àrea de Qualitat, Seguretat i Relació amb Proveïdors del CTTI publicarà aquesta guia al repositori d'estàndards de la intranet del CTTI.

8. REVISIÓ

Aquesta guia ha de ser revisada cada 18 mesos.

En cas de produir-se una incidència de seguretat relacionada amb aquesta guia, caldrà fer una revisió de compliment i completesa.

9. GLOSSARI DE TERMES

Còpia en calent: Mecanisme que permet la realització de la còpia de seguretat sense necessitat d'aturar el servei.

Entorn: Diferents àmbits (desenvolupament, integració, consolidació, pre-producció, producció) corresponents a un servei.

Responsable del servei i/o aplicació: Persona designada com a responsable d'un servei o aplicació.

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.

RTO (Recovery Time Objective): Temps "acceptable" de parada dels sistemes des del moment d'interrupció fins que les infraestructures crítiques tornen a funcionar.

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).

Suport: Dispositiu (cinta, disc, CD, DVD, etc.) on s'emmagatzema informació.

10. DOCUMENTACIÓ REFERENCIADA

- GE-NOR19 – Norma de mesures de seguretat en el Nus Corporatiu TIC de la Generalitat
- GE-GUI49 – Guia de classificació dels tractament de la informació
- GE-GUI44 – Guia eliminació segura d'informació en la reutilització o destrucció de suports

NOTA: Consulteu aquests documents de referència en la seva última versió

11. PARAULES CLAU

Còpia, backup, incremental, diferencial, total, retenció, reglament, legislació, LOPD, dades de caràcter personal.

12. HISTÒRIC DEL DOCUMENT

Versió 1.0

Versió inicial.

Correspon a l'adaptació del document NOR-GSEG-070308-v1.0 Norma de còpies de seguretat a estàndard Generalitat.

Versió 2.0

Revisió periòdica de l'estàndard.

Nous controls incorporat: N15, N25.
Controls eliminats de la versió 1, per formar part d'altres guies referenciades o bé estar duplicats: N3,N9,N14,N36.
Controls modificats: N1 (afegir referència als requeriments de continuïtat), N2 (afegir referència a la guia de classificació dels tractaments d'informació), N19, N20 (afegir referència a la guia d'eliminació segura d'informació en suports d'informació).
El control N35 de la versió 1 s'ha modificat a recomanació.