ÍNDEX

Versió	Redactat / revisat per	Aprovat per	Data aprovació	Data publicació
1.0.	CTTI – QSRaP	Comitè Operatiu del CTTI	4/5/2009	18/5/2009

Estàndard signat digitalment pel:
Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.05.18 10:21:04 +02'00'

RESPONSABLE DEL DOCUMENT: CTTI – Qualitat, Seguretat i Relació amb Proveïdors

RESUM

OBJECTIU

L'objectiu d'aquesta norma és establir les pautes de seguretat que s'han de tenir en consideració en el procés de construcció / adopció de sistemes d'informació, amb l'objectiu d'assegurar la disponibilitat, integritat, confidencialitat i privacitat de la informació.

ÀMBIT

Aquesta norma és d'aplicació a la construcció de qualsevol sistema d'informació de la Generalitat de Catalunya, tant si es tracta d'un desenvolupament a mida com si és un producte tancat. En aquest darrer cas, caldrà validar el compliment dels controls d'aquesta norma per part del producte a adquirir.

Va dirigida a gestors de projectes, desenvolupadors i gestors tecnològics.

La norma serà d'aplicació:

- Per a tots els sistemes desplegats a la Generalitat de Catalunya a partir del dia 1 de gener del 2010.
- Per a tots aquells sistemes el desenvolupament dels quals es liciti després de la data de publicació de la norma.
- Per a tots aquells productes tancats, desplegats en els sistemes de la Generalitat de Catalunya després de la data de publicació d'aquesta norma.

DESCRIPCIÓ

- Seguretat en la fase de planificació.
- Seguretat en el codi.
- Seguretat en les proves.
- Seguretat en els entorns.
- Documentació.

1 OBJECTIU

L'objectiu d'aquesta norma és establir les pautes de seguretat que s'han de tenir en consideració en el procés de construcció / adopció de sistemes d'informació, amb l'objectiu d'assegurar la disponibilitat, integritat, confidencialitat i privacitat de la informació que serà tractada en els sistemes d'informació.

El CTTI ha desenvolupat una metodologia de Seguretat en el Desenvolupament de Sistemes d'Informació. Aquesta norma està alineada amb la metodologia, que fa un plantejament molt més extens de les mesures de seguretat a considerar en la construcció d'un sistema d'informació.

Per a garantir una bona protecció de la informació és necessari disposar d'una guia de classificació de la informació, que estableixi diferents nivells de classificació de la informació en funció del seu grau de confidencialitat o criticitat per a l'organització, així com els controls a aplicar per al tractament de la mateixa al llarg de tot el seu cicle de vida.

En aquesta norma s'exposen algunes mesures orientades a la protecció d'informació sensible o confidencial que seran d'obligat compliment en absència d'una guia de classificació de la informació. Si es disposa d'una guia de classificació de la informació, en tot allò que estigui considerat dins de la guia, s'hauran de seguir les pautes recollides en la mateixa.

En l'apartat de "Documentació referenciada" es pot consultar informació addicional per al desenvolupament de certs tipus de sistemes d'informació (aplicacions web), així com la publicació d'un recull dels errors més freqüents en la programació.

2 ÀMBIT I VIGÈNCIA

Aquesta norma és d'aplicació a la construcció de qualsevol sistema d'informació de la Generalitat de Catalunya, tant si es tracta d'un desenvolupament a mida com si és un producte tancat. En aquest darrer cas, caldrà validar el compliment dels controls d'aquesta norma per part del producte a adquirir.

Va dirigida a gestors de projectes, desenvolupadors i gestors tecnològics.

La norma serà d'aplicació:

- Per a tots els sistemes desplegats a la Generalitat de Catalunya a partir del dia 1 de gener del 2010.
- Per a tots aquells sistemes el desenvolupament dels quals es liciti després de la data de publicació de la norma, és a dir, el 18 de maig de 2009.
- Per a tots aquells productes tancats, desplegats en els sistemes de la Generalitat de Catalunya després de la data de publicació d'aquesta norma.

Romandrà vigent fins la propera versió aprovada de la mateixa.

3 COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT

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

- 12.1.1 Anàlisi i especificacions dels requeriments de seguretat
- 12.2.1 Validació de les dades introduïdes
- 12.2.2 Control de processament intern
- 12.2.3 Integritat dels missatges
- 12.2.4 Validació de les dades resultants

4 DESCRIPCIÓ DELS CONTROLS

Es presenten a continuació els controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació dels sistemes. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D, privacitat - P).

4.1. Seguretat en la fase de planificació

OBJECTIUS	
Identificació dels objectius de seguretat al projecte.	
CARACTERÍSTIQUES	
Descripció	**Categoria**

C1. Cal analitzar el tipus d'informació tractada pel sistema d'informació en construcció. Quan existeixi una guia de classificació de la informació, s'utilitzarà aquesta i es recolliran els requeriments de tractament d'informació que corresponguin.	C I D
C2. A partir de la criticitat de la informació, s'hauran de definir els nivells de confidencialitat, privacitat, integritat i disponibilitat del sistema d'informació.	C I D
C3. Durant la fase de planificació d'un projecte, cal identificar tots els controls de seguretat necessaris tenint en compte els requeriments de confidencialitat, integritat, disponibilitat i privacitat de la informació que serà tractada. Els controls de seguretat han de cobrir com a mínim les següents àrees: • Arquitectura. • Compliment normatiu • Compliment legal • Gestió d'usuaris • Traçabilitat • Pla de necessitats per garantir la continuïtat dels processos de negoci.	C I D
C4. Durant aquesta mateixa fase també s'identificaran les necessitats de seguretat tenint en compte la legislació vigent o regulatòria, l'aplicabilitat dels estàndards existents (tals com ISO 27002), i les polítiques, normes i procediments en l'àmbit d'aplicació del desenvolupament.	C I D
C5. Cal preveure els recursos que utilitzarà el sistema d'informació de cara a un correcte dimensionament (CPU, disc, memòria, etc.).	D
C6. Els requeriments de seguretat resultants han de ser incorporats al plec de contractació de construcció del sistema d'informació.	C I D

4.2. Seguretat en el codi

Els controls que es presenten a continuació estan destinats a implementar-se durant la fase de desenvolupament de l'aplicació i pretenen reduir el risc de seguretat del sistema d'informació minimitzant el número de vulnerabilitats potencials.
En cas de productes tancats, caldrà validar el compliment dels requeriments per part del producte.

4.2.1 Usuaris i control d'accés

OBJECTIUS	
Establir controls raonables d'autenticació d'usuaris.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C7. En les autenticacions amb parells usuari i contrasenya, utilitzar la política de contrasenyes existent (veure *GE-GUI19-01 Guia de contrasenyes)* i aplicar-la en totes les autenticacions de l'aplicació.	C I D
C8. Els processos d'autenticació han de ser acords a la criticitat de les dades del mòdul al qual s'hi accedeix, tenint en compte que el parell usuari/contrasenya pot ser efectiu per validar un usuari estàndard però insuficient per obtenir privilegis administratius d'un servei, o accedir a dades especialment protegides o confidencials. Per tant, s'utilitzarà *autenticació de doble factor* quan el tipus d'informació a accedir ho requereixi.	C
C9. Implementar mecanismes per evitar el nombre d'intents d'accés reiterats i infructuosos.	C
C10. Per a la connectivitat entre sistemes, i sempre que sigui viable, s'han de crear llistes de control d'accés, limitant els accessos als orígens lícits.	C I
C11. Cal redactar un procediment de gestió d'alta, modificació i baixa d'usuaris. Per a fer-ho es poden utilitzar els models creats a tal efecte (veure punt 10. Documentació Referenciada).	C I D

Recomanacions

R1. Analitzar la integració del nou sistema amb GICAR, el sistema de Gestió d'Identitats i Control d'Accés als Recursos de la Generalitat de Catalunya.

R2. És recomanable informar als usuaris de l'última[1] connexió realitzada en l'aplicació (mitjançant data, hora).

4.2.2 Gestió de privilegis, de sessions i autorització

OBJECTIUS	
Establir el principi de mínims privilegis, per a protegir els recursos vers escalades de privilegis.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C12. Definir els rols d'accés al sistema segons el principi de *mínim privilegi*.	C I
C13. Les aplicacions han de controlar i garantir els privilegis d'accés per part d'un usuari a cada recurs al que s'hi accedeix, evitant la possibilitat d'heretar aquests privilegis al canviar de mòdul, recurs o zona de l'aplicació.	C I
C14. En el control d'accés, s'ha de validar la identitat amb els *tokens* rebuts de l'usuari, i evitar en la mesura del possible que sigui visible en la interfície de l'aplicació.	C
C15. En el control de sessions, s'ha de mantenir una associació d'autenticació robusta durant la sessió, i gestionar-ne l'accés. Aquesta sessió s'ha de finalitzar quan l'usuari realitzi la sortida de l'aplicació, o hi hagi una expiració de sessió. En aquest sentit cal: • Utilitzar algoritmes criptogràfics de sessió robustos. • Capacitat de detectar intents reiterats de provatures amb tokens de sessió. • Eliminació de les sessions en el moment de fer logout. • Forçar l'expiració de la sessió en cas d'inactivitat.	C

4.2.3 Seguretat en les interfícies administratives

OBJECTIUS	
Establir una segregació de funcions usuaris/administradors.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C16. S'ha de segmentar la part d'administració de la part d'usuaris amb l'objectiu de limitar l'accés per part dels administradors del sistema d'informació.	C I D
C17. Procurar una segregació de funcions entre els usuaris i els administradors. Els usuaris no poden realitzar tasques administratives, i els administradors no poden realitzar les operacions pròpies dels usuaris estàndard.	C I D
C18. Utilitzar protocols de xifrat en totes les accions realitzades pels administradors.	C I D

4.2.4 Criptografia i xifrat de dades

OBJECTIUS	
Assegurar la confidencialitat, integritat, i el no repudi de la informació, segons els requeriments definits en la fase de definició/disseny del projecte i la criticitat de la informació, o els marcs legals/ bones pràctiques que hi apliquen (LOPD, PCI, ISO 27002, COBIT, etc).	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C19. Mantenir la confidencialitat de dades mitjançant tècniques criptogràfiques. En aquest sentit cal: • Utilitzar protocols xifrats (SSL/TLS) en comunicacions amb dades sensibles o confidencials (exemple: autenticació d'usuaris).	C I

[1] Darrera connexió realitzada per l'usuari, abans de la connexió actual.

• Utilitzar mecanismes de xifrat en l'emmagatzematge de la informació sensible o confidencial.	
C20. Utilitzar claus suficientment robustes: • >=256 bits efectius en el xifrat de dades amb claus simètriques. (AES). • >=2048 bits efectius en el xifrat de dades amb claus asimètriques (RSA). • >=256 bits efectius destinats al hash (SHA2). Es prohibeix l'ús d'algorismes dèbils com MD4, MD5.	C I
C21. Quan sigui necessari garantir el no repudi d'una acció, implementar: • Ús de certificats de doble via, de servidor per assegurar el canal, i d'origen per assegurar la identitat i confidencialitat. • Signatura digital de l'emissor amb timestamp per assegurar la identitat de l'emissor i la data de la transacció. Serà necessari realitzar una validació per part del receptor.	C I
C22. Identificar clarament els mòduls de l'aplicació que utilitzen criptografia.	C D
C23. Definir els requeriments d'emmagatzemament i custòdia de les claus criptogràfiques recollint: • Ubicació, amb accés restringit només als mòduls del sistema que ho requereixin. • Accés, només als usuaris autoritzats. • Emmagatzemament en dispositius criptogràfics (HSM, tókens...). • Registre d'accessos a les claus.	C D
C24. Realitzar una gestió dels certificats digitals que contempli: • Procediment d'admissió de certificats digitals. • Instal·lació de certificats vàlids i vigents. • Procediment per a la renovació de certificats.	C I
C25. Definir un procediment per a la revocació o suspensió dels certificats digitals, així com la seva destrucció, prèvia revocació dels mateixos.	C I
C26. La gestió de la criptografia del sistema d'informació, ha d'estar documentada en un procediment d'ús de criptografia, que reculli els requeriments indicats en aquest apartat.	C I D

4.2.5 Validació de dades d'entrada, de procés i de sortida

OBJECTIUS	
Establiment de mesures de control de dades per evitar problemes amb la lògica de l'aplicació.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C27. Validar les dades d'entrada en l'aplicació per garantir que aquestes són correctes i adequades abans del seu processament, i independentment que s'obtinguin a partir d'usuaris, en processos interns, o de fonts externes. La validació de les dades es realitzarà com a mínim a la part servidor del sistema. És una bona pràctica la comprovació de les dades introduïdes abans del seu processament: i. Valors en els rangs esperats. ii. Caràcters permesos. iii. Comprovacions d'integritat.	C I
C28. S'ha de controlar la longitud de les dades d'entrada per a evitar desbordaments en el procés del sistema.	C I D
C29. En la recepció de fitxers, s'han de realitzar les següents validacions: • Tipus de fitxer esperat. Comprovació que el format rebut és l'esperat pel sistema (p.ex. PDF, DOC, ...). • Ubicació del fitxer correcta. Emmagatzemament un una ruta del sistema autoritzada. • Control antivirus.	I

Recomanacions

R3. Per tal de realitzar validacions d'entrada, és recomanable l'ús de mòduls o classes de seguretat destinats a tal efecte.

R4. És convenient incorporar processos de consolidació mitjançant comprovacions de validació i integritat de dades, per tal de detectar qualsevol anomalia deguda a errors de processament, de comunicacions o provocats.

R5. Sempre que sigui possible, evitar l'ús de camps de text lliure (típicament camps d'observacions o comentaris) per a minimitzar el risc d'entrada de dades personals afectades per la llei de protecció de dades de caràcter personal. En general, no s'hauria de donar peu a l'usuari a entrar dades més enllà de les estrictament necessàries, per eliminar el risc que aquestes dades (no previstes) augmentin el nivell de seguretat del fitxer, i per tant, sigui necessari aplicar mesures de seguretat més estrictes per tal de donar compliment a la llei de protecció de dades de caràcter personal. En aquesta línia, sempre que sigui possible, és preferible donar l'opció de triar una resposta d'una llista, que obrir un camp de text lliure.

4.2.6 Control d'errors

OBJECTIUS	
Gestionar els errors de l'aplicació per evitar la revelació de situacions inesperades del sistema, alhora de donar traçabilitat dels mateixos en cas de necessitat o debug.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C30. Els missatges d'error de l'aplicació no esperats, sovint donen informació que pot ser molt valuosa per a usuaris malintencionats, que poden conèixer la resposta de l'aplicació a determinades accions. S'han de controlar tots els missatges d'error que es retornen a l'usuari.	C I D
C31. Enregistrar mitjançant logs d'aplicació tota informació que provingui d'errors no esperats en la interfície de l'usuari, per tal de poder analitzar possibles problemes i aplicar-hi solucions.	D

4.2.7 Traçabilitat

OBJECTIUS	
Establir traçabilitat d'accions en l'aplicació	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C32. Cal donar compliment a la *Norma de gestió de traces* on s'especifiquen els requeriments quant a la definició, generació i emmagatzemament de les traces.	C I D
C33. Cal definir clarament la ubicació de les traces de negoci per a garantir que són gestionades de forma correcta.	C I D

4.2.8 Codi font

OBJECTIUS	
Assegurar la disponibilitat i custòdia del codi font del sistema d'informació.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C34. Emmagatzemament del codi font del sistema d'informació en un repositori central de codi.	C I D

Recomanacions

R6. Es recomana realitzar una revisió del codi font amb l'objectiu de detectar problemes en el desenvolupament.

4.3. Seguretat en les proves

Els controls que es presenten a continuació estan destinats vetllar per a la correcta definició i utilització de les dades que s'utilitzin durant la fase de proves del sistema d'informació.

4.3.1 Jocs de prova

OBJECTIUS	
Controlar i gestionar els jocs de prova que s'utilitzaran durant les proves del sistema d'informació.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C35. S'han de generar jocs de prova específics destinats a comprovar els requeriments del sistema tant a nivell tècnic com de negoci.	C I D
C36. Les proves d'integració a les plataformes finals han d'incloure la revisió dels nivells d'accés a altres recursos, els nivells de cada grup d'usuaris i/o els nivells en funció dels rols definits.	C I
C37. Els jocs de prova no podran fer servir dades reals. Només es podran utilitzar dades reals en el cas que es faci una dissociació de les mateixes o que es garanteixin en l'entorn de proves les mateixes mesures de seguretat que en l'entorn productiu.	C I
C38. Tant els jocs de prova utilitzats com les proves realitzades hauran de quedar documentades i entregades juntament amb la resta de documentació del desenvolupament.	C I D

Recomanacions

R7. Es recomana realitzar proves d'estrès al sistema d'informació per a comprovar el correcte funcionament del mateix, especialment quan es prevegi la concurrència d'un gran volum d'usuaris.

4.4. Seguretat en els entorns

Els controls que es presenten a continuació estan destinats a ser implementats durant les fases posteriors al desenvolupament del sistema d'informació. Pretenen reduir riscos de seguretat del sistema minimitzant altres factors no directament relacionats amb el desenvolupament del sistema d'informació.
Aplicaran els controls a tots els entorns (producció, preproducció, integració, ...) del sistema d'informació.

4.4.1 Configuració segura del sistema d'informació

OBJECTIUS	
Establir seguretat en l'entorn de l'aplicació.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C39. No es podrà publicar a Internet cap sistema d'informació que no estigui sota adreçament IP de la Generalitat de Catalunya.	I
C40. La plataforma que allotgi el sistema d'informació ha de donar compliment a les diferents guies de protecció de sistemes així com a la resta de normes de seguretat (Mesures de Seguretat en el Nus Corporatiu TIC de la Generalitat de Catalunya, Creació de DMZ's, etc.)	C I D

Recomanacions

R8. Es recomana realitzar una auditoria de seguretat del sistema d'informació abans de la seva posada en producció.

4.4.2 Manteniment

OBJECTIUS	
Assegurar un servei post-productiu correcte	
CARACTERÍSTIQUES	
Descripció	**Categoria**

C41. Durant el període de garantia de la contractació, s'exigirà un servei de correcció de problemes que no s'hagin identificat o manifestat durant les fases d'integració i preproducció.	C I D

Recomanacions

R9. Es recomana extendre el suport de manteniment una vegada exhaurit el període de garantia del sistema d'informació.

4.5. Documentació

A banda de la documentació ja esmentada al llarg d'aquest document, a continuació es mostra una relació d'altres documents que cal generar durant la construcció del sistema, per tal de donar cobertura a diferents aspectes de seguretat.

4.5.1 Documentació tècnica

OBJECTIUS	
Assegurar la documentació necessària per tal de donar cobertura a aspectes tècnics de seguretat.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C42. Diagrama dels fluxos d'informació interns de l'aplicació, i dels fluxos externs d'intercanvi d'informació amb altres aplicacions o usuaris.	D
C43. Esquema de comunicacions, especificant l'origen i destí de les comunicacions, el sentit, els protocols utilitzats, i els ports necessaris per efectuar aquesta comunicació.	D
C44. Processos de còpia de seguretat per cobrir tota la informació relativa a l'aplicació i a les dades que s'hi tracten.	C I D
C45. Tota la documentació exigida en la llei orgànica de protecció de dades i el reglament que la desenvolupa (es pot trobar informació addicional a la Guia *GE-GUI39-01 Protocol LOPD*).	P

5 CONTROL

En l'àmbit dels Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya gestionats pel CTTI (d'ara endavant "*Serveis TIC Centrals*"), el control del compliment d'aquesta norma es realitzarà mitjançant auditories periòdiques segons s'estableix en el *Pla d'auditories de seguretat*. Per altres àmbits, es recomana realitzar auditories cada 6 mesos.

En el cas que no s'apliqui algun dels controls d'aquesta norma, caldrà justificar i documentar aquestes excepcions.

Previ al lliurament d'un sistema d'informació, el seu desenvolupador haurà de signar una carta on garanteixi el compliment dels controls d'aquesta norma.

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

6 PENALITZACIONS

Quan l'explotació / manteniment dels sistemes estigui subcontractat, en cas d'incompliment aplicaran les penalitzacions recollides en el contracte de la prestació del servei.

Si l'administració del sistema recau en personal intern de la Generalitat de Catalunya, l'incompliment d'aquesta norma 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 norma al repositori d'estàndards de la intranet del CTTI.

8 REVISIÓ

Aquesta norma ha de ser revisada anualment.

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

9 GLOSSARI DE TERMES

Autenticació de doble factor: Mètode d'autenticació format per una banda d'un element físic (p.ex. una tarja) i de l'altra una informació que coneix l'usuari (p.ex. un número secret –PIN–). Cal disposar dels dos factors per a obtenir una autenticació satisfactòria.

Mínim privilegi: Assignació als usuaris dels privilegis estrictament necessaris i no més, per al desenvolupament de les tasques encomanades.

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

- GE-GUI19 Guia de contrasenyes
- GE-GUI39 Protocol LOPD
- GE-GUI07 Guia protecció entorns Linux
- GE-GUI08 Guia protecció entorns Solaris
- GE-GUI09 Guia protecció entorns virtuals VMWARE
- GE-GUI10 Guia protecció entorns Windows 2003
- GE-GUI11 Guia protecció entorns web Apache
- GE-GUI12 Guia protecció entorns web IIS
- GE-GUI13 Guia protecció entorns SQL Server 2000
- GE-GUI14 Guia protecció entorns Oracle
- GE-GUI15 Guia protecció entorns servidor aplicacions Tomcat
- GE-GUI16 Guia protecció entorns servidor aplicacions Weblogic
- GE-GUI20 Guia gestió comptes administrador sistemes
- GE-GUI28 Guia de mesures de seguretat en el Nus Corporatiu TIC de la Generalitat
- GE-GUI27 Guia protecció entorns HP-UX
- Guia protecció entorns AIX
- Procediment ABM d'Usuaris_Public[2]
- Procediment ABM d'Usuaris_Administradors[2]

NOTA: Consulteu aquests documents en la seva última versió.

ALTRES REFERÈNCIES:

OWASP (Open Web Application Security Project):
http://www.owasp.org/index.php?title=Main_Page&setlang=es

CWE/SANS TOP 25: Els 25 errors més perillosos a l'hora de programar:
http://cwe.mitre.org/top25/

11 PARAULES CLAU

Construcció de sistemes, traçabilitat, joc de proves, control d'errors, aplicació, planificació, projecte, sistema d'informació, codi font.

12 HISTÒRIC DEL DOCUMENT

Versió 1.0

Versió inicial.

[2] Procediment disponible a l'àrea pública de la intranet del CTTI, secció *Quins Serveis Oferim / Serveis TIC Centrals Continuats / Oficina de Seguretat*.