Politicile si Procedurile Operationale ale Arhivei Digitale si Centrului de Date

administrate de

SC *CERTSIGN SA*

Versiunea 2.3

Data: Decembrie, 2018

Numar de referinta: PPRO8

Istoria documentului

Versiune	Data	Motiv	Persoana care a facut modificarea
1.0	Iulie 2009		Manager Servicii Electronice
2.0	Iunie 2013		Information Security Officer
2.1	Noiembrie 2015		Information Security Officer
2.2	Mai 2018	Alinierea la GDPR	CISO
2.3	Decembrie 2018	Noua locatie a centrului de date	CISO

Acest document a fost creat si este proprietatea:

Proprietar	Autor	Data crearii
Manager Servicii Electronice	Manager Servicii Electronice	Iulie 2009
Director Arhivare Electronica		Iunie 2013

Lista de Distributie

Destinatar	Data distribuirii
Intranet	August 2009
Intranet	Iunie 2013
Intranet	Noiembrie 2015
Intranet	Mai 2018
Intranet	Decembrie 2018

Acest document a fost aprobat de

Versiune	Nume	Data

1.0	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	August 2009
2.0	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Iunie 2013
2.1	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Noiembrie 2015
2.2	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Mai 2018
2.3	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Decembrie 2018

Cuprins

1 Introducere

1.1 Privire de ansamblu asupra procesului de arhivare digitala

Termenul arhiva se foloseste astazi pentru a se face referiri la o mare varietate de functii si sisteme de stocare si pastrare a informatiei. Arhivele traditionale sunt intelese ca acele entitati sau organizatii care pastreaza inregistrari, generate original de o structura guvernamentala, institutie sau firma pentru accesarea de catre comunitati publice sau private. O arhiva indeplineste aceasta sarcina, preluand controlul asupra inregistrarilor, asigurandu-se ca aceste pot fi intelese de catre comunitatea care le acceseaza si administrandu-le astfel incat sa le pastreze continutul informational si autenticitatea. De-a lungul timpului, aceste inregistrari au existat sub forma de carti, documente, harti, fotografii sau filme, care pot fi citite directe de oameni, sau cu ajutorul unor dispozitive optice simple. In pastrarea acestor informatii accentul principal a cazut pe asigurarea stabilitatii pe termen lung a suportului informational si pe controlul accesului.

Cresterea exploziva a formelor digitale ale informatiei a creat o provocare uriasa nu numai pentru arhivele traditionale si pentru sursele lor de informatii, ci si pentru multe alte organizatii economice sau non-profit. Acestea sunt in curs de a afla, sau vor afla in curand ca trebuie sa se preocupe serios de pastrarea informatiilor digitale cu care lucreaza, preluand functii asociate de obicei cu arhivele traditionale sau apeland la organizatii care sa faca acest lucru. In caz contrar, ar putea fi confruntate cu riscul foarte mare de a pierde aceste informatii, caci informatia digitala poate fi usor pierduta sau distrusa.

Un sistem digital de arhivare este diferit de un sistem normal de procesare a informatiei, tocmai prin aceea ca accentul cade in aces caz pe pastrarea si accesarea informatiei pe termen lung. Un sistem modern de arhivare a informatiei (si prin acest lucru nu se intelege numai tehnologia implicata, ci toate activitatile adiacente) trebuie sa raspunda urmatoarelor cerinte:

- sa poate negocia si accepta informatii corespunzatoare
- sa obtina suficient control asupra informatiei obtinute pentru a ii putea asigura pastrarea pe termen lung
- sa determine care sunt comunitatile care o vor accesa si care vor trebui sa inteleaga informatia arhivata
- sa se asigure ca informatia pastrata este inteligibila in mod independent, adica comunitatea care o acceseaza o poate intelege fara asistenta celor care au produs-o.

- sa dispuna si sa se conformeze unor politici si proceduri care sa asigure faptul ca informatia va fi pastrata indiferent de accidentele care ar putea surveni si care sa dea siguranta faptului ca informatia este originala sau copii autentice ale originalului.
- Sa puna informatia la dispozitia comunitatii desemnate

Componente si functii esentiale ale unui serviciu de arhivare:

Inregistrare: Componenta care asigura acceptarea pachetelor de informatii si pregatirea continutului pentru pastrare si administrare in cadrul arhivei prin: asigurarea calitatii pachetelor de informatii, generarea de informatii despre pachetele de informatii arhivate care sa fie conforme cu formatul datelor arhivate , extragerea de informatii descriptive din pachetele de informatii arhivate si actualizarea componentelor care asigura stocarea arhivelor si managementul datelor.

Stocarea Arhivelor: Componenta care furnizeaza serviciile si functiile de stocare, administrare si regasire a pachetelor de informatii arhivate prin: primirea de pachete de informatii arhivate de la componenta de inregistrare si stocarea lor permanenta, administrarea ierarhiei de stocare, executarea de rutine de verificare a erorilor, furnizarea de pachete de arhivare catre componenta de acces.

Managementul Datelor: Componenta care furnizeaza serviciile si functiile de populare, intretinere si accesare atat a informatiilor descriptive care identifica si documenteaza informatia arhivata, cat si a datelor administrative utilizate la managementul arhivei. Managementul datelor se realizeaza prin : administrarea functiilor de baza de date ale arhivei (mentinerea definitie schemei si a reprezentarilor si integritatea referentiala), actualizarea bazei de date, executarea de cautari in datele de management.

Administrarea: Componenta care asigura serviciile si functiile de operare ale intregului sistem de arhivare. Functiile de administrare includ: auditarea informatiilor depuse spre arhivare pentru a se asigura ca respecta standardele arhivei si managementul configuratiei hardware si software a sistemului. In plus, ofera functii de monitorizare si imbunatatire a operatiilor de arhivare, functii de inventariere, raportare si migare/actualizare a continutului arhivei. Este de asemenea componenta responsabila pentru stabilirea si mentinerea de standarde si politici de arhivare, suport al clientilor etc.

Planificarea Stocarii : Componenta care ofera servicii si functii pentru monitorizarea mediului exterior sistemului de arhivare si care furnizeaza recomandari pentru a asigura faptul ca informatia arhivata ramane accesibila comunitatii ei de clienti si utilizatori pe termen lung , chiar daca

sistemul informatic initial devine depasit. Componenta include functiile de: evaluarea continutului arhivei si recomandarea periodica de migrari ale continutului, dezvoltarea de recomandari pentru standarde si politici de arhivare si monitorizeaza schimbarile in mediul tehnologic exterior si in cerintele de servicii ale comunitatii de clienti si utilizatori.

Access: Componenta care ofera functii si servicii care sprijina clientii si utilizatorii in a determina existenta , descrierea , localizarea si disponibilitatea infomatiei arhivate si le permite acestora sa ceara si sa primeasca informatii. Functiile oferite includ: primirea de cereri de acces, aplicarea de controale la acces, generarea si livrarea de raspunsuri.

1.2 Identificarea documentului

Denumirea acestui document este: Politicile şi Procedurile Operationale ale Arhivei Digitale si Centrului de Date administrate de certSIGN. Documentul este disponibil sub formă electronica în Depozit la adresa http://www.certsign.ro/repository sau pe baza unei cereri trimisă pe adresa office@certsign.ro;

1.3 Părţile implicate

Acest document reglementează cele mai importante relaţii dintre entităţi aparţinând certSIGN, echipele de consultanţi (inclusiv auditorii) şi clienţii (utilizatorii serviciilor furnizate) acesteia:

- Administratorul Arhivei
- Abonaţii Arhivei
- Utilizatorii Arhivei.

Administratorul arhivei este in acest caz firma certSIGN. Abonatii sunt acele persoane fizice sau juridice care depun documente in arhiva administrata de certSIGN, in timp ce termenul de utilizatori ai arhivei se refera la toate persoanele care au dreptul sa acceseze documentele din arhiva.

certSIGN oferă servicii de arhivare digitala pentru orice *persoană fizică* sau *juridică* care doreste acest lucru si incheie in prealabil un contract. Scopul acestor document (ce include politicile si procedurile operationale ale arhivei digitale si al centrului de date şi securitatea sistemului

informaţional) este acela de a garanta utilizatorilor ca serviciile de arhivare oferite de certSIGN sunt de incredere, prin asta intelegand atat pastrarea integritatii si disponibilitatii documentelor, cat si controlul accesului la acestea.

1.4 Adresa de contact

Adresa: Sos. Oltenitei nr. 107A, C1, parter, Cod poştal 041303

E-mail: office@certsign.ro

Telefon: 021 311 99 04

Fax: 021 311 99 05

Informaţii adiţionale despre acest document, ca si despre serviciile de arhivare se pot obţine prin poşta electronica la adresa: office@certsign.ro.

2 Prevederi generale

Acest capitol descrie obligaţiile / garanţiile şi responsabilităţile administratorului arhivei, abonatilor si utilizatorilor finali ai arhivei. Obligaţiile şi responsabilităţile sunt guvernate de contracte între părţile menţionate mai sus.

Contractele încheiate de certSIGN cu Abonaţii si, eventual, cu utilizatorii descriu tipurile de servicii furnizate de certSIGN, obligaţiile mutuale şi responsabilităţile acestora.

2.1 Obligaţii

2.1.1 Obligaţiile certSIGN

certSIGN garantează că:

- activitatea sa comercială se bazează pe echipamente fiabile şi aplicaţii software de încredere,
- activitatea şi serviciile sale sunt în concordanţă cu prevederile legale, nu încalcă drepturile de autor şi nici drepturile terţelor părţi,
- serviciile sale sunt în concordanţă cu normele larg acceptate
- respectă şi impune procedurile descrise în prezentul document, în special cele cu privire la:

  asigură protecţia datelor cu caracter personal în concordanţă cu REGULAMENTUL (UE) 2016/679 (GDPR) AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date si cu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;

certSIGN se angajează:

- sa inregistreze si sa tina evidenta tuturor documentelor in format electronic intrate in arhiva electronica in cadrul unui registru in forma electronica.

- sa acopere prejudiciile pe care le-ar putea cauza cu prilejul desfasurarii activitatilor de arhivare electronic
- sa indeplineasca conditiile legale privind protectia informatiilor clasificate, in cazul in care arhiva contine sau urmeaza sa contina documente clasificate
- sa asigure intretinerea si sa puna la dispozitie programe informatice, care sa permita translatarea oricarui document in forma electronica arhivat din formatul in care a fost generat intr-un format care sa permita vizualizarea, reproducerea si stocarea documentului respectiv la nivelul tehnologiilor in uz curent.
- in momentul arhivarii unui document generat intr-un format nerecunoscut de produsele existente in biblioteca de algoritmi si programe informatice, administratorul arhivei electronice are obligatia ca, odata cu arhivarea documentului, sa adauge in biblioteca descrierea formatului acestuia, precum si programele informatice cu care documentul a fost generat si poate fi vizualizat.
- Sa respecte regimul de acces la document, stabilit de catre titularul dreptului de dispozitie asupra documentului, atat la arhivare, cat si la acordarea accesului la documentul in forma electronica din arhiva.
- Sa intretina arhiva electronica
- sa creeze o arhiva electronica de siguranta care sa cuprinda toate documentele in forma electronica arhivate si care se actualizeaza permanent off-line;
- sa utilizeze un sistem de securitate omologat, care sa garanteze integritatea, securitatea si, unde este cazul, confidentialitatea documentelor in forma electronica arhivate
- sa asigure redarea oricarui document in forma electronica continut in arhiva
- sa asigure, la cererea emitentului sau proprietarului documentelor si cu respectarea normelor legale aplicabile arhivelor, distrugerea documentelor a caror perioada de arhivare a expirat;

2.1.2 Obligaţiile Abonaţilor

Pentru depunerea unui document în arhiva electronică, beneficiarul trebuie să îndeplinească următoarele condiţii:

a)să posede un cont valabil de acces la arhiva electronica, accesul fiind facut fie cu un certificat digital calificat pentru semnătura electronică, fie prin nume utilizator si parola;
b) certificatul digital calificat să fie valabil;
c) să comunice administratorului informaţiile necesare verificării valabilităţii certificatului folosit pentru semnarea electronică a documentelor stocate în arhiva electronică.

Prin contract, Abonatul final se angajează:

- să fie de acord cu termenii contractului;
- să nu puna la dispozitia persoanelor neautorizate mijloacele de autentificare la serviciile arhivei

2.1.3 Obligaţiile Utilizatorilor

Utilizatorii care primesc de la abonatii arhivei dreptul de acces la documente clasificate depuse de acestia agreeaza cu abonatii drepturile si obligatiile asociate. Obligatiile utilizatorilor pot decurge si din contractele incheiate direct cu certSIGN.

2.2 Răspunderea

Răspunderea părţilor ce oferă, sau utilizează servicii în domeniul gestionat de certSIGN, este stabilită prin contractele încheiate între acestea.

Răspunderea juridică, nu elimină şi nici nu substituie răspunderea ce decurge din contractele încheiate între părţi sau din acte normative.

2.2.1 Răspunderea Abonaţilor

Răspunderea juridică a Abonaţilor rezultă din obligaţiile şi garanţiile specificate în Capitolul 2.1.2. Condiţiile în care intervine această răspundere sunt stipulate în contractul încheiat de abonat cu certSIGN.

2.2.2 Răspunderea Utilizatorilor

Răspunderea juridică a utilizatorilor rezultă din drepturile şi obligaţiile stipulate în Capitolul 2.1.3. Condiţiile în care intervine răspunderea sunt stipulate în contractul încheiat de utilizatori cu certSIGN, sau cu un Abonat.

2.3 Responsabilităţi de natură financiară

certSIGN va acoperi prejudiciile pe care le-ar putea cauza cu prilejul desfăşurării activităţii de arhivare digitala in conditiile impuse de lege.

2.4 Legea aplicabilă. Durata. Aplicabilitate. Alte rezoluţii

2.4.1 Intrarea în vigoare. Durata

2.4.1.1 Intrarea în vigoare. Durata. Modificarea clauzelor

Prevederile prezentului document intră în vigoare la data notificarii către autoritatile statului şi sunt valabile până la data unei noi versiuni.

Modificările prevederilor prezentului document, sau introducerea de noi prevederi se desfăşoară în concordanţă cu procedurile prezentate în Capitolul 6.

2.4.1.2 Excepţii de la durata de valabilitate

Dacă înţelegerile încheiate pe baza prezentului document conţin clauze de confidenţialitate asupra conţinutului, clauze privind confidenţialitatea informaţiilor deţinute de părţi, clauze referitoare la respectarea drepturilor de copyright, sau drepturilor de autor, aceste clauze sunt considerate în

vigoare şi după expirarea perioadei de valabilitate a înţelegerii dintre părţi, pentru o perioadă care se va defini la momentul realizarii intelegerii respective si cu respectarea normelor legale in vigoare.

2.5 Auditul

Auditurile au ca obiectiv verificarea consistenţei acţiunilor certSIGN sau a entităţilor delegate de aceasta cu declaraţiile şi procedurile acestora. Auditurile desfăşurate de certSIGN urmăresc în principal centrele de procesare a datelor şi procedurile de arhivare. Auditurile desfăşurate de certSIGN pot fi efectuate de echipe interne (audit intern) sau de organizaţii independente (audit extern). În ambele cazuri, auditul se desfăşoară la cererea şi sub supravegherea administratorului de securitate.

2.5.1 Frecvenţa auditării

Auditul extern prin care se verifică compatibilitatea cu reglementările legale şi procedurale se desfăşoară ori de cate ori este nevoie, în timp ce un audit intern este efectuat cel puţin o dată pe an.

2.5.2 Identitatea / calificările auditorului

Auditul extern este realizat de către o instituţie românească autorizată şi independentă faţă de certSIGN sau de către o instituţie internaţionala având reprezentanţă sau orice sediu secundar în România. O asemenea instituţie trebuie să:

- angajeze personal având cunoştinţe şi experienţă tehnică corespunzătoare (să dispună de documente care să certifice acest lucru) în domeniul infrastructurilor de chei publice, tehnologiilor şi dispozitivelor de securitate informatică şi de auditare a securităţii sistemelor.
- fie organizaţie sau societate înregistrată şi de renume.

Auditul intern este realizat de către departamentul de calitate şi audit al certSIGN.

2.5.3 Domeniile supuse auditării

Auditurile interne şi externe se desfăşoară conform regulilor şi procedurilor acceptate pe plan internaţional pentru centrele de date si arhivele digitale şi vizează:

- securitatea fizică a certSIGN,
- procedurile de furnizare a serviciilor,
- securitatea aplicaţiilor software şi a accesului la reţea,
- securitatea personalului certSIGN,
- jurnalele de evenimente şi procedurile de monitorizare a sistemului,
- arhivarea şi regasirea datelor,
- procedurile de arhivare,

2.5.4 Măsurile întreprinse ca urmare a descoperirii unei deficienţe

Rezultatele auditurilor interne şi externe sunt transmise managementului certSIGN. În termen de 14 zile de la transmiterea rezultatelor, acesta trebuie să pregătească o opinie scrisă cu privire la deficienţele sesizate şi să propună un plan de acţiune şi termene de rezolvare, pentru eliminarea deficienţelor. Informaţiile referitoare la modul de rezolvare a deficientelor vor fi trimise auditorului.

2.6 Confidenţialitatea şi caracterul privat al informaţiilor

Toate informaţiile pe care le deţine certSIGN au fost obţinute, păstrate şi procesate în concordanţă cu legile în vigoare, în mod special cu REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date şi cu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice. Relaţiile dintre un Abonat, un utilizator şi certSIGN se bazează pe încredere.

O parte va fi exonerată de răspunderea pentru dezvăluirea de informaţii confidenţiale, dacă:

a) informaţia era cunoscută părţii contractante înainte ca ea să fi fost primită de la cealaltă parte contractantă;

sau

b) informaţia a fost dezvăluită după ce a fost obţinut acordul scris al celeilalte părţi pentru asemenea dezvăluire;

sau

c) partea a fost obligată în mod legal să dezvăluie informaţia.

Dezvăluirea oricărei informaţii faţa de persoanele implicate în îndeplinirea obligaţiilor, se va face confidenţial şi se va extinde numai asupra acelor informaţii necesare în vederea îndeplinirii obligaţiilor.

2.6.1 Tipuri de informaţii considerate ca fiind private sau confidenţiale

Angajaţii certSIGN sunt obligati să păstreze secretul informaţiilor, atât pe durata, cât şi după încetarea contractului de munca. Sunt catalogate drept informaţii private sau confidenţiale:

- informaţiile furnizate de Abonaţi si clasificate ca atare de catre acestia,
- informaţiile furnizate de, sau către Abonaţi (de exemplu, conţinutul contractelor încheiate cu Abonaţii sau Utilizatorii, conturi bancare, aplicaţiile software utilizate); o parte din informaţiile menţionate mai sus poate fi dezvăluită doar cu aprobarea şi în scopul menţionat de proprietarul informaţiilor (de exemplu, Abonatul),
- înregistrările corespunzătoare tranzacţiilor din sistem (toate tipurile de tranzacţii, precum şi datele pentru controlul tranzacţiilor, aşa numitele loguri ale tranzacţiilor din sistem)
- înregistrările corespunzătoare evenimentelor (loguri) ce ţin de serviciile de arhivare, păstrate de către certSIGN,
- rezultatele auditurilor interne şi externe, dacă acestea reprezintă o ameninţare pentru securitatea certSIGN,
- planurile în caz de urgenţă,

- informaţiile referitoare la măsurile luate pentru protecţia dispozitivelor hardware şi aplicaţiilor software, informaţiile referitoare la modul de administrare a serviciilor de arhivare.

2.6.2 Tipuri de informaţii care nu sunt considerate ca fiind private sau confidenţiale

Nu sunt considerate ca private sau confidentiale informatiile din arhiva care sunt considerate in mod expres de Abonat ca publice. O parte din informaţiile furnizate de, sau către Abonaţi poate fi pusă la dispoziţia altor entităţi, doar cu acordul scris al Abonatului şi în scopul menţionat în contractul încheiat cu Abonatul.

2.6.3 Dezvăluirea informaţiilor confidenţiale către autorităţile legale

Informaţiile confidenţiale pot fi dezvăluite reprezentanţilor autorităţilor legale numai după îndeplinirea tuturor formalităţilor cerute de legislaţia în vigoare în România.

2.7 Drepturile de proprietate intelectuală

Toate mărcile, patentele, siglele, licenţele, imaginile grafice etc. folosite de către certSIGN sunt şi vor rămâne proprietatea intelectuală a deţinătorilor legali ai acestora. certSIGN se obligă să specifice acest lucru conform cerinţelor impuse de deţinători.

Toate mărcile, patentele, siglele, licenţele, imaginile grafice etc., aparţinând certSIGN sunt şi rămân proprietatea acesteia, indiferent dacă sunt însoţite sau nu de patente, modele de utilitate, copyright sau altele asemenea şi nu pot fi reproduse sau furnizate unei terţe părţi fără acordul prealabil în scris al certSIGN.

2.7.1 Marci Inregistrate

“Certsign nu verifica daca Abonatul este persoana în numele căreia marca este înregistrată în Registrul Naţional al Mărcilor sau daca beneficiaza de dreptul, acordat de titularul marcii, de utilizare a acesteia, Abonatul fiind singurul raspunzator pentru corectitudinea informaţiilor furnizate in vederea furnizarii serviciului. Oficiul de Stat pentru Invenţii şi Mărci este organul de specialitate al administraţiei publice centrale, unica autoritate care asigură pe teritoriul României protecţia mărcilor şi indicaţiilor geografice. In conformitate cu prevederile Legii nr. 84/1998

privind mărcile şi indicaţiile geografice, “Dreptul asupra mărcii este dobândit şi protejat prin înregistrarea acesteia la Oficiul de Stat pentru Invenţii şi Mărci.” (Art. 4).”

3 Politicile si procedurile operationale de arhivare

3.1 Politici

3.1.1 Planificarea prezervarii

Arhiva foloseste strategii de prezervare documentate si pentru fiecare clasa de informatie prezervata, dispune de o metodologie de prezervare identificabila. Arhiva identifica proprietatile pe care le va prezerva la obiectele digitale. Arhiva poate furniza evidente a succesului planificarii prezervarii. Arhiva dispune de mecansisme pentru a isi schimba planurile de prezervare ca urmare a activitatilor sale de monitorizare. Arhiva obtine suficient control fizic asupra obiectelor digitale pentru a le putea prezerva. Arhiva poate demonstra cand responsabilitatea prezervarii a fost acceptata formal pentru datele supuse arhivarii.

3.1.2 Definirea AIP

Arhiva are o definitie scrisa si identificabila pentru fiecare AIP sau clasa de informatie arhivata. Aceste definitii corespund nevoilor de prezervare pe termen lung si sunt conforme cu standardele de prezervare acceptate (de ex PERM, ISO9015.2, DTR checklist). Arhiva verifica fiecare AIP pentru completitudine si corectitudine in momentul crearii sale.

3.1.3 Metadatele de Prezervare

Arhiva creeaza informatii descriptive de prezervare pentru informatia arhivata. Arhiva indeplineste cel putin cerintele minime legale pentru metadate, pentru a permite comunitatii de utilizatori sa descopere si sa identifice materialul de interes.

3.1.4 Managmentul Metadatelor

Arhiva dispune de un proces scris si identificabil pentru managementul metadatelor , care include planificarea managementului ciclului de viata al metadatelor si deciziile de acces la metadate.

3.1.5 Identificatori Persistenti

Arhiva dispune si utilizeaza o conventie de nume care genereaza in mod demonstrabil identificatori unici si vizibili pentru toate AIPurile (un pachet infomational, constand din informatia de continut si informatia descriptiva de prezervare asociata, care este arhivat in sistem)

3.1.6 Provenienta

Arhiva dispune de un sistem pentru urmarirea evenimentelor relevante asociate ciclului de viata. Acesta se refera la schimbari la modul sau de operare, ale procedurilor, software-ului si hardware-ului, trasabile – daca este cazul- la strategiile sale de prezervare. Arhiva dispune de o istorie documentata a schimbarilor modului sau de operare, al procedurilor, software-ului si hardware-ului care, atunci cand este necesar, este legata de strategiile de prezervare si descrie efectele potentiale asupra prezervarii continutului digital.

3.1.7 Dezvoltarea Colectiilor

Arhiva intretine un set de cerinte de eligibilitate a continutului de arhivat, incluzand atat criterii de acceptare de nivel inalt, cat si decizii de la caz la caz.

3.1.8 Validarea sursei

Arhiva dispune de un proces pentru a se asigura asupra faptului ca informatia acceptata provine dintr-o sursa cunoscuta si acceptabila.

3.1.9 Managementul inregistrarilor electronice

Arhiva dispune de reguli documentate pentru pastrarea si distrugerea sau arhivarea permanenta a diferitelor tipuri de inregistrari electronice.

3.1.10 Informatia de reprezentare

Arhiva poate demonstra faptul ca are acces la instrumentele si resursele necesare pentru a stabili contextul semantic sau tehnic al obiectelor digitale pe care le contine. Arhiva inregistreaza informatia de reprezentare (inclusiv formatul) primita in arhiva.

3.1.11 Migrarea Formatului Continutului

Arhiva dispune de un proces documentat pentru monitorizarea viabilitatii formatelor informatiei continute si migrarea continutului la noi formate in caz de necesitate.

3.1.12 Versionare

Arhiva dispune de un proces documentat de administrare a multiplelor versiuni ale aceluiasi continut.

3.1.13 Suport pentru Format

Arhiva identifica acele formate de fisiere pe care accepta sa le arhiveze. Arhiva publica formatele suportate si incurajeaza abonatii sa utilize acele formate.

3.1.14 Integritatea Referentiala a Informatiei Descriptive

Arhiva poate demonstra ca integritatea referentiala este creata si mentinuta intre toate obiectele arhivate si informatia descriptiva asociata.

3.2 Procedurile de arhivare

În continuare sunt prezentate procedurile de bază ale procesului de arhivare. Fiecare procedură începe cu trimiterea, de către Abonat, a unei cereri de arhivare continand un set de informatii. Pe baza cererii, administratorul ia o decizie în legătură cu furnizarea / respingerea serviciului cerut. Cererile trimise trebuie să conţină informaţiile necesare pentru identificarea corectă a Abonatului.

certSIGN oferă acces la următoarele servicii de bază:

a. Primirea de pachete de informatii

b. Stocarea si prezervarea pachetelor de informatii

c. Acces controlat la pachetele de informatii.

d. Scoaterea din arhiva a pachetelor de informatii sau distrugerea acestora

Programul de lucru

Serviciile de acces al arhivei, fie pentru adaugare, consultare, retragere documente din arhiva sunt oferite on-line. Serviciile online de acces la arhiva sunt oferite permanent, iar cele de suport si asistenta in utilizarea serviciilor online sunt oferite prin telefon sau posta electronica , de luni până vineri, între orele 9 şi 18.

3.2.1 Trimiterea cererii

Cererile online sunt trimise prin protocoale de comunicaţie precum HTTP, S/MIME sau TCP/IP.

certSIGN furnizeaza serviciile mentionate numai pe baza cererilor de transmitere (inregistrare), arhivare (stocare si prezervare), modificare format, accesare, retragere sau distrugere a pachetelor de informatii.

Cererile pot fi trimise de persoane fizice autorizate de companii sau in nume propriu, sau pot fi trimise automat de dispozitive care indeplinesc anumite conditii de siguranta.

Primirea unui document in forma electronica in arhiva electronica este conditionata de indeplinirea urmatoarelor cerinte:
a) semnarea documentelor in forma electronica cu semnatura electronica extinsa a titularului dreptului de dispozitie asupra documentului, denumit, in continuare semnatura electronica
b) valabilitatea semnaturii electronice a titularului dreptului de dispozitie asupra documentului;

Mai departe, documentul in forma electronica ce indeplineste conditiile mentionate mai sus este semnat electronic de catre administratorul arhivei electronice, cu semnatura electronica in care se atesta si faptul ca documentul respectiv are valoare de original sau copie, conform hotararii titularului dreptului de dispozitie asupra documentului. Documentul in forma electronica astfel identificat, este arhivat in locatia stabilita de administratorul arhivei electronice.

Fiecare cerere de transmitere (inregistare) de informatii in arhiva trebuie insotita de urmatoarele informatii:

a) proprietarul documentului in forma electronica
b) titularul dreptului de dispozitie asupra documentului;

c) tipul documentului in forma electronica
d) nivelul de clasificare a documentului in forma electronica
e) regimul de acces al documentului
f) formatul digital in care este arhivat documentul in forma electronica

g) cuvintele-cheie necesare identificarii documentului in forma electronica
h) data emiterii documentului;
i) termenul de pastrare a documentului.

Administratorul arhivei electronice ataseaza pentru fiecare document arhivat in forma electronica, o fisa in forma electronica ce va contine aceste informatii, plus:

j) elementele de localizare a suportului fizic
k) data arhivarii

3.2.2 Procesarea cererilor

certSIGN acceptă cereri înaintate individual sau colectiv. Cererile pot fi trimise *on-line* şi *off-line*.

Cererea trimisă off-line se poate face:

- Prin prezentarea în persoană a Abonatului sau a reprezentantului autorizat al companiei la centrul(ele) de relatii cu publicul al(e) arhivei, caz în care se completează şi se semnează de mână cererea, se semnează contractul cu privire la prestarea serviciilor de arhivare şi se agreeaza metodele sigure de transmitere si accesare a informatiilor spre si dinspre arhiva.
- Prin trimiterea prin poştă a cererii şi a copiilor documentelor necesare verificării identităţii solicitantului;.

Fiecare cerere scrisă pe hârtie este procesată după cum urmează:

- operatorul arhivei primeşte cererea Abonatului
- operatorul verifică datele din cerere
- ca urmare a verificării, operatorul confirmă identitatea dintre datele declarate şi cele cuprinse în cerere; dacă cererea conţine date neconforme este respinsă
- cererea confirmată este trimisă catre administratorul arhivei.

3.2.3 Efectuarea operatiilor

După primirea şi procesarea unei cereri, administratorul arhivei efectueaza operatiile solicitate. La inregistarea unui pachet nou de informatii, acesta primeste un numar unic de inregistrare in cadrul sistemului. Concomitent cu înregistrarea se completează fişa electronică a documentului.
Administratorul arhivei electronice va inregistra si va lua in evidenta toate documentelor in forma electronica intrate in arhiva electronica in cadrul unui registru in forma electronica.

3.2.4 Timpul necesar pentru efectuarea unei operatii

Timpul maxim de efectuare a oricarei operatii este agreat intr-un SLA care este parte integranta a fiecarui contract.

3.2.5 Notificarea operatiilor

Dupa efectuarea cu succes a oricarei operatii, abonatul este informat despre acest lucru. In cazul in care operatia nu poate fi efectuata, administratorul arhivei va lua toate masurile necesare pentru asigurarea succesului operatiei prin comunicarea cu Abonatul.

3.2.6 Respingerea unei solicitari de operatii

certSIGN poate refuza inregistrarea (primirea) unui pachet de informatii in arhiva fără a-şi asuma vreo obligaţie sau responsabilitate pentru posibilele daune sau pierderi pe care le poate suferi Abonatul ca urmare a acestui refuz. Refuzul inregistrarii unui pachet de informatii poate surveni în următoarele situaţii:

- dacă există suspiciune sau certitudine cu privire la falsificarea sau folosirea unor date false de către Abonat
- daca abonatul nu trimite datele solicitate conform 3.3
- dacă Abonatul, într-o manieră neconvenabilă, angajează resurse şi mijloace de procesare ale certSIGN prin trimiterea unui număr de cereri în mod clar mai mare decât nevoile pe care le are acesta,
- din alte motive decât cele de mai sus.

Informaţiile privind decizia refuzului de furnizarea serviciului şi motivele acesteia sunt trimise solicitantului. Solicitantul poate cere din nou efectuarea aceleiasi operatii numai după ce motivele care au dus la refuzul emiterii au încetat.

3.2.7 Accesarea pachetelor de informatii

Administratorul arhivei ia toate masurile necesare pentru ca regimul de acces la pachetele de informatii din arhiva sa se faca asa cum a stabilit Abonatul. In acest sens, orice accesare sa face numai cu autentificare prealabila prin mijloace sigure si numai cu transmiterea criptata a informatiilor. Toate operatiile sunt inregistrate pentru ca, ulterior, abonatul, auditorii sau

autoritatile abilitate ale statului sa poata urmari sirul operatiilor si trasabilitatea acestora la persoane sau dispozitive.

3.2.8 Retragerea sau distrugerea pachetelor de informatii

Retragerea pachetelor de informatii din arhiva sau distrugerea acestora nu pot fi dispuse decat de catre Abonat sau de catre persoanele autorizate de acesta. Operatiile se efectueaza numai dupa autentificarea cererii si numai cu actualizarea registrului arhivei. Administratorul arhivei se asigura ca legaturile referentiale la alte pachete de informatii din arhiva sunt actualizate corespunzator si ca in arhiva nu mai ramane nicio urma fizica a datelor retrase sau distruse.

3.3 Înregistrarea evenimentelor şi procedurile de auditare

Pentru a gestiona eficient sistemele certSIGN şi pentru a putea audita acţiunile utilizatorilor şi personalului certSIGN, toate evenimentele care apar în sistem sunt înregistrate. Informaţiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente şi trebuie păstrate în aşa fel încât să permită ulterior accesarea informaţiilor corespunzătoare necesare rezolvării disputelor, sau să detecteze tentativele de compromitere a securităţii certSIGN. Evenimentele înregistrate fac obiectul procedurilor de arhivare. Arhivele sunt păstrate si în afara incintei unde se afla centrul de date certSIGN.

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. Fiecare înregistrare în log, electronic sau de mână, este păstrata şi dezvăluita atunci când se desfăşoară un audit.

În sistemele certSIGN, auditorul intern de securitate este obligat să realizeze anual un audit referitor la respectarea politicilor si procedurilor de către mecanismele şi procedurile implementate şi să evalueze eficienţa procedurilor de securitate existente.

3.3.1 Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securităţii certSIGN este înregistrată în log-urile de evenimente şi arhivată.

Log-urile de evenimente certSIGN conţin înregistrări cronologice ale tuturor activităţilor generate de componentele software din cadrul sistemului. Aceste înregistrări sunt împărţite în trei categorii separate:

- **înregistrări de sistem** – conţin informaţii despre cererile clienţilor şi răspunsurile server-ului (sau invers) la nivelul protocolului de reţea (de exemplu http, https); datele concrete care se înregistrează sunt: adresa IP a staţiei sau a server-ului, operaţiunile executate (de exemplu: căutare, editare, scriere etc.) şi rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- **erori** – conţine informaţii despre erori la nivelul protocoalelor de reţea şi la nivelul modulelor aplicaţiilor;
- **audit** – conţin informaţii specifice serviciilor de arhivare

Jurnalele de evenimente de mai sus sunt comune fiecărei componente instalate pe un server sau staţie de lucru şi au o capacitate prestabilită. Atunci când se depăşeşte această capacitate, este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat şi şters de pe disc.

Fiecare înregistrare, automată sau manuală, conţine următoarele informaţii:

- tipul evenimentului,
- identificatorul evenimentului,
- data şi ora apariţiei evenimentului,
- identificatorul persoanei responsabile de eveniment.

Conţinutul înregistrărilor se refera la:

- alertele firewall-urilor şi IDS-urilor,
- operaţiile asociate înregistrării, scrierii pe suport fizic, conversiei de format, accesarii, stergerii, migrarii datelor
- modificări ale structurii hard sau soft,
- modificări ale reţelei şi conexiunilor,
- înregistrările fizice în zonele securizate şi violările de securitate,
- schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,
- accesul reuşit şi nereuşit la bazele de date şi la aplicaţiile serverului,

- istoria creării copiilor de backup şi a arhivelor cu înregistrări.

Accesul al jurnalele de evenimente (log-uri) este permis în exclusivitate administratorului de securitate, administratorului arhivei şi auditorilor.

3.3.2 Frecvenţa analizei jurnalelor de evenimente

Înregistrările din jurnalul de evenimente trebuie revăzute în detaliu cel puţin o dată pe lună. Orice eveniment având o importanţă semnificativă trebuie explicat şi descris într-un jurnal. Procesul de verificare a jurnalului include verificarea unor eventuale falsificări, sau modificări şi verificarea fiecărei alerte sau anomalii consemnată în log-uri. Orice acţiune executată ca rezultat al funcţionări defectuoase detectate trebuie înregistrată în jurnal.

3.3.3 Perioada de retenţie a jurnalelor de evenimente

Înregistrările evenimentelor sunt stocate în fişiere pe discul sistem până când acestea ajung la capacitatea maximă permisă. În tot acest timp sunt disponibile on-line, la cererea fiecărei persoane, sau proces autorizat. După depăşirea spaţiului alocat, jurnalele sunt păstrate în arhive şi pot fi accesate numai off-line, de la o anumită staţie de lucru.

Jurnalele arhivate sunt păstrate cel puţin 2 ani.

3.3.4 Protecţia jurnalelor de evenimente

Un jurnal de evenimente poate fi revăzut numai de administratorului de securitate, administratorul arhivei, sau de către un auditor. Accesul la jurnalul de evenimente este configurat în aşa fel încât:

- numai entităţile de mai sus au dreptul să citească înregistrările jurnalului,
- numai administratorul de securitate poate arhiva sau şterge fişiere (după arhivarea acestora) care conţin evenimentele înregistrate,
- nici o entitate nu are dreptul să modifice conţinutul unui jurnal.

3.3.5 Procedurile de backup pentru jurnalele de evenimente

Procedurile de securitate certSIGN solicita ca jurnalul de evenimente să facă obiectul backup-ului lunar. Aceste backup-uri sunt stocate în locaţii auxiliare ale certSIGN.

3.3.6 Notificarea entităţilor responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente şi sesizează automat activităţile suspecte sau pe cele care au ca scop compromiterea securităţii. În cazul activităţilor care au influenţă asupra securităţii sistemului, sunt notificaţi automat administratorul de securitate şi administratorul arhivei. În celelalte cazuri, notificarea este direcţionată numai către administratorul de sistem. Transmiterea informaţiilor către persoanele autorizate despre situaţiile critice – din punctul de vedere al securităţii sistemului – se face prin alte mijloace de comunicare, protejate corespunzător, de exemplu, , telefon mobil, poştă electronica. Entităţile notificate iau măsurile corespunzătoare pentru a proteja sistemul faţă de ameninţarea detectată.

3.4 Analiza vulnerabilităţilor

certSIGN se obliga să facă o analiză a vulnerabilităţilor pentru fiecare procedură internă, aplicaţie şi sistem informatic. Cerinţele de analiză pot, de asemenea, să fie stabilite de către o instituţie externă, autorizată să auditeze certSIGN. Administratorul de securitate are sarcina de a solicita audituri interne prin care să verifice conformitatea înregistrărilor din jurnalul de securitate, corectitudinea copiilor de backup, activităţile executate în cazul apariţiei unei ameninţări şi conformitatea cu politicile si procedurile.

Instituţia externă care efectuează auditul de securitate, trebuie să desfăşoare această activitate respectând recomandările ISO/IEC 13335 (Guidelines for Management of IT Security) şi ISO/IEC 17799 (Code of Practice for Information Security Management).

3.5 Procedura de backup si restaurare

Copiile de siguranţă permit restaurarea completă (dacă este necesar, de exemplu, după distrugerea sistemului) a datelor sistemului de arhivare electronica. Pentru a realiza acest lucru, sunt copiate următoarele aplicaţii şi fişiere:

- kit-urile de instalare a aplicaţiilor sistem (de exemplu sistemul de operare),
- kit-urile de instalare a aplicaţiilor care compun sistemul informatic de arhivare.
- kit-ul serverului Web şi kit-ul de instalare a sistemelor de gestiune a bazelor de date,
- datele privind Abonaţii şi personalul certSIGN,
- baza de date a aplicatiei de arhivare
- jurnalele de evenimente.

Metoda de creare a copiilor de backup are o influenţă deosebită asupra timpului şi costului restaurării sistemului informatic de arhivare după defectarea, sau distrugerea sistemului. certSIGN foloseşte atât backup-uri full (săptămânale), cat şi backup-uri incrementale (zilnice), toate copiile sunt clonate şi clonele sunt păstrate în altă locaţie, în aceleaşi condiţii de securitate ca şi cele din locaţia primară.

Procedura de restaurare va fi verificata periodic, pentru a se verifica utilitatea backup-ului, in caz de crash. Va trebui sa se verifice daca datele salvate sunt suficiente pentru restaurarea sistemului in cel mai scurt timp posibil. Concluziile testelor vor fi inregistrate

3.6 Arhivarea înregistrărilor

Pe langa arhivarea pachetelor de informatii (activitate care reprezinta insasi esenta serviciului de arhivare digitala) este necesar ca cererile trimise de Abonaţi, informaţiile despre Abonaţi, pachetele de informatii arhivate (metadatele) să fie arhivate.

Pe baza arhivelor se creează copiile de siguranţă care sunt ţinute în afara locaţiei certSIGN.

3.6.1 Tipurile de date arhivate

Următoarele date sunt incluse în procesul de arhivare:

- cererile primite şi deciziile emise, în formă electronica, trimise de, sau către un Abonat sub formă de fişiere sau mesaje electronice,
- baza de date cu Abonaţi,
- metadatele,

- logurile sistemului informatic de arhivare

3.6.2 Compromiterea resurselor de calcul, a aplicaţiilor software şi/sau datelor

Politica de securitate a certSIGN ia în considerare următoarele ameninţări ce pot influenţa disponibilitatea şi continuitatea serviciilor oferite:

- distrugerea fizică a sistemului de calcul al certSIGN, inclusiv a resurselor de reţea – această ameninţare se referă la distrugerile provocate de situaţiile de urgenţă,
- funcţionarea defectuoasă a aplicaţiilor, având ca efect imposibilitatea accesării datelor - aceste deteriorări se referă la sistemul de operare, aplicaţiile utilizatorilor şi executarea de aplicaţii periculoase, cum ar fi viruşii, viermii, caii troieni,
- pierderea unor servicii de reţea importante pentru activitatea certSIGN . Acestea se referă în primul rând la căderile de tensiune şi distrugerea legăturilor de reţea.
- distrugerea unei părţi din Intranetul folosit de certSIGN pentru a furniza servicii – acest lucru poate duce la obstrucţionarea clienţilor şi refuzul (neintenţionat) al serviciilor.

Pentru a preveni sau limita efectele ameninţărilor de mai sus:

- Politica de securitate a certSIGN include un Plan de continuitate a afacerii şi recuperare în caz de dezastru,
- În cazul apariţiei unui eveniment ce blochează funcţionarea certSIGN, în maxim 48 de ore, va fi activată locaţia auxiliară ce poate substitui toate funcţiile importante ale centrului de date si ale arhivei până la restaurarea locaţiei principale. Distanta dintre locatia primara si cea secundara corespunde normelor europene în domeniu si este suficienta pentru ca majoritatea potentialelor dezastre care pot afecta locatia primara sa nu afecteze in acelasi timp si locatia secundara.
- Instalarea de versiuni noi ale aplicaţiilor software în producţie se poate face numai după testarea intensivă a acestora într-un mediu de test, în conformitate cu procedurile descrise. Orice modificare a sistemului necesită aprobarea administratorului de securitate al certSIGN.

- Sistemul certSIGN dispune de aplicaţii pentru crearea copiilor de backup pe baza cărora se poate face în orice moment restaurarea sistemului şi auditarea acestuia. Copiile de siguranţă includ toate datele relevante din punct de vedere al securităţii.

3.6.3 Coerenţa securităţii după dezastru

După fiecare recuperare a sistemului ca urmare a unui dezastru, administratorul de securitate sau administratorul arhivei trebuie să acţioneze în conformitate cu Planul de continuitate a afacerii şi recuperare în caz de dezastru.

3.7 Încetarea activităţii arhivei digitale sau transferarea serviciilor

Obligaţiile prezentate mai jos sunt stabilite pentru a minimiza efectele negative asupra Abonaţilor şi Utilizatorilor, ce pot apare ca urmare a deciziei arhivei digitale de a-şi înceta activitatea şi se refera la obligaţiile de a notifica în prealabil toţi Abonaţii arhivei care-şi încetează activitatea şi transferarea responsabilităţilor (servicii oferite Abonaţilor, baza de date, etc.), conform reglementărilor în vigoare, unei alte arhive.

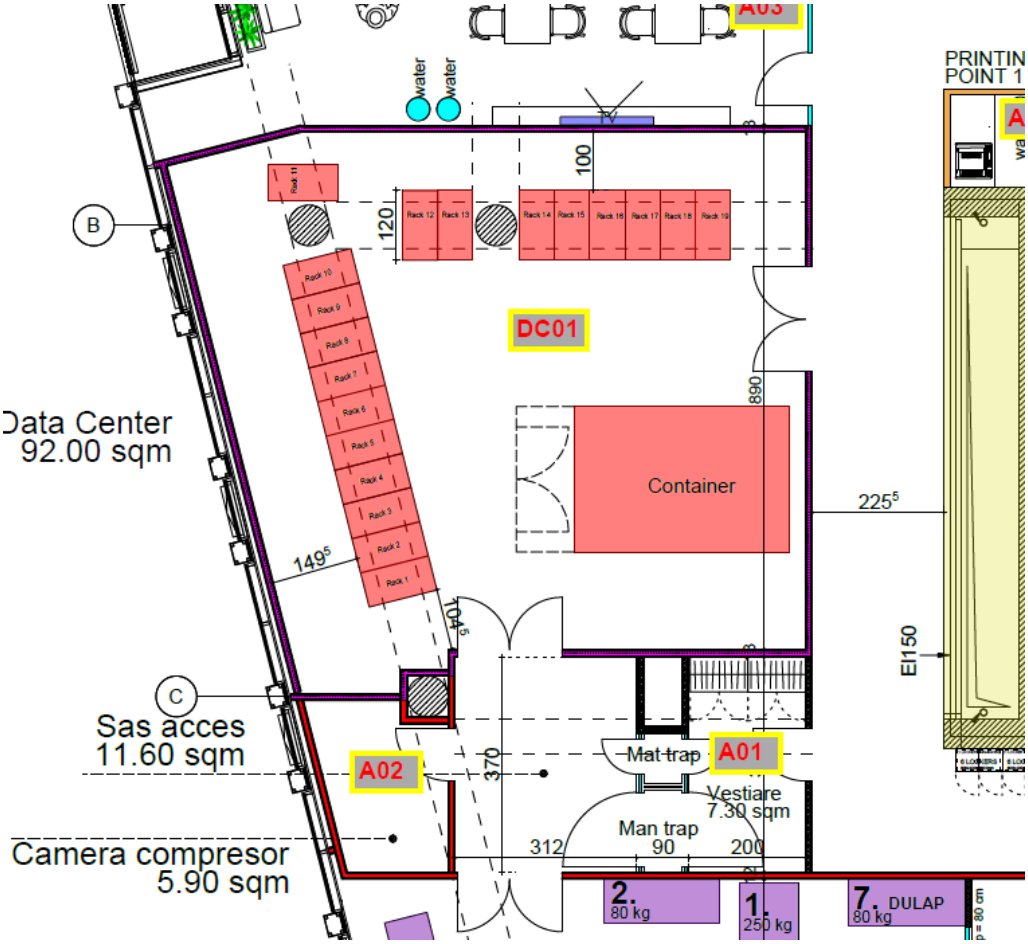
3.7.1 Cerinţe specifice transferului responsabilităţii

Înainte ca arhiva digitala să-şi înceteze activitatea, este obligată să:

- notifice autoritatea in domeniu a statului, cu cel putin 60 de zile inainte, despre intentiea de incetare a activitatii, cu exceptia cazurilor de forta majora.
- transfere arhiva electronica catre alt furnizor de servicii de arhivare electronica cu acordul autoritatii in domeniu a statului.
- sa anunţe Abonaţii săi despre decizia de a-şi înceta activitatea.
- să depună toate eforturile pentru a minimiza efectele negative asupra intereselor Abonaţilor şi persoanelor angajate în procese ce implica utilizarea pachetelor de informatii arhivate de catre arhiva digitala care îşi încheie activitatea.

4 Controale de securitate fizică, organizaţională şi de personal

Acest capitol descrie cerinţele generale privind securitatea fizică şi organizaţională, precum şi activitatea personalului certSIGN în activitatea de administrare si operare a arhivei digitale si a centrului de date.



4.1 Controale de securitate fizică

4.1.1 Controale de securitate fizică în cadrul certSIGN

Sistemele de calcul, terminalele operatorilor şi resursele informaţionale ale certSIGN sunt dispuse într-o zonă dedicată, protejată fizic împotriva accesului neautorizat, distrugerilor sau perturbării activităţii. Aceste locaţii sunt monitorizate. Fiecare intrare şi ieşire este înregistrată în jurnalul de

evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum şi temperatura sunt de asemenea monitorizate şi controlate.

4.1.1.1 Amplasarea locaţiei

Centrul primar de date certSIGN este localizat în Bucureşti, la următoarea adresă: Bd. Tudor Vladimirescu, nr.29A, Sector 5.

4.1.1.2 Accesul fizic

Accesul fizic în cadrul certSIGN este controlat şi monitorizat de un sistem de alarmă integrat. certSIGN dispune de sisteme de prevenire a incendiilor, sisteme de detectare a intruşilor şi sisteme de alimentare cu energie electrică în caz de urgenţă.

Centrul de relatii cu publicul al certSIGN este accesibil în fiecare zi lucrătoare între 9:00 şi 18:00. În restul timpului (inclusiv în zilele nelucrătoare), accesul este permis numai persoanelor autorizate de către conducerea certSIGN. Vizitatorii locaţiilor aparţinând certSIGN trebuie să fie însoţiţi permanent de persoane autorizate.

Zonele ocupate de certSIGN se împart în:

- Centrul de relatii cu publicul
- Centrul de date
- Zona operatorilor
- Zona administratorilor,
- Zona de dezvoltare şi testare.
- Alte departmamente de suport

Accesul la echipamentele centrului de date utilizat pentru arhivarea electronică a documentelor se face in mod controlat, cu precizarea mai multor niveluri de drepturi de acces ale personalului care operează sistemele.

Centrul de date este echipat cu un sistem de securitate monitorizat continuu, alcătuit din senzori de mişcare, efracţie şi incendiu. Accesul în această zonă este permis numai personalului autorizat, de exemplu, administratorul de securitate, administratorul arhivei şi administratorul de sistem.

Monitorizarea drepturilor de acces se face folosind carduri şi cititoare, montate lângă punctul de acces. Fiecare intrare şi ieşire din zonă este înregistrată automat în jurnalul de evenimente.

Controlul accesului în *zona operatorilor şi administratorilor* se face prin intermediul cardurilor şi a cititoarelor de carduri. Deoarece toate informaţiile senzitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor şi administratorilor necesită în prealabil autorizarea acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. Cheile de acces pot fi ridicate numai de personalul autorizat. În această zonă au acces numai angajaţii certSIGN şi persoanele autorizate; ultimilor nu le este permisă prezenţa în zonă neînsoţiţi.

Zona de dezvoltare şi testare este protejată într-o manieră similară cu zona operatorilor şi administratorilor. În această zonă este permisă şi prezenţa persoanelor neînsoţite. Programatorii şi dezvoltatorii nu au acces la informaţii senzitive. Dacă este necesar un astfel de acces, atunci el se poate face numai în prezenţa administratorul de securitate. Proiectele în curs de implementare şi software-ul aferent este testat în mediul de dezvoltare al certSIGN.

4.1.1.3 Sursa de alimentare cu electricitate şi aerul condiţionat

Toate zonele sunt prevăzute cu sisteme de climatizare si senzori de umiditate care asigura valorile optime de temperatura si umiditate in vederea functionarii echipamentelor in conditii de siguranta. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a grupului electrogen al clădirii. Reteaua electrica este dimensionata corespunzator, in functie de consumurile echipamentelor folosite.

4.1.1.4 Expunerea la apă

Riscul de inundaţie în zona centrului de date este controlat prin designul cladirii, al centrelor de datesi al instalatiilor care folosesc apa. Astfel, in zona centrelor de date nu exista tevi cu apa, iar peretii sunt sigilati pt ca o inundatie produsa in alta zona sa nu le afecteze. Podeaua este suprainaltata pe toata suprafata birourilor si centrelor de date, iar apa nu se poate acumula, fiind prevazute scurgeri.

Prevenirea incendiilor

Detectia incendiilor in zona office se face cu senzori aflati sub podea si sub tavan. Stingerea se face cu apa sub presiune. In centrele de date exista un sistem independent de detectie si stingere, bazat pe gaz NOVEC. Toti senzorii sunt integrati in sistemul BMS al cladirii, supravegheat in permanenta de personal autorizat.

4.1.1.5 Aruncarea deşeurilor

Hârtiile şi mediile electronice care conţin informaţii importante din punct de vedere al securităţii certSIGN sunt distruse după expirarea perioadei de păstrare. Modulele de securitate hardware sunt resetate şi şterse conform recomandărilor producătorului. Aceste dispozitive sunt, de asemenea, resetate şi şterse atunci când sunt trimise în service sau reparate.

4.1.1.6 Depozitarea backup-urilor în afara locaţiei

Copiile parolelor, codurile PIN sunt stocate în containere speciale, situate în afara locaţiei certSIGN. Arhivele sunt scopiate si in centrul de date de rezerva.

Stocarea în afara locaţiei se aplică şi în kit-urilor de instalare ale aplicaţiilor certSIGN. Acest lucru permite refacerea de urgenţă a oricărei funcţii a certSIGN în 48 de ore, în locaţia principală a certSIGN, sau în locaţia auxiliară.

4.1.2 Securitatea fizică a utilizatorilor arhivei

Utilizatorii trebuie să-şi protejeze mijloacele sigure de autentificare (parola de acces la sistem, tokenul criptografic şi PIN-ul). Utilizatorii nu trebuie să-şi lase staţia de lucru nesupravegheată atunci când aceasta se află într-o stare nesigură din punct de vedere criptografic, de exemplu, după ce au introdus parola sau PIN-ul ce activează cheia privată.

4.2 Controlul securităţii organizaţiei

Acest capitol prezintă rolurile ce pot fi atribuite personalului care administreaza si opereaza arhiva digitala si centrul de date ale certSIGN. De asemenea, tot în acest capitol sunt descrise responsabilităţile şi sarcinile specifice fiecărui rol.

4.2.1 Roluri de încredere

4.2.1.1 Roluri de încredere în certSIGN

În certSIGN sunt definite următoarele roluri de încredere, care pot fi atribuite uneia sau mai multor persoane:

- **Operator Confluence –** Responsabil de operarea zilnică a sistemelor de încredere ale arhivei si ale centrului de date
- **Administrator de securitate** – Responsabilitate globală pentru implementarea politicilor şi procedurilor de securitate.
    - Iniţiază instalarea, configurarea şi managementul aplicaţiilor software şi hardware (inclusiv resursele de reţea) ale certSIGN; iniţiază şi suspendă serviciile oferite de certSIGN; coordonează administratorii, iniţiază şi supraveghează generarea de chei şi secrete partajate; atribuie drepturi din punct de vedere al securităţii şi privilegiilor de acces ale utilizatorilor; atribuie parole pentru conturile utilizatorilor noi; verifică jurnalele de evenimente; supervizează auditurile interne şi externe; primeşte şi răspunde la rapoartele de audit; supervizează eliminarea deficienţelor constatate în urma auditului.
    - Supraveghează operatorii arhivei si centrului de date; configurează sistemele şi reţeaua, activează şi configurează mecanismele de protecţie a reţelei; creează conturile pentru utilizatorii certSIGN; verifică log-urile de sistem; verifică respectarea politicilor si procedurilor;
- **Administratorul de sistem** – Autorizat să instaleze, configureze şi să întreţină sistemele de încredere ale arhivei si ale centrului de date. Instalează dispozitivele hardware şi sistemele de operare; instalează şi configurează echipamentele de reţea.
- **Administratorul bazei de date** – autorizat sa instaleze, sa configureze si sa intretina sistemele de gestiune a bazelor de date ale arhivei
- **Administratorul aplicatiilor de arhivare** – autorizat sa instaleze, sa configureze si sa intretina aplicatiile software care ofera functiile si serviciile de arhivare. Autorizat să execute operaţiile de backup şi restaurare a sistemului;asigură continuitatea copiilor de

siguranţă şi arhivelor bazelor de date şi a creării log-urilor de sistem; are acces la informaţii confidenţiale despre Abonaţi; transferă copiile de siguranţă ale arhivei şi ale datelor curente în afara locaţiei certSIGN.

- **Auditorul de sistem** – autorizat să acceseze arhivele şi log-urile de audit ale sistemelor de încredere ale arhivei si centrului de date. Responsabil de efectuarea de audituri interne pentru respectarea politicilor si procedurilor;

*În cadrul certSIGN, rolul de **auditor** nu poate fi combinat cu nici un alt rol. O entitate care are un rol diferit de cel de auditor nu poate prelua responsabilităţile auditorului.*

4.2.1.2 Funcţiile de încredere ale Abonaţilor

Abonatul poate nominaliza o persoană (operator) care să exploateze aplicaţiile pentru schimbul electronic de date. Persoana respectivă este răspunzătoare de semnarea, criptarea şi transmiterea mesajelor.

4.2.2 Identificarea şi autentificarea pentru fiecare rol

Personalul certSIGN este supus identificării şi autentificării în următoarele situaţii:

- plasarea pe lista de persoane care au dreptul de a accesa locaţiile certSIGN ,
- plasarea pe lista de persoane care au acces fizic la sisteme şi resurse de reţea aparţinând certSIGN,
- emiterea confirmării care autorizează îndeplinirea rolului asignat,
- asignarea unui cont şi a unei parole în sistemul informatic al certSIGN,

Fiecare cont asignat:

- trebuie să fie unic şi asignat direct unei anumite persoane,
- nu poate fi folosit în comun cu nici o altă persoană,
- trebuie restricţionat conform funcţiei (ce reiese din rolul îndeplinit de persoana respectivă) pe baza software-ului de sistem al certSIGN, a sistemului de operare şi a controalelor de aplicaţii.

Operaţiile efectuate în certSIGN care necesită acces la resurse de reţea comune sunt protejate prin mecanisme de autentificare sigură şi de criptare a informaţiilor transmise.

4.3 Controlul personalului

certSIGN trebuie să se asigure că persoana care îndeplineşte responsabilităţile funcţiei, conform cu rolul atribuit:

- dispune de calificarile, certificarile si/sau acreditarile necesare,
- este cetăţean român,
- a semnat un contract care descrie rolul şi responsabilităţile sale în cadrul sistemului,
- a beneficiat de un stagiu de pregătire avansată în conformitate cu obligaţiile şi sarcinile asociate funcţiei sale,
- a fost instruit cu privire la protecţia datelor personale şi informaţiilor confidenţiale sau private,
- a semnat un contract ce conţine clauze referitoare la protejarea informaţiilor senzitive (din punctul de vedere al securităţii certSIGN) şi a datelor confidenţiale şi private ale Abonaţilor,
- nu îndeplineşte sarcini care pot genera conflicte de interese.

4.3.1 Experienţa personală, calificările şi clauzele de confidenţialitate necesare

Personalul angajat al certSIGN care îndeplineşte un rol de încredere, trebuie să obţină avizul responsabilului de securitate si al administratorului arhivei. Avizul nu este necesar în cazul persoanelor care nu exercită un rol de încredere.

Întreg personalul angajat care îndeplineşte funcţii ce necesită acces la informaţii clasificate este autorizat în acest sens de către ORNISS (Oficiul Registrului Naţional al Informaţiilor Secrete de Stat).

Îndeplinirea unei funcţii de încredere ca administrator de securitate sau administrator al arhivei permite accesul la informaţiile confidentiale. Dezvăluirea neautorizată a acestor informaţii poate

cauza pierderea sau compromiterea intereselor, apărate de lege, ale unei persoane fizice sau ale unei organizaţii.

4.3.2 Cerinţele de pregătire a personalului

Personalul care îndeplineşte roluri şi sarcini ca urmare a angajării la certSIGN, trebuie să fie instruit cu privire la:

- Politica de securitate,
- Politicile si procedurile operationale,
- aplicaţiile software ale sistemului digital de arhivare si ale centrului de date,
- responsabilităţile ce decurg din rolurile şi sarcinile executate în sistem,
- procedurile ce trebuie executate ca urmare a apariţiei unei defecţiuni în funcţionarea sistemului informatic.

După încheierea pregătirii, participanţii semnează un document prin care confirmă luarea la cunostinta a politicilor si procedurilor şi acceptarea restricţiiore şi obligaţiilor impuse.

4.3.3 Frecvenţa stagiilor de pregătire

Pregătirea descrisă mai sus trebuie repetată de fiecare dată când apar modificări semnificative în politici , proceduri sau in sistemul informatic.

4.3.4 Sancţionarea acţiunilor neautorizate

În cazul descoperirii sau existenţei suspiciunii unui acces neautorizat, administratorul arhivei împreună cu administratorul de securitate (în cazul angajaţilor certSIGN) poate suspenda accesul persoanei respective la sistemul certSIGN. Măsurile disciplinare pentru astfel de incidente trebuie descrise în regulamente corespunzătoare şi trebuie să fie conforme cu prevederile legale.

4.3.5 Personalul angajat pe baza de contract

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicaţii etc.) face obiectul unor verificări similare ca şi în cazul angajaţilor certSIGN . În plus, personalul angajat pe bază de contract, pe timpul cât îşi desfăşoară activitatea în locaţia certSIGN, trebuie permanent însoţit de către un angajat al certSIGN , cu excepţia celor care au primit avizare din

partea administratorului de securitate şi care poate accesa informaţii clasificate intern sau în conformitate cu normele legale în vigoare.

4.3.6 Documentaţia oferită personalului

certSIGN trebuie să ofere personalului său accesul la următoarele documente:

- Politica de securitate,
- Politicile si procedurile operationale,
- Responsabilităţile şi obligaţiile asociate rolului deţinut în sistem.

5 Controale tehnice

5.1 Politici referitoare la tehnologie

Managementul tehnologiei

Centrul de date si sistemul informatic al arhivei digitale utilizeaza numai sisteme de operare si aplicatii software de sistem bine cunoscute, cu o acceptare larga si cu suport bine pus la punct.

Replicarea infrastructurii

Toate sistemele informatice folosite trebuie sa dispuna de o functie de backup suficienta pentru toate serviciile oferite de arhiva si de centrul de date si pentru datele procesate.

Managementul Hardwareului

Centrul de date si arhiva trebuie sa dispuna de tehnologii hardware corespunzatoare serviciilor pe care le ofera comunitatilor de utilizatori si de proceduri prin care sa se monitorizeze si notifice necesitatea schimbarii acestora.

Managementul Softwareului

Centrul de date si arhiva trebuie sa dispuna de tehnologii software corespunzatoare serviciilor pe care le ofera comunitatilor de utilizatori si de proceduri prin care sa se monitorizeze si notifice necesitatea schimbarii acestora.

Recuperarea in caz de dezastru

Arhiva si centrul de date dispun de planuri scrise pentru asigurarea continuitatii serviciilor si pentru recuperare in caz de dezastru. Aceste planuri sunt testate periodic.

Securitate

Securitatea fizica si informatica a arhivei si a centrului de date este asigurata. Exista procese prin care se evalueaza riscurile si se stabilesc masurile de securitate necesare.

Monitorizare si raportare

Exista definitii ale unor metrici de sistem (de ex pentru utilizarea spatiului de stocare, utilizarea retelei) care trebuie urmarite. Sunt puse la punct mecanisme de monitorizare si feedback pentru a asigura continuitatea operatiilor, rezolvarea problemelor si raspunsul la noile cerinte ale utilizatorilor si abonatilor.

Roluri si Autorizari

Toate functiile si de rolurile de incredere necesita o descriere a obligatiilor si responsabilitatilor ca si autorizari prealabile.

Autentificare

Exista procese pentru autentificarea utilizatorilor interni si externi, suficiente pentru a se putea aplica politicile de control al accesului.

Replicare

Pentru fiecare obiect digital din arhiva trebuie stipulate numarul si locatiile copiilor (daca este cazul). Arhiva dispune de mecansime prin care asigura ca toate copiile obiectelor digitale sunt sincronizate.

Managementul schimbarilor

Arhiva si centrul de date dispun de un proces documentat de management al schimbarilor care identifica si urmareste schimbarile la procesele critice. (In acest fel se asigura faptul ca, in orice moment, se cunosc schimbariel facute si momentul lor).

Migrarea mediilor de stocare

Arhiva dispune de un proces controlat pentru migrarea mediilor de stocare. Procesul incorporeaza o verificare a faptului ca copierea datelor s-a desfasurat cotect.

5.2 Controalele de securitate a calculatoarelor

5.2.1 Cerinţele tehnice specifice securităţii calculatoarelor

Cerinţele tehnice prezentate în acest capitol se referă la controalele de securitate specifice calculatoarelor şi aplicaţiilor, folosite în cadrul certSIGN. Măsurile de securitate care protejează sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicaţiilor precum şi din punct de vedere fizic.

Calculatoarele aparţinând arhivei si centrului de date, ca si şi componentelor asociate acestora dispun de următoarele mijloace de securitate:

- autentificarea obligatorie la nivelul sistemului de operare şi al aplicaţiilor,
- control discreţionar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securităţii,
- calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în certSIGN ,
- separarea sarcinilor, conform rolului în cadrul sistemului,
- identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,
- protecţia criptografică a schimburilor de informaţii şi protecţia bazelor de date,
- arhivarea istoricului operaţiunilor executate pe un calculator şi a datelor necesare auditării,
- o cale sigură ce permite identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicaţilor şi a sistemului de operare,

- mijloace de monitorizare şi alertare în cazul accesului neautorizat la resursele de calcul.

5.2.2 Semnatura digitala administrator de arhiva

Administratorul arhivei semneaza digital documentele arhivate folosind un certificat digital calificat emis pe un token criptografic securizat.

5.2.3 Evaluarea securităţii calculatoarelor

Managementul securitatii in cadrul certSIGN respectă cerinţele descrise în standardul ISO 27001.

5.3 Controale tehnice specifice ciclului de viata

5.3.1 Controale specifice dezvoltării sistemului

Fiecare aplicaţie, înainte de a fi folosita în producţie de certSIGN, este instalata astfel încât să se permită controlul versiunii curente şi să se prevină instalarea neautorizată de programe sau falsificarea celor existente.

Reguli similare se aplică în cazul înlocuirii componentelor hardware, cum ar fi:

- dispozitivele fizice sunt furnizate în aşa fel încât să poată fi urmărita şi evaluată ruta fiecăruia, până la locul său de instalare,
- livrarea unui dispozitiv fizic pentru înlocuire se realizează într-un mod similar celui de livrare al dispozitivului original; înlocuirea se realizează de către personal calificat şi de încredere.

5.3.2 Controale pentru managementul securităţii

Scopul controalelor pentru managementului securităţii este acela de a superviza funcţionalitatea sistemelor certSIGN, garantând astfel că acestea operează corect şi în concordanţă cu configurarea acceptată şi implementată.

Configuraţia curentă a sistemelor certSIGN, precum şi orice modificare şi actualizare a acestora, este înregistrată şi controlată.

Controalele aplicate sistemelor certSIGN permit verificarea continuă a integrităţii aplicaţiilor, versiunii şi autentificarea şi verificarea originii dispozitivelor hardware.

5.4 Controale de securitatea a reţelei

Serverele şi staţiile de lucru de încredere aparţinând certSIGN sunt conectate prin intermediul unei reţele locale (LAN), divizate în mai multe subretele, cu acces controlat. Accesul dinspre Internet către orice segment, este protejat prin intermediul unui firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului şi a filtrelor de trafic aplicate la nivelul ruterelor şi serviciilor Proxy.

Mijloacele de asigurare a securităţii reţelei acceptă doar mesajele transmise prin protocoalele http, https, NTP, POP3 şi SMTP. Evenimentele (log-urile) sunt înregistrate în jurnalele de sistem şi permit supravegherea folosirii corecte a serviciilor furnizate de certSIGN.

6 Managementul politicilor si procedurilor operationale

Fiecare versiune a prezentului document este în vigoare (starea sa este **valida**) până în momentul publicării şi aprobării noii sale versiuni. O nouă versiune este dezvoltată de către certSIGN şi publicata pentru comentarii cu menţiunea **spre aprobare** (daca este cazul). După primirea şi includerea comentariilor, documentul intra în procedura de aprobare interna. Responsabil de aprobarea formei finale este Comitetul pentru managementul politicilor si procedurilor serviciilor de incredereResponsabil pentru intretinerea documentului este directorul departamentului care asigura furnizarea serviciilor de arhivare. După terminarea procedurii de aprobare, noua versiune este transmisa autoritatii abilitate a statului si apoi, in termen de 10 zile, este publicata şi marcată ca fiind în starea **validă**.