

Politici generale

CertDigital

EMISĂ DE:			
DEPARTAMENT	**NUME**	**SEMNĂTURA**	**DATA**
CERTDIGITAL	OFIȚER DE SECURITATE IT		_____

APROBATĂ DE:			
DEPARTAMENT	**NUME**	**SEMNĂTURA**	**DATA**
CONDUCERE	DIRECTOR GENERAL		_____

ISTORICUL MODIFICĂRILOR:

VERSIUNE	AUTOR	DETALII MODIFICĂRI	DATA:
1.0	COMP. CERTDIGITAL	Publicare versiune initiala.	17.03.2011
1.1	CERTDIGITAL	Actualizare document, prevederi legislative.	01.01.2017
1.2	CERTDIGITAL	Actualizare document, conform Legii 214/2024.	06.10.2025
1.3	CERTDIGITAL	Actualizare document pentru serviciul CERTDIGITAL QPS (Qualified preservation service)	01.11.2025
2.0	OFIȚER DE SECURITATE IT	Rescriere pe structura ETSI EN 319 401 V3.1.1 pentru cele 14 servicii: guvernanță, gestionarea riscurilor (2025/2530, NIS2), securitatea informației, resurse umane, controale criptografice, operațiuni, incidente (ADR/DNSC/ANSPDCP), păstrare 10 ani, continuitate (RTO/RPO), încetare, conformitate; partea de certificare mutată în Politica de certificare și DPC; temeiul informării clienților și al publicării tarifelor: art. 11 alin. (1) și, pentru certificate, alin. (3) din Legea nr. 214/2024	27.10.2026
2.1	OFIȚER DE SECURITATE IT	Statutul serviciilor descris exact (secțiunea 1.2): serviciile de la lit. a)–e) sunt calificate și înscrise în Lista de încredere, iar pentru cele de la lit. f)–n) se solicită statutul calificat și nu se prestează ca servicii calificate	27.10.2026

		până la înscriere (art. 21 alin. (3) din Regulamentul eIDAS); trimiterile la documentele asociate, la versiunile în vigoare	
2.2	OFIȚER DE SECURITATE IT	Trimiterile la celelalte documente CertDigital nu mai au număr de versiune: se aplică versiunea în vigoare, publicată la adresa fixă din depozit, iar versiunile anterioare sunt în arhivă; precizarea despre versiunea în vigoare, după tabelul din secțiunea 1.3	27.10.2026
2.3	OFIȚER DE SECURITATE IT	Pagina de emitere și antetul, cu diacritice; conținutul neschimbat	28.10.2026
2.4	OFIȚER DE SECURITATE IT	Trimiterea la Politica de securitate fizică și de mediu (cap. 8) și la documentul privind structura organizatorică și imparțialitatea (2.2); denumirea procedurii de generare a cheilor (7.3)	02.11.2026
2.5	OFIȚER DE SECURITATE IT	Securitatea fizică (cap. 8): accesul se descrie ca autentificare în mai mulți factori, fără enumerarea factorilor și a ordinii lor, care rămân în Politica de securitate fizică și de mediu (document intern); conținutul neschimbat în rest	03.11.2026
2.6	OFIȚER DE SECURITATE IT	Documentele asociate (1.3): regulamentele interne de identificare, cu versiunea în vigoare (RIS 1.4, RVA 9, PIV 1.1 și DIV 1.2), ca excepție de la trimiterile fără versiune; instruirea operatorilor, inclusiv a celor ai partenerilor mandatați de	10.11.2026

		CERTDIGITAL (5.2); destinatarii datelor de identificare (14.2); locul contractării și al identificării, inclusiv la partenerii mandatați (15.1)	
2.7	OFIȚER DE SECURITATE IT	Copiile de siguranță (9.3): copia offline păstrată separat de ambele centre de date, verificarea integrității copiilor și testul de restaurare cu proces-verbal; pentru arhivarea electronică calificată, copiile criptate, păstrate cel mult 90 de zile, și testul de restaurare la 6 luni	12.11.2026
2.8	OFIȚER DE SECURITATE IT	Dosarul ADR din 04.12.2026 (10 servicii): s-au scos serviciile Ledgers/Q, EDS/Q, EDS/REM/Q și EAA/Q, care se notifică separat (1.2, 1.3, 2.2, 8, 12, 14.1)	18.11.2026

Cuprins

1. Scop și domeniu de aplicare 8
1.1. Scop 8
1.2. Serviciile acoperite 8
1.3. Relația cu celelalte documente 8
2. Organizare și guvernanță 11
2.1. Responsabilitatea conducerii 11
2.2. Independența și imparțialitatea 11
2.3. Resurse financiare și asigurare 11
2.4. Publicarea informațiilor 11
2.5. Modificarea serviciilor și a documentelor 12
3. Gestionarea riscurilor 13
3.1. Cadrul de gestionare a riscurilor 13
3.2. Evaluarea riscurilor 13
3.3. Măsuri de securitate cibernetică 13
4. Politica de securitate a informației 14
4.1. Principii 14
4.2. Clasificarea informațiilor 14
4.3. Utilizarea acceptabilă 14
4.4. Achiziția și dezvoltarea sistemelor 14
5. Resurse umane 15
5.1. Angajare și verificări 15
5.2. Instruire și conștientizare 15
5.3. Confidențialitate și sancțiuni 15
5.4. Încetarea sau schimbarea raporturilor de muncă 15
6. Gestionarea activelor și controlul accesului 16
6.1. Inventarul activelor 16
6.2. Gestionarea conturilor 16
6.3. Autentificarea 16
7. Controale criptografice 17
7.1. Module criptografice 17

7.2. Algoritmi 17
7.3. Ceremonia cheilor 17
8. Securitatea fizică și a mediului 18
9. Securitatea operațiunilor și a rețelei 19
9.1. Gestionarea schimbărilor 19
9.2. Gestionarea vulnerabilităților 19
9.3. Copii de siguranță 19
9.4. Jurnalizare și sincronizarea timpului 19
9.5. Securitatea rețelei 19
10. Gestionarea incidentelor 20
11. Păstrarea înregistrărilor 21
12. Continuitatea activității 22
13. Încetarea activității 23
14. Conformitate 24
14.1. Cadrul legal 24
14.2. Protecția datelor cu caracter personal 24
14.3. Evaluarea conformității și auditul 24
14.4. Accesibilitate 24
15. Relația cu clienții 26
15.1. Accesul la servicii 26
15.2. Reclamații și litigii 26
15.3. Date de contact 26

1. Scop și domeniu de aplicare

1.1. Scop

Prezentul document stabilește politicile generale aplicate de CENTRUL DE CALCUL S.A. (marca CertDigital, denumită în continuare „CERTDIGITAL”), în calitate de prestator de servicii de încredere calificat, pentru toate serviciile sale de încredere. Politicile răspund cerințelor generale din ETSI EN 319 401 V3.1.1, art. 24 din Regulamentul (UE) nr. 910/2014 și Regulamentului de punere în aplicare (UE) 2025/2530.

1.2. Serviciile acoperite

Nr.	Serviciul de încredere calificat	Tip (ETSI TS 119 612)
a)	Certificat calificat pentru semnătură electronică	CA/QC
b)	Certificat calificat pentru sigiliu electronic	CA/QC
c)	Marcă temporală electronică calificată	TSA/QTST
d)	Validarea calificată a semnăturilor electronice calificate	QESValidation/Q
e)	Validarea calificată a sigiliilor electronice calificate	QESValidation/Q
f)	Păstrarea calificată a semnăturilor electronice calificate	PSES/Q
g)	Păstrarea calificată a sigiliilor electronice calificate	PSES/Q
h)	Gestionarea calificată la distanță a dispozitivului calificat de creare a semnăturii electronice	RemoteQSigCDManagement/Q
i)	Gestionarea calificată la distanță a dispozitivului calificat de creare a sigiliului electronic	RemoteQSealCDManagement/Q
j)	Arhivare electronică calificată	ElectronicArchiving/Q

Serviciile de la lit. a)–e) sunt servicii de încredere calificate, înscrise în Lista de încredere a României (https://trustedlist.adr.gov.ro/). Pentru serviciile de la lit. f)–j) se solicită acordarea statutului calificat și înscrierea în Lista de încredere (art. 21 din Regulamentul eIDAS); până la înscriere, aceste servicii nu se prestează ca servicii de încredere calificate (art. 21 alin. (3)). Documentația specifică fiecărui serviciu este publicată la https://www.certdigital.ro/repository/, la adrese fixe, care nu se schimbă la o versiune nouă (de exemplu, prezentul document: https://www.certdigital.ro/repository/politici/certdigital_pg_ro.pdf); versiunile anterioare rămân disponibile la https://www.certdigital.ro/repository/arhiva/.

1.3. Relația cu celelalte documente

Document	Conținut	Identificator (OID)
Politica serviciilor de certificare; DPC CERTDIGITAL G4, pentru ROOT CA G4 și QUALIFIED CA G4; DPC CERTDIGITAL G5, pentru ROOT CA G5 și QCA G5	cerințele și practicile pentru certificatele calificate (lit. a)–b))	politicile de certificat 1.3.6.1.4.1.47898.4.* (G4) și 1.3.6.1.4.1.47898.5.* (G5), cu QCP-n-qscd / QCP-l-qscd

Document	Conținut	Identificator (OID)
Politica și declarația de practici a serviciului calificat de marcare temporală (PDP-QTST)	marcarea temporală (lit. c))	BTSP 0.4.0.2023.1.1
Politica și declarația de practici a serviciului calificat de validare (PDP-QESVal)	validarea (lit. d)–e))	1.3.6.1.4.1.47898.9.1
Politica și declarația de practici a serviciului de păstrare (PSPPS)	păstrarea (lit. f)–g))	1.3.6.1.4.1.47898.10.1
Politica și declarația de practici a serviciului de gestionare la distanță a QSCD (PDP-rQSCD)	gestionarea la distanță (lit. h)–i))	1.3.6.1.4.1.47898.11.1
Politica și declarația de practici a serviciului calificat de arhivare electronică (PDP-QEArch)	arhivarea electronică (lit. j))	1.3.6.1.4.1.47898.12.1
Termenii și condițiile fiecărui serviciu (TC-CERT, TC-TSA, TC-QESVal, TC-QPS, TC-rQSCD, TC-QEArch)	condițiile de utilizare și declarația de informare a fiecărui serviciu (TC-CERT cuprinde și informațiile din ETSI EN 319 411-1, anexa A)	trimit la identificatorii de mai sus
Declarația de informare a PKI (PDS), în limba română și în limba engleză	rezumatul condițiilor pentru certificatele calificate, la care trimite declarația QcPDS din certificate	—
CERTDIGITAL_OID_MAP	identificatorii de obiect ai prestatorului	arcul 1.3.6.1.4.1.47898
Politica de protecție a datelor (00d)	protecția datelor cu caracter personal	—
Procedura de notificare a incidentelor (00q)	notificarea incidentelor	—
Procedura de continuitate operațională și de recuperare în caz de dezastru (PO_SI_63) și Planul de continuitate a afacerii (PO_C_SI_S_63)	continuitatea activității	—
Planul de încetare a serviciilor (00r) și versiunea lui publică (PIS)	încetarea activității	—
Politica privind relațiile cu clienții și soluționarea reclamațiilor (PRC)	asistența clienților și reclamațiile	—
Declarația privind accesibilitatea serviciilor (DAS)	accesibilitatea serviciilor	—
Gestionarea riscurilor serviciilor de încredere (GR-TSP)	evaluarea și tratarea riscurilor	—
Lista standardelor aplicabile (00n)	standardele aplicate	—
Regulamentul privind identificarea și cererea certificatelor digitale calificate (RIS), versiunea 1.4 din 03.11.2026; Regulamentul de validare și aprobare a cererii de certificat (RVA), versiunea 9 din 03.11.2026; Procedura de lucru privind identificarea video la distanță – Operatori (PIV), referința 18/2026, versiunea 1.1 din 14.07.2026; Descrierea procesului de identificare video la distanță (DIV), referința 11/2026, versiunea 1.2 din 14.07.2026 (documente interne)	identificarea titularului, cererea și validarea ei și identificarea video la distanță, pentru certificatele calificate (lit. a)–b)) și pentru gestionarea la distanță (lit. h)–i)); materialele de instruire ale operatorilor și ale partenerilor mandatați	—

Documentele de mai sus se aplică în versiunea în vigoare. Regulamentele interne de identificare și de validare (RIS, RVA, PIV și DIV) se citează cu versiunea: trimiterile la ele indică versiunea în vigoare la data aprobării prezentului document. O versiune nouă a unui regulament se aplică după instruirea operatorilor și a partenerilor mandatați și se preia în prezentul document la versiunea lui următoare. Documentele publice sunt în depozitul https://www.certdigital.ro/repository/, iar versiunile lor anterioare, în arhiva depozitului.

Prezentul document prevalează asupra procedurilor interne. Documentele specifice serviciilor detaliază cerințele de mai jos și nu le pot reduce.

2. Organizare și guvernanță

2.1. Responsabilitatea conducerii

Directorul General aprobă prezenta politică, politicile și declarațiile de practici ale serviciilor, alocă resursele necesare și răspunde de conformitatea serviciilor. Ofițerul de securitate IT coordonează implementarea politicii de securitate a informației și verifică documentele serviciilor înainte de aprobare.

2.2. Independența și imparțialitatea

Deciziile privind emiterea, revocarea și furnizarea serviciilor se iau nediscriminatoriu, pe baza criteriilor publicate. Personalul cu roluri de încredere nu are interese care să îi afecteze imparțialitatea. Structura organizatorică a serviciilor de încredere, separarea funcțiilor care decid emiterea și revocarea de compartimentele comerciale și financiare și declarațiile anuale de imparțialitate și de lipsă a conflictelor de interese ale conducerii și ale personalului cu roluri de încredere sunt stabilite în documentul intern „Structura organizatorică a serviciilor de încredere și asigurarea imparțialității” (SOI), aprobat de Directorul General și pus la dispoziția organismului de evaluare a conformității și a organismului de supraveghere (ETSI EN 319 401, cl. 7.1 și 7.2).

2.3. Resurse financiare și asigurare

CERTDIGITAL dispune de resursele financiare necesare funcționării serviciilor și aplicării Planului de încetare. CERTDIGITAL răspunde, conform art. 13 din Regulamentul eIDAS și, pentru certificatele calificate, conform art. 30 din Legea nr. 214/2024, pentru prejudiciile cauzate cu intenție sau din neglijență prin nerespectarea obligațiilor care îi revin; limitele de utilizare ale fiecărui serviciu sunt cele din documentele lui. CENTRUL DE CALCUL S.A. deține, pentru fiecare serviciu de încredere calificat, câte o poliță distinctă de asigurare de răspundere civilă profesională, cu limita răspunderii de 500.000 EUR pe perioada asigurată, în condițiile art. 24 alin. (2) lit. c) din Regulamentul eIDAS, ale art. 5 alin. (2) lit. b) din procedura aprobată prin Ordinul MEDAT nr. 102/2026 și, pentru certificatele calificate, ale art. 12 alin. (6) din Legea nr. 214/2024; în fiecare poliță, ADR, în calitate de organism de supraveghere, are calitatea de asigurat adițional. Polițele se reînnoiesc înainte de expirare; datele lor de identificare (asigurătorul, seria și numărul, perioada de valabilitate) sunt comunicate ADR și se pun la dispoziție la cerere.

2.4. Publicarea informațiilor

Pentru fiecare serviciu, CERTDIGITAL publică la https://www.certdigital.ro/repository/ politica și declarația de practici, termenii și condițiile (cu declarația de informare a serviciului), tarifele și informațiile privind statutul calificat. Înainte de încheierea contractului, clientul este informat clar și complet asupra condițiilor de utilizare a serviciului,

inclusiv asupra limitărilor acestuia (art. 24 alin. (2) lit. (d) din Regulamentul eIDAS; art. 11 alin. (1) și, pentru certificate, alin. (3) din Legea nr. 214/2024).

2.5. Modificarea serviciilor și a documentelor

Orice modificare a prezentului document primește o versiune nouă, aprobată de Directorul General și publicată în depozitul de documente; versiunile anterioare rămân disponibile. Modificările care afectează prestarea serviciilor calificate se comunică ADR cu cel puțin o lună înainte de aplicare (cu cel puțin trei luni în cazul încetării unui serviciu). Categoriile de modificări care se notifică ADR (art. 1 din Regulamentul de punere în aplicare (UE) 2025/2530, lit. a)–j)), conținutul notificării și termenele sunt stabilite în Procedura de notificare (00q, cap. 12). Titularii și părțile care se bazează sunt informați prin publicare pe site cu cel puțin 30 de zile înainte de intrarea în vigoare, timp în care titularii pot formula obiecții sau pot solicita revocarea certificatului, fără costuri. Corecturile de redactare care nu modifică drepturile sau obligațiile părților se publică cu versiune nouă, fără termen de preaviz.

3. Gestionarea riscurilor

3.1. Cadrul de gestionare a riscurilor

CERTDIGITAL aplică un cadru de gestionare a riscurilor juridice, comerciale, operaționale și de securitate cibernetică, conform art. 24 alin. (2) lit. (fa) din Regulamentul eIDAS, art. 2 din Regulamentul de punere în aplicare (UE) 2025/2530 și art. 21 din Directiva (UE) 2022/2555. Cadrul acoperă înregistrarea și integrarea clienților, controalele procedurale și administrative și gestionarea serviciilor, pentru fiecare serviciu.

3.2. Evaluarea riscurilor

Riscurile se identifică, se evaluează și se tratează conform documentului „Gestionarea riscurilor serviciilor de încredere” (GR-TSP), Procedurii de evaluare și tratare a riscului de securitate a informației (PO_C_SI_S_59) și Planului de tratare a riscurilor IT; evaluarea în vigoare a fost aprobată de Directorul General la 26.10.2026. Evaluarea se reia cel puțin anual, înaintea introducerii unui serviciu nou sau a unei modificări semnificative și după fiecare incident semnificativ. Riscurile reziduale sunt acceptate de Directorul General.

3.3. Măsuri de securitate cibernetică

CENTRUL DE CALCUL S.A. este entitate esențială în sensul OUG nr. 155/2024 (Registrul Entităților nr. E-210D02, sectorul Infrastructură digitală) și aplică măsurile de gestionare a riscurilor de securitate cibernetică prevăzute de Regulamentul de punere în aplicare (UE) 2024/2690.

4. Politica de securitate a informației

4.1. Principii

CERTDIGITAL protejează confidențialitatea, integritatea și disponibilitatea informațiilor și a sistemelor care susțin serviciile de încredere. Fiecare angajat răspunde de protejarea informațiilor la care are acces. Politica se aplică și furnizorilor și colaboratorilor externi care au acces la informațiile sau la resursele CERTDIGITAL.

4.2. Clasificarea informațiilor

Clasă	Descriere	Exemple
Publică	aprobată pentru publicare; dezvăluirea nu produce prejudicii	politici, DPC, PDS, termeni și condiții, certificatele autorităților, CRL
Internă	utilizare numai în cadrul CERTDIGITAL	proceduri operaționale, organigrame, date de contact interne
Restricți onată	cel mai ridicat nivel de confidențialitate; acces numai pe baza necesității	chei și date de activare, configurații de securitate, documente de identificare ale clienților, înregistrări video, jurnale, rapoarte de incident

Fiecare document poartă clasificarea pe pagina de gardă. Accesul se acordă pe principiul „necesității de a cunoaște”.

4.3. Utilizarea acceptabilă

– informațiile și sistemele CERTDIGITAL se utilizează numai în scopuri de serviciu aprobate;

– este interzisă instalarea de programe neautorizate și folosirea programelor licențiate CERTDIGITAL pe echipamente personale;

– activitățile utilizatorilor sunt jurnalizate; încălcarea politicii poate duce la retragerea drepturilor de acces și la sancțiuni disciplinare;

– echipamentele mobile care accesează date restricționate sunt criptate și administrate centralizat;

– protecția împotriva programelor malițioase este activă pe toate sistemele, cu actualizare automată.

4.4. Achiziția și dezvoltarea sistemelor

Produsele și serviciile achiziționate pentru serviciile de încredere se evaluează din punctul de vedere al securității înainte de utilizare; pentru modulele criptografice se folosesc numai produse certificate (secțiunea 7). Dezvoltarea internă separă mediile de dezvoltare, test și producție.

5. Resurse umane

5.1. Angajare și verificări

Personalul cu roluri de încredere are calificarea și experiența necesare. Înainte de atribuirea rolului se verifică CV-ul, diplomele, referințele și cazierul judiciar, în condițiile legii (ETSI EN 319 401, cl. 7.2; Codul muncii; GDPR).

5.2. Instruire și conștientizare

Fiecare angajat participă la instruire privind securitatea informației la angajare și apoi cel puțin anual. Personalul primește politicile și procedurile aplicabile și confirmă în scris respectarea lor. Regulamentele RIS, RVA și PIV, în versiunile indicate în secțiunea 1.3, sunt materialele de instruire ale operatorilor de verificare a identității, de validare și de aprobare și emitere și ale partenerilor mandatați pentru identificarea prin prezență fizică (art. 16 alin. (3) lit. a) din Legea nr. 214/2024; ETSI EN 319 401, REQ-7.2-02). La o versiune nouă a unui regulament, operatorii și partenerii sunt instruiți înainte de aplicarea ei, iar instruirea se consemnează.

5.3. Confidențialitate și sancțiuni

Personalul și colaboratorii semnează angajamente de confidențialitate și sunt obligați la păstrarea secretului profesional (art. 11 alin. (5) din Legea nr. 214/2024). Încălcările se sancționează conform Codului muncii și regulamentului intern.

5.4. Încetarea sau schimbarea raporturilor de muncă

Drepturile de acces se revocă la încetarea contractului de muncă, pe baza fișei de lichidare, și se ajustează la schimbarea postului. Mijloacele de acces (carduri, tokenuri) se recuperează.

6. Gestionarea activelor și controlul accesului

6.1. Inventarul activelor

CERTDIGITAL ține inventarul activelor informaționale și al echipamentelor care susțin serviciile, cu proprietarul și clasificarea fiecăruia. Suporturile cu date restricționate se șterg securizat sau se distrug înainte de eliminare.

6.2. Gestionarea conturilor

Conturile se creează, se modifică și se dezactivează numai pe baza unei cereri aprobate de superiorul direct. Conturile sunt nominale și nepartajate. Drepturile sunt cele minime necesare rolului și se revizuiesc cel puțin anual.

6.3. Autentificarea

Accesul administrativ și accesul la sistemele serviciilor de încredere se face cu autentificare cu cel puțin doi factori. Parolele respectă regulile de complexitate și de schimbare stabilite în procedura internă și nu se divulgă.

7. Controale criptografice

7.1. Module criptografice

Cheile autorităților și ale serviciilor de încredere se generează, se păstrează și se utilizează numai în module criptografice hardware certificate Common Criteria EAL4+ conform EN 419 221-5 și ca dispozitive calificate conform Regulamentului eIDAS (Utimaco CryptoServer CP5 5.1.2.0 pentru generația G4; Thales Luna PCIe HSM 7 A790, firmware 7.8.5, pentru generația G5), sub control multipersoană.

7.2. Algoritmi

Algoritmii și lungimile de cheie respectă documentul „Agreed Cryptographic Mechanisms" al ECCG (ENISA). Cheile noi ale autorităților se generează cu RSA de cel puțin 4096 de biți și exponent public 65537; începând cu 01.03.2027, cheile titularilor de pe token sunt chei ECDSA pe curba NIST P-256, în locul cheilor RSA 2048, care se folosesc numai în perioada de tranziție, până la 28.02.2027 (DPC CERTDIGITAL G4, secțiunea 6.1.5). Pentru cheile gestionate în QSCD la distanță (serviciul rQSCD) se admit RSA de cel puțin 3072 de biți sau ECDSA pe curbele NIST P-256 / P-384; aceste chei se utilizează numai sub controlul exclusiv al semnatarului, prin modulul de activare a semnăturii (SAM), conform PDP-rQSCD.

7.3. Ceremonia cheilor

Generarea, transferul, copierea de rezervă și distrugerea cheilor autorităților se fac conform Procedurii privind generarea cheilor (document intern), cu proces-verbal, martor și înregistrare video. ADR este informată cu cel puțin o lună înainte de punerea în funcțiune a unei autorități noi.

8. Securitatea fizică și a mediului

Infrastructura serviciilor de încredere este găzduită în două centre de date proprii din municipiul Târgu Jiu, aflate în clădiri separate: un centru principal și un centru secundar de rezervă, pregătit să preia serviciile (activ-pasiv), inclusiv cu modul criptografic (HSM). Riscurile comune celor două locații sunt evaluate în GR-TSP (riscul R-12), cu măsura M-12. Centrul principal este proiectat după recomandările TIA-942 pentru nivelul Tier 3. Accesul fizic este controlat pe zone de securitate, cu autentificare în mai mulți factori. Măsurile sunt stabilite în Politica de securitate fizică și de mediu (PSFM), document intern aprobat de Directorul General, aplicabilă tuturor sistemelor serviciilor de încredere, și se pun la dispoziția organismului de evaluare a conformității și a organismului de supraveghere. Politica tratează controlul accesului fizic, protecția împotriva dezastrelor naturale, a incendiilor, a căderii utilităților (energie, telecomunicații), a prăbușirii structurii, a scurgerilor de apă, a furtului și a efracției, precum și recuperarea în caz de dezastru (ETSI EN 319 401, cl. 7.6).

9. Securitatea operațiunilor și a rețelei

9.1. Gestionarea schimbărilor

Modificările de configurație și de programe în producție se aprobă, se testează și se jurnalizează. Modificările semnificative ale serviciilor calificate se comunică ADR conform secțiunii 2.5.

9.2. Gestionarea vulnerabilităților

Vulnerabilitățile se identifică prin monitorizarea buletinelor producătorilor, prin scanări de vulnerabilitate trimestriale, cu raport, și prin teste de penetrare efectuate de un terț independent pe toate punctele de acces, la punerea în funcțiune, după modificările semnificative ale infrastructurii sau ale aplicațiilor și cel puțin o dată pe an (ETSI EN 319 401, REQ-7.8-13 – REQ-7.8-19X; măsura M-08 din GR-TSP). Vulnerabilitățile critice se tratează în cel mult 48 de ore de la descoperire (REQ-7.9.2-09X). Pentru fiecare vulnerabilitate se aplică un plan de remediere sau se documentează motivul pentru care remedierea nu este necesară (REQ-7.9.2-10X). Corecțiile vulnerabilităților critice se aplică în cel mult 7 zile, iar remedierea se verifică.

9.3. Copii de siguranță

Copiile de siguranță se realizează zilnic, se păstrează în centrul de date secundar și, suplimentar, offline, separat de ambele centre de date; integritatea copiilor se verifică după creare, iar restaurarea se testează cel puțin anual, cu proces-verbal (ETSI EN 319 401, cl. 7.11.2). Pentru arhivarea electronică calificată, copiile, inclusiv cea offline, sunt criptate și se păstrează cel mult 90 de zile, iar restaurarea se testează cel puțin o dată la 6 luni (PDP-QEArch, secțiunea 14.3). Datele serviciilor critice se replică în centrul de date secundar la cel mult 5 minute.

9.4. Jurnalizare și sincronizarea timpului

Evenimentele relevante pentru securitate și pentru serviciile de încredere se jurnalizează centralizat, cu protecție împotriva modificării. Toate sistemele sunt sincronizate cu sursa de timp UTC a CERTDIGITAL (documentul „Sursa de timp”, 00u).

9.5. Securitatea rețelei

Rețeaua este segmentată pe zone de securitate. Între zone sunt permise numai fluxurile necesare serviciilor, prin firewall-uri cu filtrare și monitorizare; administrarea se face numai din rețeaua internă dedicată; comunicațiile externe ale serviciilor sunt criptate (TLS). Conexiunile la rețele externe se aprobă de ofițerul de securitate IT.

10. Gestionarea incidentelor

CERTDIGITAL aplică o procedură de gestionare și notificare a incidentelor de securitate (Procedura de notificare a incidentelor, 00q). Orice încălcare a securității sau pierdere a integrității cu impact semnificativ asupra serviciilor de încredere ori asupra datelor cu caracter personal se notifică, fără întârzieri nejustificate:

– **Autorității pentru Digitalizarea României**, în cel mult 24 de ore de la luarea la cunoștință (art. 24 alin. (2) lit. (fb) din Regulamentul eIDAS);

– **Directoratului Național de Securitate Cibernetică**: avertizare timpurie în cel mult 24 de ore, notificare în cel mult 72 de ore și raport final în cel mult o lună (OUG nr. 155/2024; CENTRUL DE CALCUL S.A. este înscrisă în Registrul Entităților ca entitate esențială, nr. E-210D02);

– **Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal**, în cel mult 72 de ore, dacă sunt afectate date cu caracter personal (art. 33 GDPR);

– **persoanelor afectate**, fără întârzieri nejustificate, dacă incidentul le poate afecta (art. 24 alin. (2) lit. (fb) din Regulamentul eIDAS; art. 34 GDPR);

– publicului sau altor autorități, la cererea ADR.

La compromiterea sau suspiciunea de compromitere a cheii private a unei autorități de certificare, CERTDIGITAL oprește emiterea, revocă certificatele afectate, informează ADR, titularii și părțile care se bazează, și aplică, după caz, Planul de încetare. Incidentele se înregistrează într-un registru păstrat 10 ani.

Angajații raportează imediat ofițerului de securitate IT orice eveniment suspect. Procedurile interne de management al incidentelor (PO_SI_S_52) și de administrare a incidentelor și problemelor IT (PO_SI_45) descriu tratarea tehnică.

11. Păstrarea înregistrărilor

CERTDIGITAL păstrează certificatele emise, documentele și datele utilizate la verificarea identității (inclusiv înregistrările video realizate prin CERTDIGITAL KYC), cererile, înregistrările de revocare și jurnalele de evenimente relevante pentru o perioadă de cel puțin 10 ani de la încetarea valabilității certificatului (expirare sau revocare). Jurnalele serviciilor de marcare temporală și de păstrare se păstrează cel puțin 10 ani de la data înregistrării. În caz de încetare a activității, înregistrările sunt păstrate și puse la dispoziție conform Planului de încetare. Duratele pentru celelalte servicii se stabilesc în documentația fiecăruia, cu respectarea art. 24 alin. (2) lit. (h) din Regulamentul eIDAS.

12. Continuitatea activității

Continuitatea serviciilor este asigurată conform Procedurii de continuitate operațională și de recuperare în caz de dezastru (PO_SI_63) și Planului de continuitate a afacerii (PO_C_SI_S_63). Centrul de date secundar se activează atunci când întreruperea estimată depășește durata maximă de restabilire (RTO) a serviciului afectat. Duratele principale:

Serviciu / componentă	**RTO**	**RPO**
OCSP, CRL, depozitul de certificate	4 ore	cel mult 5 minute
Primirea și procesarea cererilor de revocare	24 de ore	cel mult 5 minute
Marcarea temporală	8 ore	cel mult 5 minute (jurnale)
Păstrarea calificată	24 de ore	cel mult 5 minute
Validarea calificată	8 ore	cel mult 5 minute (rapoartele de validare)
Gestionarea la distanță a QSCD	8 ore	cel mult 5 minute
Arhivarea electronică calificată	24 de ore	cel mult 5 minute
Emiterea certificatelor	72 de ore	cel mult 5 minute (baza de date CA)
CERTDIGITAL KYC	24 de ore	cel mult 5 minute
Site-ul și portalul client	8 ore	6 ore

Comutarea în centrul de date secundar se testează cel puțin anual, cu proces-verbal. Disponibilitatea-țintă este de 99,5% pe an pentru OCSP, CRL, marcarea temporală și păstrare și de 99% pe an pentru depozit și site.

13. Încetarea activității

Încetarea unui serviciu de încredere se face conform Planului de încetare a serviciilor (00r), a cărui versiune publică (PIS) este publicată la https://www.certdigital.ro/repository/politici/certdigital_plan-incetare_ro.pdf, și anexei acestuia pentru serviciul respectiv. ADR este informată cu cel puțin 3 luni înainte (art. 24 alin. (2) lit. (a) din Regulamentul eIDAS), iar în cazul unei încetări neprevăzute, în cel mult 24 de ore. Titularii și părțile care se bazează sunt informați în termenele prevăzute în plan. Informațiile privind starea certificatelor rămân disponibile și după încetare (art. 24 alin. (4) din Regulamentul eIDAS), prin succesor sau custode, inclusiv ultima CRL emisă înaintea distrugerii cheii autorității de certificare. Pentru certificate, ultima CRL se emite numai după ce toate certificatele din domeniul ei au expirat sau au fost revocate și are nextUpdate „99991231235959Z”, iar înainte de expirarea certificatului unei autorități se calculează, pentru fiecare certificat emis de aceasta, un ultim răspuns OCSP cu aceeași valoare (DPC, secțiunea 5.8; ETSI EN 319 411-1, CSS-6.3.9-06; ETSI EN 319 411-2, CSS-6.3.10-07 – CSS-6.3.10-11). Înregistrările se păstrează 10 ani prin custode. Cheile private ale autorităților se distrug pe bază de proces-verbal.

Retragerea unei autorități de certificare dintr-o generație (de exemplu G3) nu reprezintă încetarea serviciului, dacă serviciul continuă printr-o altă generație. Aceasta se tratează ca modificare (secțiunea 2.5).

14. Conformitate

14.1. Cadrul legal

Serviciile sunt furnizate în conformitate cu: Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183; Regulamentul de punere în aplicare (UE) 2025/2530 și actele de punere în aplicare specifice fiecărui serviciu: (UE) 2025/1943 (certificate calificate), 2025/1929 (mărci temporale), 2025/1942 și 2025/1945 (validare), 2025/1946 (păstrare), 2025/1567 (gestionarea la distanță a QSCD), 2025/2532 (arhivare electronică); Directiva (UE) 2022/2555 și Regulamentul de punere în aplicare (UE) 2024/2690; Regulamentul (UE) 2016/679; Legea nr. 214/2024; Ordinul MEDAT nr. 102/2026 și deciziile ADR; OUG nr. 155/2024; Legea nr. 190/2018 și Legea nr. 506/2004; Codul civil, Legea nr. 193/2000, OUG nr. 34/2014 și OG nr. 38/2015. Standardele aplicate sunt cele din documentul 00n. Organismul de supraveghere este Autoritatea pentru Digitalizarea României.

14.2. Protecția datelor cu caracter personal

CERTDIGITAL prelucrează datele cu caracter personal conform Regulamentului (UE) 2016/679, Legii nr. 190/2018 și Politicii de protecție a datelor cu caracter personal (00d, versiunea în vigoare, publicată la https://www.certdigital.ro/protectia-datelor/). Partenerii mandatați pentru identificarea prin prezență fizică prelucrează datele de identificare ale titularilor în numele CERTDIGITAL, ca persoane împuternicite (art. 28 din Regulamentul (UE) 2016/679). Responsabilul cu protecția datelor poate fi contactat la dpo@centruldecalcul.ro. Comunicările comerciale prin e-mail se transmit numai cu consimțământul prealabil al destinatarului (art. 12 din Legea nr. 506/2004).

14.3. Evaluarea conformității și auditul

Serviciile de încredere calificate sunt evaluate de un organism de evaluare a conformității acreditat conform Regulamentului de punere în aplicare (UE) 2025/2162, cel puțin o dată la 24 de luni, inclusiv în privința cerințelor de la art. 21 din Directiva (UE) 2022/2555 (art. 20 alin. (1) din Regulamentul eIDAS). ADR este informată cu cel puțin o lună înainte de evaluarea planificată și poate participa ca observator; raportul se transmite ADR în cel mult 3 zile lucrătoare de la primire. CERTDIGITAL efectuează cel puțin anual un audit intern, realizat de personal independent de operarea serviciilor.

14.4. Accesibilitate

CERTDIGITAL urmărește ca site-ul și documentele publicate în format PDF să respecte cerințele WCAG 2.1, nivel AA (EN 301 549), conform art. 15 din Regulamentul eIDAS și Legii nr. 232/2022. Persoanele cu dizabilități pot solicita asistență prin telefon (+40 253 214

767), prin e-mail (office@certdigital.ro) sau la sediu. Declarația privind accesibilitatea serviciilor (DAS) este publicată în depozitul de documente.

15. Relația cu clienții

15.1. Accesul la servicii

Serviciile se contractează la sediul și la punctele de lucru ale CERTDIGITAL, la partenerii mandatați de CERTDIGITAL (partenerii sunt prezentați pe https://www.certdigital.ro/parteneri/, iar lista punctelor lor se comunică la cerere) sau online, prin portalul client, pe baza contractului și a termenilor și condițiilor fiecărui serviciu. Identificarea titularului prin prezență fizică se face de operatorii de verificare a identității CERTDIGITAL sau de operatorii partenerilor mandatați, care acționează în numele și sub răspunderea CERTDIGITAL, conform Regulamentului privind identificarea și cererea certificatelor digitale calificate (RIS), versiunea 1.4 din 03.11.2026; operatorii de validare CERTDIGITAL verifică cererea și documentele, înainte de aprobare, conform Regulamentului de validare și aprobare a cererii de certificat (RVA), versiunea 9 din 03.11.2026. Tarifele serviciilor sunt cele din lista de tarife publicată pe site-ul https://www.certdigital.ro/ sau cele din oferta transmisă la cerere (art. 11 alin. (1) și, pentru certificate, alin. (3) lit. b) din Legea nr. 214/2024).

15.2. Reclamații și litigii

Litigiile se soluționează pe cale amiabilă, pe baza unei reclamații transmise la office@certdigital.ro. Reclamațiile se tratează conform Politicii privind relațiile cu clienții și soluționarea reclamațiilor (PRC, https://www.certdigital.ro/repository/politici/certdigital_relatii-clienti_ro.pdf):
CERTDIGITAL confirmă primirea în cel mult trei zile lucrătoare și răspunde în scris în cel mult 30 de zile de la înregistrare. În lipsa unei soluții amiabile, litigiile cu profesioniștii sunt de competența instanțelor de la sediul CENTRUL DE CALCUL S.A. (Târgu Jiu). Consumatorii se pot adresa instanțelor competente potrivit legii, inclusiv celor de la domiciliul lor, și pot apela la procedurile de soluționare alternativă a litigiilor (SAL) prevăzute de OG nr. 38/2015 (ANPC – https://anpc.ro/sal).

15.3. Date de contact

CENTRUL DE CALCUL S.A. (marca CertDigital), Str. Tudor Vladimirescu nr. 17, Târgu Jiu, județul Gorj, cod poștal 210132, România; J1991000103187; EUID ROONRC.J1991000103187; CUI RO2163993; tel. +40 253 214 767; office@certdigital.ro; https://www.certdigital.ro/. Revocarea certificatelor: 24/7, prin portalul client, precum și prin e-mail semnat electronic calificat sau prin cerere scrisă depusă la sediu, în programul de lucru (DPC, secțiunea 4.9.3).