DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

GHID PENTRU ELABORAREA PLANULUI DE CONTINUITATE A AFACERII (BCP) DIN PERSPECTIVA SECURITĂȚII CIBERNETICE

IULIE 2026 - v.1.0

TLP:CLEAR

Cuprins

1. Sumar Executiv

În această secțiune se vor preciza contextul, scopul și importanța existenței și aplicării Planului de Continuitate a Afacerii din perspectiva securității cibernetice în organizație.

Ordonanța de urgență nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, aprobată prin Legea nr. 124/2025, impune entităților esențiale și importante să adopte măsuri tehnice, operaționale și organizatorice proporționale și adecvate pentru continuitatea activității, inclusiv gestionarea copiilor de rezervă, redresarea în caz de dezastru și managementul crizelor.

Documentul este parte a setului de recomandări propuse de Directoratul Național de Securitate Cibernetică (DNSC) cu scopul de a contribui la realizarea unui spațiu cibernetic sigur și vine în sprijinul organizațiilor care își desfășoară activitatea în spațiul cibernetic civil românesc, pentru elaborarea propriului Plan de Continuitate a Afacerii (BCP – Business Continuity Plan).

Prezentul ghid este referință pentru elaborarea Planului de Continuitate a Afacerii din perspectiva securității cibernetice. Documentul are caracter orientativ, nu substituie obligațiile legale aplicabile fiecărei organizații și trebuie adaptat de fiecare organizație cu cerințele sale specifice de continuitate operațională, protecție a datelor, arhivare, resurse umane, siguranță fizică și alte obligații sectoriale sau legale aplicabile.

Planul de Continuitate a Afacerii (BCP – Business Continuity Plan) stabilește cadrul organizatoric, procedural și tehnic pentru asigurarea continuității operațiunilor organizației în situații de criză, asigurând:

- menținerea continuității funcțiilor critice ale organizației în caz de incident major sau dezastru;
- reducerea la minimum a timpului de întrerupere a serviciilor esențiale și a pierderii de date;
- asigurarea conformității cu cerințele legale și de reglementare aplicabile în România și la nivel european;
- protejarea reputației instituționale și menținerea încrederii partenerilor și publicului;
- furnizarea unui cadru structurat de răspuns la evenimente perturbatoare, inclusiv cele de natură cibernetică.

2. Domeniul de aplicare

Delimitarea clară a domeniului de aplicare este esențială pentru o implementare coerentă și verificabilă a măsurilor de continuitate.

În această secțiune se vor trece categoriile de informații, procesele operaționale critice ale organizației, infrastructura IT&C, managementul furnizorilor critici și al lanțului de aprovizionare asupra cărora se aplică prevederile Planului de Continuitate a Afacerii, respectiv eventualele excepții. Se va acorda, în mod special, atenție identificării tuturor dependențelor operaționale identificate prin analiza de impact asupra activității (BIA) relevante pentru domeniul de activitate al organizației.

BCP este conceput ca document-cadru[1] integrat, complementar Planului de Recuperare în Caz de Dezastru (DRP) și Planului de Răspuns la Incidente (IRP), în cadrul unui sistem unitar de management al continuității afacerii (BCM).

Deși prezentul ghid este axat pe scenariile de securitate cibernetică, BCP trebuie completat de fiecare organizație, după caz, și cu alte tipuri de evenimente perturbatoare majore (fizice, naturale, operaționale), în măsura în care acestea afectează continuitatea activității.

Planul de Continuitate a Afacerii în cadrul organizației se aplică de către structurile organizaționale:

[1] Conceptul de document-cadru integrat exprimă funcția BCP de document de guvernanță unic la nivelul organizației, care stabilește principiile, structura de comandă și strategiile generale de continuitate, fără a relua sau a contrazice detaliile tehnice și operaționale reglementate distinct prin DRP și IRP; astfel, BCP asigură coerența, trasabilitatea deciziilor și interoperabilitatea dintre documentele componente ale sistemului de management al continuității afacerii (BCM).

- proceselor operaționale critice din organizație;
- sistemelor informatice și de comunicații gestionate sau operate în cadrul organizației;
- mecanismelor de lucru cu partenerii, furnizorii și operatorii de servicii esențiale cu care există raporturi contractuale.

3. Cadrul legal și normativ aplicabil

Planul de Continuitate a Afacerii se elaborează în raport cu cadrul legal și normativ aplicabil organizației, precum și cu bunele practici cunoscute în domeniul continuității activității și securității informației. În funcție de sectorul de activitate și de statutul juridic, fiecare organizație trebuie să ia în considerare și alte acte normative sau standarde față de cele menționate în continuare.

- Ordonanța de urgență nr. 155 din 30 decembrie 2024 privind instituirea unui cadru pentru se curitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil https://www.dnsc.ro/vezi/document/monitorul-oficial-partea-i-nr-1332-oug-nis2-31122024
- Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României LEGE 58 14/03/2023 - Portal Legislativ
- CyberFundamentals Framework | CyFun Standard dezvoltat de CCB Belgia;
- HG nr. 585/2002 Standardele naționale de protecție a informațiilor clasificate https://orniss.ro/ro/legislatie/pdf/HG%20585.pdf
- Legea nr. 182/2002 - informații clasificate https://orniss.ro/ro/legislatie/pdf/L%20182.pdf
- Regulamentul DORA – (UE) 2022/2554 - Autoritatea de Supraveghere Financiară - Regulamentul (UE) nr. 2022/2554 (DORA)
- Regulamentul privind IA (UE) 2024/1689 (AI Act) https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:L_202401689
- Directiva CER – (UE) 2022/2557 - Reziliența entităților critice; Publications Office
- Regulamentul de punere în aplicare (UE) 2024/2690 https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:L_202402690
- ISO 22301:2019 https://www.iso.org/standard/75106.html
- ISO 22313:2020 https://www.iso.org/standard/75107.html
- ISO/TS 22317:2021 https://www.iso.org/standard/79000.html
- ISO/TS 22318:2021 https://www.iso.org/standard/79001.html
- ISO/IEC 27001:2022 - https://www.iso.org/standard/27001
- ISO/IEC 27002:2022 https://www.iso.org/standard/75652.html
- ISO/IEC 27035:2023 - https://www.iso.org/standard/78973.html
- NIST SP 800-34 Rev.1 https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final
- NIST SP 800-61 Rev.3 https://csrc.nist.gov/pubs/sp/800/61/r3/final
- NIST Cybersecurity Framework 2.0 - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- Availability Management — ITIL 4 Practice Guide (oficial): https://www.axelos.com/resource-hub/practice/availability-management-itil-4-practice-guide
- IT Service Continuity Management — ITIL 4 Practice Guide (oficial): https://www.axelos.com/resource-hub/practice/service-continuity-itil-4-practice-guide

4. Guvernanță și responsabilități

Guvernanța continuității activității reprezintă ansamblul structurilor decizionale, responsabilităților formalizate și mecanismelor de supervizare prin care organizația asigură elaborarea, implementarea, testarea și actualizarea Planului de Continuitate a Afacerii. Conducerea organizației aprobă cadrul de guvernanță, stabilește resursele necesare și desemnează persoanele responsabile în conformitate cu cerințele legale aplicabile și cu structura internă.

În conformitate cu articolul 14 din OUG 155/2024, se impune implicarea directă a organelor de conducere în aprobarea măsurilor de gestionare a riscului cibernetic și în supervizarea implementării BCP. Conducerea organizației răspunde personal pentru implementarea și eficacitatea acestor măsuri, inclusiv în ceea ce privește alocarea resurselor și asigurarea formării profesionale necesare. Totodată, conform OUG 155/2024 (astfel cum a fost aprobată prin Legea nr. 124/2025), organele de conducere stabilesc mijloacele permanente de contact, asigură alocarea resurselor necesare pentru punerea în aplicare a măsurilor de gestionare a riscurilor de securitate cibernetică și desemnează, în termen de 30 de zile de la comunicarea deciziei directorului DNSC de identificare și înscriere în registru, responsabilii cu securitatea rețelelor și sistemelor informatice. Această cerință ar trebui reflectată în structura Echipei de Continuitate a Afacerii (BCP Team).

Implementarea cu succes a BCP depinde de definirea clară a rolurilor și responsabilităților pentru toți angajații/ echipele responsabile pentru fiecare componentă. Toate persoanele responsabile desemnate și înlocuitorii acestora au acces la versiunea aplicabilă a planului, în funcție de rol și de necesitatea operațională și sunt instruite periodic cu privire la responsabilitățile lor. Datele de contact operaționale și mijloacele alternative de contact sunt menținute actualizate. Responsabilii de nivel managerial trebuie să se asigure că membrii echipei din subordine alocați în plan cunosc acest lucru și sunt eliberați de alte sarcini în caz de dezastru pentru a se putea dedica recuperării.

4.1. Structura de comandă în situații de criză

Structura de coordonare în situații de criză definește lanțul ierarhic de autoritate și responsabilitate activat la declararea unei situații de criză. Rolurile de mai jos sunt orientative; fiecare organizație le adaptează la organigrama, regulamentul intern și obligațiile sectoriale proprii. Structura de coordonare ar trebui să includă, după caz, funcții pentru coordonare executivă, securitate cibernetică, infrastructură IT, juridic, comunicare, resurse umane și logistică.

Planul de Continuitate în cadrul organizației este activat și coordonat, în principiu, prin structura ierarhică de mai jos, care funcționează ca Echipă de Continuitate a Afacerii (BCP Team):

Tabel 1. Roluri și responsabilități

Rol/ Structură responsabilă	Responsabilitate principală
[Director General]	Autoritate supremă; declararea stării de criză; comunicare publică
[Director General Adjunct]	Coordonare operațională; înlocuitor Director General
[BCP Manager (coordonator plan)]	Activarea, coordonarea și monitorizarea BCP; raportare
[CISO/Responsabil Securitate] Cibernetică	Evaluare tehnică incident; coordonare răspuns cibernetic
[Responsabil IT/Infrastructură]	Implementare soluții tehnice de recuperare; DRP
[Responsabil Juridic]	Notificări legale (DNSC prin PNRISC, ANSPDCP); conformitate
[Responsabil Comunicare]	Comunicare internă și externă; management reputațional
[Responsabil HR]	Asigurarea personalului esențial; protecție angajați
[Responsabil Achiziții/Logistică]	Contracte furnizorii critici; resurse logistice

4.2. Fluxul de escaladare a incidentelor

Fluxul de escaladare definește traseul decizional parcurs de un incident de securitate cibernetică, de la detecția operațională până la nivelul de criză strategică. Escaladarea se realizează pe niveluri clar definite, astfel încât răspunsul să fie proporțional cu severitatea incidentului și cu impactul asupra proceselor critice. Activarea măsurilor BCP se face de către persoana sau organul desemnat prin decizie internă, iar ceilalți actori inițiază, recomandă sau validează escaladarea, potrivit atribuțiilor stabilite.

Escaladarea structurată pe patru niveluri — operațional, tactic, strategic și național — permite organizației să calibreze răspunsul proporțional cu severitatea incidentului, evitând atât sub-reacția (care amplifică impactul), cât și supra-reacția (care consumă inutil resurse în cazul incidentelor minore).

În cadrul organizației, fluxul de escaladare pe cele patru niveluri este stabilit astfel:

- Nivel 1 (Operațional): Incident detectat de echipele tehnice; evaluare inițială; aplicare proceduri standard.

- Nivel 2 (Tactic): Incident cu impact mediu; activarea parțială a BCP; notificarea BCP Manager și CISO.
- Nivel 3 (Strategic): Incident major cu impact sever; activarea completă a BCP; convocare Celulă de Criză; notificare Director General.
- Nivel 4[2] (Criză cibernetică cu impact național): Incident cu impact la nivel național; activarea structurilor interinstituționale (DNSC, SRI, MAI, MApN, etc.); escaladare internațională prin DNSC către rețeaua CSIRTs (CSIRTs Network) și, după caz, prin mecanismul EU-CyCLONe pentru crize de amploare.

4.3. Aprobarea și revizuirea Planului

BCP este aprobat de conducerea organizației și revizuit periodic, cel puțin anual, precum și ori de câte ori intervin modificări semnificative organizaționale, tehnologice, operaționale, contractuale sau legislative. Revizuirile post-incident, revizuirile organizaționale și revizuirile tehnologice se realizează în funcție de relevanța evenimentului și de evaluarea de risc. Calendarul de revizuire prezentat mai jos ilustrează frecvența minimă recomandată pentru revizuire.

BCP este aprobat de conducerea organizației și revizuit periodic conform tabelului de mai jos:

Tabel 2. Calendarul de revizuire a BCP

Tip revizuire	Frecvență	Declanșator
Revizuire periodică planificată	Anual (minim)	Calendar organizatoric
Revizuire post-incident	După fiecare incident major	Raport post-incident aprobat
Revizuire legislativă	La modificarea cadrului legal	Intrarea în vigoare a noilor norme
Revizuire organizatorică	La schimbări structurale majore	Decizie de reorganizare
Revizuire tehnologică	La schimbări semnificative de infrastructură	Audit tehnic / proiect major

5. Analiza impactului asupra activității (BIA)

Analiza Impactului asupra Activității (BIA) reprezintă fundamentul Planului de Continuitate a Afacerii și se realizează prin interviuri structurate, chestionare standardizate, analiză documentară și validarea rezultatelor cu factorii de decizie relevanți. BIA acoperă atât procesele de afaceri, cât și resursele tehnologice, umane și informaționale critice. Pentru fiecare proces sau activ critic se identifică dependențele, impactul indisponibilității, soluțiile alternative și parametrii de recuperare, inclusiv RTO, RPO și MTD.

Realizată conform ISO 22317:2021, BIA presupune un proces iterativ de identificare, analiză și validare cu factorii de decizie din organizație, asigurând că prioritățile de recuperare reflectă atât criticitatea operațională, cât și obligațiile legale asumate față de autorități, parteneri și beneficiarii serviciilor.

5.1. Metodologia BIA

BIA se realizează prin interviuri structurate cu responsabilii de procese (process owners), chestionare standardizate și analiză documentară. Analiza este centrată pe procesele de activitate ale organizației, urmând ca instrumentele tehnologice, aplicațiile și resursele de monitorizare care susțin aceste procese să fie identificate ca dependențe și inventariate ca active critice în cadrul subcapitolului 5.3. Pentru fiecare instrument critic se identifică dependențele față de procesele de muncă, impactul indisponibilității, soluțiile alternative sau instrumentele de substituție, precum și cerințele de recuperare (RTO/RPO). Rezultatele BIA trebuie validate de conducerea organizației și actualizate cel puțin anual sau

[2] Nivelul 4 nu este relevant pentru toate organizațiile care utilizează acest ghid. Activarea structurilor interinstituționale naționale (DNSC, SRI, MAI, MApN) și a mecanismelor europene (rețeaua CSIRTs, EU-CyCLONe) presupune ca incidentul să atingă pragul de criză cibernetică în sensul art. 2 lit. k) din Ordonanța de urgență a Guvernului nr. 104/2021. Pentru majoritatea entităților importante, cu impact limitat la propriul perimetru operațional, escaladarea se oprește de regulă la Nivelul 3 (notificare DNSC prin PNRISC, fără activarea structurilor interinstituționale de criză). Fiecare organizație trebuie să evalueze, în funcție de propriul profil de risc și de încadrarea sa (esențială/importantă/critică), dacă și în ce condiții un incident propriu ar putea justifica escaladarea la Nivelul 4.

ori de câte ori intervin modificări organizatorice, tehnologice sau de configurație a mediului operațional. Metodologia descrisă mai jos urmează cerințele ISO 22317:2021 și poate fi adaptată la dimensiunea și complexitatea organizației.

Analiza impactului asupra activității (BIA) în cadrul organizației este realizată conform ISO 22317:2021 și cuprinde:

- identificarea proceselor și funcțiilor critice;
- cuantificarea impactului unei întreruperi (financiar, operațional, reputațional, legal, de securitate);
- stabilirea parametrilor RTO, RPO și MTD pentru fiecare proces critic;
- identificarea dependențelor interne și externe (sisteme, furnizori, personal cheie);
- prioritizarea proceselor pentru recuperare.
- [altele, după caz].

5.2. Inventarul proceselor critice

Organizațiile identifică procesele și funcțiile critice proprii, precum și parametrii de continuitate asociați (RTO, RPO, MTD). Identifică, de asemenea, dependențele interne și externe față de furnizori terți de servicii cloud și lanțul de aprovizionare, precum și resursele disponibile pentru recuperare. Valorile RTO/ RPO/ MTD se determină în urma BIA-ului propriu al organizației. Lista de mai jos are caracter orientativ și ar trebui înlocuită sau completată integral cu procesele critice identificate prin BIA proprie a organizației. Valorile de prioritate, RTO, RPO și MTD se stabilesc individual, în funcție de criticitatea reală și de toleranța la întrerupere a fiecărui proces. Fiecare organizație va înlocui sau completa tabelul cu propriile procese critice, identificate prin BIA proprie.

În cadrul unei organizații pot fi identificate următoarele procese critice[3] și atribuite nivelele de criticitate corespunzătoare. Sunt de asemenea stabilite RTO/ RPO/ MTD, conform tabelului de mai jos:

Tabel 3. Inventarul proceselor critice și parametrii de recuperare (BIA)

Proces / Funcție critică	**Nivel de Prioritate** Critică/ ridicată/ medie/ redusă	**RTO** Zile/Ore/ min	**RPO** Ore/ min	**MTD** Zile/Ore/ min
Monitorizare și alertare cibernetică				
Gestionare incidente de securitate cibernetică				
Comunicații securizate interne și externe				
Notificări și raportări legislative				
Servicii de informare publică și comunicare				
Sisteme administrative (HR, financiar, achiziții)				
Arhivare electronică și managementul documentelor				
[altele, după caz]				

5.3. Managementul și inventarul activelor critice

Capacitatea unei organizații de a asigura continuitatea activității în situații de criză este condiționată în mod direct de cunoașterea exhaustivă a activelor (hardware, software, date și informații critice etc.) pe care se bazează procesele sale critice. Principiul fundamental al oricărui program robust de management al continuității afacerilor stipulează că nu poate fi protejat ceea ce nu este cunoscut și inventariat. Managementul activelor critice se înscrie în cerințele de securitate cibernetică instituite prin OUG 155/2024 și se corelează direct cu BIA realizată conform prevederilor aceluiași act normativ. OUG 155/2024 impune entităților esențiale și importante adoptarea unor măsuri tehnice, operaționale și organizatorice adecvate și proporționale pentru gestionarea riscurilor de securitate cibernetică, incluzând în mod explicit gestionarea activelor.

[3] Exemplele sunt orientate spre domeniul securitate cibernetică; fiecare organizație va adapta lista la specificul activității proprii.

Fiecare activ critic este identificat, clasificat și corelat cu procesele pe care le susține. Clasificarea activelor se realizează în funcție de criticitatea lor pentru continuitatea proceselor organizației și se actualizează ori de câte ori apar modificări semnificative în infrastructură, în modelul de operare sau în profilul de risc. Registrul activelor critice constituie un instrument de management dinamic, utilizat în BIA, în evaluarea riscurilor, în planificarea recuperării și în alocarea resurselor. Clasificarea se realizează pe patru niveluri, descrise mai jos, și este direct corelată cu obiectivele de recuperare stabilite prin BIA: Obiectivul de Timp de Recuperare (RTO), Obiectivul de Punct de Recuperare (RPO) și Toleranța Maximă de Întrerupere Admisă (MTD).

- Critic: Activul susține direct un proces critic din BIA; indisponibilitatea sa conduce la depășirea MTD al procesului asociat. Recuperarea are prioritate absolută.
- Ridicat: Activul susține procese importante; întreruperea poate fi tolerată pe o durată definită, fără a compromite obligațiile legale fundamentale.
- Mediu: Activul susține procese operaționale cu impact moderat; pierderea temporară poate fi compensată prin proceduri manuale.
- Redus: Activul susține activități auxiliare; indisponibilitatea sa nu afectează semnificativ continuitatea operațiunilor critice.

Registrul activelor critice nu este un document static. El constituie un instrument de management dinamic, care alimentează în mod continuu BIA, evaluarea nivelului de risc cibernetic, strategiile de recuperare după dezastru (DRP) și planificarea resurselor necesare continuității. Orice modificare semnificativă a infrastructurii tehnologice, a structurii organizatorice sau a modelului de afaceri al organizației trebuie să se reflecte imediat în actualizarea registrului.

În scopul elaborării și menținerii Planului de Continuitate a Afacerii, la nivelul organizației sunt identificate activele critice din categoriile de mai jos (cu caracter orientativ), fiind stabilit pentru fiecare, și nivelul de criticitate pentru continuitatea proceselor organizației.

- Active hardware;
- Active software;
- Date și informații critice;
- Servicii cloud și furnizori de servicii gestionate;
- Personal cheie;
- Spații fizice și facilități;
- Altele, după caz.

5.4. Scenarii de risc și amenințări cibernetice

Scenariile de risc[4] reprezintă punctul de pornire pentru BIA și pentru planificarea măsurilor de continuitate. Lista de mai jos este orientativă; fiecare organizație va completa și adapta scenariile în funcție de sectorul de activitate, profilul de amenințare și rezultatele evaluărilor proprii de risc. Evaluarea nivelului de risc este un proces continuu, integrat în ciclul de viață al BCP.

OUG 155/2024 instituie obligația entităților esențiale și importante de a realiza și transmite anual către DNSC, și după caz, autorității competente sectorial, o autoevaluare a nivelului de maturitate a măsurilor de gestionare a riscurilor de securitate cibernetică. Entitățile esențiale au obligația suplimentară, de a transmite către DNSC, și, după caz, către autoritatea competentă, în termen de 30 de zile de la realizarea autoevaluării, un plan de măsuri pentru remedierea deficiențelor identificate. Responsabilitatea pentru autoevaluare revine organelor de conducere.

Evaluarea nivelului de risc nu este un demers punctual, limitat la momentul înscrierii în registrul DNSC. Aceasta trebuie înțeleasă ca un proces continuu, integrat în ciclul de viață al BCP, actualizat la apariția modificărilor semnificative de infrastructură sau organizatorice și revizuit periodic, cu o frecvență minimă anuală, în concordanță cu revizuirea BCP. Niciun scenariu nu trebuie exclus a priori — relevanța sa va fi determinată de analiza de risc a organizației.

[4] A se vedea și *Ghid practic de management al riscurilor cibernetice*

În cadrul organizației, pot fi luate în considerare următoarele scenarii de risc:

Tabel 4. Scenarii de risc

Scenariu de risc	**Probabilitate** Înaltă/ Medie/ Redusă	**Impact** Critic/ Înalt/ Sever/ Moderat	**Nivel risc** Critic/ Înalt/ Mediu
Atac ransomware asupra infrastructurii			
Compromiterea conturilor privilegiate			
Incident la furnizor de servicii cloud (supply chain)			
Afectare majoră a centrului de date			
Incident de securitate fizică (acces neautorizat sediu)			
Pandemie / absenteism masiv personal cheie			
Atac de tip APT (Advanced Persistent Threat)			

6. Strategii de continuitate și recuperare

Strategiile de continuitate și recuperare reprezintă răspunsul planificat al organizației la scenariile de risc identificate prin BIA. Acestea acoperă atât dimensiunea tehnică, cât și dimensiunea operațională și de comunicare. Fiecare organizație selectează, adaptează și completează strategiile în funcție de procesele critice, de arhitectura tehnologică și de resursele disponibile. Selecția strategiilor se realizează pe baza raportului cost-eficacitate, ținând cont de valorile RTO și RPO stabilite.

Abordarea bazată pe principiul redundanței, pe principiul Privacy by Design și pe arhitectura Zero Trust asigură că organizația dispune de capacitatea de a continua funcțiile critice chiar și în contextul unui incident cibernetic major, minimizând atât durata întreruperii, cât și pierderea de date.

6.1. Strategii generale

Strategiile generale definesc opțiunile și principiile de continuitate adoptate de organizație la nivel de arhitectură și guvernanță. Ele reprezintă decizii pre-criză, validate prin BIA, care stau la baza procedurilor detaliate din Capitolul 7. Fiecare organizație selectează, adaptează și documentează aceste strategii în funcție de procesele critice proprii, resursele disponibile și valorile RTO/RPO stabilite.

Strategia de continuitate a organizației se bazează pe principiile: redundanță (redundancy), confidențialitate integrate în proiectare (Privacy by Design), arhitectură bazată pe principiul încrederii zero (Zero Trust). Pot fi avute in vedere următoarele elemente:

- Duplicarea infrastructurii critice; site secundar;
- Backup conform regulii 3-2-1-1-0;
- Soluții de asigurare a continuității serviciilor pentru sistemele de monitorizare și alertare cibernetică;
- Acorduri de servicii alternative (contracte de back-up cu furnizori alternativi de conectivitate și cloud);
- Disponibilitate personal: telemuncă securizată, convenții de partajare resurse cu instituții partenere;
- Altele, după caz.

6.2. Strategia de backup și recuperare a datelor

Organizația definește frecvențele de backup, retenția, mediile de stocare, locațiile și frecvența testelor de restaurare în funcție de RTO, RPO și de cerințele operaționale proprii. Detaliile tehnice se documentează în politica de backup și în procedurile asociate. Testarea restaurării se realizează periodic, iar rezultatele se înregistrează și se analizează.

Conform ISO/IEC 27002:2022 (control 8.13) și principiului 3-2-1-1-0, organizația implementează următoarele tipuri de backup și stabilește și frecvența testării restaurării (Restore Test Frequency) asociată fiecăruia:

Tabel 5. Strategia de backup și recuperare a datelor

Nivel backup	**Frecvență** La fiecare oră/ ore/ zilnic/ săptămânal	**Tip stocare** Locală/ bandă magnetică/ replicare/ cloud	**Locație** Site primar/ off-site/ cloud	**Retenție** Ore/ zile/ luni
Backup complet				
Backup diferențial				
Backup incremental				
Snapshot sisteme critice				
Copie offline (air-gapped)				
[altele, după caz]				

6.3. Strategia de recuperare în caz de dezastru

În cadrul organizației, Planul de continuitate a afacerii acoperă continuitatea proceselor de afaceri în ansamblu, în timp ce DRP detaliază recuperarea tehnică a sistemelor IT. Cele două planuri sunt interdependente și se activează simultan în caz de incident major.

Planul de recuperare în caz de dezastru[5] (DRP) se elaborează distinct, dar complementar BCP, și detaliază arhitectura tehnică de recuperare, inclusiv topologia, failover-ul, replicarea, responsabilitățile tehnice și acordurile de nivel de serviciu cu furnizorii relevanți. BCP și DRP sunt interdependente, dar au roluri diferite: BCP acoperă continuitatea proceselor de afaceri, iar DRP recuperează funcționalitatea tehnică a sistemelor după incident.

Conținutul planului de recuperare în caz de dezastru (DRP) este conceput în conformitate cu ISO/IEC 27002:2022, control 5.30 (Pregătirea TIC pentru continuitatea activității). Structura DRP trebuie proiectată înainte de producerea unui incident, nu improvizată în criză.

6.4. Strategia de comunicare în criză

Comunicarea eficientă în criză este la fel de importantă ca recuperarea tehnică. Comunicarea deficitară poate amplifica impactul unui incident prin pierderea încrederii părților interesate sau prin netransmiterea la timp a notificărilor legale. Comunicarea în criză este parte esențială a continuității. Organizația stabilește canale alternative de comunicare, mesaje pre-aprobate, reguli de validare și proceduri de notificare internă, instituțională și publică, în funcție de natura incidentului și de obligațiile legale aplicabile. Termenele și canalele de notificare se stabilesc potrivit cadrului legal incident și instrucțiunilor autorității competente.

Notificările formale se realizează conform art. 15 din OUG 155/2024.

Comunicarea în situații de criză în cadrul organizației se desfășoară pe trei paliere complementare, activate coordonat la declararea crizei.

- La nivel intern, sunt activate canale de comunicare alternative (telefonie prin satelit, mesagerie securizată off-network, SMS-uri de urgență), menite să asigure transmiterea promptă a instrucțiunilor către echipele de criză și către personalul implicat, indiferent de starea infrastructurii IT&C obișnuite.
- La nivel inter-instituțional, se asigură îndeplinirea obligațiilor legale de notificare, prin transmiterea de notificări formale către autoritățile competente (DNSC, prin platforma PNRISC; ANSPDCP, atunci când incidentul implică date cu caracter personal; CSIRT-urile sectoriale relevante, după caz), cu respectarea termenelor stabilite prin OUG 155/2024.

[5] A se vedea și: *DNSC Ghid pentru elaborarea unei politici de recuperare în caz de dezastru*

- La nivel public, organizația gestionează încrederea părților interesate externe prin comunicate de presă aprobate de managementul organizației, prin actualizări pe pagina web instituțională și pe canalele de social media, precum și printr-o linie telefonică dedicată informării directe a publicului și partenerilor afectați.

6.5. Telemunca și accesul de la distanță

OUG 155/2024 impune entităților esențiale și importante adoptarea unor măsuri tehnice și organizatorice care să acopere, în mod explicit, securitatea resurselor umane și controlul accesului, inclusiv în scenariile de muncă la distanță. Standardul ISO/IEC 27002:2022, controlul 6.7 (Teleworking), stabilește că organizațiile trebuie să implementeze măsuri de securitate specifice pentru protejarea informațiilor accesate, procesate sau stocate în regim de telemuncă.

În contextul telemuncii și al accesului de la distanță, organizația stabilește măsuri de autentificare puternică, acces condiționat, segregarea mediilor, protecția datelor și reguli de utilizare a echipamentelor și canalelor de comunicație. Accesul de la distanță se acordă doar în condiții controlate și pe baza principiului necesității de a cunoaște și de a accesa.

Planul de Continuitate a Afacerii identifică scenariile în care telemunca devine necesară ca răspuns la o situație de criză. Organizația va adapta măsurile specifice unei situații de criză la contextul propriu și va documenta pentru fiecare scenariu condițiile de activare, sistemele vizate și responsabilitățile specifice.

Scenarii specifice de activare a regimului de telemuncă în criză, în cazul în care organizația are prevăzut acest tip de regim de muncă:

- incidentele cibernetice care afectează infrastructura centrală: atacuri ransomware sau alte incidente care fac nesigură utilizarea infrastructurii interne, impunând redirectarea operațiunilor către medii izolate sau alternative;
- imposibilitatea accesului fizic la sediu: cauzată de dezastre naturale (inundații, cutremur, incendiu), deteriorarea infrastructurii clădirii, restricții de acces impuse de autorități sau incidente de securitate fizică. În acest scenariu, telemunca reprezintă singura modalitate de menținere a operațiunilor critice pe durata indisponibilității sediului;
- pandemia sau absenteismul masiv: incapacitatea unui număr semnificativ de angajați de a se prezenta fizic la locul de muncă din cauza unor boli, a instituirii stării de carantină sau altor restricții de sănătate publică.

Organizația ar trebui să asigure disponibilitatea permanentă a infrastructurii tehnice necesare regimului de telemuncă, astfel încât, la momentul activării unui scenariu de criză, tranziția la acces de la distanță să se realizeze cu minimum de întârziere. Pentru asigurarea continuității în regim de telemuncă trebuie avute în vedere următoarele cerințe tehnice minime:

- rețea privată virtuală (VPN) cu autentificare multifactor (MFA;
- protecția terminalelor (Endpoint Protection);
- capacitate suficientă a infrastructurii de acces la distanță;
- accesul la aplicațiile și sistemele critice din afara perimetrului;
- canale de comunicare alternative și redundante;
- soluții de backup și recuperare accesibile de la distanță.

7. Proceduri de răspuns la incident și activare BCP

Procedurile operaționalizează strategiile de continuitate, transpunând opțiunile strategice în acțiuni concrete, cu responsabili și termene clare. Activarea procedurilor se face în baza criteriilor și a autorităților de activare stabilite în secțiunea 7.1.

Procedurile de răspuns la incident definesc acțiunile concrete, secvențiale și responsabilitățile asociate, care trebuie întreprinse din momentul detecției unui eveniment perturbator și până la reluarea deplină a operațiunilor normale. Activarea BCP este un act formal, cu criterii clare de declanșare, care angajează resurse semnificative și autoritate decizională la nivel organizațional.

Structurarea răspunsului pe faze distincte - detecție, limitarea impactului, recuperare și revenire la normal - asigură un flux de lucru ordonat, trasabil și auditabil, conform cerințelor OUG 155/2024.

7.1. Activarea BCP

Criteriile de activare a BCP trebuie să fie clare, măsurabile și cunoscute de membrii echipei de continuitate. BCP poate fi activat în urma unuia sau mai multor evenimente cu impact semnificativ asupra proceselor critice, infrastructurii, personalului, furnizorilor sau comunicării organizaționale. Activarea parțială sau completă se decide în funcție de severitatea incidentului și de timpul estimat de indisponibilitate.

În tabelul de mai jos sunt organizația va completa evenimentele declanșatoare, nivelurile de activare (parțial/complet) și autoritățile de activare în funcție de structura ierarhică proprie. Este esențial ca aceste criterii să fie clare, măsurabile și cunoscute de toți membrii echipei de continuitate - ambiguitatea în criteriile de activare poate întârzia răspunsul în criză.

La nivelul organizației, BCP va fi activat de către autoritatea de activare corespunzătoare în urma producerii unuia sau mai multor dintre evenimentele declanșatoare de mai jos:

Tabel 6. Criterii de activare a BCP și autorități de activare

Eveniment declanșator	Nivel activare BCP Parțial/ complet sau mixt	Autoritate de activare
Incident de securitate cibernetică cu impact critic asupra operațiunilor		
Atac ransomware cu criptarea datelor de producție		
Indisponibilitate centru de date primar		
Incident DDoS care afectează platformele publice		
Compromiterea conturilor privilegiate ale sistemelor critice		
Evacuarea sediului principal (incendiu, inundație, amenințare securitate fizică)		
Absenteism masiv personal cheie (> 30% din echipele critice)		

7.2. Răspunsul la incident

Etapele descrise în acest capitol reprezintă un model secvențial de răspuns. În practică, unele activități se pot suprapune sau desfășura în paralel, în funcție de natura incidentului. Organizația va adapta timpii la capacitățile tehnice și umane proprii, documentând procedurile detaliate în planul de răspuns la incidente.

În cadrul unei organizații, etapele procesului de răspuns la incidente[6] sunt stabilite astfel:

- Faza 1 – Detecție și evaluare: [minute/ ore]
- Faza 2 – Analiză și Limitarea impactului, proceduri de lucru alternative (manual/offline), izolarea și activarea BCP: [minute/ ore]
- Faza 3 – Recuperare și restaurare: [minute/ ore] – vezi RTO
- Faza 4 – Reluare operațiuni și lecții învățate: (post-incident)

8. Testare, exerciții și validare BCP

Testarea periodică a Planului de Continuitate a Afacerii este condiția esențială pentru a garanta funcționalitatea procedurilor documentate, cunoașterea rolurilor de către personalul organizației și funcționarea tehnologiilor de recuperare conform parametrilor stabiliți. Un BCP netestat este echivalent cu un plan neoperațional.

[6] A se vedea și DNSC: *Bune practici pentru elaborarea unei politici de răspuns la incidente de securitate cibernetică*

BCP se testează periodic prin exerciții de tip tabletop, exerciții operaționale, simulări de incident, teste de failover și exerciții de recuperare. Tipul exercițiului se selectează în funcție de criticitatea proceselor, de maturitatea organizației și de obiectivele de validare.

Lecțiile extrase din fiecare exercițiu sau incident real alimentează un ciclu continuu de îmbunătățire (PDCA), în conformitate cu cerințele ISO 22301:2019 și prevederilor OUG 155/2024. (continuitatea activității, inclusiv gestionarea copiilor de rezervă, redresarea în caz de dezastru, managementul crizelor și autoevaluarea eficacității măsurilor).

8.1. Tipuri de exerciții

Tipul și programul de exerciții descris mai jos, precum și participanții, vor fi adaptate de fiecare organizație la structura sa internă și la resursele disponibile. Fiecare exercițiu trebuie planificat în avans, cu obiective clare, și finalizat cu un raport de concluzii transmis conducerii.

Tabel 7. Programare exerciții și testare a BCP

Tip exercițiu	Frecvență	Participanți	Obiectiv
Tabletop Exercise (simulare pe hârtie)	Trimestrial	Celula de Criză	Testarea procedurilor decizionale
Walkthrough Exercise (parcurgere plan)	Semestrial	Echipele BCP	Familiarizarea cu planul
Functional Exercise (testare funcțională)	Semestrial	Echipele IT + CERT	Testarea procedurilor tehnice
Full-scale Exercise (exercițiu complet)	Anual	Toată organizația	Testarea integrală a BCP
Failover Test (comutare DR)	Semestrial	Echipa IT	Validarea DR site și RTO
Backup Restore Test	Lunar	Echipa IT	Validarea backupurilor (RPO)

8.2. Documentarea și lecțiile învățate

Documentarea sistematică a exercițiilor și a incidentelor reale este esențială pentru îmbunătățirea continuă a BCP. Fiecare exercițiu sau test se documentează prin raport de execuție, constatări, neconformități, lecții învățate și acțiuni corective cu termen și responsabil desemnat. Rezultatele se introduc în ciclul de îmbunătățire continuă al BCP. Organizația va stabili un format standardizat pentru rapoartele de exercițiu și va desemna un responsabil (de regulă BCP Manager) pentru urmărirea implementării recomandărilor. Lecțiile neimplementate reprezintă un risc de conformitate în cadrul auditurilor NIS2.

Procesul de lecții învățate în urma exercițiilor/ incidentelor poate avea loc sub următoarele forme:

- organizarea unor ședințe de stabilire a lecțiilor învățate cu toate părțile implicate, în cel mult câteva zile de la incident;
- generarea imediată de acțiuni corective și preventive în Registrul CAPA (modificări de configurații, reguli de securitate, actualizări de proceduri tehnice);
- revizuirea politicilor sau arhitecturilor de securitate, dacă deficiențele identificate au caracter structuralÎn cadrul.

În cadrul organizației, fiecare exercițiu și incident real va fi urmat de:

- raportul de exercițiu: obiective atinse/neatinse, deficiențe identificate, recomandări;
- planul de acțiune corectivă (CAPA): termene, responsabili, resurse necesare;
- actualizarea BCP: dacă exercițiul relevă necesitatea modificării planului;
- raportul anual de continuitate: prezentat conducerii și, dacă este cazul, autorităților de supraveghere;
- altele, după caz.

9. Managementul furnizorilor critici și al lanțului de aprovizionare

Managementul furnizorilor critici și al lanțului de aprovizionare reprezintă una dintre cerințele centrale ale cadrului NIS2, recunoscând că vulnerabilitățile unei organizații nu se limitează la perimetrul său intern,

ci se extind la întregul ecosistem de parteneri și prestatori de servicii. Un incident la un furnizor critic poate declanșa efecte în cascadă asupra continuității operaționale a organizației beneficiare.

Identificarea, evaluarea și monitorizarea furnizorilor critici, însoțite de clauze contractuale adecvate privind continuitatea serviciilor, constituie o măsură de securitate obligatorie conform prevederilor OUG 155/2024.

9.1. Identificarea furnizorilor critici

Furnizorii critici sunt identificați pe baza dependenței lor de procesele critice ale organizației și a impactului pe care întreruperea serviciilor lor îl poate avea asupra continuității. Lista furnizorilor critici se actualizează periodic și ori de câte ori intervin schimbări în arhitectura operațională sau contractuală. Un furnizor este critic dacă: (a) indisponibilitatea serviciilor sale ar determina depășirea RTO sau RPO pentru cel puțin un proces critic; sau (b) compromiterea securității sale ar putea genera un incident de securitate cibernetică cu impact semnificativ asupra organizației. Conform OUG 155/2024 (prevederile referitoare la securitatea lanțului de aprovizionare și a furnizorilor), evaluarea furnizorilor include dimensiunile de continuitate și securitate cibernetică. Organizația va menține un registru actualizat al furnizorilor critici, incluzând nivelul de dependență, datele de contact de urgență și planurile de continuitate ale furnizorului.

Conform prevederilor OUG 155/2024, organizația identifică și gestionează riscurile din lanțul de aprovizionare. Furnizorii critici includ:

- furnizori de infrastructură cloud (IaaS/PaaS/SaaS) utilizați pentru sisteme critice;
- furnizori de conectivitate internet și servicii de telecomunicații;
- furnizori de soluții de securitate cibernetică (SIEM, EDR, firewall, etc.);
- furnizori de servicii de backup și recuperare a datelor;
- furnizorii de energie electrică și sisteme UPS pentru centrele de date;
- altele, după caz.

9.2. Cerințe contractuale minime pentru furnizorii critici

Contractele cu furnizorii critici ar trebui să includă, după caz, prevederi privind disponibilitatea serviciilor, continuitatea activității, notificarea incidentelor, obligațiile de cooperare, testarea, auditul, subcontractarea, localizarea datelor și exit management-ul. Cerințele de mai jos reprezintă clauze minime obligatorii care ar trebui incluse în contractele cu furnizorii critici. Organizația va adapta formularea juridică specifică împreună cu departamentul juridic și va verifica respectarea acestor cerințe în cadrul auditurilor periodice ale furnizorilor. Furnizorii care nu pot demonstra capabilități adecvate de continuitate sunt tratați ca un risc în lanțul de aprovizionare și gestionați în consecință.

La nivelul organizației, contractele încheiate cu furnizorii critici includ în mod obligatoriu cel puțin următoarele clauze:

- clauze de continuitate a serviciilor și SLA clare (inclusiv RTO/RPO din perspectiva furnizorului);
- dreptul organizației de a audita furnizorul privind măsurile de continuitate;
- obligații de notificare a organizației în caz de incident care afectează serviciile furnizate;
- planuri de continuitate și recuperare proprii, prezentate la cerere;
- clauze de ieșire și portabilitate a datelor (exit strategy);
- conformitate cu cerințele NIS2 pentru furnizorii de servicii digitale;
- altele, după caz.

10. Obligații de notificare și raportare a incidentelor

Entitățile esențiale și importante aflate sub incidența OUG 155/2024 au obligații de raportare, către DNSC, a oricărui incident care are un impact semnificativ asupra prestării serviciilor lor. Trebuie, de asemenea, notificați și destinatarii/beneficiarii serviciilor (nu doar autoritățile) atunci când incidentul semnificativ le poate afecta activitatea.

Planul de continuitate a Afacerii se înscrie în obligațiile mai largi de securitate cibernetică prevăzute de cadrul legal aplicabil. Un incident care afectează integritatea, disponibilitatea sau confidențialitatea datelor sau sistemelor - inclusiv eșecul unui backup, coruperea copiilor de rezervă sau imposibilitatea restaurării în termenele RTO/RPO stabilite - poate constitui un incident semnificativ în sensul legii, declanșând obligațiile de raportare descrise mai jos.

Pentru entitățile esențiale și importante care intră sub incidența OUG 155/2024, raportarea incidentelor semnificative se realizează cu prioritate conform fluxului și termenelor instituite de art. 15 din OUG 155/2024 (avertizare timpurie în 24 de ore, notificare de incident în 72 de ore) prin canalele puse la dispoziție de DNSC. Celelalte entități din spațiul cibernetic civil național, care nu sunt înscrise în registrul entităților esențiale/importante, pot efectua raportări prin platforma PNRISC (conform Legii nr. 58/2023) sau prin apelarea numărului unic 1911.

N.B (1) - Este esențial ca fiecare organizație să-și documenteze propriile obligații legale aplicabile sectorului său de activitate (ex. financiar, energie, sănătate etc.).

N.B (2) - În cazul existenței unei polițe de asigurare cibernetică, trebuie revizuite clauzele referitoare la raportarea incidentelor pentru a garanta respectarea termenilor contractuali.

Organizația stabilește termenele, fluxurile interne și externe de notificare și raportare a incidentelor în conformitate cu cadrul legal aplicabil și cu rolurile definite intern. Procedurile precizează cine notifică, cui notifică, prin ce canal, în ce termen și ce informații minime se transmit.

11. Resurse necesare pentru implementarea BCP

Implementarea cu succes a unui Plan de Continuitate a Afacerii presupune alocarea resurselor umane, tehnologice și financiare necesare. Insuficiența oricăreia dintre aceste categorii de resurse poate compromite capacitatea organizației de a activa și susține planul în situații de criză reală.

Evaluarea resurselor necesare este parte integrantă a procesului de planificare BCP și ar trebui revizuită periodic, în corelare cu evoluția organizației, a infrastructurii tehnologice și a cadrului normativ aplicabil. Angajamentul conducerii pentru asigurarea resurselor adecvate este reflectat în obligațiile prevăzute de OUG 155/2024, care impune organelor de conducere să asigure alocarea resurselor necesare implementării măsurilor de securitate cibernetică.

11.1. Resurse umane

Resursele umane reprezintă componenta cea mai vulnerabilă și mai puțin substituibilă în situații de criză. Organizația identifică personalul esențial, rolurile de rezervă, înlocuitorii și competențele necesare pentru menținerea funcțiilor critice. Se asigură instruirea și disponibilitatea acestora în condiții de criză. Dependența de o singură persoană-cheie („single point of failure” uman) reprezintă un risc major care ar trebui eliminat prin redundanță de personal.

În cadrul organizației, gestionarea resursei umane necesare implementării și derulării cu succes a BCP se face asigurând următoarele:

- personal cheie identificat și documentat pentru fiecare funcție critică;
- personal de înlocuire (back-up) identificat și instruit pentru fiecare rol esențial;
- instruire periodică privind BCP (minim anual) pentru tot personalul;
- instruire specifică pentru membrii Celulei de Criză (management criză, comunicare, tehnic);
- altele, după caz.

11.2. Resurse tehnologice

Resursele tehnologice necesare continuității includ infrastructura de backup, comunicații alternative, acces securizat, soluții de monitorizare, mijloace de restaurare și mecanisme de failover, în măsura în care acestea sunt necesare conform BIA.

Infrastructura tehnică de continuitate ar trebui testată periodic — existența sa fizică nu garantează funcționalitatea în criză. Organizația va documenta în [Registrul_active_critice] toate resursele tehnologice dedicate continuității, starea lor operațională, termenele de garanție și contractele de suport. Resursele marcate ca critice vor fi prioritizate în planificarea bugetară anuală.

În cadrul uneiorganizații, gestionarea resurselor tehnologice necesare implementării și derulării cu succes a BCP se face asigurând de regulă următoarele:

- centru de date secundar (DR site) cu capacitate suficientă și conectivitate redundantă;
- sisteme de backup validate și testate conform regulii 3-2-1-1-0;
- soluții de acces de la distanță securizat (VPN cu MFA pentru tot personalul critic);
- sisteme de comunicare de urgență (satelitare, radio, GSM dedicat) independente de rețeaua principală;
- laptopuri/tablete de urgență preconfigurate și disponibile pentru activare rapidă;
- altele, după caz.

11.3. Resurse financiare

Alocarea resurselor financiare pentru BCP decurge din obligațiile organelor de conducere prevăzute în OUG 155/2024 și implică responsabilitatea directă a conducerii. Organizația estimează și alocă resurse financiare pentru implementarea, testarea, mentenanța și actualizarea BCP, în raport cu nivelul de risc și cu criticitatea proceselor.

În cadrul unei organizații, asigurarea resurselor financiare necesare implementării și derulării cu succes a BCP se face în principiu astfel:

- se alocă buget dedicat pentru implementarea și menținerea BCP (inclus în planul anual de achiziții);
- se stabilește un Fond de rezervă pentru situații de urgență (contracte cadru pre-aprobate pentru servicii de urgență);
- se încheie asigurare cibernetică[7] (cyber insurance), dacă este aplicabilă;
- altele, după caz.

12. Instruire și conștientizare

Instruirea[8] și conștientizarea personalului reprezintă componenta umană esențială a oricărui sistem de management al continuității afacerii. Chiar și cel mai bine proiectat plan tehnic poate eșua dacă personalul implicat nu cunoaște procedurile, rolurile și responsabilitățile care îi revin în situații de criză.

Organizația derulează programe periodice de instruire și conștientizare pentru personalul implicat în BCP, inclusiv pentru înlocuitori și roluri de rezervă. Tematicile includ responsabilitățile în criză, securitatea informației, comunicarea, notificarea incidentelor și procedurile de continuitate.

Programul de instruire privind BCP ar trebui diferențiat pe categorii de personal — de la nivelul de conștientizare generală pentru toți angajații, până la instruirea specializată pentru membrii celulei de criză și echipele tehnice — și ar trebui integrat în planul anual de formare profesională, în conformitate cu prevederile din OUG 155/2024 (obligația de formare a organelor de conducere, practicile de igienă cibernetică și formarea personalului în domeniul securității cibernetice).

Programul de instruire privind BCP se desfășoară conform planului anual de instruire al organizației și include, în principiu, elementele de mai jos:

Tabel 8. Programul de instruire și conștientizare

Categorie personal	Tip instruire	Frecvență	Format
Tot personalul	Conștientizare BCP – rol în situații de criză	Anual	E-learning / prezentare
Membrii Celulei de Criză	Management criză, decizii sub presiune, comunicare	Semestrial	Atelier / simulare
Echipa IT / CERT	Proceduri tehnice DR, restaurare backup, incident response	Trimestrial	Exercițiu tehnic

[7] A se vedea și *DNSC Raport privind piața asigurărilor de risc cibernetic din Romania*
[8] A se vedea și *https://www.dnsc.ro/vezi/document/dnsc-ghid-elaborarea-politici-de-instruire-in-securitate-cibernetica*

Personal nou angajat	Introducere BCP	La angajare	Training specific
Management	Responsabilități în criză, cadru legal, comunicare	Anual	Briefing dedicat

13. Conformitate, audit și îmbunătățire continuă

Managementul Continuității Afacerilor (BCM) nu este un exercițiu punctual, finalizat odată cu elaborarea Planului de Continuitate a Afacerii. Eficacitatea și relevanța BCP se mențin exclusiv printr-un ciclu continuu de planificare, implementare, verificare și îmbunătățire. Prezentul capitol descrie mecanismele prin care o organizație asigură conformitatea permanentă cu cerințele legale și normative aplicabile, monitorizează eficacitatea măsurilor implementate și operaționalizează ciclul de îmbunătățire continuă în cadrul sistemului BCM.

13.1. Ciclul PDCA aplicat Managementului Continuității Afacerilor

BCP este administrat în logica ciclului PDCA (Plan-Do-Check-Act), prin planificare, implementare, verificare și îmbunătățire continuă. Organizația stabilește responsabilități, termene, indicatori și mecanisme de raportare pentru fiecare etapă.

Standardul ISO 22301:2019 (Business continuity management systems - Requirements) structurează explicit cerințele sistemului de management al continuității afacerilor în logica ciclului PDCA (Plan - Do - Check - Act). Această abordare constituie și baza conceptuală a prezentului ghid.

Conducerea organizației răspunde, în conformitate cu prevederile OUG 155/2024, de asigurarea resurselor necesare pentru parcurgerea completă și periodică a ciclului PDCA în cadrul BCM.

13.2. Auditul de securitate cibernetică și conformitate BCP

Organizația efectuează audituri interne și, după caz, audituri externe sau evaluări independente pentru a verifica adecvarea, eficacitatea și conformitatea BCP. Auditul poate acoperi atât aspecte de continuitate, cât și controale de securitate cibernetică relevante.

13.2.1. Auditul intern

Auditul intern al sistemului de management al continuității afacerilor și al măsurilor de securitate cibernetică reprezintă un instrument esențial de verificare a conformității cu cerințele legale, normative și interne, distinct de exercițiile operaționale prevăzute la capitolul 8. În timp ce exercițiile BCP testează funcționalitatea practică a planului, auditul intern evaluează sistematic dacă măsurile documentate sunt implementate efectiv, dacă documentația este completă și actualizată și dacă organizația respectă obligațiile legale aplicabile. Auditul intern se desfășoară cu o frecvență minimă anuală și ori de câte ori se produc modificări semnificative ale infrastructurii, proceselor sau contextului organizațional.

Responsabilul pentru audit intern este desemnat de conducerea organizației și ar trebui să dispună de independență față de funcțiile auditate. Constatările auditului intern se consemnează într-un raport formal, adresat conducerii superioare și responsabilului BCP și stau la baza planului de acțiuni corective (CAPA) prevăzut la subcapitolul 13.4.

13.2.2. Auditul extern și certificarea

Organizațiile care doresc demonstrarea conformității cu cerințele NIS2 față de terți (clienți, parteneri, autorități de supraveghere) pot opta pentru certificarea sistemului de management al continuității afacerilor conform ISO 22301:2019 și/sau a sistemului de management al securității informației conform ISO/IEC 27001:2022. Certificarea de terță parte (third-party certification), realizată de un organism de certificare acreditat, oferă cea mai înaltă credibilitate în demonstrarea conformității.

Notă: Conform OUG 155/2024 astfel cum a fost aprobată prin Legea nr. 124/2025: (i) entitățile transmit rezultatele auditului de securitate cibernetică către DNSC în termen de cel mult 5 zile de la finalizarea auditului; (ii) planul de măsuri corective se transmite DNSC în termen de cel mult 15 zile lucrătoare de la data primirii raportului de audit.

13.3. Indicatori de performanță BCP (KPI)

Monitorizarea sistematică a eficacității BCP se realizează prin intermediul unui set de indicatori-cheie de performanță (KPI — Key Performance Indicators), măsurați periodic și raportați conducerii. Indicatorii de performanță permit evaluarea obiectivă a gradului în care BCP asigură continuitatea operațiunilor critice în conformitate cu obiectivele stabilite prin BIA și fundamentează deciziile de îmbunătățire.

Indicatorii de performanță se stabilesc pentru a măsura capacitatea organizației de a răspunde la incidente și de a relua activitatea în timpii asumați. Exemple: rata de succes a testelor de restaurare, timpul de activare a BCP, timpul de recuperare, procentul acțiunilor CAPA închise la termen.

Organizația stabilește indicatorii, valorile-țintă și frecvența de măsurare în funcție de specificul activității și de obiectivele stabilite prin BIA.

Tabel 9. Indicatori de performanță BCP (KPI)

KPI	Valoare-țintă orientativă	Frecvență măsurare Lunar/semestrial/anual
% exerciții BCP planificate efectuate	[x%]	
% backupuri testate cu succes (restore)	[x%]	
% personal instruit BCP	[x%]	
altele, după caz		

13.4. Managementul acțiunilor corective și preventive (CAPA)

Neconformitățile, punctele slabe și oportunitățile de îmbunătățire identificate prin audit, testare sau incident sunt tratate prin acțiuni corective și preventive, urmărite până la închidere.

În cadrul organizației, registrul CAPA este menținut de responsabilul BCP, în coordonare cu CISO-ul organizației, și este prezentat conducerii la fiecare analiză a sistemului BCM. Acțiunile CAPA cu impact semnificativ asupra BCP declanșează revizuirea formală a documentului conform procedurii de control al documentelor. Acțiunile CAPA critice (cele care vizează funcții esențiale sau cerințe legale) au prioritate maximă și nu pot fi amânate fără aprobarea expresă a conducerii.

13.5. Raportarea anuală de conformitate

Organizația întocmește, după caz, raportări periodice sau anuale privind stadiul implementării și eficacității BCP, în funcție de cerințele legale aplicabile și de cerințele conducerii. Raportul anual de conformitate cuprinde cel puțin:

- rezultatele auditului intern al BCP și ale exercițiilor de testare;
- valorile KPI înregistrate față de valorile-țintă stabilite;
- stadiul acțiunilor CAPA deschise și al celor finalizate;
- evoluția profilului de risc cibernetic față de perioada anterioară;
- autoevaluarea anuală a nivelului de maturitate a măsurilor de gestionare a riscurilor de securitate cibernetică, realizată și transmisă DNSC și, după caz, autorității competente sectorial, conform OUG 155/2024;
- evenimentele semnificative (incidente, modificări de infrastructură, schimbări organizatorice) cu impact asupra BCP, petrecute în cursul anului;
- propunerile de revizuire a BCP pentru ciclul următor.

Raportul intern de conformitate este prezentat conducerii organizației și aprobat de aceasta, în conformitate cu responsabilitățile de guvernanță stabilite.

14. Anexe

Anexele la BCP includ politici, proceduri, formulare, registre, liste de contact, scenarii, rezultate de testare și alte documente relevante pentru implementarea BCP. Lista anexelor se stabilește de fiecare

organizație în funcție de profilul de risc, cerințele sectoriale și maturitatea propriului sistem de management al continuității.

Conform OUG 155/2024, BCP trebuie susținut de un set coerent de politici și proceduri de securitate cibernetică.

În cadrul organizației, politicile, planurile și documentele enumerate în continuare sunt anexe ale BCP.

Toate politicile, planurile și documentele de mai jos sunt: (1) aprobate formal de conducerea organizației; (2) comunicate tuturor angajaților relevanți; (3) disponibile într-un sistem de gestiune a documentelor cu control al versiunilor; (4) revizuite la frecvența indicată sau ori de câte ori intervine o schimbare organizatorică, tehnologică sau legislativă semnificativă; (5) testate prin exerciții practice pentru a valida eficacitatea lor operațională.

- Politica de backup a datelor
- Politica de răspuns la încălcarea securității datelor
- Politica de răspuns la incidente
- Politica de recuperare în caz de dezastru
- Politica de criptare acceptabilă și gestionare a cheilor
- Politica de identificare, autentificare și autorizare a utilizatorilor
- Politica Bring-Your-Own-Device (BYOD)
- Politica de acces la distanță
- Politica privind instrumentele de acces la distanță
- Politica de utilizare acceptabilă
- Politica de casare a echipamentelor tehnologice
- Politica de jurnalizare a informațiilor
- Planul de Comunicare în Criză
- Politica de gestionare a riscurilor de securitate cibernetică
- Politica de securitate a lanțului de aprovizionare și a furnizorilor critici
- Politica de gestionare a activelor (hardware, software, date)
- Politica de securitate fizică și a mediului (centre de date, acces fizic)
- Politica de igienă cibernetică și instruire a personalului
- Rapoartele de audit intern de Securitate
- Detalii contractuale privind furnizorii alternativi
- Registrul riscurilor cibernetice
- Matricea RTO/RPO per process
- Lista de contacte de urgență actualizată
- altele, după caz.

15. Dispoziții finale

Planul de Continuitate al Afacerii (BCP) elaborat în baza acestui ghid va intra în vigoare imediat după aprobarea sa de către conducerea organizației. Revizuirile ulterioare ale ghidului DNSC implică , după caz, revizuirea documentelor BCP proprii.

16. Termeni și definiții

Termenii și definițiile[9] de mai jos sunt utilizați în sensul prezentului ghid și al cadrului normativ aplicabil. În cazul în care organizația utilizează termeni diferiți în documentele interne, se recomandă alinierea la terminologia standardizată sau adăugarea unui tabel de corespondență în BCP-ul final.

Tabel 10. Glosar de termeni și definiții

Termen / Acronim	Definiție
Criza cibernetică	O stare de fapt care reprezintă o amenințare reală sau o deteriorare a unei infrastructuri cibernetice, de natură să creeze daune rețelelor și sistemelor informatice care furnizează servicii esențiale, digitale sau de interes național
Atac cibernetic	Acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică
Incident de securitate cibernetică	Un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora
Recovery Time Objective (RTO)	Reprezintă timpul maxim acceptat de la momentul incidentului până la restabilirea funcționalității unui serviciu sau sistem după un dezastru
Recovery Point Objective (RPO)	Reprezintă intervalul maxim de timp pentru care datele pot fi pierdute în urma unui incident
Recuperare	Reprezintă procesul de readucere a sistemelor, serviciilor și operațiunilor la un nivel operațional acceptabil după un incident
Restaurare	Reprezintă o etapă a procesului de recuperare, constând în readucerea sistemelor și datelor din copii de siguranță sau alte mecanisme de protecție
Maximum Tolerable Downtime (MTD)	Reprezintă timpul total maxim tolerat de întrerupere

Autori: Simona Tărăbășanu-Mihăilă, Ioana Murărașu, Cristina Cristina

TLP:CLEAR se poate folosi atunci când informațiile prezintă un risc minim de utilizare abuzivă, în conformitate cu normele și procedurile aplicabile pentru publicare. Sub rezerva regulilor standard ale drepturilor de autor, informațiile TLP:CLEAR pot fi partajate fără restricții.

https://www.dnsc.ro/

[9] A se vedea *și https://www.dnsc.ro/vezi/document/dnsc-dictionar-de-termeni-de-securitate-cibernetica*