SPITALUL DE RECUPERARE NEUROMOTORIE DR. CORNELIU BARSAN
DEZNA
JUDEȚUL ARAD

Nr. 116/08.02.2022

*Aprobat,*
*Manager Spital*

# PROCEDURA OPERATIONALA
## PRIVIND MANAGEMENTUL RISCULUI

**COD: P0 - GDPR - 03**
**Editia I**
**Revizia 0**

**Avizat:** presedintele comisiei CIM. DR. HANC DANIELA /semnatura/ .....
**Verificat:** responsabil compartiment DUMEA ADRIAN /semnatura/ .....
**Elaborat:** DUMEA ADRIAN
**Data aprobarii:** 08.02.2022

## 1. Cuprins:



## 2. Scopul procedurii operaționale:

Prezenta procedura descrie modul în care se realizează gestiunea riscurilor (identificare, evaluare, analiză, tratare, monitorizare, control) în cadrul institutiei, ajutând la înțelegerea riscurilor la care este supusă instituția, astfel încât acestea să poată fi administrate în mod eficient și corect.

Stabilește un cadru general unitar de identificare, evaluare, analiză, tratare, monitorizare și gestionare a riscurilor la nivelul tuturor structurilor din cadrul instituției.

Furnizează personalului și conducerii institutiei un instrument care facilitează gestionarea riscurilor într-un mod controlat și eficient, pentru atingerea obiectivelor institutiei.

Furnizează o descriere a modului în care sunt monitorizate riscurile și utilizarea documentelor, înregistrărilor și formularelor în acest sens.

## 3. Domeniul de aplicare a procedurii operaționale:

### 3.1. Precizarea (definirea) activității la care se referă procedura operațională:

Procedura este aplicată de către Responsabilul cu protectia datelor si structurile din cadrul Spitalului de Recuperare Neuromotorie „Dr. Corneliu Barsan" Dezna.

### 3.2. Delimitarea explicită a activității procedurate în cadrul portofoliului de activități desfășurate:

Prezenta procedura gestioneaza managementul riscurilor si se aplica pentru toate activitățile specifice în vederea gestionării riscurilor care pot afecta atingerea obiectivelor specifice structurilor din cadrul institutiei.

**3.3. Listarea compartimentelor furnizoare de date și/sau beneficiare de rezultate ale activității procedurate; listarea compartimentelor implicate în procesul activității:**

- Compartiment Resurse Umane;
- Compartiment Juridic;
- Compartiment Statistica și Informatica medicala;
- Compartiment de Prevenire a Infectiilor Asociate Asistentei Medicale (CPIAAM);
- Biroul Managementul Calitatii;
- Bloc Alimentar;
- Compartiment Administrativ;
- Birou Financiar Contabil;
- Compartiment Achizitii Publice Contractare;
- Ambulatoriu integrat:
  - Cabinet Neurologie;
  - Cabinet Recuperare Medicală fizică și Balneologie;
- Secția spitalizare continuă:
  - Secția Recuperare Neuromotorie;
  - Compartiment Recuperare Neuropsihomotorie copii;
  - Compartiment Terapie ocupațională și Ergoterapie;
  - Compartiment Psihologie și Logopedie;
  - Laborator Recuperare Medicală și Balneologie (baza de tratament);
  - Alte structuri – Spălatoria.

**4. Documente de referință (reglementări) aplicabile activității procedurate:**

**4.1. Reglementări internaționale:**

- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE - Regulamentul general privind protecția datelor;
- SR ISO 27001:2018 - Tehnologia Informației; Tehnici de securitate. Cerințe pentru un sistem de management al securității informației.

**4.2. Legislație primara:**

- Legea nr. 129/2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

**4.3. Legislație secundară:**

- Ordinul nr. 600 din 20 aprilie 2018 privind aprobarea Codului controlului intern managerial al entităților publice.

**4.4. Alte documente, inclusiv reglementări interne ale entității publice:**

- Regulamentul de Organizare si Functionare;
- Regulamentul Intern;
- Fisa postului;
- Alte regulamente, diagrame de proces, etc.

**5. Definiții și abrevieri ale termenilor utilizați în procedura operationala:**

**5.1.Definiții ale termenilor**

***Procedură documentată*** - modul specific de realizare a unei activități sau a unui proces, editat pe suport hârtie sau în format electronic; procedurile documentate pot fi proceduri de sistem și proceduri operaționale.

***Procedura de sistem*** *(procedură generală)* - descrie un proces sau o activitate care se desfășoară la nivelul entității publice aplicabil/aplicabilă majorității sau tuturor compartimentelor

***Proces*** - un flux de activități sau o succesiune de activități logic structurate, organizate în scopul atingerii unor obiective definite, care utilizează resurse, adăugându-le valoare.

***Editie procedura*** - forma actuala a procedurii; editia unei proceduri se modifica atunci cand deja au fost realizate 3 revizii ale respectivei proceduri sau atunci cand modificarile din structura procedurii depasesc 50% din continutul reviziei anterioare

***Revizie procedura*** - actiunea de modificare, respectiv adaugare sau eliminare a unor informatii, date, componente ale unei editii a unei proceduri, modificari ce implica, de regula, sub 50% din continutul procedurii

***Gestionarea documentelor*** - procesul de administrare a documentelor unei entitati publice, pentru a servi intereselor acesteia, pe parcursul intregii lor durate de viata, de la inceput, prin procesul de creare, revizuire, organizare, stocare, utilizare, partajare, identificare, arhivare si pana la distrugerea lor.

***Suport informatic*** - termen general care desemnează mijloacele de înregistrare magnetice, optice sau alte modalități de înregistrare a informațiilor și a căror caracteristică esențială este capacitatea mare de stocare, ștergere, copiere și modificare rapidă și facilă a informațiilor – stik-uri de memorie, CD, HD

***Document electronic*** - document a cărui gestionare se face pe suport informatic.

***Fișier electronic*** - unitate logică și fizică de gestionare a datelor pe suport informatic, care grupează datele pe baza unor caracteristici logice comune.

***Sistem de gestiune a fișierelor*** - aplicații informatice/părți componente ale sistemelor de operare ce oferă suport utilizatorilor în operațiile curente efectuate cu fișiere: creare, actualizare, consultare, ștergere, arhivare.

***Destinații (destinatari) de difuzare*** - locații sau persoane (compartimente/birouri/servicii, funcții) care au acces la un document fie pentru gestionare, fie numai pentru consultare (citire).

***Operator*** – potrivit art. 4 din Regulamentul general privind protecția datelor, înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

***Operatori asociați*** - potrivit art. 26 din Regulamentul (UE) 2016/679, în cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor

care le revin în temeiul Regulamentului, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la articolele 13 și 14, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

***Persoana împuternicită de operator*** - potrivit art. 4 din Regulamentul (UE) 2016/679, înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

***Persoană vizată*** - orice persoană ale cărei date sunt colectate, reținute sau procesate.

### 5.2.Abrevieri ale termenilor

| Nr. Crt. | Abrevierea | Termenul abreviat |
|---|---|---|
| 1. | PO | Procedura operaționala |
| 2. | IL | Instructiune de lucru |
| 3. | E | Elaborare |
| 4. | RI | Regulament Intern |
| 5. | FP | Fisa de post |
| 6. | DCP | Date cu caracter personal |
| 7. | ANSPDCP | Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal |
| 8. | GDPR | General Data Protection Regulation - Regulamentul general privind protecția datelor |

## 6. Descrierea procedurii operaționale:

### 6.1. Generalitati

Managementul riscului reprezintă un element al sistemului de control intern, cu ajutorul căruia sunt descoperite riscurile semnificative din cadrul entității, scopul final fiind menținerea acestor riscuri la un nivel acceptabil.

Principalele obiective ale managementului riscului sunt:

- să mențină amenințările în limitele acceptabile;
- să ia decizii adecvate de exploatare a oportunităților;
- să contribuie la îmbunătățirea performanțelor.

Managementul riscurilor este un ciclu continuu de:

- **Clarificare a obiectivelor** – stabilirea obiectivelor legate de domeniul de activitate, actele normative subsecvente, regulamentele şi politicile interne;
- **Identificare a riscurilor** – examinarea amenințărilor cu care se confruntă entitatea şi a vulnerabilității acesteia;
- **Evaluare a riscurilor** – riscurile la care este supusă entitatea sunt evaluate din perspectiva probabilității producerii unui eveniment nedorit, împreună cu consecințele anticipate;

- **Abordare a riscurilor, tratarea** – se identifică şi se implementează măsuri/soluţii pentru a reduce probabilitatea şi impactul unui eveniment nedorit (risc);
- **Revizuire, Monitorizare şi Raportare a riscurilor** – se face o evaluare a eficacităţii măsurilor/soluţiilor şi se identifică şi prioritizează acţiuni de corecţie necesare.

Managementul eficient al riscurilor îmbunătăţeşte performanţa proceselor/activităţilor entităţii publice, contribuind la:

- mai mare siguranţă şi mai puţine incertitudini (în efectuarea sarcinilor);
- furnizarea de servicii mai bune;
- management mai eficient al schimbării;
- utilizarea mai eficientă a resurselor;
- management mai bun la toate nivelele companiei printr-un proces decizional îmbunătăţit, datorat unei mai bune informări;
- reducerea pierderilor;
- cheltuire mai eficientă a resurselor financiare.

Conform Paragrafului 75 din Regulamentul UE: Riscul pentru drepturile și libertățile persoanelor fizice, prezentând grade diferite de probabilitate de materializare și de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală. Exemplificarea a ceea ce se înțelege prin „prejudicii de natură materială sau morală„ este:

- discriminare;
- furt sau fraudă a identității;
- pierdere financiară;
- compromiterea reputației;
- pierderea confidențialității datelor cu caracter personal protejate prin secret profesional;
- inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială;
- privare de drepturi și libertăți;
- împiedicarea exercitării controlului asupra datelor lor cu caracter personal;
- dezvăluirea originii rasială sau etnică, opiniilor politice, religiei sau convingerilor filozofice, apartenența sindicală;
- sunt prelucrate date genetice, date privind sănătatea sau date privind viața sexuală sau privind condamnările penale și infracțiunile sau măsurile de securitate conexe;
- profilare : sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările;
- sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.

Conform Art. 32: La evaluarea nivelului adecvat de securitate, se ține seama în special de **riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod**.

Conform Paragrafului 76: **Probabilitatea** de a se materializa și **gravitatea riscului** pentru drepturile și libertățile persoanei vizate ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal. Riscul ar trebui apreciat pe baza unei evaluări obiective prin care se stabilește dacă operațiunile de prelucrare a datelor prezintă un **risc** sau un **risc ridicat**. Totodata, **un risc devine „ridicat„ în funcție de probabilitate și gravitate prin referire la natura, domeniul de aplicare, contextul și scopurile prelucrării.**

**6.1.1. Clarificarea obiectivelor**

Institutia se poate confrunta zilnic cu riscuri provenite din zone variate și în diferite domenii, cum ar fi: domeniul financiar, al resurselor umane, în relații cu clienții etc.. Modul în care aceste riscuri sunt identificate, abordate și gestionate are o importanță majoră pentru succesul organizațional.

Politica de management al riscului la nivelul institutiei este de a adopta cele mai bune practici de identificare, evaluare, tratare și control eficient al riscurilor asociate obiectivelor generale și specifice, pentru a se asigura că acestea sunt reduse la un nivel acceptabil, care nu afectează modul de funcționare a instituției sau calitatea serviciilor furnizate.

Riscurile sunt identificate și definite în raport cu obiectivele a căror realizare este afectată de materializarea riscurilor. Din această cauză, existența unui sistem de obiective clar definite în institutie, de către toate compartimentele/birourile/serviciile, constituie premisa esențială pentru identificarea și definirea riscurilor.

Obiectivele generale în ceea ce privește managementul riscurilor sunt: înțelegerea riscurilor, identificarea (determinarea), evaluarea, tratarea, monitorizarea și raportarea acestora, precum și respectarea dispozițiilor legale privitoare la protecția datelor cu caracter personal și punerea în aplicare a măsurilor tehnice și organizatorice de protejare a tuturor operațiunilor care privesc în mod direct sau indirect datele cu caracter personal și care previn prelucrările neautorizate sau ilegale, precum și pierderile sau distrugerile accidentale sau ilegale.

Obiectivele specifice sunt determinate de fiecare compartiment/birou/serviciu în parte din entitate.

**6.1.2. Identificarea riscurilor**

Procesul de identificare a riscurilor este primul pas în demersul activității de *Management al riscului.* Acesta își propune să descopere toate sursele posibile de risc, cu scopul eliminării sau diminuării probabilității și efectelor (impactului) pe care acestea le pot produce. Astfel, după stabilirea obiectivelor generale, obiectivelor specifice și a activităților aferente, structurile din cadrul entității publice își identifică vulnerabilitățile (punctele slabe interne/de la nivelul institutiei, care pot cauza apariția riscurilor) și a amenințările (care vin din exteriorul instituției).

***Identificarea riscurilor este un proces permanent, care se realizează, în funcție de gradul de maturitate și experiența entității institutiei în procesul de management al riscurilor.***

Pentru a gestiona riscurile în instituție este necesar, mai întâi, ca acestea să fie cunoscute, adică identificate. Identificarea riscurilor constituie primul pas în construirea profilului riscurilor. Pentru obiectivele stabilite se documentează activități/ acțiuni de realizare a acestora și riscuri care pot să apară în derularea lor.

Un risc identificat poate avea semnificație pentru mai multe obiective, iar probabilitatea/ impactul său poate varia în funcție de fiecare obiectiv în parte.

La nivelul unui compartiment/serviciu/birou riscurile specifice, inclusiv de prelucrare a DCP, se identifică de către fiecare angajat, având la bază Formularul de Alertă la risc.

### 6.1.3. Evaluarea riscurilor

Conform Art. 35 din regulamentul UE, având în vedere **natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat** pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. Reformulând: facem evalurea riscurilor. Dacă rezultă riscuri ridicate trebuie să facem și evaluarea impactului operațiunilor de prelucrare. Aceasta se face în 3 cazuri:

(a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10; sau

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

Scopul evaluării riscurilor este de a stabili o ierarhie a acestora la nivelul institutiei care, în funcție de tolerabilitatea la risc acceptată, permite stabilirea celor mai adecvate modalităţi de tratare a riscurilor şi de delegare a responsabilităţii de gestionare a acestora.

Evaluarea riscurilor presupune parcurgerea următoarelor etape:

- Evaluarea probabilităţii de materializare a riscului identificat;
- Evaluarea impactului asupra obiectivelor în cazul în care riscul s-ar materializa;
- Evaluarea expunerii la risc, ca o combinaţie între probabilitate şi impact;
- Stabilirea toleranţei la risc.

Parametrului **„Probabilitate de manifestare a riscului"** îi poate fi atribuită una dintre valorile „scăzută - medie - ridicată".

Evaluarea probabilităţii manifestării riscului sau a frecvenţei cu care s-ar putea manifesta riscul ar trebui să fie bazată pe cunoştinţele, pe experienţa şi pe capacitatea de judecată a personalului, folosindu-se de tabelul următor:

| **Evaluarea probabilităţii de manifestare a riscului** | |
|---|---|
| **RISC** | **DESCRIERE** |
| Ridicat | Este foarte probabil ca riscul să se manifeste de mai multe ori în timpul desfăşurării activităţii. |
| Mediu | Există posibilitatea ca riscul să se manifeste ocazional în timpul desfăşurării activităţii. |
| Scăzut | Pare improbabil ca riscul să se manifeste în timpul desfăşurării activităţii. |

Parametrului **„Impact"** îi poate fi atribuită una dintre valorile „scăzut-moderat-ridicat".

Impactul sau gravitatea riscului este nivelul prin care manifestarea riscului poate influenţa îndeplinirea obiectivelor specifice. Poate exista, de exemplu, o pierdere de fonduri provocată, de exemplu, de evenimente precum nerespectarea legislaţiei de referinţă, fraudele, sistemele şi serviciile neadecvate, etc.

| **Evaluarea impactului riscului** | |
|---|---|
| **IMPACT** | **DESCRIERE** |
| Ridicat | Impact semnificativ asupra îndeplinirii strategiei şi obiectivelor specifice (*ex. fraude, iregularităţi sistematice, probleme de caracter juridic, pierderi semnificative de active (financiare, angajaţi, materiale), costuri ridicate de funcţionare, calitatea serviciilor furnizate este afectată semnificativ, întreruperi semnificative în activitate, etc.)* |
| Mediu | Ineficienţa operaţiunilor normale, cu efect limitat asupra îndeplinirii strategiei şi a obiectivelor specifice *(ex.: întreruperi sau ineficienţe moderate ale proceselor, probleme temporare privind calitatea/serviciul), pierderi moderate de active (financiare, angajaţi, materiale), creşterea costurilor de funcţionare este moderată, calitatea serviciilor furnizate este afectată moderat, întreruperi mici în activitate, etc.)* |
| Scăzut | Niciun impact concret asupra strategiei şi asupra obiectivelor *(ex.: nu există pierderi de active (financiare, angajaţi, materiale, costurile de funcţionare nu sunt afectate, calitatea serviciilor furnizate nu este afectată, nu există întreruperi în activitate etc. )* |

Impactul trebuie să fie analizat din perspectiva valorii bunurilor afectate, precum şi a consecinţelor mai ample.

Îmbinarea acestor evaluări prin intermediul matricei prezentate mai jos permite obţinerea unei evaluări a riscului, care poate fi clasificat după cum urmează:

- ridicat (R);
- mediu (M);
- scăzut (S).

Evaluarea riscului este efectuată folosind următoarea matrice:

| | PROBABILITATE | scăzută S (1) | medie M (2) | ridicată R (3) |
|---|---|---|---|---|
| IMPACT | ridicat R (3) | M | R | R |
| | mediu M (2) | S | M | R |
| | scăzut S (1) | S | S | M |

| **Evaluarea riscului (Nivelul riscului/Expunerea)** | |
|---|---|
| Ridicat | Nivelul de risc impune prevederea unei acţiuni imediate pentru reducerea riscului la un nivel tolerabil |
| Mediu | Este un risc care trebuie gestionat cu ajutorul unei proceduri specifice şi eficace şi care trebuie monitorizat în permanenţă |
| Scăzut | Riscul trebuie gestionat cu ajutorul unei proceduri specifice. În unele cazuri, dacă riscul este foarte scăzut, poate fi oportun chiar a nu se interveni deloc |

Evaluarea riscurilor se face de către fiecare compartiment/serviciu/birou, iar rezultatele se înregistrează în formularul „Alerta la risc".

Toleranța la risc se aprobă de către conducerea instituției.
În general, limita maximă a expunerii la riscuri reziduale, respectiv până la care este permisă asumarea riscurilor, reprezintă **valorile unui risc scăzut**.

### 6.1.4. Tratarea riscurilor

Este etapa crucială în managementul riscurilor și presupune efectuarea de pași concreți, practici pentru a gestiona și controla riscul.
Tratarea riscurilor înseamnă a acționa, prin măsuri de atenuare a probabilității, a impactului sau a ambelor.
După finalizarea etapei privind evaluarea riscurilor, pentru riscurile cu nivel de risc (expunere) mediu și/sau ridicat trebuie stabilite acțiuni (măsuri/ strategii) de minimizare a acestora, responsabili cu implementarea acțiunii (măsurii/strategiei) și data limită de implementare a acțiunii (măsurii/strategiei). Aceste informații se înscriu în formularul „Alertă la risc". Formularul „Alertă la risc", completat cu informațiile specifice la nivelul compartimentului/serviciului/biroului (descrierea riscului, evaluarea riscului, strategia adoptată), este semnat de persoana care identifică riscul, de responsabilul cu riscurile și de conducătorul de compartiment, care ia și decizia cu privire la risc.
Conform Art. 24 din Regulamentul UE, **ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate** pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar. Operatorul face asta cu ajutorul responsabilului cu securitatea datelor (informatician sau o firma IT) care, printre altele, furnizează consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia.

### 6.1.5 Revizuirea riscurilor

Este faza care încheie procesul de gestionare a riscurilor. Riscurile, precum și strategiile de management al riscurilor, trebuie revizuite periodic.
Revizuirea trebuie:

- să dea asigurări că toate aspectele procesului de gestionare a riscurilor sunt analizate cel puțin o dată pe an;
- să ofere asigurări că riscurile sunt supuse revizuirii cu o frecvență corespunzătoare, stabilită în raport cu mobilitatea circumstanțelor și a naturii instrumentelor de control intern ce urmează a fi implementate;
- să stabilească mecanisme de alertare ale nivelelor superioare manageriale în privința noilor riscuri sau a schimbărilor suferite de riscurile deja identificate, astfel încât aceste schimbări să fie abordate corespunzător.

### 6.1.6 Monitorizarea riscurilor

**Monitorizarea permanentă a riscurilor** - acest tip de răspuns la risc constă în **acceptarea riscului cu condiția menținerii sale sub o permanenta supraveghere**. Probabilitatea este parametrul supravegheat cu precădere, deoarece **strategia monitorizării se aplica în cazul riscurilor cu impact semnificativ**, dar cu probabilitate mică de apariție.
***Orice risc care este acceptat, monitorizat sau tratat - trebuie însoțit de măsuri de control intern***, *care să descrie acțiunile ce trebuie întreprinse în cazul în care riscurile se materializează.*
Măsurile de control privind gestionarea riscurilor trebuie să asigure un nivel acceptabil, respectiv toleranța la risc.

După aplicarea măsurilor de control, riscul rezidual (riscul rămas din riscul inerent) trebuie să se încadreze în toleranță la risc.

**Monitorizarea măsurilor de control se realizează astfel:**

a) **Pentru compartimentele din cadrul entității publice** - periodic, în funcție de tipurile de risc; în acest caz responsabilii cu riscurile raportează superiorului ierarhic al structurii, riscurile identificate în Registrul de riscuri pe compartiment.
b) **Pentru *planul de implementare a măsurilor de control* de la nivelul entității** publice - se realizează anual; în acest caz responsabilii cu riscurile raportează conducătorului compartimentului și Responsabilului de protecția DCP, in cazul prelucrării DCP riscurile semnificative/strategice identificate în Registul de riscuri pe entitate.

După elaborarea registrului de riscuri pe entitate, pe baza profilului de risc şi prin stabilirea tipului de strategie se întocmeşte un **Plan de implementare a măsurilor de control, aferent riscurilor semnificative/strategice în cadrul entității publice .**

**Planul de măsuri cuprinde:**

- denumirea riscului
- măsurile de control
- termenele de implementare
- responsabilii cu implementarea măsurilor de control

*Notă:* Planul de măsuri ar trebui să cuprindă inclusiv recomandările cu privire la măsurile de control, cuprinse în rapoartele de audit (structura internă de audit; Curtea de Conturi; Autoritatea de audit; structurile de audit ale Comisiei Europene).

După întocmirea Planului de implementare a măsurilor de control acesta, împreună cu Formularul de alertă la risc ce stă la baza lui, se va transmite pentru aprobare conducerii instituției.
**Procesul de monitorizare vizează stabilirea stadiului implementării măsurilor** prevăzute în **Planul de implementare a măsurilor de control** prin Fişele de urmărire a riscurilor

**6.1.7 Raportarea riscurilor**

Rezultatele revizuirilor trebuie raportate pentru a se asigura monitorizarea continuă a situației riscurilor şi pentru a sesiza schimburile majore care impun modificarea priorităților.

- Principala acțiune necesarăa în această fază este completarea „Registrului de riscuri" de către fiecare compartimentelor /serviciilor/ birourilor.

**Anexa 5** la prezenta procedură, prin preluarea din Planul de implementare a măsurilor de control, a tuturor riscurilor şi datelor necesare.
Registrele de riscuri aferente compartimentelor de specialitate se transmit la Secretariatul tehnic CIM pentru centralizare în Registrul de riscuri al institutiei, cel puțin o dată pe an.
Registrul de riscuri aferente prelucrării datelor cu caracter personal este ținut de către Responsabilul cu protecția DCP.

**6.2. Documente utilizate**

**Lista şi proveniența documentelor**

- Nomenclatorul arhivistic.

**Conținutul şi rolul documentelor**

- Continutul documentelor este prezentat la prezenta procedura.

**Circuitul documentelor**

- Grafic de circulatie a documentelor aprobat la nivel de institutie.

**6.3. Resursele necesare**

**Resurse materiale**

- conform Necesarului de materiale - stabilit.

**Resurse umane**

- conform organigramei entitatii.

**Resurse financiare**

- planificarea activităţilor se realizează pe baza Bugetului de venituri şi cheltuieli.
- determinarea fondurilor necesare se face anual - în trimestrul IV al anului în curs pentru anul următor.

**7. Responsabilităţi şi răspunderi în derularea activităţii:**

**7.1. Manager spital**

- Dispune monitorizarea riscurilor către toate compartimentele/serviciile/birourile.
- Dispune alocarea resurselor necesare pentru realizarea obiectivelor.
- Aprobă Profilul de risc şi limita de toleranţă a riscurilor.
- Aprobă Măsuri tehnice şi organizatorice.
- Aprobă Planul de implementare a măsurilor de control.

**7.2. Responsabilii de riscuri din cadrul institutiei:**

- Elaborează "Lista obiectivelor, activităţilor şi riscurilor" la nivelul compartimentelor /serviciilor/ birourilor.
- Colectează riscurile aferente activităţilor.
- Identifică strategia de risc.
- Elaborează Registrul de riscuri la nivelul compartimentelor din primul nivel de conducere.
- Propune măsuri de control şi monitorizează implementarea acestora, după ce în prealabil acestea au fost aprobate de către conducătorul compartimentului.
- Completează formularul de Alertă la risc de la nivelul compartimentelor /serviciilor/ birourilor după semnalarea riscului.
- Elaborează "Planul de implementare a măsurilor de control" la nivelul compartimentelor/ serviciilor/ birourilor.

**7.3. Responsabilul de protecţia DCP**

- să furnizeze consiliere la cerere în ceea ce priveşte evaluarea impactului asupra protecţiei datelor şi să monitorizeze funcţionarea acesteia, în conformitate cu art. 35 din Regulamentul (UE) 679/2016;
- să acorde avizul solicitat de conducerea instituţiei în legătură cu următoarele aspecte:

1. dacă să efectueze sau nu evaluarea impactului asupra protecţiei datelor;
2. ce metodologie să fie folosită la efectuarea evaluării impactului asupra protecţiei datelor;
3. dacă să efectueze intern sau să externalizeze evaluarea impactului asupra protecţiei datelor;
4. ce garanţii (inclusiv măsuri tehnice şi organizaţionale) să pună în aplicare pentru reducerea oricăror riscuri la adresa drepturilor şi intereselor persoanelor vizate;

5. dacă evaluarea impactului asupra protecției datelor a fost sau nu efectuată corect și dacă respectivele concluzii (dacă să continue sau nu prelucrarea și ce garanții să pună în aplicare) respectă Regulamentul (UE) 2016/679;
6. să prioritizeze activitățile sale și să-și concentreze eforturile asupra problemelor care prezintă riscuri mai mari pentru protecția datelor.
7. să participe la ședințele Comisiei de monitorizare.

## 8. Formular evidență modificări:

| Nr. Crt. | Editie | Data editiei | Revizie | Data reviziei | Nr. pagina modificata | Descriere modificare | Semnatura responsabil compartiment |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | I | | 0 | | | Procedura a fost elaborata in conf. Cu Ord. 600/2018 | |

## 9. Formular analiză procedură:

| Nr. crt | Compartiment | Nume si prenume responsabil compartiment | Inlocuitor de drept sau delegat | Aviz favorabil | | Aviz nefavorabil | | |
|---|---|---|---|---|---|---|---|---|
| | | | | *Data* | *Semnatura* | *Observatii* | *Data* | *Semnatura* |
| 1. | SCIM | DR. MANC DANIELA | | 08.02 2022 | | | | |
| 2. | | | | | | | | |
| 3. | | | | | | | | |
| 4. | | | | | | | | |

**10. Formular distribuire procedură:**

| Nr. Crt. | Scopul difuzării | Compartiment | Funcţia | Nume şi prenume | Data primirii | Data retragerii | Semnătură |
|---|---|---|---|---|---|---|---|
| 10.1. | informare | Secretariat SCIM | | CRIŞTEA L. | 08.02.2022 | | |
| 10.2. | aplicare | Servicii externalizate | | NUMEA A. | 08.02.2022 | | |
| 10.3. | evidenta | Secretariat SCIM | | CRIŞTEA L. | 08.02.2022 | | |
| 10.4. | arhivare | Secretariat SCIM | | CRIŞTEA L. | 08.02.2022 | | |

**11. Anexe:**

- Conform legislatiei in vigoare.

**12. Diagrama de proces**