

**S.R.L “CloudSentinel”**

**EVALUAREA RISCURILOR ȘI METODOLOGIA DE TRATARE A RISCURILOR**

|  |  |
| --- | --- |
| Cod: | ERMTR-01 |
| Versiune: | 0.4.1a |
| Data versiunii: | Jun 5, 2024 |
| Creat de: | Chirita Stanislav |
| Aprobat de: | Boboc Sandu |
| Nivelul de confidențialitate: | Confidențial |

**Istoricul modificărilor**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 2024-01-15 | 0.1.0 | Chihai Adrian | Schița documentului de bază |
| 2024-01-20 | 0.2.6d | Vozian Vladimir | Niveluri de confidențialitate adăugate |
| 2024-01-25 | 0.3.1 | Chirita Stanislav | Politica revizuită de criptare a datelor |
| 2024-02-05 | 0.4.1 | Vozian Vladimir | Măsuri de control al accesului actualizate |
| 2024-02-10 | 0.4.1a | Boboc Sandu | Revizuirea finală și aprobarea |

**Cuprins**

[1. Scop, domeniu de aplicare și utilizatori 3](#__RefHeading___Toc1408_4092408322)

[2. Documentele de referință 3](#__RefHeading___Toc1410_4092408322)

[3. Evaluarea Riscurilor și Metodologia de Tratare a Riscurilor 3](#__RefHeading___Toc1412_4092408322)

[3.1. Evaluarea riscurilor 3](#__RefHeading___Toc1414_4092408322)

[3.1.1. Procesul 3](#__RefHeading___Toc1416_4092408322)

[3.1.2. Active, vulnerabilități și amenințări 3](#__RefHeading___Toc1418_4092408322)

[3.1.3. Determinarea proprietarilor de risc 4](#__RefHeading___Toc1420_4092408322)

[3.1.4. Consecințe și probabilitate 4](#__RefHeading___Toc1422_4092408322)

[3.2. Criterii de acceptare a riscului 5](#__RefHeading___Toc1424_4092408322)

[3.3. Gestionarea riscurilor 5](#__RefHeading___Toc1426_4092408322)

[3.4. Revizuiri periodice ale evaluării riscurilor și ale tratamentului riscurilor 6](#__RefHeading___Toc1428_4092408322)

[3.5. Declarația de Aplicabilitate și Planul de tratare a riscurilor 6](#__RefHeading___Toc1430_4092408322)

[3.6. Raportare 6](#__RefHeading___Toc1432_4092408322)

[4. Gestionarea înregistrărilor păstrate pe baza acestui document 7](#__RefHeading___Toc1434_4092408322)

[5. Valabilitatea și managementul documentelor 8](#__RefHeading___Toc1436_4092408322)

[6. Anexe 8](#__RefHeading___Toc1438_4092408322)

# Scop, domeniu de aplicare și utilizatori

Scopul acestui document este de a defini metodologia pentru evaluarea și tratarea riscurilor de informații în CloudSentinel și de a defini nivelul acceptabil de risc conform standardului ISO/IEC 27001. Evaluarea riscurilor și tratarea riscurilor se aplică întregului domeniu al Sistemului de Management al Securității Informațiilor (ISMS), adică tuturor activelor care sunt utilizate în cadrul organizației sau care ar putea avea un impact asupra securității informațiilor în cadrul ISMS. Utilizatorii acestui document sunt toți angajații CloudSentinel care participă la evaluarea și tratarea riscurilor.

# Documentele de referință

* **Standardul ISO/IEC 27001, clauzele 6.1.2, 6.1.3, 8.2 și 8.3**
* **Politica de Securitate a Informațiilor CloudSentinel**
* **Lista Cerințelor Legale, Reglementare, Contractuale și Alte Cerințe pentru CloudSentinel**
* **Politica de Securitate a Furnizorilor CloudSentinel**
* **Declarația de Aplicabilitate CloudSentinel**
* **NIST SP 800-53 Revision 5 -** Security and Privacy Controls for Information Systems and Organizations
* **NIST SP 800-145 -** The NIST Definition of Cloud Computing
* **NIST SP 500-292 -** NIST Cloud Computing Reference Architecture
* **NIST SP 800-190 -** Application Container Security Guide

# Evaluarea Riscurilor și Metodologia de Tratare a Riscurilor

## Evaluarea riscurilor

### Procesul

Procesul de evaluare a riscurilor este implementat prin Tabelul de Evaluare a Riscurilor. Procesul de evaluare a riscurilor este coordonat de către responsabilul de securitate informațională(CISO), identificarea amenințărilor și vulnerabilităților este realizată de către proprietarii de active, iar evaluarea consecințelor și probabilității este realizată de către proprietarii de riscuri.

### Active, vulnerabilități și amenințări

Primul pas în evaluarea riscurilor constă în identificarea tuturor activelor din domeniul de aplicare al Sistemului de Management al Securității Informațiilor (ISMS) - adică a tuturor activelor care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor în cadrul organizației. Activele pot include documente în format fizic sau electronic, aplicații și baze de date, persoane, echipamente IT, infrastructură și servicii externe/procese externalizate. În momentul identificării activelor, este de asemenea necesar să se identifice proprietarii acestora - persoana sau unitatea organizațională responsabilă pentru fiecare activ." "Următorul pas este identificarea tuturor amenințărilor și vulnerabilităților asociate fiecărui activ. Amenințările și vulnerabilitățile sunt identificate folosind cataloagele incluse în Tabelul de Evaluare a Riscurilor. Fiecare activ poate fi asociat cu mai multe amenințări, iar fiecare amenințare poate fi asociată cu mai multe vulnerabilități.

### Determinarea proprietarilor de risc

Pentru fiecare risc, trebuie identificat un proprietar de risc - persoana sau unitatea organizațională responsabilă pentru fiecare risc. Această persoană poate sau nu să fie aceeași cu proprietarul activului.

### Consecințe și probabilitate

Odată ce proprietarii de risc au fost identificați, este necesar să se evalueze consecințele pentru fiecare combinație de amenințări și vulnerabilități pentru un activ individual dacă se materializează un astfel de risc:

|  |  |  |
| --- | --- | --- |
| Consecinţă scăzută | 0 | Pierderea confidențialității, disponibilității sau integrității nu afectează fluxul de numerar al organizației, obligațiile legale sau contractuale sau reputația acesteia. |
| Consecinţă moderată | 1 | Pierderea confidențialității, disponibilității sau integrității implică costuri și are un impact redus sau moderat asupra obligațiilor legale sau contractuale sau asupra reputației organizației. |
| Consecinţă ridicată | 2 | Pierderea confidențialității, disponibilității sau integrității are un impact considerabil și/sau imediat asupra fluxului de numerar, operațiunilor, obligațiilor legale sau contractuale ale organizației sau reputației acesteia. |

După evaluarea consecințelor, este necesar să se evalueze probabilitatea apariției unui astfel de risc, adică probabilitatea ca o amenințare să exploateze vulnerabilitatea activului respectiv:

|  |  |  |
| --- | --- | --- |
| Probabilitate scăzută | 0 | Controalele de securitate existente sunt puternice și au oferit până în prezent un nivel adecvat de protecție. Nu se așteaptă noi incidente în viitor. |
| Probabilitate moderată | 1 | Controalele de securitate existente sunt moderate și au oferit în cea mai mare parte un nivel adecvat de protecție. Noi incidente sunt posibile, dar nu foarte probabile. |
| Probabilitate ridicată | 2 | Controalele de securitate existente sunt scăzute sau ineficiente. Astfel de incidente au o probabilitate mare de a se produce în viitor. |

Prin introducerea valorilor de consecință și probabilitate în Tabelul de Evaluare a Riscurilor, nivelul de risc se calculează automat prin adăugarea celor două valori. Controalele de securitate existente trebuie introduse în ultima coloană a Tabelului de Evaluare a Riscurilor.

## Criterii de acceptare a riscului

Valorile 0, 1 și 2 sunt riscuri acceptabile, în timp ce valorile 3 și 4 reprezintă riscuri inacceptabile. Riscurile inacceptabile trebuie tratate.

## Gestionarea riscurilor

Tratarea riscurilor se implementează prin Tabelul de Tratare a Riscurilor, prin copierea tuturor riscurilor identificate ca fiind inacceptabile din Tabelul de Evaluare a Riscurilor. Tratarea riscurilor este efectuată de Manager de Riscuri și Securitate.

Una sau mai multe opțiuni de tratament trebuie selectate pentru riscurile evaluate cu 3 și 4:

1. Selecția unui control sau a unor controale de securitate din Anexa A a standardului ISO/IEC 27001 sau a altor controale de securitate
2. Transferarea riscurilor către o terță parte - de exemplu, prin achiziționarea unei polițe de asigurare sau semnarea unui contract cu furnizori sau parteneri
3. Evitarea riscului prin întreruperea unei activități de afaceri care cauzează un astfel de risc
4. Acceptarea riscului - această opțiune este permisă numai dacă selecția altor opțiuni de tratare a riscurilor ar costa mai mult decât impactul potențial dacă un astfel de risc s-ar materializa

Selectarea opțiunilor este implementată prin Tabelul de Tratare a Riscurilor. De obicei, opțiunea 1 este selectată: selectarea unuia sau a mai multor controale de securitate. Atunci când sunt selectate mai multe controale de securitate pentru un risc, sunt inserate rânduri suplimentare în tabel imediat sub rândul care specifică riscul.

Tratarea riscurilor legate de procesele externalizate trebuie abordată prin contractele cu terțe părți responsabile, conform specificațiilor din Politica de Securitate a Furnizorilor.

În cazul opțiunii 1 (selectarea controalelor de securitate), este necesară evaluarea noii valori a consecinței și probabilității în Tabelul de Tratare a Riscurilor, pentru a evalua eficacitatea controalelor planificate.

## Revizuiri periodice ale evaluării riscurilor și ale tratamentului riscurilor

Deținătorii de riscuri trebuie să revizuiască riscurile existente și să actualizeze Tabelul de Evaluare a Riscurilor și Tabelul de Tratare a Riscurilor în conformitate cu riscurile nou identificate. Revizuirea se efectuează cel puțin o dată pe an sau mai frecvent în cazul unor schimbări organizaționale semnificative, schimbări semnificative în tehnologie, schimbarea obiectivelor de afaceri, schimbări în mediul de afaceri, etc.

## Declarația de Aplicabilitate și Planul de tratare a riscurilor

Responsabilul de Securitate a Informațiilor trebuie să documenteze următoarele în Declarația de Aplicabilitate: care controale de securitate din Anexa A a standardului ISO/IEC 27001 sunt aplicabile și care nu sunt, justificarea pentru astfel de decizii și dacă acestea sunt implementate sau nu.

Din partea proprietarilor de riscuri, managementul de top va accepta toate riscurile reziduale prin intermediul Declarației de Aplicabilitate. Responsabilul de Securitate a Informațiilor va pregăti Planul de Tratare a Riscurilor în care va fi planificată implementarea controalelor. Din partea proprietarilor de riscuri, managementul de top va aproba Planul de Tratare a Riscurilor.

## Raportare

Responsabilul de Securitate a Informațiilor va documenta rezultatele evaluării riscurilor și tratamentului acestora, precum și toate revizuirile ulterioare, în Raportul de Evaluare și Tratare a Riscurilor.

Managerul de Securitate a Informațiilor va monitoriza progresul implementării Planului de Tratare a Riscurilor și va raporta rezultatele către Managerul de Riscuri și Securitate în fiecare lună."

# Gestionarea înregistrărilor păstrate pe baza acestui document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nume înregistrare | Locația de stocare | Persoana responsabilă pentru stocare | Control pentru protecția înregistrării | Perioada de reținere |
| Tabel de Evaluare a Riscurilor | Calculatorul Analistului de Securitate | Managerul de Securitate a Informațiilor | Acces controlat exclusiv pentru Managerul de Securitate a Informațiilor | Permanent |
| Tabel de Tratare a Riscurilor | Calculatorul Specialistului în Gestionarea Riscurilor | Responsabilul de Gestionare a Riscurilor | Acces controlat exclusiv pentru Responsabilul de Gestionare a Riscurilor | Permanent |
| Raport de Evaluare și Tratare a Riscurilor | Calculatorul Ofițerului de Securitate a Informațiilor | Managerul de Riscuri și Securitate | Raportul este pregătit în format PDF doar pentru citire | 3 ani |
| Declarație de Aplicabilitate | Calculatorul Directorului Departamentului de Securitate a Informațiilor | Directorul Departamentului de Securitate a Informațiilor | Acces controlat exclusiv pentru Directorul Departamentului de Securitate a Informațiilor | 3 ani |
| Plan de Tratare a Riscurilor | Calculatorul Managerului de Securitate a Informațiilor | Managerul de Securitate a Informațiilor | Acces controlat exclusiv pentru Managerul de Securitate a Informațiilor | 3 ani |

Doar Managerul de Securitate a Informațiilor poate acorda altor angajați acces la oricare dintre documentele menționate mai sus.

# Valabilitatea și managementul documentelor

Acest document este valabil începând cu 01.01.2025.

Proprietarul acestui document este Boboc Sandu(Responsabilul de Securitate a Informațiilor), care trebuie să verifice și, dacă este necesar, să actualizeze documentul cel puțin o dată pe an, înainte de revizuirea periodică a evaluării riscurilor existente.

Atunci când se evaluează eficacitatea și caracterul adecvat al acestui document, trebuie luate în considerare următoarele criterii:

• numărul incidentelor care au avut loc, dar care nu au fost incluse în evaluarea riscurilor

• numărul de riscuri care nu au fost tratate în mod corespunzător

• numărul de erori în procesul de evaluare a riscurilor și de tratare a riscurilor din cauza definiției neclare a rolurilor și responsabilităților

# Anexe

* Anexa 1: Formular - Tabel de Evaluare a Riscurilor
* Anexa 2: Formular - Tabel de Tratare a Riscurilor
* Anexa 3: Formular - Raport de Evaluare și Tratare a Riscurilor

Responsabilul de Securitate a Informațiilor

Boboc Sandu

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Semnătura