APLICABILITATEA ISO/IEC27014:2020 ÎN SISTEMELE INFORMAȚIONALE DIN DOMENIUL SĂNĂTĂȚII

Adrian STOICA

Departamentul Ingineria Software și Automatică, grupa SI-231M, Facultatea Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei, Chișinău, Republica Moldova

Autorul corespondent : Adrian STOICA, adrian.stoica@isa.utm.md

Coordonator științific: **Rodica BULAI**, Departamentul Ingineria Software și Automatică, Facultatea Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei, Chișinău, Republica Moldova

Rezumat: *În contextul "Strategia de transformare digitală a Republicii Moldova pentru anii 2023–2030, doar pentru anul 2024 sunt planificate de a fi puse în etapa pilot 3 sisteme informaționale (e-Reteta, SBTESP, eCMCD). Din aceste considerente, dar și în contextul recentului atac cibernetic asupra infrastructurii informaționale medicale din România și nu numai, implementarea standardului ISO/IEC 27014:2020 în cadrul instituțiilor medicale din Republica Moldova reprezintă o necesitate strategică vitală privind asigurarea securității informațiilor din domeniul sănătății. Articolul prezintă un cadru robust în baza standardului sus-menționat privind gestionarea securității informațiilor, într-un context în care sistemele informaționale medicale devin tot mai atractive pentru dezvoltare. Implementarea standardului implică evaluarea riscurilor, dezvoltarea politicilor și procedurilor de securitate, formarea personalului și monitorizarea constantă a conformității. Astfel, se asigură protejarea datelor medicale sensibile și menținerea încrederii pacienților în sistemele de sănătate digitalizate.*

Cuvinte cheie: *iso/iec 27014:2020, securitatea informațiilor, domeniul medical, strategie de digitalizare.*

Introducere

Trecerea la o capacitate și o integrare tehnologică îmbunătățită reprezintă o oportunitate de a construi un viitor mai bun și mai interconectat, având în vedere „noua normalitate"[1]. În cadrul articolului este analizat standardul ISO/IEC 27014:2020, elaborat pentru a oferi un cadru organizațiilor în ceea ce privește guvernanța și managementul securității informațiilor [2]. Acest standard se concentrează pe aspectele de conducere și strategie, punând accentul pe importanța luării deciziilor corecte și implementării unei abordări eficiente pentru securitatea informațiilor în cadrul organizațiilor. Este un complement al standardului ISO/IEC 27001:2022 și poate fi implementat împreună cu acesta pentru a îmbunătăți guvernarea securității informației în organizație sau individual. În baza standardului ISO/IEC 27014:2020 se creează un model de securitate pentru instituțiile medicale. Modelul creat este implementat în Instituția Medico-Sanitară Publică Asociația Medicală Teritorială Centru. Implementarea standardului ISO/IEC 27014:2020 în instituțiile medicale din Republica Moldova va contribui la consolidarea securității informațiilor și acoperirea obiectivelor de protecție ale transformării digitale și la promovarea unui mediu medical modern, sigur și eficient.

Model de Securitate conform ISO/IEC 27014:2020 în Instituțiile Medicale

Guvernarea securității informațiilor este un „sistem prin care activitățile de securitate a informațiilor unei organizații sunt direcționate și controlate" [2]. ISO/IEC 27014:2020 face parte din seria de standarde ISO/IEC 27000. „Guvernarea adecvată a securității informațiilor asigură alinierea securității informațiilor cu strategiile și obiectivele de afaceri, livrarea valorii și responsabilitatea. Sprijină atingerea vizibilității, agilității, eficienței, eficacității și conformității" [3]. Acest standard este „vizat în mod special să ajute organizațiile să-și guverneze aranjamentele

de securitate a informațiilor” [3]. Standardul oferă „îndrumare privind conceptele și principiile pentru guvernarea securității informațiilor, prin care organizațiile pot evalua, direcționa, monitoriza, comunica și asigura activitățile legate de securitatea informațiilor din cadrul organizației” și este „aplicabil tuturor tipurilor de organizații” [2]. Pentru crearea modelului sau extras elementele cheie (figura 1)

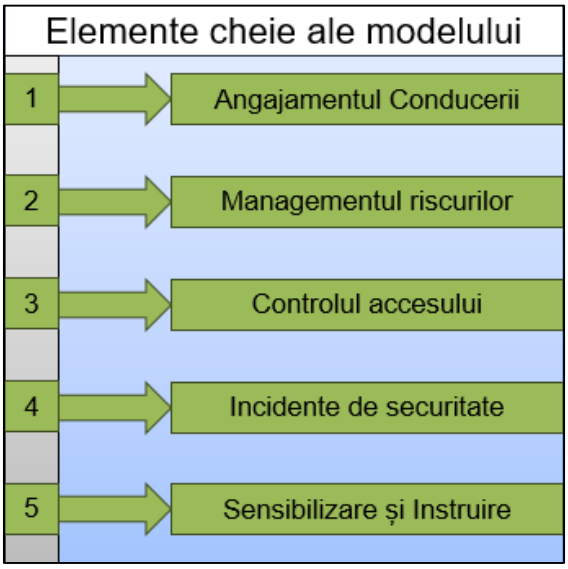

Figura 1. Elementele Cheie ale ISO/IEC 27014:2020

Fiecare element reprezintă după cum urmează :

1. Angajamentul conducerii:

- Conducerea de vârf trebuie să se angajeze activ în implementarea și menținerea modelului de securitate.
- Acest angajament se poate demonstra prin alocarea resurselor necesare, stabilirea politicilor de securitate și monitorizarea performanței.

2. Managementul riscurilor:

- Este necesară o evaluare periodică a riscurilor pentru a identifica și evalua amenințările la adresa securității informației.
- Pe baza evaluării riscurilor, se vor implementa controale adecvate pentru a reduce riscurile la un nivel acceptabil.

3. Controlul accesului:

- Accesul la datele sensibile ale pacienților trebuie să fie restricționat doar la personalul autorizat.
- Se vor implementa controale de acces, cum ar fi parolele, autentificarea multi-factor și criptarea datelor.

4. Incidente de securitate:

- Este necesară o procedură clară pentru gestionarea incidentelor de securitate.
- Procedura va include instrucțiuni pentru identificarea, raportarea și investigarea incidentelor de securitate.

5. Sensibilizare și instruire:

- Personalul trebuie instruit periodic cu privire la politicile și procedurile de securitate a informației.
- Instruirea va include informații despre amenințările la adresa securității informației, controalele de securitate și modul de raportare a incidentelor de securitate.

Pentru implementarea acestui model se propun pașii, care pot fi vizualizați în figura 2.

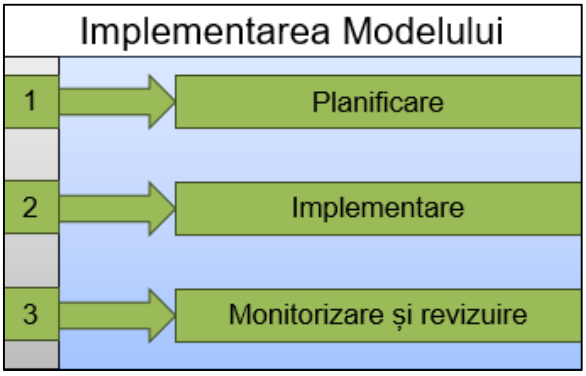

Figura 2. Pașii de implementare a modelului

Acești pași sunt descriși ca :

1. Planificare:

- Este necesară elaborarea unui plan de implementare care să definească etapele, resursele și responsabilitățile.

2. Implementare:

- Implementarea controalelor de securitate identificate în urma evaluării riscurilor.

3. Monitorizare și revizuire:

- Monitorizarea periodică a performanței modelului de securitate.
- Revizuirea periodică a modelului de securitate pentru a se asigura că este actualizat și adecvat.

Implementarea ISO/IEC 27014:2020 în IMSP AMT Centru

Instituția Medico-Sanitară Publică Asociația Medicală Teritorială Centru acordă asistenţa medicală profilactică şi curativ-diagnostică populaţiei sectorului Centru şi orăşelului Codru a municipiului Chişinău. Concomitent, acordă servicii consultative şi diagnostice la adresarea directă a populaţiei mun. Chişinău, cât şi în baza contractelor de asigurări medicale facultative încheiate cu diferite companii de asigurări sau la direct cu agenţii economici. A fost luată decizia să se implementeze ISO/IEC 27014:2020 pentru a îmbunătăți protecția datelor sensibile ale pacienților și pentru a se conforma reglementărilor din domeniul medical.

Obiectivele implementării:

- Îmbunătățirea protecției datelor sensibile ale pacienților
- Creșterea încrederii pacientului
- Respectarea reglementărilor din domeniul medical
- Reducerea costurilor asociate cu incidentele de securitate

Metodologie:

S-a format o echipă de proiect formată din reprezentanți din diferite departamente, inclusiv IT, conducerea, medici și personalul administrativ. Echipa de proiect a identificat următoarele etape:

1. **Planificare:** Echipa de proiect a elaborat un plan de implementare care a definit etapele, resursele și responsabilitățile.
2. **Evaluarea riscurilor:** A fost efectuată o evaluare a riscurilor pentru a identifica și evalua amenințările la adresa securității informației.
3. **Implementarea controalelor:** Au fost implementate controale de securitate adecvate pentru a reduce riscurile la un nivel acceptabil.
4. **Sensibilizare și instruire:** Personalul a fost instruit periodic cu privire la politicile și procedurile de securitate a informației.
5. **Monitorizare și revizuire:** Performanța modelului de securitate a fost monitorizată periodic. Modelul a fost revizuit periodic pentru a se asigura că este actualizat și adecvat.

Rezultate:

Implementarea ISO/IEC 27014:2020 a adus următoarele beneficii Instituției Medicale:

1. **Protecția sporită a datelor sensibile ale pacienților:** Accesul la datele sensibile ale pacienților este acum restricționat doar la personalul autorizat. Datele sunt criptate atât în repaus, cât și în tranzit.
2. **Creșterea încrederii pacientului:** Pacienții au acum o mai mare încredere în instituția medicală pentru a le proteja datele sensibile.
3. **Respectarea reglementărilor din domeniul medical:** IMSP AMT Centru este acum în conformitate cu reglementările din domeniul medical, cum ar fi GDPR.
4. **Reducerea costurilor asociate cu incidentele de securitate:** Implementarea controalelor de securitate a redus riscul de incidente de securitate, ceea ce a dus la o reducere a costurilor asociate cu gestionarea incidentelor.

Concluzii:

Implementarea ISO/IEC 27014:2020 este un succes pentru IMSP AMT Centru. Modelul de securitate a îmbunătățit semnificativ protecția datelor sensibile ale pacienților, a crescut încrederea pacientului și a ajutat spitalul să respecte reglementările din domeniul medical. Menționez că în cadrul instituții medicale specificate nu este prezent standardul ISO/IEC 2700:20221 și sa decis trecerea implementarea în mod individual al ISO/IEC 27014:2020, deoarece, cel din urmă este mai simplu la implementare față de ISO/IEC 27001:2022, în care este necesar de creat un sistem de management al securității informaționale (ISMS) și respectiv necesită mai puține resurse intelectuale și financiare. Un alt argument ar fi implicarea nemijlocită a conducătorului organizației. În final reieșind din faptul că sistemele informaționale care oferă acces la date personale sensibile sunt din afara instituției și nu pot fi administrate local, standardul ISO/IEC 27014:2020 este mai actual prin ghidarea în domeniul guvernării proceselor de securitate și nu implicit controlul asupra lor.

Principale lecții învățate sunt :

- Implementarea ISO/IEC 27014:2020 este un proces complex care necesită implicarea activă a conducerii de vârf.
- Este important să se realizeze o evaluare a riscurilor cuprinzătoare pentru a identifica și evalua amenințările la adresa securității informației.
- Personalul trebuie instruit periodic cu privire la politicile și procedurile de securitate a informației.
- Performanța modelului de securitate trebuie monitorizată periodic și revizuită pentru a se asigura că este actualizat și adecvat.

Se recomandă ca:

- Alte instituții medicale să ia în considerare implementarea ISO/IEC 27014:2020 pentru a-și îmbunătăți protecția datelor sensibile ale pacienților și pentru a se conforma reglementărilor din domeniul medical.
- Este important să se consulte cu experți în securitate informațională pentru a obține sprijin

Bibliografie:

[1] „Strategia de Transformare Digitală 2023-2030 – Ministerul Dezvoltării Economice și Digitalizării”. Data accesării: 1 martie 2024. [Online]. Disponibil la: https://mded.gov.md/transparenta/64373-2/

[2] „ISO - International Organization for Standardization”, ISO. Data accesării: 1 martie 2024. [Online]. Disponibil la: https://www.iso.org/home.html

[3] 14:00-17:00, „ISO/IEC 27014:2020”, ISO. Data accesării: 1 martie 2024. [Online]. Disponibil la: https://www.iso.org/standard/74046.html