MANAGEMENTUL ŞI SECURITATEA INFORMAŢIONALĂ

Ştefan MORCODEANU

Universitatea Tehnică a Moldovei

Abstract: *În lucrarea a fost descris rolul TI în managementul întreprinderii, în special în domeniul securizării informaționale. La acest capitol a fost descrise cerințele către subsitemul informțional utilizat în cadrul întreprinderilor cu scopul securizării a informației în cadrul întreprinderii, expuse în ISO 27001:2013.*

Cuvinte cheie: *management, standard, sistem informațional, securitate informațională, SMSI, ISO/IEC 27001.*

1.Noțiuni generale.

La etapa actuală informațiile sunt privite ca resurse esențiale pentru continuarea și defășurarea unei activități economice, astfel necesitatea de a securiza această informație a devenit o obligațiune. Comapniile care doresc să-și desfășoare o activitate economică sau să facă parteneriate cu diverse companii, este necesar ca ele să implimenteze un Sistem de Management al Securității Informaționale. Standartul care reglementează protejarea și securizarea informației este ISO 27001:2013.

Standartul este utilizat în numeroase tipuri de organizații, cu diferite comenii de aplicare: financiar, telecomunicații, servicii, transporturi etc. În standart este reglementat procesele de implimentarea, monitorizarea și administrarea a unui Sistem de Management al Securității Informaționale. Scopul unui astfel de sistem este să asigure o continuă dezvoltare a afacerii, să reducă la minim eventuale pagube și să asigure confidențialitatea, integritatea și disponiblitatea datelor. Implimentare uni astfel de sistem ajută la identificarea și reducerea riscurilor critice de securitate și la concentrarea eforturilor în sensul protejării informației.

Managementul securității informației se definește ca fiind ansamblul proceselor de stabilire și menținere a unui cadru de lucru și a unei structuri de administrare, care oferă garanția că strategiile de securitate a informației sunt aliniate și susținute prin obiectivele afacerii care sunt în concordanță cu legile și reglementările privind administrarea cât mai adecvată a riscurilor [1].

2.Standardul ISO 27001:2013

ISO 27001:2013 este un standard internațional de securitate a informației, publicat la data 25 septembrie 2013. El anulează și înlocuiește ISO/IEC 27001:2005 și este publicat de către *Organizația Internațională de Standardizare* (I.S.O) și *Comisia Electrotehnică Internațională* (I.E.C).

Standardul I.S.O/I.E.C 27001:2013 este cel mai cunoscut document normativ care prevede implimentarea și certificarea unui S.M.S.I. într-o organizație. De menționat faptul că ISO nu este un organ de certificare. Ca orice alt standard ISO privitor la sisteme de management, certificare I.S.O / I.E.C 27001:2013 este posibilă, însă nu este obligatorie. Unele organizații pot implimenta cerițele standadului pentru a le oferi, suplimentar, încredere părților interesate, pe cînd alte organiații aleg să implimenteze doar cerințele pentru a beneficia de bunele practice din standard [2].

În 1995 Institutul de Standardizare din Marea Britanie (BSI) a publicat standardul BS 7799-1, conținînd un set de cerințe pentru implimentarea voluntară a unui SMSI în cadrul organizaţiilor. Mai târziu apare şi partea a doua, BS 7799-2 „Information Security Management Systems - Specification with Guidance For Use". Acesta era un set de indrumări specifice şi mai detaliate pentru implementarea unui SMSI eficient. Ulterior s-a pus problema transformării acestui standard britanic, recunoscut iniţial doar de către UKAS(The United Kingdom Accreditation Service) ca standard naţional, într-un standard internaţional. În anul 2002 în BS 7799 a fost incorporată abordarea bazată pe procese PDCA (”Plan-Do-Ceck-Act”, Edward Deming) ca ulterior, în a. 2005 să se transforme în standardul internaţional ISO/IEC 27001:2005.

Datele prezentate conform ISO Survey arată că numărul certificărilor ISO 27001 în lume prezintă o creștere cu 20% în anul 2015 față de 2014 . În fig. 1 este prezentat topul țărilor după numărul de certificări pentru anul 2015.

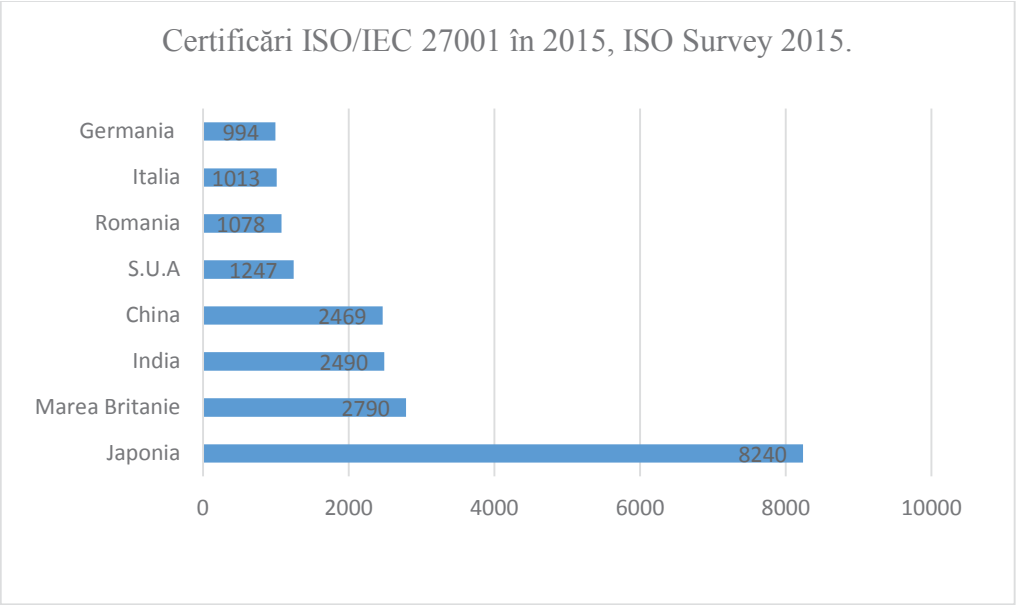

Fig.1. Certificări ISO/IEC 27001 în unele țări ale lumii
Sursa: ISO Survei, 2015

În funție de sectorul industrial certificările ISO/IEC 27001 conform datelor prezentate de ISO Survey pentru anul 2015 sunt prezentare în fig. 2.

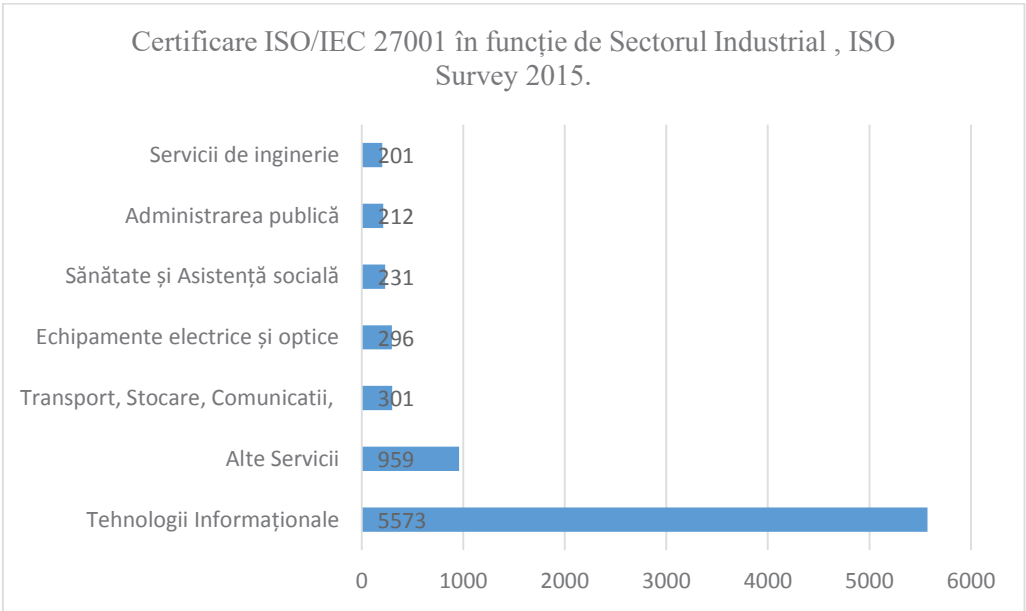

Fig.2. Sectoarele industriale cu cel mai mare număr de certificări ISO/IEC 27001,
Sursa:ISO Survei, 2015

3.Aplicarea standardului în Republica Moldova

La capitolul dat, conform datelor statistice din 2015, Republica Moldova deține 7 certificări ISO/IEC 27001 păstrînd astfel același nivel ca și în anii 2014, însă în comparație cu anii 2011-2012 cînd Moldova deținea doar un singur certficat pe țară, putem observa o creștere majoră, explicînduse prin faptul că Moldova fiind un stat în curs de dezvoltare, are tendință de modernizare și racordarea la standardele europene.

Printre companiile care au obținut acest certificat de standardizare pot fi numite: Endava – fiind prima companie din regiune obținînd certificare ISO 27001, DAAC System și MAIB care a fost prima bancă din Moldova obținînd ulterior implimentarea unui SMSI în anul 2013.

Î.S. „Fiscservinform" a inițiat procesul de implementare a SMSI conform standardului ISO 27001.

Față de Romania care este a 6-sea țară cu cel mai multe certificări a standardului ISO 27001, avînd 1078 de certificari, R.Moldova mai are de învățat și de crescut la acest capitol.

4.Implimentarea unui Sistem de Management al Securităţii Informaţionale.

Totuşi la crearea unui SMSI, este necesar de luat în considerare nu doar atingerea tuturor proprietăţilor informaţionale, ci şi specificul businessului. Spre exemplu în sectorul bancar scopul principal a SI este asigurarea integrităţii informaţiei financiare; pentru operatorii din sectorul de telecomunicaţii – accesul la resursele informaţionale, începînd cu canalele de transmisie şi pînă la serverele comerciale; pentru companiile de stat este importantă menţinerea confidialităţii informaţiilor. Însă acest lucru nu înseamnă că întreprinderile de stat nu i-au în considerare menţinerea integrităţii datelor sau că sectorul bancar nu are nevoie de accesul la informaţie.

De aceea, de la bun început se iau în considerare aspectele critice şi cele mai importante în funcţie de specificul organizaţie, pentru crearea unei arhitecturi corecte ca în final să se obţină un SMSI eficient şi sigur. Pentru realizarea a SMSI trebuie să utilizăm abordarea bazată pe PDCA(**P**lan – **D**o – **C**heck - **A**ct):

- planificarea,
- realizarea,
- verificarea,
- menţinerea.

În etapa de planificare, se asigură evaluarea riscurilor securităţii informaţie şi se propune un plan corespunzător de prelucrare a riscurilor. La etapa de realizare sunt aplicate toate deciziile luat la etapa de planificare. Etapele ulterioare, de verificare şi menţinere, redactează şi perfeţionează deciziile deja luate şi implimentate. Algortimult dat se repetă pînă SMSI ajunge să fie conform cerinţelor standardului ISO 27001 [5].

Însă, anume certificare ISO 27001 ca şi toate celalte procese de standardizare ISO constă din 3 etape:

- Prima etapă este cea preiliminară, care constă în verificarea documentaţii minime pentru implimentarea standardului, cum ar fi politica de confidenţialitate a firmei, regulamentul intern privin gradul de acces la informaţie şi alte documente care ar fi esenţiale pentru ISO 27001.
- A doua etapă este ce în care se testează sistemul de securitate a informaţiei prin cerinţele menţionate în standard. Auditorii au datoria de a căuta dovezi şi detalii prin care să confirme că Sistemul de Management al Securităţii Informaţiei a fost implimentat cu succes şi funcţionează într-un mod cît mai eficient.
- În ultima etapă presupune auditori de supraveghere, pentru a verifica dacă organizaţia certificată, mai este sau nu în conformitate cu cerinţele standardului de securitate informaţională ISO 27001. În cele din urmă organul care eliberează certificatul de standardizare, va cere ulterior audituri suplimentare pentru a verifica dacă sistemul de management a securităţii informaţiei mai este sau nu în conformitate cu ISO 27001 [6].

Pentru a afla cît timp durează implimentarea unui standard ISO, răspunsul îl oferă ISO27006 cu privire la standardele de auditare, şi anume, pentru o companie cu 2 – 10 angajaţi, auditul de certificare este bugetat cu 2 oameni, 5 zile.

Concluzii

În concluzie, putem spune că implimentare unui sistem de management al securităţii informaţiei (SMSI) conform standardului ISO/IEC 27001, trebuie să fie făcută în dependenţă de specificul companie şi punctele critice şi cele mai importante a organizaţiei în scopul creării unei arhitecturi corecte şi pentru a obţine un SMSI eficient şi sigur. Implimentarea unui SMSI este o decizie strategică a organizaţie, astfel organizaţia îşi poate identifica nivelul necesar de securitate, poate dezvolta planuri, strategii despre cum ar trebuie să securizeze informaţia în baza propriei analize, astfel luînd măsuri tehnice şi non-tehnice în vederea securizării informaţiei.

Astfel avantajele implimentării unui SMSI sunt:

- reducerea riscului la adresa securităţii informatice,
- abordarea structurală şi standartizată a sistemului informaţional,
- reducerea costurilor de operare şi administrare a securităţii,
- promovarea imaginii companiei ca un partener de afacere sigur,
- satisfacere cerinţelor partenerilor de afacere internaţionali prin evedinţierea controalelor de securitate,
- reducerea maximală a impactului unor posibile pierderi de informaţii,
- reacţionarea adecvată şi în timp la ameninţările securităţii informaţiei prin selectarea măsurilor de protecţie a informaţiei pe baza analizei de risc.

În final putem spune că în R.Moldova, acest tip de standardizare se întîlneşte în domeniul TIC şi în în sectorul bancar. Dacă pentru pentru cei din domeniul IT este o alegere să implimenteze sau nu un SMSI,

pentru cei din sectorul bancar a fost mai mult o obligație din partea Băncii Mondiale de a trece la standartului ISO/IEC 27001.

Bibliografie

[1]*Securitatea sistemelor informaţionale: Managementul securităţii SI, Controlul logic, Securitatea reţelelor locale şi a aplicaţiilor client-server*.

[2] *Comparative study regarding international standards on information security management systems in organizations: ISO/IEC 27001:2013 vs iso/iec 27001:2005*, Bogdan Ţigănoaia, Assistant Professor, PhD, Politehnica University of Bucharest

[3]ISOSurvey:http://www.iso.org/iso/the_iso_survey_of_management_system_standard_certifications_2015 .pdf

[4] *Analiza etapelor de creare a unui sistem de management al securităţii informaţiei*, Rodica BULAI, Academia „Ştefan cel Mare"

[5] *Recomandări Privind Implementarea SMSI după ISO/IEC 27001:2013,* Rodica BULAI, Ludmila DUCA

[6] ISO/IEC 27001 http://www.itco.ro/standarde/iso-iec-27001.html

[7] *Sistemul de management al securităţii informaţionale ISO/IEC 27001:2013. Algoritmul de implementare,* COJOCARU Igor, GUZUN Mihail, IONESCU Răzvan.

[8]GOROBIEVSCHI S., MODORAN R. *Societatea Informațională - direcție importantă de dezvoltare a societății umane*. În: SYMPOSIA Professorum: conf. șt. inter. Seria economie, Ed.2006. Ch.: ULIM, 2007, pp. 246-249. ISBN:9975-934-83-8.