Managementul resurselor ISO/IEC 27001:2013, A8

IDSI
Dr. conf. Guzun Mihail
Dr. Cojocaru Igor

Termeni și definiții (ISO/IEC 27000:2018)

Activ (asset)

-ceea ce reprezintă valoare pentru organizație.

Atac (attack)

- încercarea de a distruge, dezvălui, modifica, face inaccesibil, fura sau obține acces neautorizat sau utilizarea neautorizată a unui activ.

Disponibilitate (disponibility)

- proprietatea de a fi accesibil şi utilizabil la cerere de către o entitate autorizată

Confidenţialitate (confidentiality)

- proprietatea ca informaţia să nu fie făcută disponibilă sau divulgată persoanelor, entităţilor sau proceselor neautorizate

Integritate (integrity)

- proprietatea de a păstra acurateţea şi deplinătatea resurselor

Termeni și definiții (ISO/IEC 27000:2018)

Non-repudiere (non-repudiation)

- capacitatea de a confirma un eveniment sau o acțiune care a avut loc și subiecții acestora, astfel încât acest eveniment sau acțiune și subiecții implicați să nu poată fi puși la îndoială;

Control (Control)

-măsurile orientate spre modificarea riscului

Securitatea informațiilor (information security)

-păstrarea confidențialității , integrității și disponibilității informațiilor

Vulnerabilitate (vulnerability)

-punctul slab al unui activ sau control care poate fi exploatat de una sau mai multe amenințări

Termeni și definiții (ISO/IEC 27000:2018)

Amenințare (threat)

- posibila cauză a unui incident care ar putea aduce pagube unui sistem sau unei organizații.

Incident de securitate a informațiilor (information security incident)

-unul sau mai multe evenimente nedorite sau neașteptate de securitate a informațiilor care pot pune în pericol activitățile comerciale și amenință securitatea informațiilor

Nivel de risc (level of risk)

-mărimea riscului exprimată printr-o combinație de consecințe și probabilitatea acestora

Termeni și definiții (ISO/IEC 27000:2018)

Eveniment de securitate a informațiilor (information security event)

-apariția identificată a unui sistem, serviciu sau stare a rețelei care indică o posibilă încălcare a politicilor de securitate a informațiilor sau controale inadecvate sau o situație necunoscută anterior care ar putea fi semnificativă din perspectiva securității

Tipuri de resurse care trebuie să fie protejate

Resurse informaţionale: baze de date şi fişiere de date, documentaţie de sistem, documentaţie tehnică, manuale de utilizare, materiale de instruire, proceduri operaţionale şi de suport, planuri de continuitate a afacerii, planuri de rezervă (ex: planuri de acţiuni în situaţii de urgenţă, de accident de securitate informaţională, informaţii arhivate.

Resurse software: aplicaţii software, software de sistem, instrumente de dezvoltare şi programe utilitare.

Tipuri de resurse care trebuie să fie protejate (continuare)

Resurse fizice: spaţii pentru echipamente de calcul, panouri electrice, traductori de temperatură şi de umiditate, cabluri, echipamente de calcul (procesoare, monitoare, laptopuri, modemuri), echipamente de comunicaţii (routere, centrale telefonice, faxuri, roboţi telefonici), suporturi magnetice (benzi şi discuri), filme, fotografii, alte echipamente tehnice (surse de energie, aparate de aer condiţionat), mobilier, furnituri, transport auto;

Servicii: servicii de calcul sau comunicaţii, utilităţi generale, cum ar fi încălzirea, iluminatul, alimentarea cu energie electrică, aer condiţionat.

Resurse umane: oameni, calificările, priceperea şi exeperienţa lor.

Resurse nemateriale: reputația, imaginea

PROCEDURA DE CONTROL ASUPRA RESURSELOR

1. Stabilirea responsabilității pentru resurse

Obiectiv: Să se identifice resursele organizaţiei şi să se definească responsabilităţile pentru protecţia corespunzătoare.

1.1. Inventarul resurselor

1.2. Reguli de deţinere a resurselor

1.3. Reguli de utilizare a în mod acceptabil a resurselor

1.4. Returnarea resurselor

2.Clasificarea informației

Obiectiv: Să asigure ca informaţia beneficiază de un nivel de protecţie adecvat în conformitate cu importanţa sa pentru organizaţie.

2.1. Criterii de clasificare a informației

2.2. Etichetarea informaţiei clasificate

2.3. Reguli de manipulare în dependență de clasa resursei

Exemplu de clasificare a informației

Informaţii strict confidenţiale – clasa 4

Identificare:

”STRICT CONFIDENTIAL”

Drept de acces:

1._____

2._____

Informaţii cu acces limitat – clasa 3

Identificare

”ACCES LIMITAT”

Drept de acces:

1._____

2._____

Informaţii de uz intern – clasa 2

Identificare

”UZ INTERN”

3. Manipularea mediilor de stocare

Obiectiv: Să prevină divulgarea neautorizată, modificarea, îndepărtarea sau distrugerea informaţiei stocate pe mediile de stocare.

3.1. Reguli și restricții privind mediile de stocare amovibile

3.2. Reguli de distrugere controlată a mediilor de stocare

3.3. Reguli privind transferul fizic al mediilor de stocare

Forma registrului activelor

Nr. crt	Tipul resursei	Denumirea resursei	Clasdificarea resursei	Responsabil	
				Nivel logic	Nivel fizic

continuare tabel

Proprietarul resursei	Acces la resursă	Locul stocării	Locul stocării copiei (unde e aplicabil)	Denumirea documentului ce conţine regulile pentru utilizarea în mod acceptabil (unde e aplicabil)