Managementul riscului pentru infrastructuri de mari dimensiuni în regiunea transfrontalieră România - Bulgaria

Project Code 15.3.1.017

SECURITATEA DATELOR

Chestionar

1. **Ce anume determina nevoia desecuritate a unei companii?**
   a. Dimensiunea organizatiei ☐
   b. Criticitatea si confidentialitatea datelor ☐
2. **Care este Solutia cea mai viabila din punctul de vedere al securitatii in acest moment?**
   a. firewall-antivirus ☐
   b. sistemele de protecttie antiintruziune ☐
3. **Care sunt principalele componente ale securitatii IT?**
   a. tehnologie, ☐
   b. buget, ☐
   c. procese, ☐
   d. stategie, ☐
   e. educatie ☐
4. **Care este scopul protejariii datelor intr-un sistem informatic**
   a. impiedicarea folosirii lor in mod neadecvat, intentionat sau nu, de catre diversi agenti (utilizatori sau programe) ☐
   b. facilitatrea accesului la o mare cantitate de date intr-un timp scurt si eventual preluarea lor ☐
5. **Completati definitia data de Comitetul National de Securitate al Sistemelor Informationale si de Telecomunicatii din cadrul guvernului federal al SUA, securitatii sistemelor informationale:**
   Protectia sistemelor informatice impotriva …….. neautorizat la informatie sau a modificarii neautorizate a informatei, in cadrul ……., ……. sau ……., si impotriva refuzului deservirii utilizatorilor ……., sau asigurarea deservirii utilizatorilor autorizati, incluzand acele masuri necesare pentru a ……., documenta sau contracara aceste amenintari.

6. **Principalele componente ale securitatii informatiei** sunt:

a. confidentialitatea, ☐
b. integritatea, ☐
c. disponibilitatea ☐

7. Confidentialitatea poate fi obtinuta prin mai multe procedee:

a. Pastrarea secretului ☐
b. Restricția accesului ☐
c. Izolarea ☐
d. Ascunderea informatiei sau a datelor ☐
e. Criptarea ☐

8. Cum se asigura Integritatea?

a. Prin mentinerea unei conduite adecvate ☐
b. Impiedicarea accesului persoanelor neautorizate la sistemul informatic, ☐
c. Autentificarea utilizatorilor si autorizarea lor ☐
d. Semnarea unui accord de integritate ☐
e. Folosirea de sume criptografice de control si de semnaturi electronice ☐

9. Asigurarea disponibilitatii prin:

a. autentificarea si autorizarea utilizatorilor ☐
b. un sistem deschis tuturor ☐
c. impiedicarea accesului in sistem pentru utilizatorii neautorizati ☐
d. impiedicarea atacurilor de tip Denial of Service (DoS) ☐
e. realizarea de backup-uri si folosirea sistemelor de stocare RAID ☐
f. accesibilitate permisa tuturor ☐

10. Identificati categoriile de amenintari:

a. Intrusii externi ☐
b. Intrusii interni ☐
c. Personalul de service ☐
d. Personalul propriu ☐
e. Furnizorii ☐
f. Utilizatorii corupti ☐
g. Utilizatorii de buna credinta ☐

11. Masuri de protectie recomandate:

a. Securitatea statiilor de lucru ☐
b. Inchiderea calculatorului ☐
c. Autentificarea ☐

d. Autorizarea ☐
e. Folosirea calculatorului doar in prezenta celor de la Securitate ☐
f. Patch-uri de Securitate ☐
g. Antivirusi, anti-spyware ☐
h. Folosirea unei parole unice la nivelul intregii companii ☐

Raspunsuri:

1.b, **2.**b, **3.** a,c,e, **4.**a, **5.** Accesului, stocarii,procesarii, tranzitului, autorizati, detecta, **6.**a,b,c, **7.**b,c,e**, 8.** b,c,e, **9**.a,c,d,e, **10.**a,c,e,f, **11.**a,c,d,f,g,