Tema 7 Managementul Riscurilor

**Analiză: Sisteme biometrice ca factor de autentificare**

**Avantaje**

1. **Securitate sporită**  
   Datele biometrice sunt unice pentru fiecare individ, ceea ce face dificilă falsificarea sau partajarea acestora, spre deosebire de parole, care pot fi divulgate sau ghicite.
2. **Experiență de utilizare îmbunătățită**  
   Autentificarea biometrică este rapidă și comodă – utilizatorii nu trebuie să își amintească parole complexe sau să introducă coduri suplimentare.
3. **Reducerea riscului de phishing**  
   Atacurile de tip phishing sunt mai puțin eficiente, deoarece datele biometrice nu pot fi transmise sau furate la fel de ușor ca parolele.
4. **Imposibilitatea pierderii sau uitării**  
   Utilizatorii nu pot „uita” amprenta sau fața, spre deosebire de parole sau token-uri fizice.

**Dezavantaje**

1. **Costuri de implementare**  
   Implementarea infrastructurii biometrice (cititoare de amprentă, camere speciale etc.) poate fi costisitoare, mai ales la scară largă.
2. **Probleme de confidențialitate**  
   Datele biometrice sunt sensibile și, dacă sunt compromise, nu pot fi schimbate (nu poți „reseta” o amprentă).
3. **Erori de recunoaștere**  
   Sistemele biometrice pot da erori (fals pozitiv sau fals negativ), mai ales în condiții nefavorabile (de exemplu, amprente murdare, iluminare slabă).
4. **Excluderea unor utilizatori**  
   Anumite persoane pot avea dificultăți în utilizarea autentificării biometrice (de exemplu, probleme medicale, dizabilități, răni la degete etc.).