Măsuri de consolidare securitate cibernetică guvernamentală

Aria	**Copii de rezervă și recuperare post-incident**
Amenințări asociate	• Pierderea datelor prin ransomware sau malware distructiv • Ștergere accidentală sau intenționată de date (insider threat) • Defecțiuni hardware (servere, HDD, SSD) • Dezastre naturale sau incendii care afectează echipamentele locale • Backup corupt sau inaccesibil în momentul necesar
Criticitate	**Înaltă** (pierderea datelor critice poate bloca activitatea instituției și compromite continuitatea serviciilor)

Contramăsuri	• Realizarea backup-ului zilnic pentru date critice și săptămânal pentru date mai puțin sensibile.
	• Păstrarea a cel puțin 3 copii de backup (regula 3-2-1):
	  ◦ 3 copii ale datelor
	  ◦ 2 pe medii diferite (ex: disk + cloud)
	  ◦ 1 copie offline sau offsite.
	• Criptarea backup-urilor pentru protejarea confidențialității.
	• Testarea restaurării datelor cel puțin trimestrial.
	• Documentarea și respectarea unui plan de recuperare (Disaster Recovery Plan).
	• Restricționarea accesului la fișierele de backup doar pentru personal autorizat.
	• Monitorizarea integrității backup-urilor (hash/checksum).
	• Protecția backup-urilor împotriva ștergerii/modificării (immutable backups).

Indici de compromitere	• Eșecuri repetate la rularea procesului de backup. • Lipsa unor backup-uri recente disponibile. • Diminuarea bruscă a spațiului disponibil din cauza unor fișiere corupte sau criptate. • Imposibilitatea restaurării în timpul testelor.
Raportare	**Local** Utilizatorul raportează imediat incidentul la echipa IT. IT verifică, izolează dispozitivul afectat și transmite logurile. Conducere, în caz în care e afectată continuitatea. **SIS** și **INI al IGP al MAI** În caz de incident ransomware **Central** la **CERT GOV MD** Tichet www.suport.gov.md E-mail: info@cert.gov.md