



MĂSURI DE SIGURANȚĂ CIBERNETICĂ



MĂSURI PENTRU BACKUP ȘI CONTINUITĂȚEA ACTIVITĂȚII

- **Realizați Copii de Rezervă:** Asigurați-vă că toate datele critice sunt salvate periodic într-o locație securizată.
- **Plan de Recuperare:** Dezvoltați și testați un plan de recuperare în caz de dezastru pentru a relua rapid activitatea.
- **Infrastructură Redundantă:** Implementați soluții de infrastructură redundantă pentru a minimiza impactul întreruperilor.



MĂSURI DE INSTRUIRE A ANGAJAȚILOR

- **Sesiuni de Informare:** Organizați sesiuni regulate de instruire pentru a educa angajații despre riscurile cibernetice.
- **Recunoașterea Phishing-ului:** Învățați angajații să identifice și să evite emailurile de phishing și alte forme de atacuri cibernetice, explicând exemple clare:
 - **Emailuri Phishing:** Emailuri care par a fi de la bănci sau companii cunoscute, cerând să faceți clic pe un link și să introduceți date personale.
 - **Atacuri SMS:** Mesaje ce pretind a fi de la curieri, cerându-vă să accesați un link pentru a confirma o livrare.
 - **Apeluri Telefonice Înșelătoare:** Cineva sună pretinzând că este de la IT și vă cere să furnizați parolele de acces.
- **Politici de Securitate:** Stabiliți și comunicați politici clare de securitate IT pe care toți angajații trebuie să le urmeze.

