Igiena Cibernetică. Start Corect în 2026

Ghid rapid de securitate pentru angajați (Conformitate NIS2)

Dan Gurghian - Responsabil NIS2

GDPR COMPLET

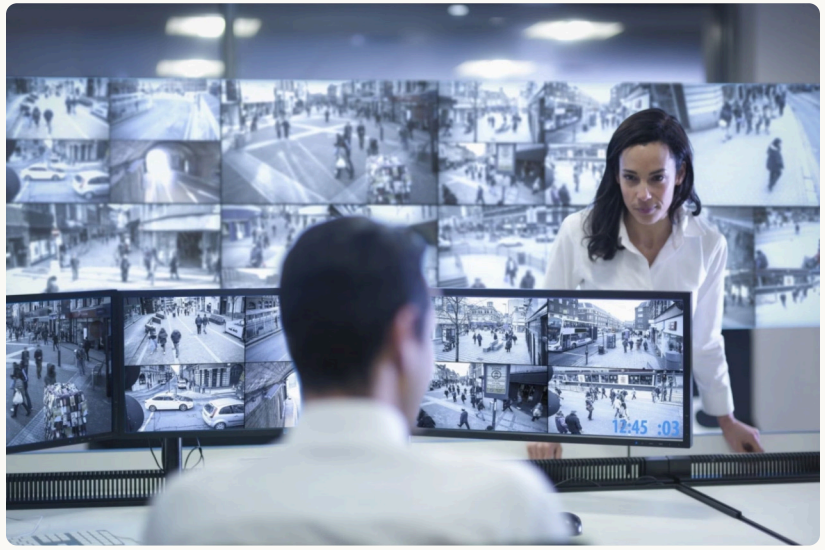
INTRODUCERE

De ce vorbim despre asta?

Siguranța datelor companiei începe cu fiecare dintre noi. Nu este doar o cerință legală impusă de Directiva NIS2, ci reprezintă o măsură esențială de protecție a muncii noastre zilnice și a informațiilor sensibile pe care le gestionăm.

În contextul transformării digitale accelerate, fiecare angajat devine un veritabil apărător al securității organizaționale. Deciziile pe care le luăm zilnic — de la gestionarea parolelor până la modul în care tratăm documentele confidențiale — au impact direct asupra întregii companii.

> **"Securitatea este un efort de echipă."**



PRACTICI ESENȚIALE

Parola nu mai e un singur cuvânt

Greșeala Clasică

Parole scurte, simple, ușor de ghicit

~~Floare123~~

~~Nume2024~~

Abordarea Modernă

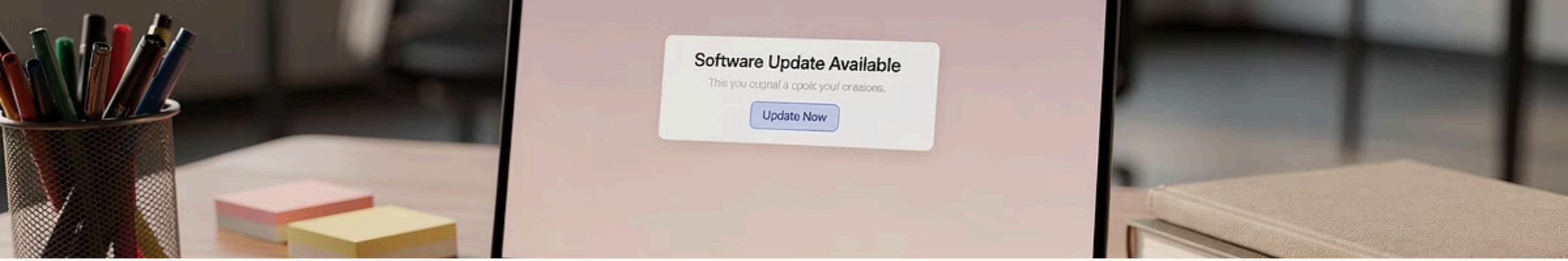
Fraze de acces (Passphrases) — lungi și memorabile

Muzica-Este-Viata!26

Cafea&Dimineata_Fericita2026

Uită de parolele scurte. Treci la conceptul de "Passphrases" — fraze de acces care combină cuvinte, simboluri și cifre într-un mod natural și ușor de reținut pentru tine, dar imposibil de ghicit pentru atacatori.

Regula de aur: Lungimea bate complexitatea. O frază de 20 de caractere cu cuvinte simple este infinit mai sigură decât 8 caractere complexe.



ACTUALIZĂRI

Actualizările salvează situația

Vulnerabilitățile software reprezintă principala poartă de intrare pentru atacurile cibernetice. Hackerii monitorizează constant breșele de securitate și profită de sistemele neactualizate pentru a penetra rețelele organizaționale.

1 — Vulnerabilitate Descoperită

Producătorul software identifică o breșă de securitate

2 — Patch Lansat

Actualizarea corectivă este pusă la dispoziție

3 — Instalare Urgentă

Fiecare zi de întârziere = risc crescut

4 — Sistem Protejat

Vulnerabilitatea este eliminată

❌ Nu apăsa "Amână"

Instalează actualizările imediat ce apar, indiferent dacă vine vorba de sistemul de operare, aplicațiile de birou sau browserul web.

✓ Acționează Acum

Un restart durează 2 minute. O recuperare după un atac de securitate durează săptămâni și poate costa compania mii de euro.

SECURITATE FIZICĂ

Clean Desk Policy: Hackerii nu sunt doar online

Atacatorii cibernetici nu lucrează exclusiv din spatele unui ecran. Mulți dintre ei pot intra fizic în birou — sub acoperirea unor vizitatori, furnizori sau chiar curieri — și pot accesa informații confidențiale lăsate la vedere sau computere deblocate.

1

Blochează Ecranul

Apasă `Win+L` (Windows) sau `Cmd+Ctrl+Q` (Mac) ori de câte ori părăsești biroul, chiar și pentru 30 de secunde. Acest gest simplu previne accesul neautorizat la datele tale.

2

Zero Post-it cu Parole

Nu nota niciodată parole, coduri PIN sau informații de acces pe hârtie. Folosește un manager de parole securizat aprobat de companie pentru a stoca credențialele în siguranță.

3

Birou Curat la Final de Zi

Încuie toate documentele confidențiale în dulapuri sau sertare. Nu lăsa contracte, rapoarte financiare, liste de clienți sau orice alt material sensibil la vedere pe birou după program.

Reminder NIS2: Politica "Clean Desk" nu este doar o recomandare, ci o cerință explicită în multe cadre de conformitate, inclusiv NIS2, pentru organizațiile care gestionează infrastructuri critice.

Alte Practici Esențiale de Securitate

Atenție la Phishing

Nu deschide atașamente sau link-uri din email-uri nesolicitate. Verifică întotdeauna adresa expeditorului și caută semne de suspiciune: greșeli gramaticale, urgență artificială sau cereri neobișnuite.

Dispozitive Mobile Protejate

Activează PIN, amprentă sau recunoaștere facială pe toate dispozitivele mobile de serviciu. Un telefon pierdut fără protecție poate deveni o breșă majoră de securitate.

Wi-Fi Public = Pericol

Evită să accesezi resurse corporative sau să introduci date sensibile când ești conectat la rețele Wi-Fi publice (cafenele, aeroporturi). Folosește VPN-ul companiei pentru conexiuni sigure.

Date în Cloud Aprobat

Folosește exclusiv soluțiile cloud aprobate de companie pentru stocarea și partajarea documentelor. Serviciile personale (Dropbox, Google Drive personal) nu oferă același nivel de control și securitate.

Recunoașterea Amenințărilor Cibernetice

Capacitatea de a identifica rapid semnalele unei potențiale amenințări poate face diferența între un incident minor și o breșă majoră de securitate. Iată principalele indicii care ar trebui să declanșeze alerta:

- **Email-uri urgente** care cer acțiuni imediate sau date confidențiale
- **Link-uri suspecte** care nu corespund cu domeniul real al companiei
- **Atașamente neașteptate**, chiar dacă par să vină de la colegi
- **Cereri de resetare parolă** pe care nu le-ai inițiat tu
- **Activitate neobișnuită** în conturile tale (logări din locații ciudate)
- **Pop-up-uri** care avertizează despre "viruși detectați" și oferă soluții

> **Principiul "Gândește înainte să dai click":** Dacă ceva pare prea bun ca să fie adevărat, urgent fără motiv sau pur și simplu ciudat — oprește-te și verifică.

PLAN DE ACȚIUNE

Misiunea ta pentru Azi

01

Audit Rapid de Securitate

Verifică-ți parola principală de acces la sistemele companiei. Dacă are mai puțin de 12 caractere sau o folosești de peste 6 luni, este momentul pentru schimbare.

02

Activează Autentificarea Multi-Factor

Dacă nu ai făcut-o deja, configurează MFA (Multi-Factor Authentication) pentru toate conturile de serviciu. Acest strat adițional de securitate te protejează chiar dacă parola este compromisă.

03

Curăță Biroul și Ecranul

Privește în jurul tău: elimină orice document confidențial lăsat la vedere și asigură-te că nu ai parole salvate pe post-it-uri sau în fișiere text neprotejate.

04

Instalează Actualizări Pending

Verifică dacă sistemul tău are actualizări în așteptare și programează un restart în următoarele 24 de ore pentru a le instala.

Raportarea Incidentelor: Tu ești Prima Linie de Apărare

Observă

Identifică orice activitate suspectă sau neobișnuită

Raportează Imediat

Contactează responsabilul NIS2 sau echipa IT

Acționează

Urmează instrucțiunile primite pentru izolarea amenințării

Ce trebuie raportat?

- Email-uri de phishing primite
- Tentative de acces neautorizat
- Dispozitive pierdute sau furate
- Comportament suspect al sistemelor
- Breach-uri accidentale de date
- Cereri neobișnuite de informații

De ce este crucial?

Conform NIS2, organizațiile au **obligația de raportare în 24 de ore** pentru incidente semnificative. Cu cât raportezi mai rapid, cu atât echipa de securitate poate reacționa mai eficient.

Nu fi temător: Este întotdeauna mai bine să raportezi un fals alarm decât să ignori o amenințare reală.

Securitatea începe cu tine

Fiecare gest contează: de la modul în care îți gestionezi parolele, până la vigilența cu care tratezi email-urile suspecte. În ecosistemul NIS2, tu nu ești doar un angajat — ești un apărător al infrastructurii critice a companiei.

Acțiunea ta Imediată

Schimbă parola principală dacă este veche sau slabă. Treci la un passphrase sigur chiar acum.

Responsabilitate Continuă

Raportează orice activitate suspectă responsabilului NIS2 sau departamentului IT imediat ce o observi.

Educație Permanentă

Participă activ la sesiunile de training în securitate cibernetică organizate de companie.

Ai întrebări despre securitatea cibernetică sau NIS2? Contactează echipa de conformitate — suntem aici să te sprijinim.

Contactează Responsabilul NIS2 | Resurse Suplimentare