cyberglobal romania

NIS2 Checklist

Acest checklist este structurat pentru a sprijini organizațiile în alinierea la cerințele directivei NIS2, vizând consolidarea rezilienței cibernetice. Documentul acoperă piloni esențiali, de la guvernanță și managementul riscului, până la protecția infrastructurii și răspunsul la incidente. Utilizarea acestuia facilitează identificarea vulnerabilităților și implementarea măsurilor de securitate necesare pentru continuitatea activității.

Guvernanță și Managementul Riscurilor de Securitate a Informației

- ☐ Există o politică de securitate a informației aprobată formal de conducere?
- ☐ Sunt definite obiectivele privind informațiile/securitatea cibernetică și aprobate de conducerea superioară?
- ☐ Sunt definite clar rolurile și responsabilitățile privind securitatea informației?
- ☐ Este numit un responsabil cu securitatea informațiilor la nivel de conducere?
- ☐ Sunt identificate obligațiile legale, de reglementare și contractuale legate de securitatea informațiilor și securitatea cibernetică?
- ☐ Este elaborată o strategie cuprinzătoare de gestionare a riscurilor legate de informații și securitatea cibernetică, care va fi actualizată atunci când apar schimbări?
- ☐ Se realizează periodic evaluări de risc pentru identificarea riscurilor de securitate?
- ☐ Sunt riscurile identificate documentate și atribuite unor responsabili?
- ☐ Sunt deciziile de tratare a riscurilor (acceptare, reducere, transfer) aprobate formal?
- ☐ Este programul de securitate a informației revizuit de conducere cel puțin anual?
- ☐ Este elaborat un proces de securitate cibernetică pentru resursele umane, aplicabil la recrutare, pe durata angajării și la încetarea contractului de muncă?
- ☐ Exista un process legat de securitatea cibernetică în lanțul de aprovizionare?
- ☐ Sunt evaluați furnizorii din punct de vedere al riscurilor de securitate înainte de contractare?
- ☐ Sunt incluse cerințe de securitate a informației în contractele cu furnizorii?
- ☐ Este accesul furnizorilor la sisteme sau date limitat și monitorizat?
- ☐ Sunt furnizorii revizuiți periodic pentru conformitate continuă?

3 Identificarea activelor și a proceselor

- [ ] Sunt identificate și inventariate activele informaționale (sisteme, date, aplicații)?
- [ ] Sunt identificate persoanele responsabile și răspunzătoare de gestionarea platformelor software și a aplicațiilor din cadrul organizației?
- [ ] Comunicarea în rețea și fluxurile de date externe ale organizației sunt mapate, documentate, autorizate și actualizate atunci când apar modificări?
- [ ] Patch-urile și actualizările de securitate pentru sistemele de operare și componentele critice ale sistemului sunt instalate in mod periodic?
- [ ] Organizația trebuie să împiedice îndepărtarea neautorizată a echipamentelor de întreținere care conțin informații critice despre sistemul organizației.
- [ ] Sunt datele clasificate (de ex.: publice, interne, confidențiale)?
- [ ] Sunt definite reguli de manipulare a datelor în funcție de clasificare?
- [ ] Este utilizată criptarea pentru datele sensibile, atât în tranzit, cât și la stocare?
- [ ] Organizația trebuie să stabilească și să mențină un proces documentat care să permită revizuirea, analiza și remedierea continuă a vulnerabilităților și să prevadă schimbul de informații, acolo unde este cazul.
- [ ] Planurile de urgență și continuitate trebuie stabilite, comunicate, menținute, testate, validate și îmbunătățite.
- [ ] Organizația va coordona elaborarea și testarea planurilor de răspuns la incidente și a altor planuri de securitate cibernetică care afectează operațiunile cu părțile interesate.

4 Protecția infrastructurii și a activelor

- [ ] Sunt conturile de utilizator create doar pe baza unei aprobări documentate?
- [ ] Este accesul acordat conform principiului „necesității de a cunoaște” (least privilege)?
- [ ] Sunt conturile cu privilegii ridicate restricționate și monitorizate?
  Este utilizată autentificarea multifactor pentru accesul critic sau de la distanță?
- [ ] Sunt drepturile de acces revizuite periodic?
- [ ] Este accesul revocat prompt la încetarea sau modificarea relației de muncă?
- [ ] Separarea sarcinilor (SoD) trebuie asigurată în gestionarea drepturilor de acces.
- [ ] Utilizatorii privilegiați vor fi gestionați monitorizați si audiati.
- [ ] Primesc angajații instruire privind securitatea informației?
- [ ] Este instruirea realizată la angajare și periodic ulterior?
- [ ] Sunt angajații instruiți privind phishing-ul și ingineria socială?
- [ ] Este respectarea politicilor de securitate comunicată și consolidată constant?
- [ ] Organizația va implementa verificări ale integrității software-ului, firmware-ului și informațiilor pentru a detecta modificările neautorizate ale componentelor critice ale sistemului său în timpul depozitării, transportului, pornirii și atunci când se consideră necesar.

- [ ] Sunt sistemele monitorizate pentru detectarea erorilor, defecțiunilor sau anomaliilor?
- [ ] Există proceduri documentate de backup și sunt acestea executate regulat?
- [ ] Sunt copiile de siguranță stocate în mod securizat și protejate împotriva accesului neautorizat?
- [ ] Sunt testate periodic procedurile de restaurare din backup?
- [ ] Sunt aplicate regulat actualizări de securitate și scanări de vulnerabilitate?
- [ ] Organizația trebuie să dezvolte, să documenteze și să mențină o configurație de bază pentru sistemele sale critice pentru activitate.
- [ ] Jurnalele ar trebui menținute, documentate și monitorizate.
- [ ] Filtre web și e-mail trebuie instalate și utilizate.
- [ ] Instalarea și executarea de software neautorizat trebuie împiedicate.
- [ ] Securitatea trebuie luată în considerare pe tot parcursul ciclului de viață al sistemelor și aplicațiilor, indiferent dacă acestea sunt dezvoltate intern sau achiziționate extern.
- [ ] Sunt modificările asupra sistemelor solicitate și documentate formal?
- [ ] Sunt evaluate impacturile de securitate înainte de implementarea modificărilor?
- [ ] Sunt modificările testate înainte de implementarea în producție?
- [ ] Sunt modificările aprobate de personal autorizat?
- [ ] Este păstrată o evidență (audit trail) a modificărilor de sistem și configurație?
- [ ] Firewall-urile trebuie instalate, configurate și actualizate în mod activ pe toate rețelele utilizate de organizație pentru a proteja împotriva accesului neautorizat și a amenințărilor cibernetice.
- [ ] Pentru protejarea sistemele critice, organizațiile trebuie să implementeze segmentarea și segregarea rețelelor în conformitate cu limitele de încredere și criticitatea activelor, limitând astfel propagarea amenințărilor și impunând un control strict al accesului.
- [ ] Este accesul fizic la infrastructura IT restricționat?
- [ ] Sunt implementate controale de acces (carduri, chei, jurnale) pentru zonele securizate?
- [ ] Sunt vizitatorii monitorizați sau însoțiți în zonele sensibile?
- [ ] Sunt implementate controale de mediu (incendiu, alimentare electrică, climatizare)?

Detectarea evenimentelor și monitorizarea continuă

- [ ] Firewall-urile trebuie instalate și operate la limitele rețelei, inclusiv firewall-urile la nivel de end-point.
- [ ] Programele antivirus, anti-spyware și alte programe anti-malware trebuie instalate și actualizate.
- [ ] Organizația va monitoriza și identifica utilizarea neautorizată a sistemelor sale critice pentru activitate prin detectarea conexiunilor locale neautorizate, a conexiunilor de rețea și a conexiunilor la distanță.
- [ ] Mediul fizic trebuie monitorizat pentru a identifica evenimente potențial adverse.

- [ ] Funcționalitatea de înregistrare a instrumentelor de protecție și detectare trebuie să fie activată. Jurnalele trebuie să fie salvate și păstrate pentru o perioadă predefinită și revizuite periodic pentru a identifica activități neobișnuite sau potențial dăunătoare.
- [ ] Organizația trebuie să evalueze impactul negativ al evenimentelor detectate asupra operațiunilor, activelor și persoanelor sale și să coreleze aceste impacturi cu rezultatele evaluărilor sale de risc.
- [ ] Informațiile privind evenimentele adverse trebuie transmise prompt personalului și sistemelor autorizate, pentru a permite detectarea, investigarea și răspunsul în timp util.
- [ ] Incidentele trebuie raportate atunci când evenimentele adverse îndeplinesc criteriile definite și documentate pentru incidente.

Raspunsul la incidente de securitate a informației.

- [ ] Există un plan de răspuns la incidente, care include roluri, responsabilități și autorități definite?
- [ ] Sunt incidentele de securitate înregistrate, investigate și soluționate?
- [ ] Sunt identificate cauzele principale și implementate acțiuni corective?
- [ ] Sunt incidentele semnificative raportate conducerii?
- [ ] Incidentele de securitate cibernetică trebuie comunicate părților interesate externe relevante în termenele definite în Planul de răspuns la incidente, inclusiv raportarea incidentelor semnificative către autorități, conform prevederilor legale.
- [ ] Se vor utiliza instrumente automatizate pentru a sprijini investigarea și evaluarea impactului incidentelor de securitate cibernetică validate.
- [ ] Organizația trebuie să detecteze accesul neautorizat sau scurgerile de date și să ia măsurile corespunzătoare de atenuare, inclusiv monitorizarea sistemelor critice la granițele externe și la punctele interne cheie.

Recuperarea în caz de dezastru

- [ ] Se va elabora și executa un proces de recuperare în caz de dezastre și incidente legate de informație/securitate cibernetică.Sunt efectuate periodic evaluări interne sau externe de securitate?
- [ ] Funcțiile și serviciile esențiale ale organizației vor fi continuate cu pierderi minime sau fără pierderi în ceea ce privește continuitatea operațională, iar continuitatea va fi menținută până la recuperarea completă a sistemului.Este păstrată documentația necesară pentru a demonstra funcționarea controalelor?
- [ ] Organizația va desemna un responsabil cu relațiile publice (PRO) pentru a gestiona comunicarea publică în timpul recuperării în urma incidentelor de securitate informatică/cibernetică.
- [ ] Organizația va implementa o strategie de comunicare în situații de criză pentru a atenua impactul negativ în timpul unei crize și pentru a contribui la restabilirea reputației sale după aceea.

8

Conformitate și Îmbunătățire Continuă

- [ ] Sunt controalele de securitate monitorizate pentru eficacitate?
- [ ] Sunt efectuate periodic evaluări interne sau externe de securitate?
- [ ] Sunt constatările din audit documentate și remediate?
- [ ] Este păstrată documentația necesară pentru a demonstra funcționarea controalelor?
- [ ] Este programul de securitate actualizat pe baza lecțiilor învățate și a modificărilor de risc?