

PARLAMENTUL ROMÂNIEI

SENAT

CAMERA DEPUTAȚILOR

Lege privind măsurile de securitate ale sistemelor informatice

Parlamentul României adoptă prezenta lege

Capitolul I Dispoziții generale

Domeniul de aplicabilitate

Art. 1. - (1) Prezenta lege reglementează sistemul de măsuri minime de securitate aplicabile sistemelor informatice din administrația publică.

(2) Sistemul de măsuri de securitate se compune din specificațiile privind măsurile de securitate organizatorice precum și măsurile de securitate tehnice luate pentru protejarea datelor.

(3) Prezenta lege nu se aplică în cazul sistemelor informatice de prelucrare a datelor secrete de stat.

Punerea în aplicare a sistemului de măsuri de securitate

Art. 2. - Punerea în aplicare a sistemului de măsuri de securitate constă în:

- a) stabilirea claselor de securitate care sunt conforme cu obiectivele de securitate;
- b) selectarea măsurilor de securitate adecvate în conformitate cu direcțiile generale pentru punerea în aplicare a unui sistem de securitate de bază pentru sistemele de informare;
- c) aplicarea măsurilor de securitate.

Definiții

Art. 3. - În înțelesul prezentei legi, termenii și expresiile de mai jos se definesc astfel:

- a) analiza securității datelor - evaluarea cu privire la importanța datelor și a daunelor generate de lipsa unor proceduri de securitate efectuate pentru determinarea clasei de securitate;
- b) măsuri de securitate de bază - măsuri de securitate standard, furnizate cu o metodă de selecție, selectarea depinzând de clasa de securitate și de componența sistemului informatic de prelucrare a datelor;
- c) securitate de bază - aplicarea măsurilor de securitate care sunt necesare pentru obținerea și păstrarea securității informației;
- d) sistem de informații - un sistem tehnic de prelucrare, salvare sau de transmitere a datelor împreună cu mijloacele, resursele și procesele necesare pentru o funcționare normală;
- e) securitatea informației - un set de procese pentru generarea, selecția și aplicarea măsurilor de securitate;
- f) măsuri de securitate - operațiunile de organizare, procese tehnice și aplicarea unor mijloace tehnice de realizare, păstrare și de securizare a datelor din sistemele de informații;
- g) clasă de securitate - nivelul cerut de asigurare a securității informației, care decurge din importanța datelor exprimat pe o scară de patru nivele; trei sub-clase de securitate apar de la cele trei obiective ale securității informației.
- h) disponibilitatea claselor de securitate - acces ușor și în timp scurt la date pe durata de timp stabilită anterior (la momente și perioade de timp stabilite) pentru persoane autorizate sau în cazul problemelor tehnice.
- i) integritatea claselor de securitate - garanția de corectitudine, caracterul complet, versiunea actuală și autenticitatea datelor, precum și absența unor modificări neautorizate.
- j) confidențialitatea claselor de securitate - accesul la date doar pentru persoanele autorizate sau în cazul problemelor tehnice.

Capitolul II

Clase de securitate și măsurile de securitate

Specificații ale măsurilor de securitate

Art. 4. - (1) Determinarea clasei de securitate, în conformitate cu obiectivele de securitate a informațiilor de către administratorul sistemelor informatice se face în urma unei analize a sistemelor informatice ale instituției publice.

(2) Clasa de securitate stabilită pentru informațiile din sistemele informatice ale instituțiilor publice, împreună cu documentația tehnică aferentă și operațiuni privind depozitarea și actualizarea datelor se aprobă în conformitate cu procedura care va fi reglementată prin Norme tehnice și metodologice.

(3) Măsurile de securitate corespunzătoare pentru o clasă de securitate se pun în aplicare înainte de momentul în care un sistem informatic este implementat și pe toată perioada folosirii acestuia.

Modul de formare și obiectivele claselor de securitate

Art. 5. - (1) Ca urmare a analizei privind securitatea, administratorul sistemelor informatice va dispune determinarea claselor de securitate corespunzătoare, independente una față de cealaltă, pe baza obiectivelor securității informației și a importanței realizării acestora.

(2) Determinarea claselor de securitate se va realiza pe baza obiectivelor securității informației, respectiv fiabilitatea, integritatea și confidențialitatea.

(3) În funcție de fiabilitatea claselor de securitate, acestea sunt determinate pe o scară de la F0 la F3, după cum urmează:

a) F0 - fiabilitatea - nu are importanță; performanță - nu are importanță;

b) F1 - fiabilitatea - 90% (suspendare de activitate total admis într-o săptămână ~ 24 de ore); viteza de răspuns în timpul de sarcină maximă la orele de vârf - ore (1 ÷ 10)

c) F2 - fiabilitate - 99% (suspendare de activitate total admis într-o săptămână ~ 2 ore); viteza de răspuns în timpul de sarcină maximă la orele de vârf - minute (1 ÷ 10);

d) F3 - fiabilitate - 99,9% (suspendare de activitate total admis într-o săptămână ~ 10 minute); viteza de răspuns în timpul de sarcină maximă la orele de vârf - secunde ($1 \div 10$).

(4) În funcție de integritatea claselor de securitate, acestea sunt determinate pe o scară de la I0 la I3 , după cum urmează:

a) I0 - sursa de informații, detectarea alterării sau distrugerii - nu are importanță, verificarea corectitudinii, integrității și dacă este ultima versiune – nu are importanță;

b) I1 - sursa de informații, detectarea alterării sau distrugerii – trebuie să fie detectabilă, verificarea corectitudinii, integrității și dacă este ultima versiune – în cazuri speciale dacă este necesară;

c) I2 - sursa de informații, detectarea alterării sau distrugerii – trebuie să fie detectabilă, verificarea periodică a corectitudinii, integrității și dacă este ultima versiune obligatorie;

d) I3 - sursa de informații, detectarea alterării sau distrugerii – trebuie să aibă valori evidențiate, verificarea în timp real a corectitudinii, integrității și dacă este ultima versiune obligatorie;

(5) În funcție de confidențialitatea datelor, clasele de securitate sunt determinate pe o scară de la C0 la C3, după cum urmează:

a) C0 – acces public: accesul la informație nu este limitat (de exemplu, toate persoane interesate au dreptul de a citi date; dreptul de a modifica datele sunt stabilite de către cerințele de integritate);

b) C1 - informații pentru uz intern: accesul la informație este permis cu condiția ca persoana care face cerere de acces să aibă un interes legitim;

c) C2 - informații confidențiale: utilizarea informațiilor este permisă numai la anumite grupuri de utilizatorii; accesul la informație este permisă cu condiția ca persoana care solicită acces să aibă interes legitim;

d) C3 - informații secrete: utilizarea informațiilor este permisă numai la anumiți utilizatorilor; accesul la informație este permis cu condiția ca persoana care solicită acces să aibă interes legitim;

Modul de formare al claselor de securitate

Art. 6. - Codul unei clase de securitate este format din codurile obiectivelor de securitate, în ordinea FIC.

Selecția măsurilor de securitate corespunzătoare claselor de securitate

Art. 7. - (1) Pentru a garanta obiectivele securității informației unui sistem informatic din Administrația Publică care prelucrează date, măsurile de securitate trebuie să fie aplicate și să se conformeze claselor de securitate stabilite, în funcție de codul de securitate rezultat în urma analizei de securitate.

(2) Măsurile de securitate se selectează în conformitate cu clasa de securitate, în conformitate cu modul de formare al claselor de securitate.

(3) Modul de implementare al măsurilor minime de securitate pentru sistemele informatice din administrația publică se aprobă de către MCSI și se publică pe pagina de Internet a instituției.