Anexa nr. 1 la Ordinul nr. 1572/10.11.2022

**INSTITUTUL NAŢIONAL DE STATISTICĂ**
**B-dul Libertăţii nr. 16 sector 5, Bucureşti**

**APROBAT,**
**PREŞEDINTE**
**Tudorel ANDREI**

ROMÂNIA
CABINETUL PREŞEDINTELUI
INSTITUTUL NAŢIONAL DE STATISTICĂ

**AVIZAT,**
**Vicepreşedinte**
**Beatrix GERED**

# Politica de securitate a informaţiilor INS

**Verificat,**

Radu Mugur Oprea, director
Mioara Rădoi, director

**Elaborat,**

Artur Emilian Simion, director
Dan Dumitru Marcu, şef serviciu
Doinița Demetrescu, şef serviciu
Cristian Beldiman, şef serviciu
Andrei Răzvan Pavel, consilier superior
Claudia Căpățână, şef serviciu

## Cuprins

# 1 Introducere

Scopul acestei politici este de a proteja activele informatice ale INS, stabilind cadrul pentru un mediu sigur.

Această politică oferă principii generale, cerințe și recomandări specifice pentru protejarea integrității, disponibilității și confidențialității activelor informatice, inclusiv hardware, software și informații, rețele și sisteme.

Această politică stabilește rolurile și responsabilitățile generale pentru structura de securitate a informațiilor.

## 1.1 Domeniul de aplicare

Politica de securitate a informațiilor se aplică tuturor funcțiilor instituţiei și acoperă sistemele informatice, rețelele, mediul fizic, persoanele relevante care susțin aceste funcții și date ale instituţiei.

Această politică se aplică tuturor angajaților INS și furnizorilor de servicii (terţi).

Obiectivul acestei politici este de a asigura securitatea activelor INS, inclusiv a rețelelor, a sistemelor informatice, a software-ului și a datelor care trebuie protejate împotriva utilizării neautorizate și divulgării.

Această politică stabilește principiile, obiectivele, organizarea și responsabilitățile de bază privind securitatea:

- Informații pe toate suporturile, inclusiv pe hârtie, și acoperă securitatea fizică a acestor medii, precum și accesul logic la acestea.
- Sisteme informatice care gestionează astfel de informații atunci când un sistem informatic este furnizat, deținut, administrat sau exploatat de o parte externă pe baza unui acord bilateral sau a unui contract cu INS, termenii acordului sau contractului trebuie să respecte această politică.

Informațiile digitale sunt considerate un atuu important și trebuie evaluate în mod corespunzător și protejate împotriva tuturor formelor de acces, utilizare, dezvăluire, modificare, distrugere sau respingere neautorizată.

Controlul securității informațiilor trebuie să fie suficient pentru a asigura confidențialitatea, integritatea, disponibilitatea, responsabilitatea și auditabilitatea informațiilor importante.

## 1.2 Angajamentul Managementului

Preşedintele INS aprobă în mod formal următoarea declaraţie ca Politică de Securitate a Informaţiei.

INS trebuie să asigure:

- respectarea obligațiilor sale privind securitatea informațiilor, și anume confidențialitatea, integritatea și nivelul de disponibilitate a informațiilor ca aspect absolut și inseparabil al confidențialității statistice și al calității serviciilor.
- să ia toate măsurile necesare pentru a asigura confidențialitatea datelor statistice în conformitate cu Regulamentul 223/2009 privind statisticile europene, astfel cum a fost modificat prin Regulamentul 759/2015, cu Regulamentul 557/2013 al Comisiei privind accesul la date confidențiale în scopuri științifice, Codul de Practici al statisticilor europene și orice altă legislație referitoare la confidențialitatea statistică în domeniul statisticilor europene.
- să se asigure că problemele de securitate sunt luate în considerare de la începutul dezvoltării și punerii în aplicare a programelor, proiectelor și activităților sale.
- să dezvolte, să-și exercite și să-și mențină sistemul de management al continuității activității.
- să asigure protecția vieții private și libera circulație a datelor cu caracter personal în conformitate cu Regulamentul specific.
- să încurajeze inițiativele adecvate de sensibilizare a personalului cu privire la furnizarea acestei politici de securitate a informațiilor, inclusiv a rolurilor, responsabilităților, proceselor și măsurilor de control.
- să verifice cu regularitate respectarea acestei politici prin audit, revizuire, testare, monitorizare tehnică și executare sau orice alte mijloace considerate adecvate.

Politicile și procedurile de securitate a informațiilor, inclusiv continuitatea activității, sunt definite, documentate, aprobate de conducerea INS, publicate intern și comunicate întregului personal și altor părți relevante.

Personalul de conducere va întreprinde acțiuni pentru punerea în aplicare a prezentei dispoziții privind politica de securitate a informațiilor în procesele din domeniile lor de activitate, direcționând și sprijinind personalul pentru a contribui la eficacitatea acestora în materie de securitate.

Această politică va fi revizuită o dată pe an sau când vor apărea modificări semnificative ale entității legate de securitatea informațiilor.

Toți angajații sunt formal obligați să respecte această politică și să-și îndeplinească responsabilitățile așa cum sunt definite.

Conducerea INS înțelege importanța protejării bunurilor informatice şi a asigurării securităţii informaţiilor, prin structurile organizatorice componente. Ofiţerul de Securitate Informatică / expertul în securitatea informațiilor (ISO) va coordona activitățile de securitate a informațiilor în cadrul INS.

ISO este sprijinit în activitatea sa prin diverse funcții din cadrul entității: Comisia de monitorizare, direcții IT, resurse umane, Serviciul securitate în muncă şi a informaţiilor.

Conducerea INS se angajează să reducă în mod continuu riscurile prin asigurarea unei protecții eficiente și rentabile proporționale cu riscurile activelor sale.

## 1.3 Obiective generale

INS va proteja toate activele informatice aflate sub controlul său, prin implementarea unui set de măsuri tehnice și non-tehnice bine echilibrate.

Obiectivele Politicii de Securitate a Informațiilor INS sunt:

- Definirea domeniului de aplicare al sistemului de management al securității informațiilor
- Exprimarea angajamentului conducerii INS pentru securitatea informațiilor
- Stabilirea de roluri și responsabilități pentru securitatea informațiilor
- Integrarea tuturor aspectelor, cerințelor și practicilor de securitate a informațiilor INS într-un singur cadru de politică coerent
- Asigurarea unui cadru pentru viitoarele evoluții în domeniul securității informațiilor în INS
- Sprijinirea continuă a procesului de sensibilizare a personalului INS în ceea ce privește securitatea informațiilor
- Asigurarea coerenței cu alte procese stabilite în INS care pot implica un element de securitate, inclusiv Managementul continuității activităților și recuperarea în caz de dezastru.

# 2 Securitatea informațiilor și a IT-ului

## 2.1 Securitatea fizică

INS trebuie să orchestreze punerea în aplicare a contramăsurilor necesare pentru a asigura protecția fizică a datelor, proceselor și sistemelor care îndeplinesc cerințele minime de securitate fizică în conformitate cu politica de securitate fizică.

### 2.1.1 Perimetrul de securitate fizică

Accesul în clădirea INS este controlat și este rezervat personalului permanent sau temporar și vizitatorilor autorizați.

### 2.1.2 Zonele securizate

Accesul în zonele cu acces restricționat este permis numai personalului autorizat, bazat pe cartele individuale de acces sau chei fizice și va fi acordat numai pentru nevoile instituției.

Se păstrează un jurnal pentru toate accesările în zonele securizate.

### 2.1.3 Securitatea echipamentelor în afara INS

Echipamentele, informațiile sau software-ul nu trebuie să fie scoase din incinta INS fără autorizație prealabilă. Trebuie să se aplice o protecție adecvată echipamentelor din afara amplasamentului, luând în considerare diferitele riscuri de lucru în afara incintei INS.

### 2.1.4 Evacuarea sau reutilizarea sigură a echipamentului

Toate echipamentele care conțin suporturi de stocare, inclusiv suporturi amovibile, fie trebuie să fie verificate pentru a se asigura că toate datele sensibile și software-ul licențiat au fost eliminate, fie au fost suprascrise în siguranță înainte de eliminare sau trimitere înapoi pentru reparare sau trebuie distruse în siguranță.

### 2.1.5 Politica biroului curat

Pentru a minimiza posibilitatea pierderii de date, a furtului sau a dezvăluirii neautorizate, personalul trebuie să adopte practici conștiente de securitate la locul de muncă. Acest lucru necesită blocarea tuturor datelor sensibile asupra materialelor fizice atunci când nu sunt utilizate (politica biroului curat). Personalul trebuie să presupună că locul de muncă poate fi accesat de către persoane din afară. Prin urmare, angajații nu trebuie să-și părăsească terminalul conectat și nesupravegheat, trebuie să aleagă parole nontriviale și să le păstreze în siguranță.

În plus, PC-urile sau stațiile de lucru cu acces la date sensibile sau acordarea privilegiilor administratorului local sunt supuse unor controale de acces îmbunătățite.

## 2.2 Managementul activelor

Datele, procesele și sistemele INS sunt considerate ca fiind active vitale și trebuie protejate într-o manieră adecvată pentru importanța și valoarea lor pentru instituție. Pentru a stabili și menține nivelul adecvat de protecție, aceste active trebuie înregistrate și clasificate.

### 2.2.1 Clasificarea informațiilor

Următoarele controale trebuie implementate:

Toate activele hardware și software importante asociate sistemelor informatice INS sunt identificate și înregistrate în registrul de active sau în inventar.

Pentru toate sistemele și datele de informare trebuie să li se atribuie un nivel de clasificare a confidențialității și un nivel de clasificare a integrității / disponibilității în conformitate cu schema definită în Politica de clasificare a informațiilor.

Toate materialele fizice (de ex. Imprimate, CD-ROM-uri, benzi de rezervă etc.) trebuie să fie marcate și manipulate în mod corespunzător, în funcție de nivelul de clasificare a informațiilor conținute, așa cum se specifică în Politica de clasificare a informațiilor.

Bunurile informatice sunt gestionate și controlate pe toată durata ciclului lor de viață (crearea, depozitarea, manipularea și eliminarea) într-o manieră adecvată cerințelor de securitate.

### 2.2.2 Responsabilitatea pentru active

Politica de securitate a informațiilor din cadrul INS este cadrul pentru asigurarea confidențialității, integrității și disponibilității informațiilor bunurilor informatice INS.

Pentru o gestionare eficientă a bunurilor informatice, aceștia trebuie să aibă un proprietar desemnat și trebuie să fie protejați într-o manieră proporțională cu valoarea și sensibilitatea lor de afaceri.

## 2.3 Continuitatea activității

INS va stabili cerințele de securitate a informațiilor în cazul unei întreruperi operaționale și le va documenta în analiza Impactului asupra activității.

Trebuie elaborat un plan pentru BCP cu lista sistemelor și a facilităților care ar trebui restaurate în timpii stabiliți de SLA și BIA.

Testele BCP trebuie să fie executate cel puțin anual, sunt programate și coordonate de ISO.

ISO coordonează procesul de continuitate a activității.

## 2.4 Managementul schimbărilor

### 2.4.1 Cerințele de securitate ale sistemelor informatice

Gestionarii sistemelor trebuie să se asigure că cerințele de securitate adecvate sunt implementate corespunzător în conformitate cu politicile și standardele în vigoare. Identificarea și gestionarea cerințelor de securitate a informațiilor și a proceselor asociate trebuie să fie integrate în stadiile incipiente ale proiectelor de sisteme informatice și să fie justificate, convenite și documentate ca parte a documentației proiectului.

Toate propunerile de noi aplicații sau modificări majore ale aplicațiilor existente trebuie să conțină o secțiune care să identifice riscurile de securitate și măsurile de combatere propuse.

Toate fazele din cadrul unei aplicații informatice / ciclul de viață al sistemului (de la inițiere până la proiectare, dezvoltare, testare, desfășurare, întreținere, operare și sprijin) adoptă măsuri adecvate, determinate de procesul de evaluare a riscurilor.

### 2.4.2 Achiziționarea și dezvoltarea de software

Decizia de achiziție sau de dezvoltare internă a unui software trebuie făcută pe baza unui studiu de fezabilitate care susține decizia. Cerințele pentru noul sistem / aplicație trebuie să includă și cerințele pentru controalele de securitate.

Pentru viitorul sistem / aplicație va fi efectuată o evaluare a riscurilor pentru a se asigura integrarea controalelor de securitate corespunzătoare.

Toate noile sisteme de informații sau îmbunătățiri ale sistemelor existente trebuie să fie autorizate de către gestionarii sistemelor și ISO.

### 2.4.3 Testarea și întreținerea software-ului

Pentru toate sistemele critice și sensibile, mediile de dezvoltare și testare trebuie separate de facilitățile operaționale. În plus, trebuie definite și documentate norme clare pentru migrarea software-ului de la dezvoltare la starea operațională.

Înainte de acceptare, toate sistemele noi sau actualizate vor fi testate pentru a se asigura că respectă cerințele politicii de securitate a informațiilor INS și cerințele de securitate a informațiilor.

### 2.4.4 Autorizarea schimbării

Toate modificările aduse sistemelor informatice, aplicațiilor sau rețelelor trebuie să fie aprobate de poziții relevante din INS înainte de a fi puse în aplicare.

### 2.4.5 Gestionarea configurației

Toate sistemele utilizate de INS sunt configurate numai de personalul desemnat.

Modificările neautorizate ale configurației sistemului sunt interzise.

## 2.5 Securitatea managementului operațional

INS va asigura funcționarea corectă și sigură a facilităților de procesare a informațiilor.

### 2.5.1 Backup și recuperare

Back-up-ul datelor INS trebuie făcut la toate mediile relevante. Toate suporturile de rezervă (casete, discuri etc.) trebuie să fie etichetate și criptate în mod clar. Datele de rezervă trebuie să fie stocate atât în cadrul INS, cât și într-o locație în afara amplasamentului. Atât locațiile INS, cât și locațiile din afara amplasamentului trebuie să implementeze controale de securitate pentru a proteja datele de accesul neautorizat sau amenințările naturale. Echipamentele din afara amplasamentului trebuie să fie amplasate la distanță de sediul INS pentru a nu fi afectate în cazul în care sediul INS ar fi grav afectat (de exemplu prin incendii, inundații, cutremure sau explozii).

### 2.5.2 Protecția împotriva malware-ului

INS a implementat măsuri pentru detectarea și protejarea sistemelor informatice, a aplicațiilor și a rețelelor împotriva virușilor și a altor programe rău intenționate (de exemplu, cai troieni, viermi, viruși etc.)

Toate echipamentele INS care permit sunt protejate de software antivirus.

Niciun software nu poate fi instalat, stocat sau utilizat în sistemele INS, cu excepția cazului în care a fost autorizat oficial.

Toate suporturile de date (stick USB, hard disk, CD / DVD-Rom, etc.) trebuie să fie verificate înainte de a fi introduse în orice sistem al INS.

Toate mesajele primite și trimise trebuie să fie scanate pentru conținut necorespunzător sau rău intenționat.

O avertizare corespunzătoare trebuie atribuită tuturor e-mailurilor trimise în afara rețelei INS.

Trebuie să existe un sistem pentru gestionarea mesajelor spam.

Toți utilizatorii sunt responsabili pentru raportarea oricărui virus sau a unei activități rău intenționate către echipa de asistență IT.

Echipa IT Helpdesk este responsabilă pentru asigurarea că toate incidentele virușilor raportate de utilizatori sunt înregistrate și investigate.

Administratorii de sistem sunt responsabili pentru:

- asigurarea instalării software-ului antivirus pe toate computerele utilizatorilor
- asigurarea faptului că definițiile virușilor sunt actuale
- sunt responsabili de protecția antivirus a serverelor.

### 2.5.3 Segregarea îndatoririlor și a facilităţilor

Atribuțiile și domeniile de responsabilitate trebuie să fie separate pentru a reduce posibilitățile de modificare neautorizată sau intenționată sau de utilizare necorespunzătoare a sistemelor informatice.

Segregarea sarcinilor este folosită pentru a împărți responsabilitatea finalizării unui proces în acțiuni distincte și responsabile și pentru a evita conflictele de interese.

Sistemele de dezvoltare, testare și operare trebuie să fie separate pentru a reduce riscul accesului neautorizat sau al modificărilor sistemului operațional.

Domeniile trebuie separate pentru a reduce posibilitățile de modificare neautorizată sau intenționată sau de utilizare necorespunzătoare a sistemelor informatice. Separarea domeniilor poate fi făcută pe baza nivelurilor de încredere (de exemplu, domeniul desktopurilor, domeniul serverelor, domeniul de acces public etc.). Perimetrul fiecărui domeniu trebuie să fie bine definit, controlând traficul între domenii utilizând un gateway activ (de exemplu, firewall, router de filtrare etc.).

### 2.5.4 Exploatarea și monitorizarea

Pentru a detecta activitățile neautorizate de prelucrare a informațiilor, INS trebuie să aibă și să mențină o abordare consecventă în ceea ce privește colectarea și analizarea datelor din logare și audit, cum ar fi activitățile utilizatorilor legate de informații sensibile, excepțiile și evenimentele de securitate ale sistemelor de informare sau defectele din facilitățile de procesare a informațiilor. Informațiile din jurnal se păstrează timp de cel puțin 3 luni pentru a sprijini investigațiile viitoare.

Facilitățile logare și informațiile din jurnal trebuie să fie protejate împotriva modificărilor, editării neautorizate sau ștergerii fișierelor de jurnal. Măsurarea capacității de stocare a suportului pentru fișierele de jurnal trebuie să fie făcută pentru a preveni depășirea acesteia, ducând la eșecul evenimentelor înregistrate sau la supra-scrierea evenimentelor înregistrate anterior.

Ceasurile tuturor sistemelor relevante de procesare a informațiilor pentru INS trebuie sincronizate cu o singură sursă de timp de referință, pentru a asigura corectitudinea jurnalelor de audit.

Toate încălcările potențiale ale securității trebuie raportate, înregistrate și investigate de echipa de investigare.

### 2.5.5 Gestionarea livrării de servicii terță parte

- Livrarea serviciilor - serviciile furnizate de terți implicând accesarea, prelucrarea, comunicarea sau gestionarea informațiilor sau a facilităților de procesare a informațiilor sau adăugarea de produse sau servicii către facilitățile de procesare a informației trebuie să aibă un control integrat corespunzător al securității. Aceste controale de securitate, definiția serviciului și nivelurile de livrare trebuie să fie documentate în acordurile de livrare ale serviciilor, astfel încât să se asigure că acestea sunt puse în aplicare, operate și întreținute în mod corespunzător de terța parte.
- Monitorizarea și revizuirea serviciilor terților - Serviciile, rapoartele și înregistrările furnizate de terți sunt gestionate de personal desemnat, monitorizate periodic și revizuite, iar audituri trebuie efectuate periodic.

## 2.6 Managementul incidentelor

Indiferent de locul în care sunt detectate, provocările semnificative cu privire la securitatea sistemelor informatice INS trebuie comunicate astfel încât să permită luarea măsurilor corective adecvate în cel mai eficient mod, în conformitate cu Politica de gestionare a incidentelor de securitate a informațiilor.

Aceasta necesită:

- stabilirea unui proces adecvat de raportare a incidentelor de securitate. Acest proces trebuie să antreneze cât mai repede posibil părțile interesate corecte și să asigure răspunsuri eficiente la aceste incidente.
- părțile interesate trebuie să evalueze fiecare eveniment de securitate a informațiilor și să decidă dacă evenimentul trebuie clasificat drept incident de securitate a informațiilor. Clasificarea și prioritizarea incidentelor poate ajuta la identificarea impactului și a amplorii unui incident.
- stabilirea unor mecanisme care să raporteze cu privire la apariția și analiza incidentelor de securitate în cadrul structurii organizatorice, pentru a se asigura că pot fi luate măsuri corective adecvate.
- întregul personal din cadrul structurii organizatorice va raporta la IT Help Desk orice deficiențe de securitate din cadrul sistemelor sau serviciilor.

Orice încălcare a politicilor de securitate a informațiilor cauzate de un angajat va fi investigată și ar putea face obiectul unor măsuri disciplinare.

## 2.7 Controlul accesului

### 2.7.1 Accesul la informații și sisteme

Un proces oficial de înregistrare a utilizatorilor și de dezabonare trebuie să fie pentru a permite alocarea drepturilor de acces, în conformitate cu Politica de control al accesului.

Accesul la sisteme și informații se bazează pe conturi individuale și se limitează doar la conturile active.

Alocarea și utilizarea privilegiilor trebuie restrânse și controlate, examinându-i drepturile de acces la intervale regulate după un proces formal.

Accesul se va acorda numai pentru îndeplinirea atribuțiilor de serviciu.

Alocarea și utilizarea privilegiilor, cum ar fi drepturile de administrare locală pentru accesul la informații confidențiale (C2 sau C3), trebuie restricționate, monitorizate și controlate.

Drepturile de acces ale angajaților și ale utilizatorilor externi ai INS la facilitățile de informare și prelucrare a informațiilor trebuie eliminate la terminarea angajării, contractului sau acordului sau ajustate după schimbare.

### 2.7.2 Acces la distanță

Accesul de la distanță la rețeaua și resursele INS trebuie să utilizeze tehnologia VPN (Virtual Private Network). Trebuie să existe implementat un mecanism puternic de autentificare și criptare.

Accesul se va acorda numai pentru îndeplinirea atribuțiilor de serviciu.

Pentru a asigura acest lucru, trebuie implementat un set de controale.

Acesul în anumite aplicații este permis numai folosind desktop-uri virtuale.

### 2.7.3 Acces la Internet

Accesul la internet prin intermediul infrastructurilor IT INS este permis să-l folosească numai în scopuri profesionale, folosind un server PROXY.

Filtrarea pe internet trebuie să fie în vigoare.

Pentru a asigura acest lucru, trebuie implementat un set de controale.

### 2.7.4 Calculatoare mobile

Dispozitivele computerizate mobile (laptop-uri, PDA-uri, telefoane mobile, telefoane inteligente și alte echipamente mobile de calcul) prezintă riscuri deosebite care trebuie atenuate prin măsuri de securitate adecvate.

# 3 Responsabilități

## 3.1 Responsabilități generale

Președintele INS este responsabil pentru securitatea activelor informaționale ale instituției. Președintele INS aprobă politica de securitate a informațiilor și asigură mijloacele de implementare. Catalizează eficiența sarcinilor ISO și se asigură că ISO are suficientă autonomie, timp, resurse și suport pentru a-și îndeplini responsabilitățile, inclusiv sprijinul activ al conducerii superioare.

Conducerea INS este responsabilă pentru numirea proprietarilor de active noi și a noilor proprietari pentru activele existente atunci când este necesar.

Întregul personal al INS este responsabil pentru aplicarea politicilor și procedurilor de securitate a informațiilor.

## 3.2 ISO

ISO este responsabil pentru:

- Coordonarea revizuirii periodice a implementării standardelor IS
- Comunicarea planului de acțiune aprobat de conducere
- Evidența activelor de informații ale INS și a riscurilor asociate acestora
- Efectuarea auditului intern, raportarea constatărilor și formularea de recomandări
- Coordonarea echipei de investigare.

## 3.3 Echipa de investigare

Echipa de investigare este responsabilă pentru:

- Analizarea incidentelor raportate
- Determinarea naturii incidentului și recomandarea acțiunilor corective pentru prevenirea și soluționarea incidentelor de securitate a informațiilor
- Urmărirea soluționării incidentelor
- Analizarea și raportarea incidentelor la conducerea INS.

## 3.4 Gestionarul de active (sisteme)

Gestionarul sistemului este responsabil pentru:

- Identificarea și gestionarea riscurilor pentru activitățile informatice
- Asigurarea accesului la informația activelor numai personalului autorizat
- Asigurarea elaborării, implementării, urmăririi și revizuirii periodice a proceselor și procedurilor locale coerente

- Monitorizarea și raportarea conformității cu legislația, statutul și contractul în ceea ce privește activele informatice
- Raportarea incidentelor.

### 3.5 Administratorii de sisteme (active informatice)

Administratorii de sisteme sunt responsabili pentru:

- Furnizarea de informații tehnice privind standardul / cadrul
- Protejarea informațiilor, inclusiv implementarea sistemelor de control al accesului pentru a preveni divulgarea inadecvată și crearea de copii de rezervă pentru ca informațiile critice să nu se piardă
- Raportarea incidentelor.

### 3.6 Personalul de conducere

Personalul de conducere este responsabil pentru:

- Documentarea proceselor / procedurilor de coordonare
- Aplicarea standardelor
- Raportarea incidentelor
- Asigurarea faptului că personalul din subordine este conștient de responsabilitățile de securitate.

### 3.7 Responsabilitățile managerilor de proiect

Managerii de proiect sunt responsabili pentru introducerea cerințelor de securitate în specificațiile funcționale pentru toate proiectele. Aceștia sunt, de asemenea, responsabili să verifice dacă soluția implementată respectă specificațiile cerute și convenite.

### 3.8 Responsabilitățile angajaților

Întregul personal al INS trebuie să asigure:

- Protejarea hardware-ului, a software-ului și a informațiilor aflate în gestiune
- Prevenirea introducerii de software rău intenționat în sistemele informatice ale INS
- Raportarea oricărei încălcări suspecte sau reale a securității
- Respectarea politicilor de securitate ale INS

# 4 Termeni și abrevieri

Administratorul de active informatice (sisteme) - persoana responsabilă de supravegherea și punerea în aplicare a controalelor tehnice și operaționale, care deține controlul tehnic asupra unui activ informativ. Un activ poate avea unul sau mai mulți administratori pentru diferite sarcini tehnice.

BCP - Planificarea continuității activităţii

Gestionarul de active informatice (sisteme) - persoana căreia i s-au alocat responsabilități și care deține răspunderea pentru un activ informativ. Aceasta are responsabilitatea de a se asigura că activele informatice sunt gestionate și operate corespunzător. Aceasta înseamnă asigurarea faptului că bunurile informaționale sunt protejate în mod corespunzător și că valoarea acestora pentru instituție este pe deplin exploatată.

ISO - Ofițer de securitate a informațiilor/Expert în securitatea informațiilor

Serverul PROXY - un computer dedicat sau un sistem software care rulează pe un computer, care acționează ca intermediar între un dispozitiv punct final, cum ar fi un computer, și un alt server de la care un utilizator sau un client solicită un serviciu.

SLA - Acord privind nivelul serviciilor

VPN - Rețea privată virtuală

# Foaie de Control

## Istoricul Reviziilor:

| Versiunea | Data | Motivul revizuirii |
|---|---|---|
| V1.1 | 12.06.2020 | Revizuire periodică |
| V1.2 | 23.06.2021 | Revizuire periodică |
| V1.3 | 08.11.2022 | Revizuire periodică |