CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ – CERT-RO

REGULAMENT

DE ORGANIZARE ȘI FUNCȚIONARE

A

CENTRULUI NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ – CERT-RO

Director general,

Petrică-Cătălin ARAMĂ

București, 06 septembrie 2019
Nr. 975

Prezentul Regulament a fost avizat de Comitetul de coordonare întrunit în ședința din data de 19.08.2019, conform etapelor stabilite în Minuta nr. 887/20 august 2019.

www.cert.ro office@cert.ro (+40) 0316.202.187 str. Italiană 22, etaj 6, sector 2, 020976 București, România

[Pagină albă]

Aviz pentru introducerea documentului pe ordinea de zi
a ședinței Consiliului Suprem de Apărare a Țării
GUVERNUL ROMÂNIEI

Vasilica-Viorica DĂNCILĂ
Prim-ministru

MINISTERUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE

Alexandru PETRESCU
Ministrul comunicațiilor și societății informaționale

[Pagină albă]

CUPRINS

[Pagină albă]

TITLU I. DISPOZIȚII GENERALE

Art. 1. – (1) Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, denumit în continuare *CERT-RO*, este instituție publică cu personalitate juridică, în coordonarea Ministerului Comunicațiilor și Societății Informaționale, denumit în continuare *MCSI*, finanțată conform prevederilor Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare.

(2) CERT-RO este autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice care asigură furnizarea de servicii esențiale ori furnizează servicii digitale în sensul prevăzut de Legea nr. 362/2018, cu modificările și completările ulterioare, cu atribuții de reglementare, autorizare, atestare, monitorizare și control, cuprinzând în structura sa o echipă națională de răspuns la incidente de securitate informatică și un punct unic de contact la nivel național.

(3) CERT-RO este o structură independentă de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice.

Art. 2. – CERT-RO este organizat și își desfășoară activitatea în conformitate cu dispozițiile Legii nr. 362/2018, cu modificările și completările ulterioare, Hotărârii Guvernului nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, cu modificările și completările ulterioare, cu legislația română în vigoare și cu prevederile prezentului Regulament de organizare și funcționare, denumit în continuare *regulament*.

Art. 3. – (1) CERT-RO are sediul central în Municipiul București.

(2) În vederea asigurării activităților și reprezentării adecvate pentru îndeplinirea obligațiilor ce îi revin în temeiul Legii nr. 362/2018, cu modificările și completările ulterioare, CERT-RO poate înființa birouri și sedii la nivel local, în limita numărului de posturi aprobate.

Art. 4. – (1) CERT-RO colaborează cu instituțiile Uniunii Europene, cu autorități similare din alte state și poate participa la activitatea unor organizații internaționale din domeniul său de activitate ori poate să devină membră a acestora.

(2) În exercitarea atribuțiilor legale, CERT-RO cooperează cu instituții publice sau alte persoane juridice de drept public sau privat, naționale sau internaționale pentru asigurarea disponibilității, confidențialității, integrității, autenticității și non-repudierii informațiilor în format electronic, în scopul prevenirii, analizei, identificării și reacției la incidente cibernetice.

(3) În calitate de autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale identificate în temeiul Legii nr. 362/2018, CERT-RO se consultă și cooperează cu autoritățile și entitățile care reglementează sectoarele și subsectoarele de activitate prevăzute în anexa la legea mai sus menționată, precum și cu autoritățile și entitățile prevăzute la art. 15 alin. (2) din aceeași lege.

Art. 5. – (1) La nivelul CERT-RO sunt gestionate și utilizate informații publice, informații nedestinate publicității și informații clasificate atât naționale, cât și NATO, UE și/sau ale statelor și organizațiilor cu care a încheiat înțelegeri de cooperare.

(2) Circuitul documentelor gestionate de CERT-RO, inclusiv modul de utilizare a registrelor utilizate în cadrul instituției, se reglementează prin proceduri operaționale sau decizii interne ale directorului general.

(3) Toate documentele intrate, ieșite ori întocmite pentru uz intern se înregistrează la nivelul CERT-RO. Înregistrarea documentelor se face la registratura generală, în registre de intrare-ieșire, precum și la nivelul Direcției Reglementare, Evidență, Autorizare și Monitorizare, fără ca numerele de înregistrare date documentelor să se repete.

(4) Anual, documentele se grupează în dosare, potrivit problemelor și termenelor de păstrare stabilite prin nomenclatorul arhivistic.

(5) Documentele clasificate se inventariază și se arhivează potrivit legislației în domeniu.

Art. 6. – (1) CERT-RO va publica pe pagina de internet www.cert.ro, până la data de 31 martie a fiecărui an, un raport privind activitatea din anul anterior.

(2) CERT-RO prezintă Consiliului Suprem de Apărare a Țării, denumit în continuare *CSAT*, până la data prevăzută la alin. (1), raportul anual privind activitatea instituției.

TITLU II. ROLUL, ATRIBUȚIILE PRINCIPALE, STRUCTURA ORGANIZATORICĂ ȘI RELAȚIILE FUNCȚIONALE

Capitolul I. Rolul și atribuțiile principale

Art. 7. – (1) În vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, CERT-RO îndeplinește rolul de autoritate națională pentru securitatea rețelelor și a sistemelor informatice, precum și pe cele de echipă națională de răspuns la incidente de securitate informatică și punct național unic de contact.

(2) În vederea prevenirii, analizei, identificării și reacției la incidente în cadrul infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori asigură servicii ale societății informaționale, CERT-RO îndeplinește rolul de punct național de contact cu structurile de tip CERT care funcționează în cadrul instituțiilor sau autorităților publice ori al altor persoane juridice de drept public sau privat, naționale ori internaționale.

Art. 8. – (1) În calitate de autoritate competentă la nivel național, CERT-RO exercită atribuțiile generale prevăzute la art. 20 din Legea nr. 362/2018, cu modificările și completările ulterioare, având ca funcții importante:

a) Evidență – în acest sens identifică și ține evidența operatorilor de servicii esențiale și furnizorilor de servicii digitale.

b) Autorizare și atestare – în acest sens autorizează, revocă sau reînnoiește autorizarea echipelor CSIRT ce deservesc operatori de servicii esențiale ori furnizori de servicii digitale, precum și a formatorilor și furnizorilor de servicii de formare a echipelor CSIRT și auditorilor de securitate, respectiv eliberează, revocă sau reînnoiește atestatele auditorilor de securitate informatică care pot efectua audit în cadrul rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale.

c) Control și monitorizare – în acest sens monitorizează aplicarea prevederilor Legii nr. 362/2018, cu modificările și completările ulterioare, și verifică respectarea de către operatorii de servicii esențiale și furnizorii de servicii digitale a obligațiilor ce le revin conform Legii nr. 362/2018.

d) Reglementare tehnică – în acest sens elaborează și actualizează normele metodologice, tehnice, precum și regulamentele privind cerințele referitoare la înființarea, autorizarea și funcționarea echipelor CSIRT, desemnarea echipelor CSIRT sectoriale, cele referitoare la atestarea auditorilor calificați cu competențe în domeniul securității serviciilor esențiale și a serviciilor digitale, precum și normele referitoare la autorizarea formatorilor și furnizorilor de servicii de formare.

e) Relaționare interinstituțională – în acest sens coordonează activitatea Grupului de lucru interinstituțional, prevăzut de art. 6 alin. (4) din Legea nr. 362/2018, și participă la Grupul de cooperare la nivelul Uniunii Europene constituit pentru a facilita cooperarea strategică și schimbul de informații între statele membre, pentru a consolida încrederea și în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană.

(2) În calitate de Punct național unic de contact, CERT-RO exercită atribuțiile generale prevăzute la art. 21 din Legea nr. 362/2018, cu modificările și completările ulterioare, având ca funcții importante:

a) Legătură internațională – în acest sens asigură legătură între autoritățile statului și autoritățile similare din alte state, Grupul de cooperare și rețeaua echipelor de răspuns la incidentele de securitate informatică.

b) Cooperare internă și internațională – în acest sens transmite la cererea autorităților sau a echipelor CSIRT, către punctele unice de contact din celelalte state membre, precum și la autoritățile prevăzute la art. 15 alin. (2) și art. 16 din Legea nr. 362/2018, cu modificările și completările ulterioare, notificările și cererile primite.

(3) În calitate de CSIRT național, CERT-RO exercită atribuțiile generale prevăzute la art. 22 din Legea nr. 362/2018, cu modificările și completările ulterioare, având ca funcții importante:

a) Monitorizare incidente – în acest sens monitorizează incidentele de securitate a rețelelor și sistemelor informatice la nivel național și emite avertizări timpurii, alerte și anunțuri și diseminează informațiile privind riscurile și incidentele către orice entitate de drept public sau privat căreia îi poate fi afectată securitatea rețelelor și sistemelor informatice.

b) Analiză impact incidente – în acest sens stabilește impactul la nivel național și transfrontalier al incidentelor și informează autoritățile relevante la nivel național, precum și autoritățile similare din alte state potențial afectate; elaborează analize dinamice de risc și de incident.

c) Răspuns la incidente de securitate – în acest sens asigură răspunsul la incidente în limitele legii; înființează, întreține și operează serviciul de alertare și cooperare cu operatorii de servicii esențiale și furnizorii de servicii digitale; participă la acțiuni comune în cadrul rețelei CSIRT la nivel european.

(4) În calitate de instituție publică de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice, CERT-RO exercită atribuțiile generale stabilite la art. 6 din HG nr. 494/ 2011, cu modificările și completările ulterioare, având ca funcții importante:

a) Analiză disfuncționalități tehnice – în acest sens analizează disfuncționalitățile procedurale și tehnice la nivelul infrastructurilor cibernetice, potrivit ariei de competență, și transmite instituțiilor sau autorităților publice ori altor persoane juridice de drept public sau privat aspectele de interes.

b) Elaborare politici publice – în acest sens asigură elaborarea și diseminarea politicilor publice de prevenire și contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competență.

c) Cercetare-dezvoltare – în acest sens desfășoară activități de cercetare-dezvoltare în domeniu și elaborează proceduri și recomandări privind securitatea cibernetică, potrivit prevederilor legale privind cercetarea științifică și dezvoltarea tehnologică.

d) Suport tehnic de specialitate – în acest sens asigură cadrul organizatoric și suportul tehnic necesar schimbului de informații dintre diverse echipe de tip CERT, utilizatori, autorități, producători de echipamente și soluții de securitate cibernetică, precum și furnizori de servicii în domeniu; organizează și desfășoară activități de instruire în domeniul securității cibernetice; asigură consultanță de specialitate autorităților publice responsabile, stabilite conform Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, aprobată cu modificări prin Legea nr.18/2011 cu modificările și completările ulterioare, cu privire la produsele și sistemele de securitate cibernetică care deservesc infrastructurile critice naționale și europene.

Art. 9. – (1) Principiile generale care stau la baza funcționării CERT-RO sunt:

a) **Principiul legalității** – CERT-RO și personalul instituției au obligația de a acționa cu respectarea prevederilor legale în vigoare și a tratatelor și a convențiilor internaționale la care România este parte.

b) **Principiul egalității** – beneficiarii activităților desfășurate de către CERT-RO vor fi tratați în mod egal, într-o manieră nediscriminatorie, corelativ cu obligația CERT-RO, în calitate de Autoritate națională pentru securitatea rețelelor și sistemelor informatice, CSIRT național și Punct național unic de

contact de a trata în mod egal pe toți beneficiarii, fără discriminare pe criteriile prevăzute de Legea nr. 362/2018, cu modificările și completările ulterioare.

c) **Principiul transparenței** – în procesul elaborării de propuneri de acte normative, CERT-RO va informa și va supune consultării și dezbaterii publice proiectele de acte normative și va permite accesul persoanelor juridice și fizice la datele și informațiile de interes public, în limitele legii. În același timp, beneficiarii activităților CERT-RO au dreptul de a obține informații de la CERT-RO, iar CERT-RO are obligația de a pune la dispoziția beneficiarilor informații din oficiu sau la cerere, în limitele legii.

d) **Principiul proporționalității** – formele de activitate ale CERT-RO trebuie să fie corespunzătoare cu Legea nr. 362/2018, cu modificările și completările ulterioare, să satisfacă interesul public, precum și echilibrate din punctul de vedere al efectelor asupra persoanelor fizice și juridice.

e) **Principiul satisfacerii interesului public** – CERT-RO, precum și personalul instituției au obligația de a urmări satisfacerea interesului public înaintea celui individual sau de grup. Interesul public național este prioritar față de interesul public local.

f) **Principiul imparțialității** – personalul CERT-RO are obligația de a-și exercita atribuțiile legale fără subiectivism, indiferent de propriile convingeri sau interese.

g) **Principiul continuității** – activitatea CERT-RO se exercită fără întreruperi, cu respectarea prevederilor legale.

h) **Principiul adaptabilității** – CERT-RO are obligația de a satisface nevoile societății.

(2) CERT-RO îndeplinește și alte atribuții prevăzute prin dispoziții legale speciale.

Capitolul II. Structura organizatorică

Art. 10. – (1) Structura organizatorică a CERT-RO cuprinde următoarele structuri funcționale: direcții, servicii și compartimente, denumite în continuare *compartimente funcționale*.

(2) Structura organizatorică a CERT-RO, prevăzută în anexa nr. 1 la prezentul regulament, se prezintă astfel:

I. CONDUCERE CERT-RO

II. STRUCTURI ORGANIZATORICE

1. Direcția Reglementare, Evidență, Autorizare și Monitorizare:

1.1. Serviciul Evidență, Atestare și Autorizare
- 1.1.1. Compartimentul Evidență Operatori și Furnizori Servicii
- 1.1.2. Compartimentul Autorizare Echipe Intervenție și Formatori
- 1.1.3. Compartimentul Atestare Auditori de Securitate Informatică

1.2. Serviciul Control

1.3. Serviciul Reglementări

2. Direcția Tehnică:

2.1. Serviciul Echipa CSIRT Națională:
- 2.1.1. Echipa CSIRT București-Ilfov
- 2.1.2. Echipa CSIRT Nord-Est
- 2.1.3. Echipa CSIRT Sud-Est
- 2.1.4. Echipa CSIRT Sud
- 2.1.5. Echipa CSIRT Sud-Vest
- 2.1.6. Echipa CSIRT Vest
- 2.1.7. Echipa CSIRT Nord-Vest
- 2.1.8. Echipa CSIRT Centru

2.2. Serviciul Investigații Digitale și Cercetare-Dezvoltare

2.2.1. Compartimentul Analiză Malware și Forensic
2.2.2. Compartimentul Cercetare-Dezvoltare Infrastructuri Cibernetice
2.3. Serviciul Monitorizare Alerte Cibernetice
2.3.1. Compartimentul Security Operations Center
2.3.2. Compartimentul Call Center pentru Securitate Cibernetică
2.4. Serviciul Administrare și Dezvoltare Infrastructură
3. Serviciul Analize, Politici și Cooperare:
3.1. Compartimentul Punct Național Unic de Contact
3.2. Compartimentul Cooperare
3.3. Compartimentul Analize și Politici Publice
3.4. Compartimentul Informare și Relații Publice
4. Serviciul Economic:
4.1. Compartimentul Financiar-Contabilitate și Bugete
4.2. Compartimentul Achiziții Publice
5. Serviciul Administrativ:
5.1. Compartimentul Logistică, Patrimoniu și Protecția Muncii
5.2. Compartimentul Gestiuni, Registratură și Secretariat
6. Unitatea de Implementare Proiecte
7. Serviciul Juridic și Resurse Umane:
7.1. Compartimentul Juridic și Contencios
7.2. Compartimentul Resurse Umane
7.3. Compartimentul Control Intern Managerial
8. Compartimentul Securitatea Informațiilor
9. Compartimentul Audit Public Intern.

Capitolul III. Principalele relații funcționale

Art. 11. – (1) Principalele tipuri de relații funcționale sunt: ierarhice, teritoriale, de cooperare, punctuale în comisii/grupuri/proiecte, de reprezentare și de control.

(2) **Relații ierarhice.** Aceste relații privesc:

a) subordonarea directorului general adjunct și a Compartimentului Audit Public Intern față de directorul general;

b) subordonarea directorilor, respectiv Direcția Reglementare, Evidență, Autorizare și Monitorizare și Direcția Tehnică, șefilor serviciilor, respectiv Serviciul Analize, Politici și Cooperare, Serviciul Economic, Serviciul Administrativ, Unitatea de Implementare a Proiectelor și Serviciul Juridic și Resurse Umane, precum și Compartimentul Securitatea Informațiilor față de directorul general adjunct;

c) subordonarea directorilor adjuncți, șefilor serviciilor și compartimentelor funcționale față de directori, după caz;

d) subordonarea personalului de execuție și a compartimentelor funcționale față de șefii serviciilor, după caz.

(3) **Relații teritoriale.** Se stabilesc între compartimente funcționale CERT-RO și compartimentele teritoriale, respectiv compartimentele regionale, prin stabilirea și transmiterea, spre aplicare, dispoziții, norme, precizări, proceduri etc. conform obiectului de activitate.

(4) **Relații de cooperare.** Se stabilesc astfel:

a) la nivel instituțional: între toate compartimente funcționale CERT-RO în vederea realizării atribuțiilor specifice;

b) la nivel interinstituțional: între compartimente funcționale CERT-RO și structuri similare din administrația publică centrală sau locală și operatori economici, din țară sau din străinătate.

(5) **Relații punctuale în comisii/grupuri/proiecte.** Relațiile se stabilesc ca urmare a unor mandate, punctuale, acordate de către directorul general unor angajați, grup de angajați sau echipe de proiect pentru personal provenind din diferite structuri executive sau de specialitate. Personalul angrenat în activități desfășurate în comisii/grupuri/proiecte se subordonează atât managerului stabilit, cât și șefului/ managerului structurii din care provine.

(6) **Relații de reprezentare.** Relațiile se stabilesc în baza și limitele stabilite de actele normative în vigoare și de mandatul de reprezentare acordat de către directorul general. Relațiile se stabilesc cu alte autorități publice și organizații, operatori economici stabiliți în accepțiunea Legii nr. 362/2018, precum și cu persoane juridice și fizice din țară sau străinătate. Directorii și personalul care reprezintă Direcția Autorizare, Reglementare și Control, CSIRT național și Punctul național unic de contact în cadrul unor organizații și grupuri internaționale, conferințe și seminarii sau alte activități cu caracter intern și/sau internațional au obligația să promoveze o imagine favorabilă atât României, cât și CERT-RO.

(7) **Relații de control.** Se stabilesc între compartimente funcționale CERT-RO și personalul care desfășoară activități de control și verificare a modului de respectare a prevederilor Legii nr. 362/2018, cu modificările și completările ulterioare, conform competențelor stabilite prin această lege.

TITLU III. ATRIBUȚIILE CONDUCERII ȘI COMPARTIMENTELOR FUNCȚIONALE

Capitolul I. Conducerea CERT-RO

Secțiunea 1. Conducerea instituției

Art. 12. – (1) Conducerea CERT-RO este asigurată de către un director general și de un director general adjunct, sprijiniți de un Comitet de coordonare.

(2) Directorul general al CERT-RO este numit prin ordin al ministrului comunicațiilor și societății informaționale și își desfășoară activitatea în baza unui contract de mandat pe o perioadă de 5 (cinci) ani, cu posibilitatea de prelungire a mandatului.

(3) Directorul general reprezintă CERT-RO în raporturile cu celelalte autorități publice, cu alte persoane juridice, cu persoane fizice, precum și cu instituții și organizații din țară și din străinătate.

(4) Directorul general îndeplinește, în condițiile legii, funcția de ordonator de credite secundar.

(5) În exercitarea atribuțiilor sale, directorul general emite decizii și instrucțiuni.

Secțiunea 2. Comitetul de coordonare

Art. 13. – (1) Comitetul de coordonare este organ colectiv, format din câte un reprezentant și un înlocuitor ai următoarelor instituții și autorități publice:

a) Ministerul Comunicațiilor și Societății Informaționale;

b) Ministerul Apărării Naționale;

c) Ministerul Afacerilor Interne;

d) Serviciul Român de Informații;

e) Serviciul de Informații Externe;

f) Serviciul de Telecomunicații Speciale;

g) Serviciul de Protecție și Pază;

h) Oficiul Registrului Național al Informațiilor Secrete de Stat;

i) Autoritatea Națională pentru Administrare și Reglementare în Comunicații.

(2) Anual, până la data de 31 ianuarie, instituțiile și autoritățile publice prevăzute la alin. (1) desemnează și comunică CERT-RO reprezentantul și înlocuitorul acestuia în Comitetul de coordonare.

(3) Directorul general al CERT-RO este președintele Comitetului de coordonare

Art. 14. – Comitetul de coordonare al CERT-RO are următoarele atribuții și competențe:

a) avizează strategiile de dezvoltare ale CERT-RO și propunerile de politici publice destinate prevenirii și contracarării incidentelor din cadrul infrastructurilor cibernetice, elaborate de CERT-RO;

b) avizează următoarele acte elaborate de CERT-RO: proiectul de buget anual, planul anual de activitate și raportul anual de activitate;

c) urmărește desfășurarea în condiții de eficiență economică și performanță profesională a activității CERT-RO;

d) la cerere, asigură consultanță, analizează și formulează puncte de vedere pentru proiectele de reglementări referitoare la asigurarea securității cibernetice, elaborate de CERT-RO potrivit competențelor legale;

e) formulează recomandări privind obiectivele urmărite în auditul de securitate, precum și managementul securității rețelelor și sistemelor informatice;

f) formulează recomandări privind punctele de vedere naționale ce trebuie susținute de reprezentanții CERT-RO în formatele de cooperare internaționale;

g) analizează activitatea CERT-RO pe baza rapoartelor de activitate prezentate de către directorul general al CERT-RO;

h) avizează modificarea Regulamentului de organizare și funcționare a CERT-RO.

Art. 15. – (1) Comitetul de coordonare al CERT-RO se întrunește semestrial sau ori de câte ori este necesar.

(2) Comitetul de coordonare este convocat de către directorul general, care propune ordinea de zi. Ordinea de zi poate fi modificată și/sau completată la propunerea președintelui sau a membrilor Comitetului de coordonare în timpul ședinței, cu aprobarea votului majorității celor prezenți.

(3) În mod excepțional, convocarea Comitetului de coordonare se poate realiza și la propunerea motivată a unei instituții sau autorități publice reprezentată în comitet, adresată directorului general al CERT-RO.

(4) Convocarea membrilor Comitetului de coordonare pentru ședințe ordinare, transmiterea ordinii de zi și comunicarea documentației aferente se realizează cu cel puțin 5 zile calendaristice înainte de data ședinței.

(5) În situațiile în care se impune convocarea membrilor comitetului de coordonare în ședințe extraordinare, transmiterea ordinii de zi și comunicarea documentației aferente se realizează cu cel puțin 24 de ore înainte de data ședinței.

(6) Ședințele ordinare și cele extraordinare ale Comitetului de coordonare se desfășoară la sediul CERT-RO.

(7) La ședințele Comitetului de coordonare pot participa, în calitate de invitați, reprezentanți ai autorităților și instituțiilor publice ori ai altor persoane juridice de drept public sau privat, asociațiilor profesionale sau alți specialiști din domeniu.

(8) În exercitarea atribuțiilor sale Comitetul de coordonare emite avize și recomandări care se adoptă cu votul majorității membrilor prezenți la ședință.

Art. 16. – (1) Secretariatul Comitetului de coordonare este asigurat de către CERT-RO.

(2) Personalul desemnat pentru activitatea de secretariat are următoarele atribuții:

a) pregătește documentațiile necesare în vederea analizării și/sau avizării de către Comitetul de Coordonare;

b) informează membrii Comitetului de coordonare despre convocarea ședințelor de lucru, locul, data, ora și ordinea de zi, în condițiile prevăzute la art. 15 alin. (4) și (5);

c) participă la ședințe și asigură redactarea documentelor de lucru ale Comitetului, întocmesc procesul-verbal al ședinței, urmărind luarea la cunoștință a acestuia prin semnătura membrilor prezenți;

d) transmite procesul-verbal al ședinței membrilor Comitetului care nu au participat, în termen de 3 zile lucrătoare de la data desfășurării acesteia;

e) ține evidența membrilor Comitetului, a înlocuitorilor acestora și a datelor de contact;

f) gestionează documentele de lucru ale Comitetului și ține evidența avizelor și recomandărilor emise de Comitetul de coordonare.

Secțiunea 3. Atribuțiile conducerii instituției

Art. 17. – Directorul general are următoarele atribuții si competențe:

a) conduce întreaga activitate a CERT-RO;

b) răspunde de elaborarea Programul general de management și strategiile de dezvoltare ale CERT-RO;

c) îndeplinește toate activitățile necesare în vederea realizării obiectului de activitate al CERT-RO, a obiectivelor stabilite prin strategiile și planurile de dezvoltare etapizată;

d) răspunde de elaborarea și îndeplinirea Planurilor anuale de activitate ale CERT-RO, avizate de Comitetul de coordonare și aprobate de CSAT;

e) asigură desfășurarea activității CERT-RO cu îndeplinirea indicatorilor de eficiență economică și performanță profesională;

f) aprobă Politica de securitate a informațiilor din cadrul CERT-RO și răspunde de asigurarea protecției informațiilor clasificate gestionate la nivelul CERT-RO;

g) răspunde de elaborarea proiectul de buget al CERT-RO pe care îl supune aprobării ministrului comunicațiilor și societății informaționale, după avizul Comitetului de coordonare;

h) acționează pentru îndeplinirea prevederilor bugetului anual aprobat, inițiază programe și măsuri pentru dezvoltarea și diversificarea surselor de venituri extrabugetare în condițiile reglementărilor în vigoare;

i) răspunde de integritatea patrimoniului, gestionarea și administrarea acestuia în condițiile legii;

j) reprezintă CERT-RO în relațiile interne și internaționale;

k) încheie și semnează în numele CERT-RO protocoale de cooperare cu persoane de drept public sau privat, naționale sau străine;

l) prezintă Comitetului de coordonare informări semestriale privind stadiul îndeplinirii obiectivelor CERT-RO;

m) răspunde de elaborarea Raportului anual de activitate al CERT-RO care se supune aprobării CSAȚ, după avizarea acestuia de către Comitetul de coordonare;

n) angajează personalul necesar îndeplinirii obiectului de activitate al CERT-RO și aprobă fișele de post ale acestuia;

o) emite decizii și instrucțiuni în vederea îndeplinirii atribuțiilor ce revin CERT-RO;

p) răspunde de organizarea și desfășurarea controlului intern managerial la nivelul CERT-RO;

q) emite decizii de înscriere, modificare/completare sau radiere a operatorilor de servicii esențiale, a furnizorilor de servicii digitale, a echipelor CSIRT, a auditorilor de securitate, precum și a formatorilor și furnizorilor de servicii de formare pentru echipe de intervenție și formatori;

r) desfășoară orice alte activități prevăzute în sarcina directorului general în conformitate cu rolul și competențele legale ale CERT-RO;

s) își deleagă responsabilitățile în funcție de necesități;

t) stabilește cadrul relațiilor de colaborare cu alte instituții publice, alte persoane de drept public sau privat, naționale și internaționale.

Art. 18. – Directorul general adjunct este numit, în condițiile legii, prin decizie a directorului general și este subordonat acestuia.

(2) Directorul general adjunct are în principal, următoarele atribuții și competențe:

a) sprijină directorul general în conducerea și coordonarea activității, asigurând funcționarea CERT-RO în condiții optime;

b) face propuneri pentru îmbunătățirea activității compartimentelor din cadrul CERT-RO;

c) organizează și controlează realizarea în termen a sarcinilor stabilite de directorul general;

d) asigură stabilitatea funcționării instituției, continuitatea conducerii și realizarea legăturilor funcționale între structurile acesteia;

e) asigură legătura operativă dintre directorul general și șefii tuturor compartimentelor funcționale din cadrul CERT-RO;

f) urmărește și răspunde de creșterea performanțelor serviciilor prestate de CERT-RO prin utilizarea eficientă a resurselor existente în instituție;

g) furnizează către mass-media informațiile de interes public cu referire la activitatea instituției, în condițiile legii;

h) asigură centralizarea lunară a serviciilor realizate, informând directorul general asupra rezultatelor obținute și a măsurilor necesare de îmbunătățire a activității CERT-RO;

i) participă la elaborarea sau realizează efectiv lucrări de complexitate sau importanță deosebită;

j) organizează și urmărește ca personalul din instituție să cunoască legislația care reglementează activitatea compartimentelor funcționale;

k) organizează și asigură instruirea personalului de specialitate pe domenii de activitate;

l) vizează bonurile de consum de materiale și verifică utilizarea materialelor exclusiv în scopul pentru care s-au efectuat achizițiile;

m) asigură desfășurarea în condiții normale a inventarierilor anuale, conform deciziilor interne date în acest scop;

n) este șeful Structurii de securitate din cadrul instituției;

o) răspunde pentru conformitatea, regularitatea și legalitatea documentelor elaborate;

p) exercită și alte atribuții stabilite de directorul general al CERT-RO, prin delegare de competențe.

Capitolul II. Compartimente funcționale CERT-RO

Secțiunea 1. Atribuții și competențe generale

Subsecțiunea 1. Conducători compartimente funcționale

Art. 19. – (1) Directorii/directorii adjuncți/șefii serviciilor sunt numiți în funcție prin decizie a directorului general, în condițiile legii.

(2) Directorii/directorii adjuncți/șefii serviciilor au în principal următoarele atribuții și competențe:

a) organizează și controlează realizarea în termen a sarcinilor stabilite de conducătorii ierarhici superiori;

b) răspund de repartizarea echilibrată a responsabilităților salariaților și elaborează fișele de post pentru posturile direct subordonate;

c) coordonează și răspund de activitățile care le sunt delegate;

d) organizează instruirea și verificarea personalului din subordine privind cunoașterea legislației care reglementează activitățile compartimentelor funcționale coordonate;

e) participă la elaborarea sau realizează efectiv lucrări de complexitate sau importanță deosebită;

f) repartizează spre rezolvare corespondența și celelalte lucrări care intră în atribuțiile compartimentelor funcționale coordonate și dau îndrumări în vederea rezolvării acestora în termenul stabilit potrivit legii;

g) semnează, potrivit competențelor stabilite, lucrările și corespondența realizată în compartimentele funcționale coordonate;

h) asigură ca normele de disciplină și ordine prevăzute în Regulamentul de Ordine Interioară să fie respectate de către toți salariații din subordine;

i) răspund de conformitatea, regularitatea și legalitatea documentelor elaborate;

j) îndeplinesc și alte atribuții stabilite de directorul general și/sau directorul general adjunct.

Subsecțiunea 2. Personalul instituției

Art. 20. – (1) Personalul CERT-RO este format din personal contractual sau detașat de la alte instituții sau alte autorități publice, în condițiile legii, și încadrat pe funcții conform statului de funcții al CERT-RO prevăzut în anexa nr. 2 la prezentul regulament.

(2) Organizarea și desfășurarea examenelor sau concursurilor vizând personalul contractual se realizează în condițiile stabilite de directorul general al CERT-RO.

(3) În cadrul instituției își desfășoară activitatea și personal provenit din activități de voluntariat, practică și internship.

(4) Promovarea, modificarea, suspendarea și încetarea raporturilor de muncă ale personalului CERT-RO se realizează prin decizie a directorului general, în condițiile legii;

(5) Personalul CERT-RO participă, pe domeniile de competență, la implementarea proiectelor care vizează creșterea capacității operaționale a CERT-RO, precum și în diferite colective de lucru constituite la nivelul CERT-RO, în conformitate cu dispozițiile conducerii instituției.

Art. 21. – (1) Personalul CERT-RO are drepturi și obligații prevăzute prin dispoziții legale, aflate în vigoare, și ale contractului individual de muncă.

(2) Personalul CERT-RO are obligații ce decurg din atribuțiile instituției de Autoritate națională, CSIRT național și Punct național unic de contact, precum și celelalte drepturi și obligații prevăzute în Regulamentul Intern, în Codul de etică și conduită profesională și în alte dispoziții legale.

(3) Atribuțiile, sarcinile și răspunderile individuale ale personalului CERT-RO sunt stabilite fișa postului, care reprezintă anexă la contractul individual de muncă și care se aprobă de directorul general al CERT-RO, cu avizul șefului ierarhic superior.

Art. 22. – (1) Responsabilități generale ale personalului CERT-RO:

a) răspunde de cunoașterea și aplicarea legislației specifice domeniului de activitate, reglementărilor profesionale și standardelor aplicabile;

b) aplică strategiile, politicile, regulamentele și procedurile stabilite de către conducerea CERT-RO, în scopul realizării obiectivelor generale ale instituției, precum și ale obiectivelor specifice structurilor executive și de specialitate;

c) răspunde de protecția informațiilor clasificate, a datelor și informațiilor nedestinate publicității, inclusiv a celor cu caracter personal, deținute sau la care are acces ca urmare a exercitării atribuțiilor de serviciu, precum și a datelor care intră în sfera secretului comercial;

d) răspunde de îndeplinirea cu profesionalism, loialitate, corectitudine și în mod conștiincios a îndatoririlor de serviciu, se abține de la orice faptă care ar putea aduce prejudicii instituției;

e) răspunde de realizarea la timp și în mod corespunzător a atribuțiilor ce-i revin potrivit legii, programelor aprobate sau dispuse expres de către conducerea CERT-RO, precum și de raportarea asupra modului de realizare a acestora;

f) răspunde, potrivit dispozițiilor legale, de corectitudinea și exactitatea datelor, informațiilor și măsurilor introduse în documentele întocmite;

g) colaborează la nivel instituțional, cu personalul CERT-RO, în vederea elaborării de răspunsuri la adrese, chestionare, solicitări de informații de interes public, precum și la soluționarea petițiilor și sesizărilor/reclamațiilor.

(2) Personalul CERT-RO poate îndeplini și alte atribuții, în domeniul specific de competență, dispuse de conducerea structurii executive, respectiv de specialitate în care își desfășoară activitatea, sau din domeniul general de activitate al instituției, dispuse de conducerea CERT-RO.

(3) În exercitarea atribuțiilor, personalul are competență:

a) să reprezinte și să angajeze instituția numai în limita atribuțiilor de serviciu și a mandatului care i s-a încredințat de către conducerea acesteia;

b) să propună elaborarea de politici, proceduri de uz intern pentru activitatea structurii din care provine sau instituției, în general;

c) să semnaleze conducerii CERT-RO orice probleme deosebite legate de activitatea instituției, despre care ia cunoștință în timpul îndeplinirii sarcinilor sau în afara acestora, chiar dacă acestea nu vizează direct domeniul în care are responsabilități și atribuții.

Secțiunea 2. Atribuțiile compartimentelor funcționale

Subsecțiunea 1. Direcția Reglementare, Evidență, Autorizare și Monitorizare

Art. 23. – (1) **Direcția Reglementare, Evidență, Autorizare și Monitorizare (DREAM)** este condusă de un director și de un director adjunct și se subordonează directorului general adjunct.

(2) DREAM este structura responsabilă pentru implementarea și monitorizarea aplicării Legii nr. 362/2018, cu modificările și completările ulterioare.

(3) DREAM este structurată pe trei servicii: Serviciul Evidență, Atestare și Autorizare, Serviciul Control și Serviciul Reglementări.

(4) DREAM identifică și ține evidența operatorilor de servicii esențiale și furnizorilor de servicii digitale, autorizează echipele CSIRT ce deservesc operatori de servicii esențiale ori furnizori de servicii digitale, atestează auditorii de securitate informatică care pot efectua audit în cadrul rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale, autorizează formatorii și furnizorii de servicii de formare și, de asemenea, elaborează normele tehnice, metodologice și regulamentele prevăzute de Legea nr. 362/2018.

(5) Pentru îndeplinirea rolului de autoritate competentă la nivel național, la nivelul DREAM se înființează, administrează și funcționează registre și evidențe specifice așa cum sunt prevăzute la art. 20 lit. o)-r) din Legea nr. 362/2018, precum și Registrul operatorilor de servicii esențiale (ROSE) prevăzut la art. 5 din aceeași lege.

Art. 24. – (1) În activitatea sa, DREAM utilizează următoarele registre, electronice sau pe suport hârtie:

a) Registrul de intrare-ieșire a corespondenței;

b) Registrul electronic pentru managementul fluxurilor DREAM «ARTEMIS»;

c) Registrul deciziilor directorului general CERT-RO pentru înscrierea/modificarea/radiere;

d) Registrul furnizorilor de servicii digitale «REFSD»;

e) Registrul operatorilor de servicii esențiale «ROSE»;

f) Registrul echipelor CSIRT «RECO»;

g) Registrul auditorilor de securitate informatică «RASI»;

h) Registrul formatori și furnizori de servicii de formare pentru CSIRT și ASI «RFCA»;

i) Registrele electronice CRONOS / RHEA/ THEMIS / ZEUS pentru evidența activităților specifice structurilor funcționale din cadrul DREAM;

j) Sistemul on-line de notificare SOLNO;

k) Registrul actelor normative elaborate și gestionate «RANEG».

(2) Prin decizia directorului general CERT-RO, la propunerea directorului DREAM, se poate institui utilizarea și altor registre decât cele prevăzute la alin. (1).

Art. 25. – (1) **Serviciul Evidență, Atestare și Autorizare (SEAA)** – este structura responsabilă cu evidența operatorilor de servicii esențiale și a furnizorilor de servicii digitale, atestarea auditorilor de securitate informatică și autorizarea echipelor CSIRT și a formatorilor și furnizorilor de servicii de formatare pentru echipele CSIRT și auditorii de securitate informatică.

(2) SEOAA este condus de un șef serviciu și este structurat pe trei compartimente: Compartimentul Evidență Operatori și Furnizori de Servicii, Compartimentul Autorizare Echipe de Intervenție și Formatori și Compartimentul Atestare Auditori de Securitate.

Art. 26. – (1) **Compartimentul Evidență Operatori și Furnizori Servicii (CEOFS)** – este structura care gestionează activitatea de evidență a operatorilor de servicii esențiale și a furnizorilor de servicii digitale.

(2) CEOFS are următoarele atribuții:

a) înființează, întreține și actualizează periodic, cel puțin o dată la doi ani de la data intrării în vigoare a Legii nr. 362/2018, Registrul operatorilor de servicii esențiale (ROSE);

b) administrează Registrul de Evidență a Furnizorilor de Servicii Digitale (REFSD);

c) identifică, cu consultarea autorităților și entităților de reglementare și administrare a sectoarelor și subsectoarelor, operatorii de servicii esențiale care au sediul social, filială, sucursală sau punct de lucru pe teritoriul României și îi înscrie în ROSE;

d) ține evidența operatorilor de servicii esențiale, a furnizorilor de servicii digitale și a persoanelor responsabile NIS pentru legătura cu DREAM;

e) gestionează și administrează procesul de notificare și comunicare cu operatorii de servicii esențiale respectiv furnizorii de servicii digitale, desfășurat direct la sediu, prin email sau prin poștă, cu scrisoare cu valoare declarată și confirmare de primire ori prin sistemul on-line de notificare (SOLNO);

f) administrează aplicația informatică CRONOS, aplicație prin care este gestionat procesul de identificare a operatorilor de servicii esențiale și a furnizorilor de servicii esențiale;

g) evaluează documentele care stau la baza identificării, modificării sau completării evidenței și radierii operatorilor de servicii esențiale, respectiv furnizorilor de servicii digitale și elaborează rapoarte de finalizare a proceselor de evaluare și înscriere, modificare/completare sau radiere;

h) asigură asistență de specialitate, în limita resurselor disponibile, operatorilor de servicii esențiale în procesul de identificare respectiv în procesul de radiere;

i) se consultă cu autoritățile omoloage din statele membre ale Uniunii Europene atât în procesul de identificare și înscriere a operatorilor de servicii esențiale, cât și în procesul de radiere acestora, când entitatea furnizează un serviciu esențial în mai multe state;

j) identifică operatorii de servicii esențiale care au sediul social, filială, sucursală, punct de lucru sau altă formă de reprezentare legal stabilită pe teritoriul României;

k) alcătuiește și actualizează periodic, cel puțin o dată la doi ani, începând cu data intrării în vigoare a Legii nr. 362/2018, lista serviciilor esențiale care îndeplinesc condițiile de la art. 6 alin. (1) din legea menționată.

Art. 27. – (1) **Compartimentul Autorizare Echipe Intervenție și Formatori (CAEIF)** – este structura care gestionează autorizările echipelor CSIRT, respectiv formatorilor și furnizorilor de servicii de formare.

(2) CAEIF are următoarele atribuții:

a) autorizează, revocă sau reînnoiește autorizarea echipelor CSIRT ce deservesc operatori de servicii esențiale ori furnizori de servicii digitale;

b) autorizează, revocă sau reînnoiește autorizarea formatorilor și furnizorilor de servicii de formare pentru echipele de intervenție, respectiv auditorii de securitate;

c) administrează aplicația informatică RHEA, aplicație prin care este gestionat procesul de acreditare a echipelor de intervenție, respectiv a formatorilor și furnizorilor de servicii de formare.

Art. 28. – (1) **Compartimentul Atestare Auditori de Securitate Informatică (CAASI)** – este structura care gestionează activitate de atestare a auditorilor de securitate.

(2) CAASI are următoarele atribuții:

a) eliberează, revocă sau reînnoiește atestatele auditorilor de securitate informatică care pot efectua audit în cadrul rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale;

b) administrează aplicația informatică THEMIS, aplicație prin care este gestionat procesului de atestare a auditorilor de securitate.

Art. 29. – (1) **Serviciul Control (SC)** – este structura responsabilă cu controlul și monitorizarea aplicării Legii nr. 362/2018, cu modificările și completările ulterioare.

(2) SC este condus de un șef serviciu.

(3) Atribuțiile SC sunt următoarele:

a) exercită controlul respectării prevederilor Legii nr. 362/2018, a obligațiilor impuse prin actele emise de CERT-RO în aplicarea legii menționate, în limitele competențelor legale de monitorizare sau de verificare;

b) verifică în condițiile art. 35-42 din Legea nr. 362/2018 respectarea de către operatorii de servicii esențiale și furnizorii de servicii digitale a obligațiilor ce le revin;

c) emite în temeiul art. 37 din Legea nr. 362/2018 dispoziții cu caracter obligatoriu pentru operatorii de servicii esențiale și furnizorii de servicii digitale, în vederea conformării și remedierii deficiențelor constatate și stabilește termenul până la care aceștia trebuie să se conformeze;

d) instituie măsuri de supraveghere ex post pentru operatorii de servicii esențiale și furnizorii de servicii digitale cu privire la neîndeplinirea obligațiilor ce le revin;

e) verifică și rezolvă sesizările primite cu privire la neîndeplinirea obligațiilor operatorii de servicii esențiale și furnizorilor de servicii digitale;

f) monitorizează aplicarea Legii nr. 362/2018, cu modificările și completările ulterioare;

g) constată contravenții, aplică sancțiuni pentru încălcarea prevederilor Legii nr. 362/2018 și stabilește măsuri necesare pentru a asigura încetarea încălcării și remedierea situației produse;

h) solicită sprijin operativ de la autoritățile publice, precum și de la organele de poliție în cazuri temeinic justificate, în vederea identificării și localizării persoanelor fizice sau juridice care săvârșesc fapte de natură contravențională;

Art. 30. – (1) **Serviciu Reglementări (SR)** – este structura responsabilă cu elaborarea și gestionarea proiectelor de acte normative specifice implementării și aplicării Legii nr. 362/2018, respectiv normele tehnice, metodologice și regulamentele prevăzute de această lege, precum și elaborarea analizelor și informărilor specifice DREAM.

(2) SR este condus de către un șef serviciu.

(3) SR are următoarele atribuții:

a) elaborează și actualizează normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice;

b) elaborează și actualizează normele tehnice privind îndeplinirea obligațiilor de notificare a incidentelor de securitate de către operatorii și furnizorii;

c) coordonează activitatea și asigură secretariatul tehnic al Grupului de lucru interinstituțional menționat la art. 6 alin. (4) din Legea nr.362/2018;

d) elaborează și actualizează normele metodologice, tehnice, precum și regulamentele privind cerințele referitoare la înființarea, autorizarea și funcționarea echipelor CSIRT, desemnarea echipelor CSIRT sectoriale, cele referitoare la atestarea auditorilor calificați cu competențe în domeniul securității serviciilor esențiale și a serviciilor digitale, precum și normele referitoare la autorizarea formatorilor și furnizorilor de servicii de formare;

e) elaborează și promovează practici comune pentru administrarea incidentelor și a riscurilor și pentru sistemele de clasificare a incidentelor, riscurilor și informațiilor și, de asemenea, elaborează ghiduri de bune practici și recomandări în domeniul securității cibernetice;

f) desfășoară activități de normare prevăzute la art. 20 lit. b)-e) și r) din Legea nr. 362/2018;

g) participă, prin reprezentanți, la Grupul de cooperare la nivelul Uniunii Europene constituit pentru a facilita cooperarea strategică și schimbul de informații între statele membre, pentru a consolida încrederea și în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană;

h) elaborează proceduri și recomandări privind securitatea cibernetică, potrivit prevederilor legale privind cercetarea științifică și dezvoltarea tehnologică;

i) elaborează reglementari în domeniile de activitate ale CERT-RO, analize și informări pentru Comisia Europeană, precum și analize și propuneri privind standardele incidente;

j) ține evidența actelor normative și reglementărilor elaborate și gestionate la nivelul DREAM.

Subsecțiunea 2. Direcția Tehnică

Art. 31. – (1) **Direcția Tehnică (DT)** este condusă de un director și un director adjunct și se subordonează directorului general adjunct.

(2) DT este structura responsabilă pentru monitorizarea permanentă a alertelor și incidentelor de securitate cibernetică; cu gestionarea și administrarea Sistemul de alertă timpurie și informare în timp real privind incidentele cibernetice, precum și cu realizarea prevenirii, analizei, identificării și reacției la incidente în cadrul infrastructurilor cibernetice.

(3) DT, în calitate de CSIRT național, îndeplinește atribuțiile stabilite la art. 22 din Legea nr. 362/2018, cu modificările și completările ulterioare.

(4) DT este structurată pe patru servicii: Serviciul Echipa CSIRT Națională, Serviciul Investigații Digitale și Cercetare-Dezvoltare, Serviciul Monitorizare Alerte Cibernetice și Serviciul Administrare și Dezvoltare Infrastructură.

Art. 32. – (1) **Serviciul Echipa CSIRT Națională (SECNR)** – este structura responsabilă cu asigurarea intervenției și reacția la incidente în cadrul infrastructurilor cibernetice, precum și stabilirea impactului la nivel național și transfrontalier al incidentelor, realizând informarea autorităților relevante la nivel național și autorităților similare din alte state potențial afectate.

(2) SECNR este condus de un șef serviciu și este structurat pe opt compartimente funcționale: Echipa CSIRT București-Ilfov; Echipa CSIRT Nord-Est; Echipa CSIRT Sud-Est; Echipa CSIRT Sud; Echipa CSIRT Sud-Vest; Echipa CSIRT Vest; Echipa CSIRT Nord-Vest; Echipa CSIRT Centru.

(3) SECNR are următoarele atribuții:

a) asigură desfășurarea activităților specifice echipei CSIRT naționale (Level III) având responsabilități la nivelul întregii țări și pe toate domeniile stabilite prin Legea nr. 362/2018, precum și cele stabilite prin HG nr. 494/2011;

b) asigură răspunsul la incidentele de securitate cibernetică, la nivel național;

c) asigură intervenția la fața locului și preluarea de artefacte digitale:

d) contribuie la emiterea de avertizări timpurii, alerte și anunțuri, precum și la diseminarea informațiilor privind riscurile și incidentele

e) cooperează, la nivel național, cu echipele CSIRT în cadrul unei platforme de management al incidentelor și pentru schimbul de informații

f) participă la acțiunile comune în cadrul rețelei CSIRT la nivel european, precum și, după necesități, la acțiunile solicitate în cadrul rețelelor internaționale de cooperare;

g) oferă servicii publice de tip preventiv, reactiv și de consultanță în domeniul prevenirii și răspunsului la incidente de securitate cibernetică.

Art. 33. – (1) **Serviciul Investigații Digitale și Cercetare-Dezvoltare (SIDCD)** – este structura responsabilă cu efectuarea analizelor de laborator, malware și forensic, precum și cu cercetarea-dezvoltarea în domeniul protecției infrastructurilor cibernetice.

(2) SIDCD este condus de un șef de serviciu și este structurat pe două compartimente: Compartimentul Analiză Malware și Forensic și Compartimentul Cercetare-Dezvoltare Infrastructuri Cibernetice.

Art. 34. – (1) **Compartimentul Analiză Malware și Forensic (CAMF)** – este structura responsabilă cu investigarea, cercetarea și analiza atacurilor cibernetice la nivelul României (Level II).

(2) CAMF are următoarele atribuții:

a) desfășoară activități specifice de investigații digitale, respectiv analize malware și forensic;

b) analizează și cercetează atacuri cibernetice de pe spațiul cibernetic național și, la nevoie, participă în echipe complexe de investigații în teren;

c) analizează impactul la nivel național și transfrontalier a incidentelor de securitate cibernetică și elaborează analize dinamice de risc și de incidente;

d) organizează și întreține o bază de date privind amenințările, vulnerabilitățile și incidentele de securitate cibernetică identificate sau raportate, tehnici și tehnologii folosite pentru atacuri, precum și bune practici pentru protecția infrastructurilor cibernetice;

e) emite anunțuri privind amenințări nou-identificate pe plan național și internațional.

f) realizează activități de documentare a noilor vulnerabilități;

g) realizează auditări și evaluări de securitate sau teste de penetrare;

h) aduce la cunoștința publicului, periodic și ori de câte ori este necesar avertizări, alerte și informări privind riscuri și amenințări, posibile măsuri de prevenire și contracarare, în scopul cunoașterii de către public a acestora și luării măsurilor adecvate, și publică statistici privitoare la incidentele identificate la nivel național.

Art. 35. – (1) **Compartimentul Cercetare-Dezvoltare Infrastructuri Cibernetice (CCDIC)** – este structura responsabilă cu cercetarea-dezvoltarea infrastructurii cibernetice naționale.

(2) CCDIC are următoarele atribuții:

a) testează și evaluează tehnologii, echipamente și soluții de securitate cibernetică;

b) activități de cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice;

c) desfășoară activități de cercetare-dezvoltare în domeniu și elaborează ghiduri, recomandări și proceduri privind securitatea cibernetică.

Art. 36. – (1) **Serviciul Monitorizare Alerte Cibernetice (SMAC)** – este structura responsabilă cu asigurarea activității specifice componentelor de monitorizare și triere incidente de securitate la nivelul României (Level I), și cu asigurarea legăturii între autoritățile statului și autoritățile similare din alte state.

(2) SMAC este condus de un șef de serviciu și este structurat pe două compartimente: Compartimentul Operațiuni de Securitate Informatică și Compartimentul Alerte și Incidente Cibernetice.

Art. 37. – (1) **Compartimentul Security Operations Center (CSOC)** – este structura responsabilă cu monitorizarea incidentelor de securitate a rețelelor și sistemelor informatice la nivel național și transmiterea către statele membre, la cererea acestora, de notificări și solicitări privind incidentele ce afectează funcționarea serviciilor esențiale și a celor digitale de pe teritoriul respectivelor state.

(2) CSOC are următoarele atribuții:

a) monitorizează platformele de preluare a alertelor/incidentele de securitate cibernetică;

b) creează reguli de filtrare și generează rapoarte statistice;

c) asigură suportul tehnic de specialitate pentru incidentele de securitate identificate la nivel național și internațional care afectează infrastructura cibernetică națională;

d) împreună cu SIDCD stabilește, în baza notificărilor primite, impactul la nivel național și transfrontalier al incidentelor și informează autoritățile relevante la nivel național, precum și autoritățile similare din alte state potențial afectate;

e) înființează, întreține și operează serviciul de alertare și cooperare cu operatorii de servicii esențiale și furnizorii de servicii digitale;

f) emite avertizări timpurii, alerte și anunțuri și diseminează informațiile privind riscurile și incidentele de securitate cibernetică.

Art. 38. – (1) **Compartimentul Call-Center pentru Securitate Cibernetică (CCSC)** – este structura responsabilă cu monitorizarea și procesarea notificărilor privind incidentele care afectează rețelele și sistemele operatorilor de servicii esențiale ori ale furnizorilor de servicii digitale, primite telefonic și/sau prin alte tipuri de comunicații.

(2) CCSC are următoarele atribuții:

a) primește notificări privind incidentele care afectează rețelele și sistemele operatorilor de servicii esențiale ori ale furnizorilor de servicii digitale;

b) asigură trierea și clasificarea incidentelor de securitate la nivelul României (Level I);

c) asigură suport primar de specialitate pentru persoane fizice și juridice din România și străinătate cu privire la incidentele de securitate cibernetică;

d) colectează sesizările și informațiile despre incidente de securitate cibernetică, atât manual, cât și automatizat, și furnizează informații relevante în ceea ce privește acțiunile ulterioare.

Art. 39. – (1) **Serviciul Administrare și Dezvoltare Infrastructură (SADI)** – este structura specializată cu dezvoltarea și administrarea infrastructurii, precum și asigurarea instrumentelor și mecanismelor de securitate a rețelelor și sistemelor proprii.

(2) SADI este condus de un șef de serviciu.

(3) SADI are următoarele atribuții:

a) realizează întreținerea și dezvoltarea tuturor componentelor sistemelor informatice și de comunicații ale CERT-RO;

b) asigură funcționarea în condiții optime a tuturor echipamentelor și accesul utilizatorilor, în condiții de securitate conform politicii aprobate la nivel de instituție, la resursele de calcul (hardware și software) ale CERT-RO;

c) monitorizează funcționarea componentelor rețelelor și sistemelor informatice și de comunicații ale CERT-RO, iar în acest sens acordă asistență tehnică, răspunzând solicitărilor formulate de utilizatorii echipamentelor de calcul referitoare la funcționarea defectuoasă sau nefuncționarea uneia sau mai multor componente ale echipamentului sau a soft-urilor instalate;

d) redactează specificații tehnice pentru echipamentele și software-ul ce urmează a fi achiziționat în baza Planului Anual de Achiziții și participă la recepționarea lucrările de reparații efectuate de terți la echipamentele IT;

e) organizează activitatea de testare și evaluare a tehnologiilor de securitate și a aplicațiilor specifice, identificarea de nevoi de dezvoltare și conceperea de aplicații informatice necesare funcționării optime a CERT-RO;

f) păstrează cărțile tehnice ale echipamentelor IT în care operează evenimentele și alte informații în legătură cu acestea conform normelor legale în vigoare;

g) contribuie la organizarea și desfășurarea exercițiilor de securitate cibernetică și, de asemenea, participă la conferințe și întâlniri tehnice, legate de securitatea cibernetică;

h) oferă suport pentru analiza, dezvoltarea, implementarea și mentenanța de baze de date specifice, precum și pentru analiza, dezvoltarea, implementarea și mentenanța de aplicații specifice ariei de competență.

Subsecțiunea 3. Serviciul Analize, Politici și Cooperare

Art. 40. – (1) **Serviciul Analize, Politici și Cooperare (SAPC)** este condus de un șef serviciu și se subordonează directorului general adjunct.

(2) SAPC este structura responsabilă pentru legătura și cooperarea cu instituții europene și naționale.

(3) SAPC în calitate de Punct național unic de contact îndeplinește atribuțiile stabilite la art. 21 din Legea nr. 362/2018, cu modificările și completările ulterioare.

(4) SAPC este structurat pe patru compartimente: Compartimentul Punct Național Unic de Contact, Compartimentul Cooperare și Relații Interne, Compartimentul Analize și Politici Publice și Compartimentul Comunicare și Relații Publice.

Art. 41. – (1) **Compartimentul Punctul Național Unic de Contact (CPNUC)** – este structura responsabilă cu exercitarea funcției de legătură între autoritățile statului și autoritățile similare din alte state, Grupul de cooperare și rețeaua echipelor de răspuns la incidentele de securitate informatică.

(2) CPNUC are următoarele atribuții:

a) exercită o funcție de legătură între autoritățile statului și autoritățile similare din alte state, Grupul de cooperare și rețeaua echipelor de răspuns la incidentele de securitate informatică;

b) elaborează și transmite Grupului de cooperare rapoarte de sinteză privind notificările primite și acțiunile întreprinse;

c) transmite la cererea autorităților sau a echipelor CSIRT, către punctele unice de contact din celelalte state membre, notificările și solicitările privind incidentele ce afectează funcționarea serviciilor esențiale și a celor digitale de pe teritoriul respectivelor state.

Art. 42. – (1) **Compartimentul Cooperare (CC)** – este structura responsabilă cu elaborarea planurilor de cooperare și participarea în grupuri sau la activități specifice.

(2) CC are următoarele atribuții:

a) dezvoltă relații de parteneriat cu alte structuri naționale sau internaționale cu competențe și responsabilități în domeniul securității cibernetice;

b) participă la negocierea de memorandumuri/protocoale de cooperare în limitele mandatului dat de directorul general, și păstrează evidența documentelor de cooperare cu aceștia;

c) organizează activități de instruire în domeniul de referință cu sprijinul Direcției Tehnice și DREAM;

d) dezvoltă parteneriate publice-private;

e) asigură încheierea protocoalelor de cooperare/colaborare cu instituțiile publice sau alte persoane juridice de drept public sau privat, naționale sau internaționale;

f) asigură cadrul organizatoric necesar schimbului de informații dintre diversele echipe de tip CERT, utilizatori, autorități, producători de echipamente și soluții de securitate cibernetică, precum și furnizorii de servicii în domeniu.

Art. 43. – (1) **Compartimentul Analize și Politici Publice (CAPP)** – este structura responsabilă cu elaborarea analizelor și rapoartelor de sinteză pentru autoritățile statului și autoritățile similare din alte state, precum și practici comune pentru administrarea incidentelor și a riscurilor.

(2) CAPP are următoarele atribuții:

a) realizează analize de risc în materie de securitate cibernetică, precum și în ceea ce privește riscurile neîndeplinirii atribuțiilor specifice CERT-RO;

b) elaborează propuneri privind modificarea cadrului legislativ în vederea stimulării dezvoltării securității infrastructurilor cibernetice ce asigură funcționalitatea de utilitate publică ori asigură servicii ale societății informaționale;

c) asigură suport de specialitate MCSI pentru urmărirea și controlul aplicării prevederilor cuprinse în actele normative în vigoare sau în acordurile internaționale în domeniul de competență;

d) elaborează statistici folosind surse de informare proprii sau datele cuprinse în rapoartele publice;

e) elaborează politici publice de prevenire și contracarare a incidentelor de securitate cibernetică din cadrul infrastructurilor cibernetice;

f) asigură diseminarea politicilor publice de prevenire și contracarare a incidentelor de securitate din cadrul infrastructurilor cibernetice.

Art. 44. – (1) **Compartimentul Informare și Relații Publice (CIRP)** – este structura responsabilă cu asigurarea relaționării cu mass-media, difuzarea informații utile prin canalele de social media, precum și conștientizarea populației cu privire la securitatea rețelelor și sistemelor informatice

(2) CIRP are următoarele atribuții:

a) furnizează către mass-media informațiile de interes public cu referire la activitatea instituției, în condițiile legii;

b) diseminează informațiile destinate publicului larg prin diferite canale social media, inclusiv pe pagina de internet a instituției, www.cert.ro, cu respectarea prevederile legale;

c) asigură activitatea specifică instituției purtătorului de cuvânt;

d) întocmește proiecte de reacție și propune puncte de vedere ale instituției pe teme apărute în mass-media sau care suscită interesul mass-mediei;

e) primește și soluționează petițiile adresate CERT-RO (lucrări ce nu intră în competența de rezolvare a unui alt compartiment specializat din cadrul CERT-RO).

Subsecțiunea 4. Serviciul Economic

Art. 45. – (1) **Serviciul Economic (SE)** este condus de un șef serviciu și se subordonează directorului general adjunct.

(2) SE este structura responsabilă cu asigurarea resurselor financiare necesare continuității activităților și disponibilității permanente a serviciilor, gestionarea veniturilor proprii și asigurarea bugetului necesar desfășurării activităților CERT-RO, precum și activitatea de achiziții publice.

(3) SE este structurat pe două compartimente: Compartimentul Financiar-Contabilitate și Bugete și Compartimentul Achiziții Publice.

Art. 46. – (1) **Compartimentul Financiar-Contabilitate și Bugete (CFCB)** – este structura responsabilă care asigură resursele financiare necesare continuității activităților și disponibilității permanente a serviciilor CERT-RO.

(2) CFCB are următoarele atribuții:

a) fundamentează și elaborează, anual, proiectul de buget al CERT-RO, planificând și programând în proiectul de buget propriu resursele financiare necesare realizării politicilor elaborate în domeniile de competență ale CERT-RO;

b) monitorizează execuția bugetară pe structura clasificației bugetare;

c) asigură relațiile funcționale cu trezoreria;

d) efectuează plăți din creditele bugetare, cu respectarea prevederilor legale, în limita și pe structura bugetului aprobat;

e) asigură plata drepturilor salariale și a altor drepturi de natură salarială;

f) asigură, în limita bugetului aprobat, fondurile necesare deplasării în țară și în străinătate; ține evidența operativă a acestora și verifică deconturile, conform reglementărilor în vigoare;

g) asigură decontarea la timp și în conformitate cu prevederile contractuale a obligațiilor față de furnizorii de bunuri și prestatorii de servicii;

h) întocmește situația privind execuția cheltuielilor bugetare angajate;

i) organizează activitatea casieriei în conformitate cu prevederile legale, ia măsuri pentru efectuarea tuturor plăților în numerar, precum și pentru efectuarea operațiunilor curente cu băncile;

j) organizează și conduce evidența contabilă, potrivit dispozițiilor legale în vigoare, asigurând efectuarea corectă și la timp a înregistrărilor;

k) asigură organizarea, evidența și raportarea angajamentelor bugetare și legale;

l) răspunde de ținerea corectă și la zi a evidenței financiar – contabile, conform dispozițiilor legale;

m) întocmește documentele financiare privind avansurile, decontările și înregistrarea lor în contabilitate;

n) asigură și ține evidența contabilă a valorilor materiale și bănești, a mijloacelor fixe și obiectelor de inventar, precum și a operațiunilor financiare ale CERT-RO pentru activitatea finanțată din bugetul de stat;

o) elaborează și urmărește respectarea normelor proprii privind acordarea și exercitarea controlului financiar preventiv.

Art. 47. – (1) **Compartimentul Achiziții Publice (CAP)** – este structura responsabilă cu activitățile din sfera achizițiilor publice pentru desfășurarea în bune condiții a activităților specifice ale CERT-RO.

(2) CAP are următoarele atribuții:

a) elaborează, actualizează și supune spre aprobare Planul anual al achizițiilor publice;

b) derulează procedurile prevăzute de lege și date în competența acestei structuri în scopul achiziționării de bunuri și servicii, în baza solicitărilor compartimentelor funcționale ale CERT-RO;

c) efectuează cercetări de piață și estimări pentru achizițiile publice de produse, servicii sau lucrări;

d) inițiază, derulează și finalizează proceduri de achiziție publică de produse, lucrări și servici, inclusiv achiziții directe și întocmește toate documentele necesare, în conformitate cu reglementările legale în vigoare;

e) participă, după caz, în comisiile de evaluare/negociere a contractelor de achiziție publică;

f) întocmește documentații pentru returnarea garanțiilor de participare sau a garanțiilor de bună execuție la finalizarea contractelor;

g) întocmește acorduri cadru, contracte de achiziție publică, contracte subsecvente, acte adiționale și le supune aprobării.

Subsecțiunea 5. Serviciul Administrativ

Art. 48. – (1) **Serviciul Administrativ (SA)** este condus de un șef serviciu și se subordonează directorului general adjunct.

(2) SA este structura responsabilă cu suportul logistic pentru desfășurarea activităților de bază ale CERT-RO, întreținerea și exploatarea mijloacelor mobile (autospeciale, autovehicule etc.) necesare asigurării mobilității structurilor CERT-RO, întreținerea patrimoniului, a gestiunilor și spațiilor de depozitare și constituire a arhivei CERT-RO.

(3) SA este structurat pe două compartimente: Compartimentul Logistică, Patrimoniu și Protecția Muncii și Compartimentul Gestiune Registratură și Secretariat.

Art. 49. – (1) **Compartimentul Logistică, Patrimoniu și Protecția Muncii (CLPPM)** – asigură administrarea patrimoniului, suportul logistic pentru susținerea activităților de bază a structurilor CERT-RO, asigură activități specifice securității și sănătății în muncă și administrarea mijloacelor mobile (autospeciale, autovehicule etc.) necesare asigurării mobilității structurilor CERT-RO.

(2) CLPPM are următoarele atribuții:

a) asigurare a suportului logistic pentru desfășurarea activității de bază la nivelul CERT-RO (curățenie, utilități etc.) și aprovizionare, asigură suportul compartimentelor de specialitate în derularea fazelor de angajare și ordonanțare a cheltuielilor conform procedurilor interne

b) asigurare a suportului auto pentru desfășurarea activităților, întreținerea parcului auto și gestionarea consumului de combustibili la nivelul CERT-RO;

c) asigură administrarea patrimoniului; actualizează datele bunurilor imobile din inventarul centralizat al bunurilor din domeniul public/privat al statului; asigură completarea, păstrarea și conservarea înscrisurilor referitoare la întregul patrimoniu imobiliar al CERT-RO; răspunde de activitatea privind urmărirea comportării în exploatare a construcțiilor sub toate formele și asigură întocmirea și păstrarea cărții tehnice a construcției și ține la zi jurnalul evenimentelor;

d) aplicarea legislației privind securitatea și sănătatea în muncă.

Art. 50. – (1) **Compartimentul Gestiuni, Registratură și Secretariat (CGRS)** – asigură trierea corespondenței, transmiterea acesteia, arhivarea și fluxul informațional la nivelul CERT-RO, precum și evidența tehnico-operativă a mijloacelor fixe și a obiectelor de inventar achiziționate de către CERT-RO.

(2) CGDS are următoarele atribuții:

a) asigură gestiunea bunurilor de natura stocurilor (obiecte de inventar, consumabile, ambalaje, mobilier), gestiunea mijloacelor fixe (echipamente IT, PHARE, mobilier, terenuri și alte echipamente), gestiunea și distribuirea consumabilelor necesare bunei funcționări a activității instituției;

b) asigură evidența tehnico-operativă a mijloacelor fixe și a obiectelor de inventar achiziționate de către CERT-RO;

c) îndrumă și coordonează activitatea de inventariere a mijloacelor financiare și materiale, la intervale de timp prevăzute de legislația în vigoare;

d) organizează evidența, selecționarea, păstrarea și casarea documentelor din arhiva instituției în conformitate cu prevederile Legii Arhivelor Naționale nr.16/1996, cu modificările și completările ulterioare;

e) organizează activitatea de arhivare a documentelor de la nivelul CERT-RO;

f) întocmește și actualizează Nomenclatorul arhivistic al CERT-RO;

g) asigură trierea corespondenței, transmiterea acesteia, arhivarea și fluxul informațional la nivelul CERT-RO;

h) asigură coordonarea și îndrumarea activităților de primire, înregistrare, repartizare și expediere a corespondenței din cadrul compartimentelor funcționale;

i) asigură activități specifice de registratură și secretariat.

Subsecțiunea 6. Unitatea de Implementare Proiecte

Art. 51. – (1) **Unitatea de Implementare Proiecte (UIP)** este condusă de un șef serviciu și se subordonează directorului general adjunct.

(2) UIP este structura responsabilă cu implementarea proiectelor din diverse surse de finanțare, urmărește atât pe timpul implementării, cât și în perioada de sustenabilitate funcționarea și atingerea obiectivelor asumate prin finanțare.

(3) UIP are următoarele atribuțiile:

a) identificarea de programe de asistență financiară acordate la nivel național/european/ internațional în scopul stabilirii de parteneriate interinstituționale și accesării de fonduri/grant-uri;

b) analizează oportunitățile de implicare a CERT-RO în proiecte în calitate de partener;

c) elaborează, în colaborare cu celelalte compartimente funcționale, documentațiile necesare atragerii de fonduri, respectiv a cererilor de finanțare, precum și a altor documente necesare conform surselor și ghidurilor identificate, pe baza evaluării nevoilor existente;

d) colaborează cu autoritățile de management și organismele intermediare ce coordonează și asigură asistență financiară din fonduri nerambursabile;

e) asigură monitorizarea proiectelor în conformitate cu prevederile contractelor/acordurilor de finanțare, având drept scop realizarea obiectivelor proiectului cu maximă diligență și eficiență și prezintă managerilor de proiecte, în situațiile care impun, rapoarte vizând eventuale neconcordanțe/ întârzieri/ nereguli rezultate în urma activităților desfășurate în cadrul proiectelor respective;

f) centralizează și ține evidența proiectelor pe care CERT-RO le derulează.

Subsecțiunea 7. Serviciul Juridic și Resurse Umane

Art. 52. – (1) **Serviciul Juridic și Resurse Umane (SJRU)** este condus de un șef serviciu și se subordonează directorului general adjunct.

(2) SJRU este structura de specialitate responsabilă cu asigurarea legalității actelor emise la nivelul instituției și reprezentarea instituției în instanțele de judecată, cu gestionarea resursei umane, precum și implementarea controlului intern managerial la nivelul CERT-RO.

(3) SJRU este structurat pe trei compartimente: Compartimentul Juridic și Contencios, Compartimentul Resurse Umane și Compartimentul Control Intern Managerial.

Art. 53. – (1) **Compartimentul Juridic și Contencios (CJC)** – asigură asigurarea legalității actelor emise la nivelul instituției, precum și reprezentarea instituției în instanțele de judecată.

(2) CJC are următoarele atribuții:

a) reprezintă CERT-RO pe baza delegației date de conducerea instituției și apără drepturile și interesele acesteia în fața instanțelor judecătorești și a altor organe de jurisdicție, precum și în raporturile cu alte organisme, cu persoane fizice sau juridice;

b) avizează, din punct de vedere al legalității, documentațiile de atribuire a contractelor de achiziții publice, alte documente prevăzute de legislația din domeniul achizițiilor publice;

c) verifică din punct de vedere al legalității și avizează contractele civile și comerciale în care CERT-RO are calitatea de parte;

d) verifică din punct de vedere al legalității și avizează actele administrative/documentele privind încheierea, modificarea, suspendarea sau încetarea raporturilor de muncă ale angajaților; precum și protocoale, convenții, acorduri de colaborare încheiate de CERT-RO în domeniul său de activitate;

e) asigură consultanță juridică tuturor compartimentelor funcționale ale CERT-RO.

Art. 54. – (1) **Compartimentul Resurse Umane (CRU)** – asigură activități specifice gestionării resursei umane, recrutarea și administrarea personalului, precum și implementarea politicilor privind pregătirea personalului.

(2) CRU are următoarele atribuții:

a) asigură procesul de management al resursei umane, respectiv recrutarea și selecția de personal, angajarea și mobilitatea internă personalului, gestionarea dosarelor de personal și a contractelor individuale de muncă;

b) asigură administrarea drepturilor de natură salarială stabilite prin contractul individual de muncă și fișele de post, inclusiv evidența REVISAL, și gestionarea fișelor de post;

c) îndeplinește atribuții specifice pentru dezvoltarea profesională a angajaților prin instruirea și consilierea acestora, de management al performanței profesionale individuale, de management al carierei angajaților prin promovarea acestora în funcție, de administrare a drepturilor de natură non-salarială (concedii), de evidență a timpului lucrat, de management al eticii în organizație și de gestionare a declarațiilor de avere și de interese;

d) elaborează și gestionează documentația prevăzută de reglementările în vigoare referitoare la activitatea de resurse umane pentru personalul instituției (gestionarea fișelor de post, gestionarea fișelor de evaluare a angajaților, elaborarea actelor administrative privind angajarea, modificarea, suspendarea, promovarea, încetarea raporturilor de muncă ale salariaților etc.);

e) solicită compartimentelor funcționale informații necesare în vederea întocmirii programării pentru anul următor a concediilor de odihnă ale salariaților; ține evidența acestora, precum și a concediilor fără plată și a celor pentru studii;

f) acordă, la cerere, asistență de specialitate personalului de conducere al instituției în vederea îndeplinirii obligațiilor ce le revin pentru administrarea personalului din subordine (întocmirea fișelor de post, evaluarea activității profesionale a salariaților, etc);

g) gestionează activitățile de voluntariat, practică și internship.

Art. 55. – (1) **Compartimentul Control Intern Managerial (CCIM)** – elaborează procedurile interne și documentele strategice, de planificare și organizare a activității CERT-RO; asigură implementarea controlului intern managerial la nivelul instituției, precum și organizarea, planificarea și calitatea proceselor instituționale.

(2) CCIM are următoarele atribuții:

a) propune și elaborează proceduri de lucru pentru eficientizarea activității instituției, precum și de implementare a sistemului de control managerial intern la nivelul CERT-RO;

b) elaborează și gestionează Registrul riscurilor;

c) desfășoară activități specifice privind organizarea, planificarea și calitatea proceselor instituționale la nivelul CERT-RO;

d) întocmește, în colaborare cu celelalte compartimente funcționale, Regulamentul de ordine interioară al instituției și Codul de etică și conduită profesională;

e) întocmește statul de funcții, organigrama și regulamentul de organizare și funcționare, toate acestea fiind documente de organizare ale CERT-RO;

f) asigură componenta de etică și integritate la nivelul CERT-RO și urmărește implementarea Strategiei Naționale Anticorupție la nivelul CERT-RO;

g) menținere și dezvoltare a sistemului de control intern managerial în cadrul CERT-RO.

Subsecțiunea 8. Compartimentul Securitatea Informațiilor

Art. 56. – (1) **Compartimentul Securitatea Informațiilor (CSI)** este subordonat directorului general adjunct.

(2) CSI este structura responsabilă cu asigurarea implementării politicilor de securitate la nivelul CERT-RO reprezentând structura de securitate, atât ca și componentă PIC, cât și INFOSEC; implementarea politicilor privind protecția datelor cu caracter personal, precum și relaționarea cu ANSPDCP, precum și gestionarea și organizarea situațiilor de urgență.

(3) CSI are următoarele atribuțiile:

a) elaborează și actualizează procedurile, politicile și regulile necesare implementării și menținerii cerințelor sistemului de management al securității informațiilor al CERT-RO (SMSI);

b) elaborează, implementează și urmărește respectarea măsurilor organizatorice și procedurale aferente activității de protecție și gestiune a informațiilor clasificate, naționale și NATO/UE;

c) desfășoară activității în domeniul situațiilor de urgență, activității de evidență militară și mobilizare la locul de muncă, dacă e cazul, precum și activității de prevenire a terorismului cibernetic;

d) întocmește programul de prevenire a scurgerii de informații clasificate și acționează pentru aplicarea acestuia;

e) organizează, coordonează, îndrumă și verifică modul în care se execută evidența, manipularea, multiplicarea, păstrarea și transportul documentelor clasificate, la nivelul CERT-RO;

f) operaționalizează și asigură funcționarea ”Punctului de lucru NATO/UE” – componentă a sistemului național de registre,

g) exercită activități specifice de suport al responsabilului cu protecția datelor cu caracter personal în vederea monitorizării respectării legislației naționale și UE referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date;

h) organizează celula de urgență a CERT-RO în timpul situațiilor de urgență.

Subsecțiunea 9. Compartimentul Audit Public Intern

Art. 57. – (1) **Compartimentul Audit Public Intern (CAPI)** este subordonat directorului general.

(2) CAPI este structura responsabilă care exercită atribuțiile prevăzute de Legea nr. 672/2002 privind auditul public intern, republicată, cu modificările și completările ulterioare, precum și prin Normele generale privind exercitarea activității de audit public intern, aprobate prin Hotărârea Guvernului nr.1086/2013, precum și efectuarea activității de audit public intern.

(3) CAPI are următoarele atribuțiile:

a) evaluează, în vederea îmbunătățirii acestora, procesele de management al riscului, de control și guvernanță, precum și nivelurile de calitate atinse în îndeplinirea responsabilităților CERT-RO;

b) efectuează activități de audit public intern asupra tuturor activităților desfășurate în compartimentele funcționale din cadrul CERT-RO.

TITLU IV. DISPOZIȚII FINALE

Art. 58. – (1) Prezentul regulament se aplică tuturor compartimentelor funcționale din componența structurii organizatorice a CERT-RO și are caracter obligatoriu.

(2) Compartimentele funcționale CERT-RO au obligația de a comunica Compartimentului Control Intern Managerial (CCIM), în termen maxim de 5 de zile de la apariție, orice modificare intervenită în atribuțiile specifice domeniului de activitate, ca urmare a punerii în aplicare a deciziilor conducerii instituției sau a legislației apărute ulterior aprobării prezentului Regulament.

(3) CCIM analizează propunerile formulate de șefii/responsabilii compartimentelor funcționale privind modificarea atribuțiilor menționate în regulament în raport cu celelalte prevederi ale acestuia și procedează la actualizarea regulamentului, după aprobarea directorului general al CERT-RO.

Art. 59. – (1) În termen de 15 de zile de la intrarea în vigoare a prezentului regulament, șefii structurilor organizatorice din cadrul CERT-RO întocmesc/actualizează fișele posturilor în conformitate cu prevederile acestuia.

(2) În termen de 30 de zile de la intrarea în vigoare a prezentului regulament, Compartimentul Gestiuni, Registratură și Secretariat (CGRS) va întocmi, cu consultarea tuturor structurilor organizatorice, Nomenclatorul arhivistic al CERT-RO.

Art. 60. – Prevederile regulamentului sunt aduse la cunoștința tuturor angajaților prin publicarea în rețeaua intranet și la cunoștința oricărei persoane interesate, prin publicarea pe pagina de internet a CERT-RO.

Art. 61. – (1) Prezentul regulament intră în vigoare la data emiterii hotărârii CSAT pentru aprobarea acestuia, dată de la care încetează aplicarea regulamentului anterior.

(2) Încadrarea personalului în numărul și structura posturilor aprobate se face cu respectarea procedurilor aprobate de către directorul general al CERT-RO.

Art. 62. – Prezentul regulament se aprobă și poate fi revizuit prin hotărâre a CSAT la propunerea ministrului comunicațiilor și societății informaționale.

Art. 63. – Prevederile prezentului regulament se completează cu prevederile Regulamentului de ordine interioară, Codului de etică și conduită profesională, procedurilor operaționale, altor decizii emise de către directorul general al CERT-RO pentru delegarea de competențe, precum și ale actelor normative în vigoare.

Art. 64. – Compartimentele funcționale CERT-RO îndeplinesc, potrivit specificului lor, și alte activități decât cele cuprinse în prezentul regulament, rezultate din legislația în vigoare.