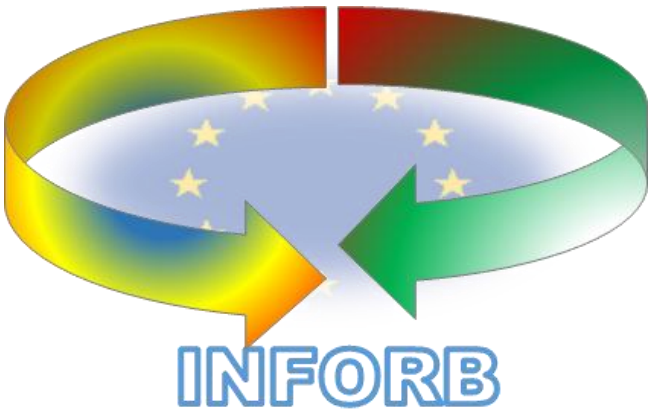


PROGRAME DE FORMARE PENTRU MANAGEMENTUL ENTITĂȚILOR ȘI A OFIȚERILOR DE SECURITATE CIBERNETICĂ DIN SECTORUL ALIMENTAR

LIVRABIL D5.2

Versiunea V1.0

REZUMAT

Livrabilul D5.2 ”Programe de formare pentru managementul entităților și a ofițerilor de securitate cibernetică din sectorul alimentar” rezumă metodologiile de instruire, strategiile regionale de implementare și evaluările rezultatelor derivate din concentrarea proiectului INFORB pe consolidarea capacității de securitate cibernetică în sectorul alimentar din România și Bulgaria.

Raportul evidențiază abordarea dublă care vizează personalul de conducere și ofițerii de securitate cibernetică, disparitățile regionale în ceea ce privește gradul de conștientizare și pregătire și prezintă recomandări practice pentru îmbunătățirea durabilă aliniată la Directiva NIS2.

Informații despre controlul documentelor

Setări	Valoare
Titlul documentului:	Programe de formare pentru managementul entităților și a ofițerilor de securitate cibernetică din sectorul alimentar
Numărul proiectului:	101128047
Nume proiect:	Implementarea Directivei NIS în sectorul producției, procesării și distribuției de alimente din România și Bulgaria
Acronimul proiectului:	INFORB
Autorul (autorii) documentului:	Bogdan Radu, Gheorghiță Comăneci, Silviu-Nicolae Dorobanțu, Mihai Rotariu, Gergana Rakova, Eli Kuyamova, Panayotka Panayotova
Identificator livrabil:	D5.2
Termen de livrare:	31.07.2025
Data livrării:	31.07.2025
Manager de proiect (PM):	Constantin Călin
Versiunea documentului:	V1.0
Sensibilitate:	PU-Public
Dată:	30.07.2025

Evaluarea documentelor și evaluatorii

Nume	Rol	Acțiune	Dată
Bogdan Radu	Coordonator WP5	Proiect de document creat	08.07.2025
Bogdan Radu	Coordonator WP5	Versiunea originală (DNSC)	11.07.2025
Silviu Dorobanțu	Expert în securitate cibernetică		
Gergana Rakova	Proiect	Actualizare versiune (MGBEG)	25.07.2025
Eli Kuyamova	Expert IT de proiect		
Panayotka Panayotova	Lider de proiect al echipei BG		
Consiliul consultativ de experți	Evaluare	Versiune convenită	30.07.2025
Bogdan Radu	Coordonator WP5	Actualizați versiunea	30.07.2025
Constantin Călin	Manager de proiect	Documentul final preluat și livrat	31.07.2025

Istoricul documentului

Recenzie	Dată	Creat de	Scurtă descriere a modificărilor
V0	08.07.2025	Expert în securitate cibernetică	Proiect de document creat. Documentare, analiza surselor. Documentare, analiza surselor.

V0.1	11.07.2025	Expert în securitate cibernetică și Coordonator WP5	Document actualizat cu informații
V0.1.1	22.07.2025	Expert în securitate cibernetică și Coordonator WP5	Document actualizat
V0.1.2	25.07.2025	Coordonator/Lider de proiect	Actualizat de experți bulgari
V0.1.3	28.07.2025	Expert în securitate cibernetică și Coordonator WP5	Document actualizat
V0.1.4	30.07.2025	Consiliul consultativ de experți	Recenzie
V1.0	30.07.2025	Coordonator WP5 și expert în securitate cibernetică	Documentul final versiunea 1

Cuprins

SECȚIUNEA 1. CONTEXT ȘI OBIECTIVE

Includerea **sectorului alimentar** în Directiva (UE) 2022/2555 (Directiva NIS2) reflectă o recunoaștere din ce în ce mai mare a faptului că perturbările în producția, prelucrarea și distribuția alimentelor prezintă riscuri grave pentru sănătatea publică, stabilitatea economică și securitatea națională. Transformarea digitală a lanțului de aprovizionare cu alimente a creat o dependență de sistemele informatice care sunt mai expuse amenințărilor cibernetice.

Proiectul **INFORB** răspunde acestei realități concentrându-se pe construirea rezilienței cibernetice în sectorul alimentar atât în România, cât și în Bulgaria. Obiectivul său este de a sprijini entitățile în înțelegerea noilor obligații care le revin în temeiul **Directivei NIS2**, de a le pregăti pentru a identifica și raporta incidentele cibernetice și de a încuraja colaborarea transfrontalieră.

Proiectul include:

- Identificarea și clasificarea entităților esențiale și importante din sectorul alimentar.
- Dezvoltarea de scheme de conștientizare cibernetică și formare adaptate rolurilor specifice din cadrul organizațiilor.
- Proiectarea unei platforme de cooperare transfrontalieră (CORB) pentru a facilita schimbul securizat de informații între România și Bulgaria.
- Executarea de campanii de conștientizare pentru a stimula adoptarea practicilor de securitate cibernetică și utilizarea platformei CORB.

Componenta de formare a proiectului vizează două grupuri de bază:

1. **Managementul -** pentru a sprijini luarea deciziilor strategice, guvernanța și conformitatea legală.
2. **Personalul de securitate cibernetică -** pentru a-i ghida pe cei responsabili de implementarea și supravegherea măsurilor de securitate cibernetică.

Prin investiții în aceste inițiative de formare, INFORB își propune să promoveze o cultură a securității cibernetice care să permită entităților din sectorul alimentar să se protejeze în mod proactiv și să contribuie la securitatea ecosistemului digital european mai larg.

Scopul programului este de a echipa persoanele în roluri de conducere cu cunoștințele necesare pentru a lua decizii informate cu privire la investițiile și politicile de securitate cibernetică, pregătind în același timp ofițerii de securitate cibernetică pentru a implementa și gestiona protocoale eficiente de gestionare a riscurilor și de răspuns la incidente, în perspectiva **Directivei NIS2**. În plus, prin promovarea colaborării transfrontaliere, programul va permite schimbul de cunoștințe și asistența reciprocă, ceea ce este esențial pentru abordarea naturii transnaționale a amenințărilor cibernetice.

Conștientizarea securității cibernetice este esențială pentru companii, deoarece eroarea umană rămâne una dintre cele mai semnificative vulnerabilități în postura de securitate a oricărei organizații. Angajații care nu sunt conștientizați în mod corespunzător cad adesea victime ale atacurilor de phishing, descarcă din greșeală malware sau manipulează greșit date sensibile, creând puncte de intrare pentru infractorii cibernetici. În special în sectorul alimentar, unde tehnologia operațională se intersectează din ce în ce mai mult cu sistemele informatice, personalul inconștient poate compromite din greșeală atât activele digitale, cât și procesele fizice de producție. Mai mult, o forță de muncă educată în fundamentele securității cibernetice servește drept primă linie de apărare, capabilă să recunoască amenințările din timp și să răspundă în mod corespunzător. Această abordare centrată pe om a securității este deosebit de vitală pe măsură ce amenințările cibernetice devin mai sofisticate și cadrele de reglementare precum **NIS2** pun o mai mare responsabilitate asupra organizațiilor pentru a demonstra măsuri de securitate cuprinzătoare care se extind dincolo de soluțiile tehnice pentru a cuprinde întreaga cultură organizațională.

SECȚIUNEA 2. EVALUAREA NEVOILOR DE FORMARE CENTRATĂ PE SECTOR

2.1 Prezentare generală a amprentei digitale și a suprafeței amenințărilor din sectorul alimentar

În cadrul NIS2, sectorul alimentar este recunoscut atât ca important, cât și critic, dar se confruntă cu riscuri unice de securitate cibernetică care sunt adesea subestimate. Aceste riscuri sunt accentuate de dependența sa de lanțuri de aprovizionare interconectate, sisteme moștenite, automatizare și servicii terțe. Mai multe tipuri de amenințări prezintă daune operaționale, economice și reputaționale:

Întrerupere operațională: Atacurile cibernetice, cum ar fi ransomware, pot opri liniile de producție sau pot dezactiva sistemele logistice, ducând la penurie de alimente, risipă și pierderi de venituri.

Punctele slabe ale lanțului de aprovizionare: Un număr mare de entități din sectorul alimentar colaborează cu mai mulți furnizori și parteneri logistici. O singură vulnerabilitate în sistemul unui partener se poate transforma într-un incident mai mare.

Riscuri de integritate și siguranță a datelor: Modificarea sau pierderea datelor referitoare la siguranța alimentară, controlul temperaturii sau trasabilitatea ingredientelor poate duce la produsele nesigure pe piață.

Expunerea la IoT și automatizare: Senzorii inteligenți, roboții de procesare și sistemele automate de inventariere sunt adesea minim securizate și vulnerabile la exploatarea de la distanță.

Spionaj cibernetic sau sabotaj: Tensiunile geopolitice sau sabotaj competitiv pot viza sectorul alimentar pentru a provoca perturbări publice sau pentru a obține avantaje neloiale pe piață.

Maturitate scăzută a securității cibernetice: În special în întreprinderile mici și mijlocii, funcțiile de securitate cibernetică sunt adesea insuficiente și nu dispun atât de instrumente tehnice, cât și de personal calificat.

Aceste amenințări specifice sectorului necesită măsuri de securitate cibernetică adaptate, conștientizare practică la toate nivelurile organizaționale și o colaborare strânsă între autoritățile naționale și sectorul privat.

Industria alimentară a suferit o transformare digitală semnificativă, creând o suprafață de atac extinsă care se întinde de la fermă la masă:

- **IoT și agricultură inteligentă**: Senzori pentru monitorizarea condițiilor solului, a vremii, a sănătății animalelor și a creșterii culturilor.
- **Sisteme de management al lanțului de aprovizionare**: Platforme digitale de urmărire și logistică pentru mișcarea produselor.
- **Operațiuni de producție**: Sisteme de control industrial (ICS/SCADA) pentru prelucrarea și ambalarea alimentelor.
- **Managementul lanțului frigorific**: Sisteme de monitorizare și control al temperaturii pentru produsele perisabile.
- **Sisteme de întreprindere**: ERP, CRM și alte platforme financiare sau de management.
- **Comerț electronic și comenzi** digitale: Platforme online pentru tranzacții B2B și B2C.
- **Sisteme de siguranță alimentară**: Platforme digitale de monitorizare a trasabilității și conformității.

Incidentele ransomware care vizează acest sector au crescut la 212 în 2024, reprezentând 5,8% din toate aceste atacuri, o creștere de la 167 de incidente în 2023[1]. Industria alimentară este vulnerabilă

[1] https://cybersecurityguide.org/industries/food-and-agriculture/

la atacuri cibernetice, cu nu mai puțin de 167 de atacuri ransomware raportate numai în 2023[2], potrivit unui raport al Centrului de Analiză și Schimb de Informații pentru Alimente și Agricultură (Food and Ag-ISAC).

Vectori de atac majori:

1. **Ransomware as a Service (RaaS):** "RansomHub" a apărut ca un jucător cheie, un grup ransomware-as-a-service care a câștigat proeminență oferind afiliaților oportunități profitabile[3].
2. **Vulnerabilități ale lanțului de aprovizionare**: Atacul ransomware JBS Foods servește ca un studiu de caz crucial, forțând închiderea unităților care furnizează aproximativ o cincime din aprovizionarea cu carne a Americii[4].
3. **Exploatarea arhitecturii de rețea**: Atacatorii au exploatat vulnerabilitățile arhitecturii de rețea pentru a se deplasa lateral prin sistemele organizației, ridicând îngrijorări în industrie după atacul JBS.
4. **Vulnerabilități IoT și OT**: Utilizarea tot mai mare a dispozitivelor IoT duce la o suprafață de atac crescută, probabil să atragă mai multe exploit-uri care vizează lanțurile de aprovizionare IoT[5].

2.2 Lacune identificate în ceea ce privește conștientizarea, practicile și capacitățile tehnice

Înainte de a dezvolta programele de formare, echipa de proiect INFORB a efectuat o evaluare specifică a stării securității cibernetice și a lacunelor de capacitate din sectorul alimentar. Această evaluare s-a bazat pe sondaje, contribuții ale experților și o revizuire a practicilor actuale din cadrul entităților care operează în producție, procesare și distribuție. În plus, mai multe evaluări evidențiază faptul că o mare parte din sectorul alimentar, în special întreprinderile mici și mijlocii (IMM-uri), nu înțelege în mod cuprinzător riscurile de securitate cibernetică și a celor mai bune practici. Multe companii operează fără personal dedicat securității cibernetice, bazându-se în schimb pe personal IT generalist, care adesea nu are expertiza specializată necesară pentru a aborda eficient amenințările cibernetice moderne.

Este esențial să se recunoască legătura directă dintre riscurile de securitate cibernetică și siguranța alimentară, în special în mediile în care punctele critice de control (CPC) sunt gestionate prin sisteme digitale, cum ar fi SCADA și alte instrumente de automatizare industrială. Directiva NIS2 plasează sectorul alimentar sub obligații de infrastructură critică, ceea ce înseamnă că întreruperile cauzate de incidente cibernetice (cum ar fi ransomware, manipularea sistemului sau accesul neautorizat) pot avea consecințe imediate asupra integrității produselor și siguranței consumatorilor. În paralel, cadrele de siguranță alimentară precum ISO 22000 și HACCP identifică PCC ca etape esențiale în procesul de producție în care eșecul poate duce la alimente nesigure. Multe dintre aceste CCP se bazează pe sisteme digitale de monitorizare și control, iar un atac cibernetic de succes asupra acestor sisteme poate provoca abateri de temperatură, timp, presiune sau trasabilitate, parametri care sunt vitali pentru conformitatea cu siguranța alimentară. De exemplu, dacă malware-ul dezactivează un senzor de temperatură în depozitele frigorifice sau modifică setările dintr-o unitate de pasteurizare, este posibil ca produsele rezultate să nu îndeplinească standardele de sănătate, chiar dacă nu sunt prezente probleme vizibile. Prin urmare, formarea în domeniul securității cibernetice atât pentru personalul de conducere, cât și pentru personalul tehnic trebuie să includă scenarii în care incidentele cibernetice afectează procesele de siguranță alimentară (o mapare a securității cibernetice NIS2 la

[2] https://foodinstitute.com/focus/5-cybersecurity-tips-for-2025/
[3] https://cybersecurityguide.org/industries/food-and-agriculture/
[4] https://www.elisity.com/blog/cybersecurity-for-food-manufacturing-in-2025-protecting-modern-production-operations
[5] https://unit42.paloaltonetworks.com/iot-supply-chain/

HACCP/ISO22000 siguranța alimentară, inclusiv o strategie integrată de siguranță și securitate). Participanții ar trebui să înțeleagă cum să identifice dependențele digitale pentru fiecare CPC, cum să securizeze aceste sisteme și cum să reacționeze atunci când sunt detectate anomalii. Printre subiectele cheie care trebuie abordate în cadrul sesiunilor de instruire se numără segmentarea rețelei între IT și OT, controlul securizat al accesului pentru SCADA, backup-uri regulate ale setărilor de control, procedurile de raportare a incidentelor și colaborarea dintre echipele de securitate cibernetică și ofițerii de calitate a alimentelor. Integrarea acestor elemente în schemele de formare asigură că entitățile din sectorul alimentar dezvoltă atât conformitatea cu NIS2, cât și reziliența de-a lungul lanțului de producție. În cele din urmă, tratarea securității cibernetice ca parte integrantă a siguranței și securității alimentare (ca sistem de management integrat) construiește o cultură a conștientizării inter-funcționale și ajută la prevenirea atât a pierderilor economice, cât și a riscurilor pentru sănătatea publică.

<u>Lacune majore de conștientizare identificate</u>:

Cunoștințe fundamentale de securitate: Lipsa de securitate a personalului și de conștientizare se numără printre principalele riscuri de securitate cibernetică în zilele noastre.

Percepția riscului: Companiile intră într-o perioadă în care abordările tradiționale de securitate cibernetică sunt din ce în ce mai inadecvate față de peisajul amenințărilor în evoluție, necesitând schimbări fundamentale în modul în care organizațiile abordează reziliența cibernetică[6].

Amenințări specifice sectorului: Înțelegere limitată a modului în care amenințările la adresa securității cibernetice afectează în mod specific siguranța alimentară, integritatea lanțului de aprovizionare și cerințele de conformitate cu reglementările.

2.3 Lacune de implementare a practicii

Programe de formare inconsecvente: Multe organizații mici din sectorul alimentar nu dispun de o instruire cuprinzătoare în domeniul securității cibernetice, specifică rolului, care să abordeze atât mediile IT, cât și OT.

Proceduri de securitate învechite: Organizațiile operează adesea cu practici de securitate moștenite care nu țin cont de amenințările moderne, cum ar fi operațiunile ransomware-as-a-service.

Coordonare inter-funcțională: Integrare slabă între echipele de securitate IT și personalul de tehnologie operațională, creând puncte oarbe în acoperirea securității.

Managementul furnizorilor: Conștientizarea inadecvată a riscurilor terților și a cerințelor de securitate a lanțului de aprovizionare în rândul echipelor de achiziții și operaționale.

2.4 Lacune de capacitate tehnică

Deficitul de competențe: Sectorul alimentar se confruntă cu același deficit de talente în domeniul securității cibernetice ca și alte industrii, dar cu complexitatea suplimentară de a avea nevoie de profesioniști care înțeleg atât securitatea IT tradițională, cât și mediile tehnologice operaționale.

Integrarea sistemului moștenit: Capacități tehnice limitate pentru a securiza sistemele de control industrial îmbătrânite și echipamentele de procesare a alimentelor care nu au fost proiectate având în vedere securitatea cibernetică.

Arhitectura rețelei: Multe organizații mici nu au expertiza tehnică necesară pentru a segmenta corect rețelele între mediile IT și OT, creând căi pentru mișcarea laterală în timpul atacurilor.

[6] https://www.weforum.org/stories/2025/02/biggest-cybersecurity-threats-2025/

Monitorizare și detectare: Capacități insuficiente pentru a monitoriza și detecta amenințările în medii complexe care includ totul, de la senzori de fermă la controale ale instalațiilor de procesare.

Răspuns la incidente: Capacități tehnice limitate pentru răspuns rapid la incidente care ar putea afecta siguranța alimentară sau continuitatea producției.

2.5 Considerații specializate în sectorul alimentar

Integrarea siguranței alimentare: Înțelegerea modului în care incidentele de securitate cibernetică pot afecta direct sistemele de siguranță alimentară, trasabilitatea și conformitatea cu reglementările.

Complexitatea lanțului de aprovizionare: Conștientizarea limitată a riscurilor de securitate cibernetică în lanțurile de aprovizionare cu alimente complexe, pe mai multe niveluri, care implică numeroase părți interesate.

Conformitate cu reglementările: Înțelegere insuficientă a reglementărilor emergente de securitate cibernetică specifice sectorului alimentar și a modului în care acestea se integrează cu cerințele existente de siguranță alimentară.

Continuitate operațională: Lipsa de conștientizare a modului în care incidentele de securitate cibernetică pot perturba operațiunile critice de producție și distribuție a alimentelor.

2.6 Recomandări de îmbunătățire

Instruire specifică sectorului: Dezvoltați programe de conștientizare a securității cibernetice adaptate operațiunilor din sectorul alimentar, inclusiv scenarii care implică sisteme de siguranță alimentară și întreruperi ale lanțului de aprovizionare.

Consolidarea capacităților tehnice: Investiți în dezvoltarea expertizei hibride de securitate IT/OT în cadrul forței de muncă, potențial prin parteneriate cu instituții de învățământ.

Colaborare în industrie: Folosiți organizații precum *Food and Agriculture Information Sharing and Analysis Center (Food and Ag-ISAC)* pentru a împărtăși informații despre amenințări și cele mai bune practici. În prezent, **nu există un ISAC specific european** axat exclusiv pe alimentație/agricultură.

Abordare integrată: Adoptarea unui model de instruire integrat care îmbină conștientizarea securității cibernetice cu programele de instruire în domeniul siguranței alimentare și HACCP, asigurând o abordare unificată a managementului riscurilor care să reflecte atât realitățile de reglementare, cât și cele operaționale.

Combinația unică a sectorului alimentar de medii IT și OT, cerințe de reglementare și responsabilități de sănătate publică necesită abordări specializate de conștientizare a securității cibernetice care abordează atât amenințările cibernetice tradiționale, cât și vulnerabilitățile specifice sectorului.

2.7 Modul în care conștientizarea poate contribui la securitatea cibernetică în sectorul alimentar

Dezvoltarea firewall-ului uman: Instruirea de conștientizare transformă angajații în prima linie de apărare, ajutându-i să recunoască și să răspundă la atacurile de inginerie socială, tentativele de phishing și activitățile suspecte care ar putea compromite sistemele de siguranță alimentară.

Recunoașterea riscurilor: Implementarea unor practici robuste de securitate cibernetică, cum ar fi actualizări regulate ale sistemului, instruire de conștientizare a phishing-ului, segmentarea rețelei și copii de rezervă securizate ale datelor sunt esențiale pentru îmbunătățirea rezilienței sectorului. Conștientizarea ajută personalul să înțeleagă de ce contează aceste practici și cum să le implementeze eficient.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Transformare culturală: Construirea unei culturi conștiente de securitate, în care securitatea cibernetică devine integrată în operațiunile zilnice, mai degrabă decât o gândire ulterioară, deosebit de importantă având în vedere mediul tehnologic operațional al sectorului.

Îmbunătățirea răspunsului la incidente: Angajații conștienți pot identifica și raporta mai rapid potențialele incidente de securitate, reducând timpul de așteptare și minimizând impactul asupra producției alimentare și a sistemelor de siguranță.

Relevanța coordonării transfrontaliere pentru lanțurile de aprovizionare transnaționale: Lanțul european de aprovizionare cu alimente este puternic interconectat, materialele, ingredientele și produsele traversând frontierele de mai multe ori în timpul producției și distribuției. Un incident cibernetic care afectează o entitate se poate răspândi rapid în lanțul de aprovizionare, provocând întreruperi în mai multe afaceri și potențial afectând disponibilitatea sau siguranța alimentelor. Securitatea cibernetică eficace necesită mecanisme solide de colaborare internațională și schimb continuu de informații despre amenințări în diferite jurisdicții naționale, asigurând o apărare unificată și proactivă împotriva riscurilor cibernetice în evoluție. O astfel de coordonare este esențială pentru identificarea și atenuarea amenințărilor care pot proveni dintr-o țară, dar au consecințe în întreaga Uniune Europeană.

SECȚIUNEA 3. REZULTATELE PREGĂTIRII

3.1 Abordarea pregătirii în România

România este împărțită în opt regiuni de dezvoltare, fiecare cu caracteristici economice distincte:

- **București-Ilfov: Este** cea mai dezvoltată și urbanizată regiune, caracterizată prin cel mai mare PIB pe cap de locuitor și un sector de servicii robust. Strategia de implicare aici a valorificat infrastructura tehnologică avansată a regiunii și alfabetizarea digitală ridicată.
- **Vest**: Fiind a doua cea mai dezvoltată și urbanizată regiune, cu o bază industrială puternică și o rată ridicată de ocupare a forței de muncă, părțile interesate ale sesiunilor de formare vor reflecta probabil peisajul industrial avansat al regiunii și preocupările specifice de securitate cibernetică.
- **Centru**: Cu o combinație echilibrată de industrii și servicii și un PIB pe cap de locuitor ridicat, părțile interesate recunosc natura interconectată a nevoilor de securitate cibernetică a industriei și serviciilor.
- **Nord-Vest: Părțile** interesate din această regiune se caracterizează printr-o creștere economică dinamică, investiții semnificative în industrie și servicii și un angajament robust în afaceri.
- **Nord-Est**: Deoarece aceasta este regiunea cel mai puțin dezvoltată, cu o populație rurală semnificativă și un PIB pe cap de locuitor mai mic, programele de formare ar trebui să se concentreze pe înțelegerea principiilor de securitate cibernetică și accesibilitatea la instrumentele și ghidurile de securitate digitală.
- **Sud-Est**: Economia acestei regiuni include o combinație de activități agricole, industriale și de pescuit de coastă, influențând conținutul de instruire pentru a reflecta cerințele de securitate cibernetică specifice sectorului.
- **Sud-Muntenia**: Influențată economic de apropierea de București, beneficiind de efecte de propagare, în special în servicii și industrie.
- **Sud-Vest (Oltenia):** Pentru a aborda provocările generate de PIB-ul mai mic pe cap de locuitor și rate mai mari ale sărăciei, sesiunile de instruire trebuie să se concentreze pe metode de livrare accesibile și materiale de sprijin pentru părțile interesate.

Sesiunile de instruire, desfășurate în perioada noiembrie 2024 – iulie 2025, au fost livrate online, de către echipa DNSC și echipa Expertware, folosind platforma Microsoft Teams completată de implicare interactivă prin intermediul platformei Slido. Această abordare virtuală a asigurat o accesibilitate largă, diseminarea eficientă a informațiilor și interacțiunea în timp real, în ciuda dispersiei geografice.

3.2 Abordarea pregătirii în Bulgaria

Bulgaria este împărțită în 6 (șase) regiuni economice și statistice, care sunt utilizate în scopul planificării regionale, analizei și alocării fondurilor europene. Ele nu sunt unități administrative, ci joacă un rol semnificativ în politica economică și socială a țării.

Regiunea Sud-Vest, dominată de capitala Sofia, este un important centru de distribuție și producție industrială în sectorul alimentar. Deși producția agricolă primară este relativ limitată, găzduiește sedii mari de întreprinderi și complexe logistice care asigură procesarea, ambalarea și distribuția eficientă a alimentelor. Sofia este o piață cheie cu un consum ridicat și un loc pentru inovație și tehnologii de înaltă performanță în sectorul alimentar.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Regiunea Centru-Sud este una dintre cele mai puternice regiuni alimentare din Bulgaria, datorită resurselor agricole bogate și industriei dezvoltate în orașe precum Plovdiv. Fructele, legumele, carnea și produsele lactate sunt produse și procesate aici, o parte din producție fiind exportată în afara țării. Prezența zonelor industriale și a unei bune infrastructuri de transport susțin lanțul de aprovizionare, permițând transportul și depozitarea rapidă.

Regiunea de nord-est include Dobrogea – una dintre principalele regiuni producătoare de cereale din țară, precum și Varna – un important centru portuar. Aici se dezvoltă mori, mori de ulei și industrii de lactate. Logistica joacă un rol semnificativ, portul Varna facilitând exporturile, iar legăturile de transport intern sprijinind aprovizionarea producătorilor cu materii prime și distribuția produselor finite.

Regiunea de sud-est este cunoscută pentru producția de vinuri de înaltă calitate, în special în zonele din jurul Yambol și Sliven. Stara Zagora este un centru de prelucrare energetică și industrială a cărnii și produselor lactate. Burgas oferă o platformă logistică importantă prin portul său. Lanțul de aprovizionare de aici este bine dezvoltat, regiunea fiind orientată spre exportul de vinuri, conserve și alte produse.

În regiunea central-nordică, orașe precum Ruse și Veliko Tarnovo sunt centre pentru industria conservelor, a cărnii și a lactatelor. Această regiune se caracterizează prin prezența unei diverse producții primare – de la cereale la fructe și legume. Transportul dunărean prin Ruse creează oportunități de acces la piețele internaționale, deși regiunea se confruntă cu dificultăți din cauza declinului demografic și a infrastructurii îmbătrânite.

Regiunea de nord-vest este cea mai puțin dezvoltată regiune economică din Bulgaria, iar acest lucru se reflectă și în sectorul alimentar. Principala producție aici este concentrată în agricultură și creșterea animalelor, dar prelucrarea industrială este limitată la micile fabrici de lactate și producătorii locali.

Lanțul de aprovizionare din sectorul alimentar din Bulgaria este extrem de important pentru funcționarea cu succes a sectorului. Diferențele regionale în producția primară, procesare și logistică determină avantajele competitive și punctele slabe ale fiecărei regiuni. În timp ce regiunile de sud-vest și centrul de sud sunt lideri în ceea ce privește inovarea și producția industrială, regiunea de nord-vest necesită o atenție și investiții speciale pentru a îmbunătăți rețeaua logistică și capacitățile de producție.

3.3 Instruirea managementului entităților din România

Sesiunile de instruire s-au adresat reprezentanților managementului din diverse subsectoare din industria alimentară, la care au participat 71 de participanți. Acești participanți au provenit din domenii cheie precum prelucrarea cărnii și a păsărilor de curte, industria fructelor de mare și a lactatelor, măcinarea și procesarea cerealelor, producția de ulei și grăsimi, producția de panificație și băuturi, alimentarea cu apă potabilă îmbuteliată, întreprinderile de ambalare a alimentelor și comerțul cu amănuntul alimentar, inclusiv supermarketurile.

Agenda de formare a fost concepută, de către echipa DNSC, pentru a aborda responsabilitățile specifice de securitate cibernetică la nivel de management și a oferit o înțelegere cuprinzătoare a peisajului de reglementare în temeiul Directivei NIS2. Subiectele principale abordate au inclus o introducere a Directivei NIS2 și a transpunerii acesteia în legislația națională, rolurile managementului și CISO, obligațiile de conformitate și o prezentare interactivă a platformei CORB concepută pentru a consolida cooperarea națională și transfrontalieră în domeniul securității cibernetice.

Participanții au fost, de asemenea, instruiți cu privire la cele mai bune practici și măsuri strategice pentru gestionarea incidentelor cibernetice relevante pentru rolurile manageriale. Pentru a consolida abilitățile practice, instruirea a inclus un exercițiu de tip test menit să pregătească echipele de management pentru gestionarea eficientă a incidentelor de securitate cibernetică.

La nivel regional, București-Ilfov, fiind cea mai dezvoltată regiune, și-a valorificat infrastructura tehnologică avansată și alfabetizarea digitală ridicată, atrăgând 21 de participanți.

Feedback-ul participanților a fost pozitiv, toate răspunsurile evaluând foarte mult instruirea. Participanții au apreciat în special claritatea informațiilor furnizate și caracterul practic al demonstrației platformei CORB. În plus, feedback-ul a indicat că a fost deosebit de util pentru participanți să clarifice direcția de punere în aplicare a Directivei NIS2, să înțeleagă pe deplin aplicabilitatea practică a Directivei NIS2 și să înțeleagă clar cerințele sale specifice.

În timpul sesiunilor de întrebări și răspunsuri, au fost ridicate mai multe întrebări, subliniind în special preocupările legate de securitatea cibernetică a lanțului de aprovizionare, inclusiv identificarea măsurilor necesare pentru a asigura reziliența lanțului de aprovizionare. Participanții și-au exprimat, de asemenea, interesul de a înțelege amenzile aplicabile managementului în temeiul Directivei NIS2 și au solicitat consiliere cu privire la cursurile de formare și cursuri suplimentare recomandate pentru îmbunătățirea competențelor manageriale în materie de securitate cibernetică.

Observații valoroase au reieșit din aceste sesiuni, inclusiv importanța implicării continue a managementului și necesitatea unor sesiuni periodice de reîmprospătare pentru a menține nivelurile de conștientizare și pregătire.

3.4 Instruirea managementului entităților din Bulgaria

În Bulgaria, training-urile pentru managerii entităților alimentare au fost 6 și s-au desfășurat în perioada 26.06.2025 - 18.07.2025 în întregime într-un mediu electronic, prin intermediul platformei Webex. Numărul total de participanți la sesiuni a fost de 83 de persoane.

Principalele subiecte de pe agenda instruirilor au inclus:

- introducerea Directivei NIS 2 și transpunerea acesteia în legislația națională,
- roluri și responsabilități de conducere în ceea ce privește respectarea cerințelor,
- prezentarea interactivă a platformei CORB, concepută pentru a sprijini cooperarea națională și transfrontalieră în domeniul securității cibernetice.
- prezintă riscuri și amenințări în securitatea cibernetică. Cum poate fi pregătită o organizație pentru Directiva NIS 2? Managementul riscurilor și răspunderea.
- pregătire practică.

În cadrul instruirilor, participanții au primit informații despre bunele practici și măsurile strategice de răspuns la incidentele cibernetice legate de responsabilitățile managementului organizației. Pentru a îmbunătăți abilitățile practice, instruirea a inclus un exercițiu de tip chestionar, publicat de platforma EU Survey, menit să pregătească managerii pentru un răspuns eficient la incidentele de securitate cibernetică.

În cadrul sesiunilor, participanții au fost impresionați de nivelul sancțiunilor aplicabile managerilor în temeiul Directivei NIS 2 și au solicitat sfaturi cu privire la instruirea și cursurile recomandate pentru îmbunătățirea competențelor de management în domeniul securității cibernetice.

Feedback-ul participanților a fost pozitiv, toți apreciind eforturile depuse de echipa de proiect în organizațiile de formare din sector. Participanții au apreciat importanța informațiilor furnizate și caracterul practic al acestora și au fost impresionați de exercițiul practic pregătit. A fost deosebit de util pentru participanți să își clarifice angajamentele în ceea ce privește punerea în aplicare a Directivei NIS 2, să înțeleagă pe deplin aplicabilitatea practică a acestui document și să își facă o idee clară despre cerințele sale specifice pentru gestionarea organizației.

3.5 Instruirea personalului de securitate cibernetică din România

Instruirea pentru personalul de securitate cibernetică a adunat 80 de participanți reprezentând diferite segmente ale sectorului alimentar, inclusiv prelucrarea cărnii și a păsărilor de curte, industria fructelor de mare și a lactatelor, măcinarea cerealelor, producția de ulei și grăsimi, producția de panificație și băuturi, alimentarea cu apă potabilă îmbuteliată, companiile de ambalare a alimentelor și comercianții cu amănuntul și supermarketuri.

Sesiunile de instruire au acoperit în mod cuprinzător domeniile cheie esențiale pentru personalul de securitate cibernetică, inclusiv responsabilitățile și obligațiile specifice în cadrul rolurilor lor, metode detaliate pentru securizarea tehnologiei operaționale (OT) și a sistemelor IT, informații practice despre cerințele Directivei NIS2, controale tehnice și termene de conformitate. Participanților li s-au oferit ghiduri de adoptare, seturi esențiale de instrumente de securitate cibernetică și metodologii pentru a îmbunătăți securitatea de-a lungul întregului lanț de aprovizionare. În plus, o demonstrație amănunțită a platformei CORB a oferit informații despre autoînscrierea entităților din sectorul alimentar și mecanismele generale de cooperare națională și transfrontalieră.

Feedback-ul participanților a fost pozitiv, toate cele nouă răspunsuri subliniind natura practică a instruirii. Mai exact, participanții au evidențiat valoarea de a vedea dezvoltarea continuă a aplicației de raportare a Directivei NIS2, de a obține informații actuale despre peisajul securității cibernetice din România și de a clarifica cerințele detaliate ale Directivei NIS2, alături de cele mai bune practici. Participanții au apreciat îndrumările simple oferite cu privire la protejarea infrastructurii digitale și operaționale în sectorul alimentar, ceea ce le-a sporit încrederea în implementarea unor controale de securitate cibernetică eficiente aliniate la Cadrul de fundamente cibernetice și la cerințele derivate din Directiva NIS2.

Feedback-ul a subliniat importanța și impactul acestor sesiuni de instruire, precum și nevoia de conștientizare continuă a securității cibernetice.

3.6 Instruirea personalului de securitate cibernetică din Bulgaria

Instruirile pentru experții implicați în implementarea Directivei NIS 2, precum și pentru specialiștii IT și cibernetic, au fost desfășurate la fața locului în regiunea de planificare respectivă, conform cerințelor proiectului. Instruirile au fost implementate în perioada 03.07 – 16.07.2025 în următorul program:

- Pentru Regiunea de Planificare Nord-Vest – în data de 03.07.2025 de la 13.00 la 15.00 - Vratsa, Hotel "Leva" (strada Georgi Benkovski 33), sală de ședințe.
- Pentru Regiunea de Planificare Sud-Vest – în data de 07.07.2025 de la 10.30 la 12.30 - Sofia, Ministerul Guvernării Electronice (str. Gen. Gurko nr. 6), sală de ședințe la parter
- Pentru Regiunea de Planificare Nord-Est – în data de 10.07.2025 între orele 14:30 și 16:30 - Varna, Centrul Regional de Informare-Varna (Piața Sf. Chiril și Metodiu (Kozirkata, Varna Center), sală de ședințe
- Pentru Regiunea de Planificare Nord-Centrală – în data de 11.07.2025 între orele 10.30 și 12.30 - Veliko Târnovo, Clădirea Administrației Municipale (Piața Mama Bulgaria Nr. 2), Sala de Ritualuri
- Pentru Regiunea de Planificare Central-Sud – în data de 15.07.2025 între orele 11.00 și 13.00 - Plovdiv, Centrul Cultural Boris Hristov (strada Gladstone nr. 15), sală mică de conferințe
- Pentru Regiunea de Planificare Sud-Est – în data de 16.07.2025 între orele 11.00 și 13.00 - Stara Zagora, Clădirea Administrației Municipale Stara Zagora (107 Tsar Simeon Veliki Blvd.), Sala Slaveykov.

Un total de 91 de participanți din diverse sectoare ale industriei alimentare, precum și organizații publice și neguvernamentale, au participat la întâlnirile de la fața locului.

Scopul formării a fost de a examina responsabilitățile specifice ale acestor profesioniști din domeniul securității cibernetice, precum și de a asigura o înțelegere cuprinzătoare a cadrului de reglementare introdus prin Directiva privind măsurile pentru un nivel comun ridicat de securitate cibernetică în UE (Directiva NIS 2).

Instruirile au acoperit aspecte cheie ale activităților specialiștilor în securitate cibernetică, cu accent pe responsabilitățile și obligațiile lor specifice în cadrul organizațiilor lor.

Programul de instruiri a inclus:

- informații actualizate privind cadrul de reglementare în domeniul securității cibernetice.
- riscuri și amenințări contemporane în securitatea cibernetică. Cum se pregătește entitatea pentru Directiva NIS 2? Managementul riscurilor și responsabilitățile specialiștilor în securitate cibernetică.
- exercițiu practic pentru specialiștii în securitate cibernetică.

O atenție deosebită a fost acordată platformei CORB, prin intermediul căreia participanții au primit o demonstrație detaliată a funcționalităților sistemului care sprijină cooperarea națională și transfrontalieră în timp real, inclusiv mecanismele de schimb de informații și de răspuns la incidente.

La nivel regional, cel mai mare număr de participanți (22 de persoane) la instruiri a fost în Stara Zagora (regiunea de planificare de sud-est), urmată de orașul Veliko Târnovo pentru regiunea Centru-Nord - 20 de persoane.

Observații valoroase au fost făcute ca urmare a acestor instruiri, inclusiv importanța implicării continue a specialiștilor IT și cibernetici în organizație și necesitatea organizării de sesiuni periodice de instruire pentru a-și menține nivelul de conștientizare și pregătire pentru a răspunde la incidente. Publicului i s-a reamintit importanța partajării, raportării incidentelor în intervalele de timp necesare, păstrării copiilor de rezervă ale informațiilor din sisteme într-un mediu offline și implementării protecției cu doi factori pentru accesul utilizatorilor la aceste sisteme ale organizației.

SECȚIUNEA 4. REZULTATE ȘI IMPACT

4.1 Rezultate și impact în România

Sesiunile de instruire au implicat în mod eficient participanți din diverse regiuni economice ale României, reflectând diferite grade de interes regional și pregătire în ceea ce privește securitatea cibernetică. Regiunea Nord-Vest a prezentat cel mai mare angajament general, sugerând un interes regional puternic legat de o concentrație mai mare de entități relevante de securitate cibernetică. Regiunea centrală a arătat, de asemenea, o participare robustă, indicând o conștientizare substanțială și o pregătire existentă pentru provocările de securitate cibernetică.

București-Ilfov și regiunea Sud au demonstrat un angajament moderat, participarea personalului de securitate cibernetică depășind-o ușor pe cea a managementului, evidențiind o mai mare conștientizare tehnică sau roluri de securitate cibernetică clar identificate la nivel operațional.

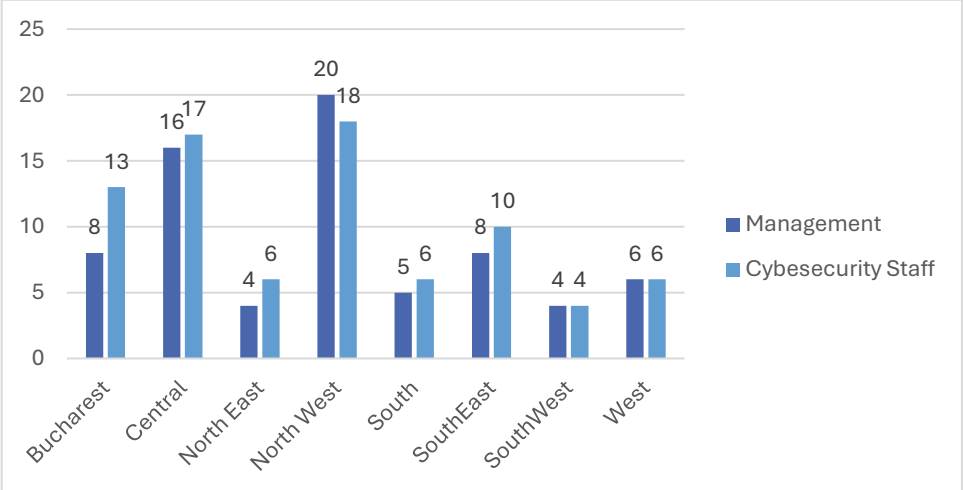
În schimb, regiuni precum sud-est, sud-vest și vest au prezentat rate de participare semnificativ mai mici, indicând domenii potențiale pentru informare și sprijin în inițiativele viitoare. Aceste disparități subliniază necesitatea unor strategii adaptate, specifice regiunii.

Un rezultat pozitiv semnificativ în majoritatea regiunilor a fost implicarea puternică a personalului managerial, reflectând angajamentul organizațional sporit față de responsabilitățile de securitate cibernetică impuse de Directiva NIS2. Acest angajament între roluri promovează alinierea internă, esențială pentru o guvernanță eficientă a securității cibernetice și reziliența operațională.

Instruirea a îmbunătățit semnificativ atât conștientizarea strategică, cât și pregătirea operațională în domeniul securității cibernetice în rândul părților interesate din sectorul alimentar, încurajând pregătirea pentru conformitatea cu reglementările și răspunsul la incidente din lumea reală. Disparitățile observate între regiuni evidențiază domenii critice pentru acțiuni ulterioare specifice, asigurându-se că toate regiunile beneficiază în mod egal de inițiativele viitoare de formare.

Pentru a îmbunătăți rezultatele viitoare, eforturile direcționate ar trebui să se concentreze pe regiunile subreprezentate, valorificând strategiile de succes din regiunile cu implicare ridicată, cum ar fi nord-vestul și centrul. În plus, ar trebui să se acorde prioritate formării tehnice susținute și mai profunde pentru personalul de securitate cibernetică, alături de mecanismele de asistență continuă și continuitate post-instruire.

Sesiunile de instruire din cadrul proiectului INFORB au ajuns la părțile interesate din toate regiunile economice ale României. Participanții au fost împărțiți în două grupe principale: **Management** și **Personal de securitate cibernetică** (ofițeri de securitate cibernetică sau personal desemnat). Graficul demonstrează distribuția inegală a participării atât în funcție de regiune, cât și de rol, oferind informații despre angajamentul regional și dinamica rolurilor organizaționale.



Cifră 1. Repartizarea participanților la sesiunile de instruire pe regiuni economice și public țintă

Informații despre distribuția regională

Cea mai mare participare:

- **Cea mai mare participare**: Regiunea Nord-Vest a avut cea mai mare participare pentru ambele categorii de public țintă (management și personal de securitate cibernetică), indicând o implicare regională puternică sau o concentrare mai mare de entități relevante în regiunea respectivă.
- **Implicare puternică a regiunii centrale**: Regiunea centrală urmărește îndeaproape, sugerând un interes semnificativ sau o conștientizare existentă cu privire la nevoile de formare în domeniul securității cibernetice.

Participare moderată:

- Regiunea București-Ilfov și regiunea Sud înregistrează o prezență moderată, cu o participare a **personalului de securitate cibernetică** puțin mai mare decât cea a managementului în ambele.

Regiuni cu implicare mai mică:

- Sud-Est, Sud-Vest și Vest au o prezență vizibil mai mică, cu variații minime între managementul și **personalul de securitate cibernetică**. Aceste domenii pot necesita o informare specifică sau sprijin suplimentar în inițiativele viitoare.

Implicarea publicului țintă:

- În majoritatea regiunilor, publicul de management a egalat sau a depășit participarea **personalului de securitate cibernetică**. Acest lucru indică un rezultat pozitiv: conducerea entităților din sectorul alimentar se angajează în responsabilitățile de securitate cibernetică și de reglementare.
- Cu toate acestea, în regiuni precum București-Ilfov și Sud, prezența **personalului de securitate cibernetică** a depășit managementul, reflectând fie o mai mare conștientizare tehnică, fie o mai bună identificare a rolurilor de securitate cibernetică la nivel operațional.
- Având în vedere regiunile cu implicare ridicată (nord-vest, central), utilizarea strategiilor de informare de succes și a metodelor de formare utilizate aici ar putea crește participarea în regiunile cu implicare mai scăzută.

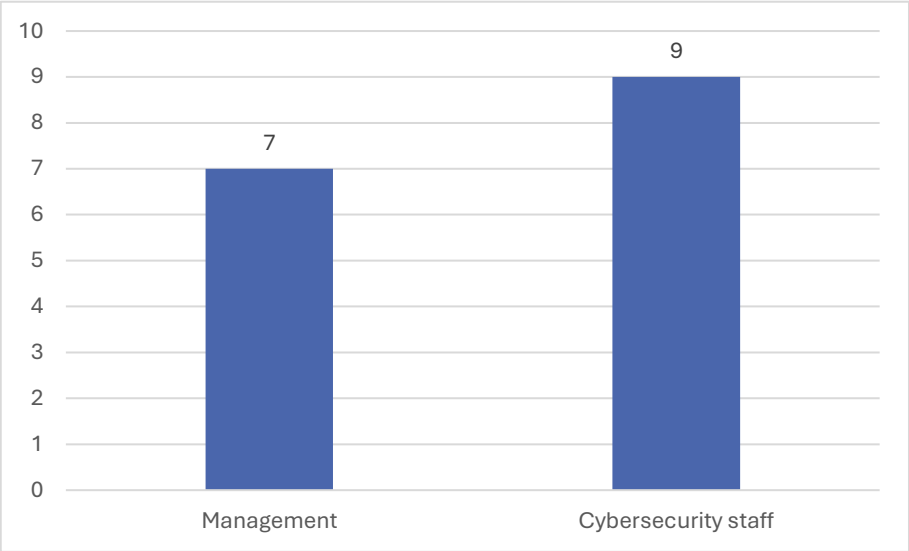
Impacturi observate:

- **Creșterea gradului de conștientizare:** Participarea rolurilor strategice și operaționale confirmă o mai bună conștientizare a responsabilităților de securitate cibernetică ale sectorului alimentar în cadrul NIS2.
- **Variabilitatea regională:** Disparitățile de participare evidențiază necesitatea unor strategii specifice regiunii, în special în zonele cu implicare mai scăzută, unde infrastructura critică poate fi încă lipsită de o expunere suficientă la aceste probleme.
- **Comunicare între roluri:** Implicarea atât a managerilor, cât și a personalului tehnic favorizează alinierea internă, care este esențială pentru o guvernanță eficientă a riscurilor cibernetice.

Implicații pentru acțiunile viitoare:

- **Concentrați-vă pe regiunile subreprezentate:** Viitoarele sesiuni de instruire ar trebui să acorde prioritate sud-vestului, vestului și sud-estului, potențial prin parteneriate locale, camere de comerț, asociații guvernamentale sau industriale.

- **Implicarea mai profundă a rolurilor personalului de securitate cibernetică:** Deși participarea personalului de securitate cibernetică a fost consecventă, ar trebui extinsă cu mai mult conținut tehnic și oportunități de urmărire, în special în regiunile în care implicarea managementului este deja puternică.



Cifră 2. Numărul de sondaje de feedback completate de publicul țintă

Continuitatea post-instruire: Entitățile care au participat activ, în special în regiunile de nord-vest și centru, ar putea fi recrutate ca ambasadori sau mentori pentru a promova cele mai bune practici în cadrul rețelelor lor.
Sondajul de feedback, publicat cu ajutorul platformei EU Survey, indică un nivel de implicare sau de reacție marginal mai ridicat în rândul profesioniștilor din domeniul securității cibernetice în ceea ce privește activitățile de feedback. De asemenea, ar putea reflecta un interes mai mare pentru îmbunătățirea continuă și detaliile tehnice în rândul grupului de personal de securitate cibernetică, subliniind poziția lor proactivă față de rezultatele și relevanța formării în domeniul securității cibernetice. Pentru viitoarele sesiuni de instruire, intensificarea eforturilor de încurajare a managementului să ofere feedback ar putea ajuta la echilibrarea perspectivelor atât din perspectiva strategică, cât și din cea operațională.

4.2 Rezultate și impact în Bulgaria

Inițiativele de formare au implicat cu succes părți interesate din diverse regiuni economice ale Bulgariei, evidențiind atât punctele forte ale regiunilor, cât și lacunele în ceea ce privește pregătirea pentru securitate cibernetică în sectorul alimentar. Regiunea de sud-est a arătat cel mai mare angajament general, sugerând un interes regional puternic. Regiunea nord-centrală a arătat, de asemenea, o participare puternică, indicând o conștientizare semnificativă a existenței și a pregătirii de a aborda provocările de securitate cibernetică.

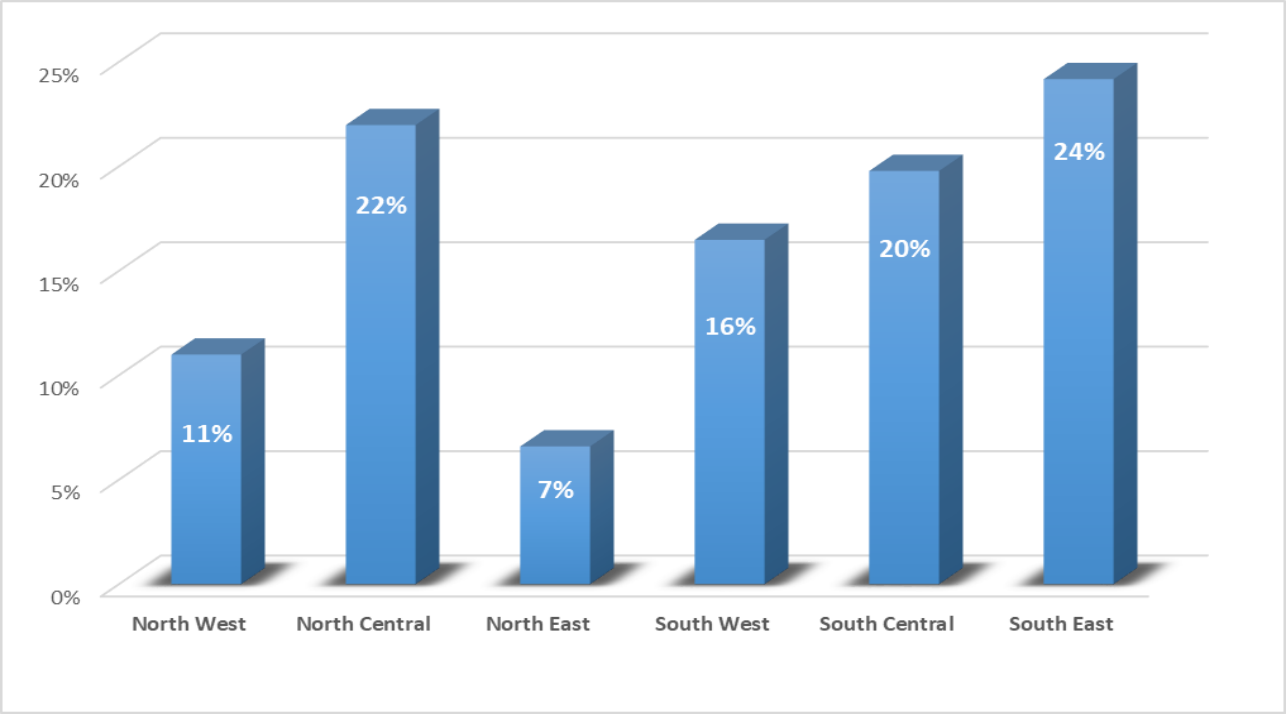
Regiunile rămase, cum ar fi sud-vestul și sud-centrul, au demonstrat rate de participare mai scăzute și sugerează domenii potențiale pentru informare și sprijin în inițiativele viitoare.

Un rezultat pozitiv semnificativ în majoritatea regiunilor a fost implicarea puternică a ambelor – managerii și experții în securitate cibernetică, reflectând angajamentul organizațional sporit față de responsabilitățile de securitate cibernetică atribuite de Directiva NIS 2. Acest angajament încurajează organizația să respecte cerințele de reglementare, ceea ce este crucial pentru un management eficient al securității cibernetice și asigură sustenabilitatea operațională.

Instruirile au crescut în mod eficient gradul de conștientizare a riscurilor și amenințărilor și responsabilităților contemporane de securitate cibernetică cu care se confruntă entitățile alimentare, participanții văzând progrese atât în înțelegerea strategică, cât și în capacitățile practice de implementare. Diferențele observate între regiuni evidențiază domenii critice pentru acțiuni viitoare specifice, asigurându-se că toate regiunile vor beneficia în mod egal de inițiativele viitoare de formare.

Pentru a îmbunătăți rezultatele viitoare, eforturile specifice trebuie să se concentreze asupra regiunilor subreprezentate, cum ar fi regiunile de planificare de nord-vest și nord-est. În plus, este necesar să se acorde prioritate instruirii periodice a personalului în domeniul securității cibernetice, precum și mecanismelor de sprijin continuu și continuitate după instruire.

Sesiunile de formare din cadrul proiectului INFORB au ajuns la părțile interesate din toate regiunile de dezvoltare economică din Bulgaria. Participanții au fost împărțiți în două grupe principale: echipă de management și specialiști în securitate cibernetică și în implementarea cerințelor Directivei NIS 2 și ale Legii privind securitatea cibernetică. Graficul demonstrează distribuția inegală a participării pe regiuni, pe baza numărului de participanți la instruirile de la fața locului.



Cifră 3. Repartizarea participanților la sesiunile de instruire la fața locului pe regiuni economice

Date de distribuție regională:

1. **Cea mai mare participare:**

• **Cea mai mare participare:** Regiunea Nord-Est a avut cea mai mare participare, indicând un angajament regional puternic și o concentrare mai mare a părților interesate din sector.

• **Implicare puternică în regiunea nord-centrală**: regiunea nord-centrală a demonstrat un interes semnificativ sau o mai bună conștientizare a nevoilor de formare în domeniul securității cibernetice.

2. **Participare medie:**

• **Regiunile Sud-Centrale și Sud-Vest** au demonstrat o prezență moderată.

3. **Regiuni cu implicare mai mică:**

• **Regiunile de nord-vest și nord-est** au avut o prezență semnificativ mai mică. Aceste domenii pot necesita activități de informare specifice sau sprijin suplimentar în inițiativele viitoare.

Implicarea publicului țintă:

• În majoritatea regiunilor, audiența a fost mixtă, atât cu experți în management, cât și în securitate cibernetică, precum și cu alte părți interesate relevante din organizație. Acest lucru demonstrează un rezultat pozitiv al eforturilor echipei: angajații din entitățile alimentare sunt implicați în securitatea cibernetică și cu cerințele de reglementare din domeniu.

• Luând în considerare regiunile cu niveluri importante de participare/implicare (Nord-Est, Nord-Central), utilizarea mai multor instruiri poate crește interesul pentru participare în regiunile cu niveluri mai scăzute de implicare.

Impacturi observate:

• **Creșterea gradului de conștientizare:** Participarea atât a actorilor strategici, cât și a celor operaționale confirmă o mai bună conștientizare a responsabilităților sectorului alimentar în materie de securitate cibernetică în cadrul NIS 2.

• **Variabilitatea regională**: Diferențele de participare evidențiază necesitatea unor strategii specifice regiunii, în special în zonele cu niveluri mai scăzute de implicare, unde infrastructura critică poate fi încă subexpusă la aceste probleme.

• **Comunicare între roluri**: implicarea atât a personalului de conducere, cât și a personalului tehnic promovează alinierea internă, care este esențială pentru gestionarea eficientă a riscurilor cibernetice.

Implicații pentru acțiunile viitoare:

• **Concentrarea pe regiunile subreprezentate:** Viitoarele sesiuni de instruire ar trebui să acorde prioritate regiunilor de Nord-Est și Nord-Vest, prin parteneriate locale, camere de comerț, asociații guvernamentale sau industriale.

• **Implicarea mai profundă a personalului în securitatea cibernetică**: Deși implicarea personalului în securitatea cibernetică a fost consecventă, instruirile ar trebui extinse cu conținut mai tehnic și oportunități de monitorizare, în special în regiunile în care implicarea conducerii este deja puternică.

• **Continuitate după instruire:** Organizațiile care au participat activ, în special în nord-est și nord-central, ar putea fi numite ambasadori pentru a promova bunele practici în cadrul organizațiilor lor.

SECȚIUNEA 5. PERSPECTIVE ȘI RECOMANDĂRI STRATEGICE

5.1 Perspective strategice în România

Analiza datelor de participare și a feedback-ului părților interesate din sesiunile de formare INFORB oferă o perspectivă valoroasă asupra stării actuale a conștientizării și pregătirii în materie de securitate cibernetică în sectorul alimentar. Aceste date oferă informații cheie și ne ajută să formulăm recomandări pentru a ajuta sectorul alimentar să obțină reziliență și o bună postură de securitate cibernetică. Acest capitol prezintă principalele perspective strategice derivate din rezultatele formării și propune recomandări specifice pentru a spori impactul și sustenabilitatea consolidării capacităților de securitate cibernetică în sectorul alimentar.

Angajamentul managementului este esențial și realizabil:

- Participarea puternică a managementului în anumite regiuni (de exemplu, Nord-Vest, Central) arată că părțile interesate la nivel executiv își recunosc responsabilitatea în temeiul Directivei NIS2.
- Cu toate acestea, variațiile între regiuni arată că nu toate echipele de conducere sunt la fel de conștiente sau pregătite, mesajele strategice și stimulentele contează.

Disparitățile regionale semnalează o pregătire cibernetică inegală:

- Regiuni precum Sud-Vest, Sud-Est și Vest au avut cea mai mică participare. Acest lucru ar putea reflecta o conștientizare locală limitată, mai puține întreprinderi alimentare mari sau probleme de acces logistic.
- Aceste zone pot fi mai vulnerabile din cauza lipsei de pregătire și ar beneficia de sprijin specific.

Rolurile de securitate cibernetică au nevoie de sprijin mai profund și continuu:

- Participarea personalului de securitate cibernetică a fost moderată, deși acest lucru este de așteptat, având în vedere numărul lor mai mic în organizații, poate indica o lipsă de responsabilități structurate de securitate cibernetică la nivel operațional.
- Multe entități, din sectorul alimentar, se bazează pe generaliști IT sau furnizori externi, ceea ce slăbește continuitatea și pregătirea instituțională.

Participarea între roluri pune bazele alinierii interne:

- Acolo unde au fost reprezentați atât personalul de management, cât și cel de securitate cibernetică (de exemplu, Central, Nord-Vest), organizațiile sunt mai bine poziționate pentru a implementa o strategie unificată de securitate cibernetică și pentru a stabili un Centru de Analiză și Schimb de Informații (ISAC) pentru a îmbunătăți informațiile despre amenințări și capacitățile de apărare colaborativă.
- Acest angajament dublu este o condiție prealabilă pentru construirea unei culturi a responsabilității cibernetice care depășește conformitatea.

5.2 Perspective strategice în Bulgaria

Analiza datelor privind participarea și feedback-ul părților interesate din sesiunile de instruire INFORB oferă informații valoroase la nivel național cu privire la starea actuală a conștientizării și pregătirii în materie de securitate cibernetică în sectorul alimentar. Aceste date oferă informații cheie și ajută la formularea de recomandări pentru a ajuta sectorul alimentar să obțină reziliență și o bună postură de securitate cibernetică.

Această secțiune prezintă principalele concluzii strategice care decurg din rezultatele formării și oferă recomandări specifice pentru a crește impactul și sustenabilitatea consolidării capacităților de securitate cibernetică în sectorul alimentar.

Implicarea conducerii este esențială și realizabilă:

• Părțile interesate din poziții de conducere își recunosc responsabilitatea în temeiul Directivei NIS 2.

• Lipsa unei mari participări a entităților la instruire sau lipsa feedback-ului din partea managerilor întreprinderilor importante pentru sector, demonstrează lipsa unei conștientizări suficiente a publicului cu privire la subiectul angajamentelor viitoare care le privesc ca urmare a adoptării de către Adunarea Națională a Legii privind modificarea Legii privind securitatea cibernetică.

Rolurile de securitate cibernetică au nevoie de un sprijin mai profund și mai susținut:

• Având în vedere numărul total redus de participanți la evenimente, bazat pe numărul total de entități alimentare înregistrate în țară, poate indica o lipsă de responsabilități structurate de securitate cibernetică la nivel operațional.

• Multe organizații se bazează probabil pe specialiști IT/cibernetici sau furnizori externi, ceea ce reduce continuitatea instituțională și pregătirea pentru răspunsul la incidente.

5.3 Recomandări pentru România

Extindeți acoperirea țintită în regiunile cu implicare scăzută:

- Prioritizați **sud-estul, sud-vestul și vestul** cu campanii de urmărire și ateliere localizate.
- Implicarea asociațiilor regionale de afaceri, a clusterelor din industria alimentară și a cooperativelor agricole pentru a mobiliza participanții.

Instituționalizați instruirea în securitate cibernetică pentru ambele roluri:

- Stabiliți sesiuni periodice de conștientizare pentru **management** (de exemplu, informări anuale, exerciții de simulare a incidentelor).
- Dezvoltați o cale dedicată de consolidare a capacităților pentru **personalul de securitate cibernetică**, cu îndrumări practice, webinarii tehnice și canale de asistență comunitară.

Încurajați definirea rolurilor în cadrul entităților:

- Sprijinirea organizațiilor din sectorul alimentar în desemnarea oficială **a ofițerilor de securitate cibernetică sau a punctelor focale**, în special în întreprinderile mici și mijlocii.
- Furnizați descrieri ale rolurilor, așteptări minime și politici de șabloane prin intermediul platformei CORB.

Profitați de regiunile cu implicare ridicată ca centre de asistență de la egal la egal:

- Folosiți participanți activi din regiuni precum **Nord-Vest și Central** pentru a îndruma sau consilia zonele mai puțin implicate.
- Promovați învățarea de la egal la egal prin povești de succes, paneluri între regiuni sau schimb de cunoștințe digitale prin CORB.

Integrarea securității cibernetice în managementul riscurilor sectorului mai larg:

- Încadrați securitatea cibernetică ca parte a siguranței alimentare, a asigurării calității și a continuității afacerii pentru a rezona mai mult cu liderii sectorului.

- Includeți-l în certificări, audituri și evaluări ale furnizorilor pentru a încorpora responsabilitatea în lanțul de aprovizionare.

Utilizați platforma CORB pentru a menține implicarea și raportarea:

- Încurajarea utilizării regulate a CORB pentru partajarea incidentelor, a bunelor practici și a actualizărilor privind conformitatea cu reglementările.
- Dezvoltarea unui **buletin sau tablou de bord de securitate cibernetică** în cadrul CORB pentru entitățile din sectorul alimentar, inclusiv alerte, actualizări legale și studii de caz.

Consolidarea colaborării cu instituțiile academice și de cercetare:

- Stabilirea de parteneriate formale cu universități și centre de cercetare în domeniul securității cibernetice pentru a dezvolta în comun programe de formare, pentru a facilita accesul la resurse de specialitate și pentru a promova cercetarea sectorială privind amenințările cibernetice și reziliența digitală în industria alimentară.

5.4. Recomandări pentru Bulgaria

Extinderea acoperirii țintă în regiunile cu implicare scăzută:

- Prioritizarea regiunilor de Nord-Est și Nord-Vest cu campanii de conștientizare ulterioare și seminarii/instruiri locale.
- Implicarea asociațiilor regionale de afaceri, clusterelor, hub-urilor și altor organizații din sectorul alimentar pentru a mobiliza participanții la evenimente și instruiri.

Instituționalizarea instruirii în securitate cibernetică pentru ambele roluri:

- Stabilirea unor sesiuni periodice de sensibilizare pentru manageri (de exemplu, întâlniri anuale, exerciții de simulare a incidentelor).
- Sprijinirea consolidării capacităților profesioniștilor IT și cibernetici cu îndrumări practice, webinarii tehnice și canale de asistență online.

Utilizarea regiunilor cu implicare ridicată ca hub-uri pentru sprijin de la egal la egal:

- Utilizarea participanților din regiunile active ca ambasadori ai bunelor practici în materie de securitate cibernetică.
- Promovarea schimbului de experiență de la egal la egal, inclusiv prin intermediul platformei online dezvoltate în cadrul proiectului.

Integrarea securității cibernetice în gestionarea riscurilor în sectorul mai larg:

- Implicarea în certificarea, auditurile și evaluările furnizorilor pentru a-și asuma responsabilitatea de-a lungul lanțului de aprovizionare.

Utilizați platforma online CORB pentru a menține implicarea și raportarea:

- Încurajarea utilizării regulate a CORB pentru a face schimb de incidente, bune practici și informații actualizate privind conformitatea cu reglementările.
- Dezvoltarea unui buletin sau a unui tablou de bord de securitate cibernetică CORB pentru entitățile din sectorul alimentar, inclusiv alerte, actualizări legislative și studii de caz.

Stabilirea unui cadru juridic adecvat adaptat nevoilor specifice de securitate cibernetică ale sectorului alimentar:

- Accelerarea transpunerii Directivei NIS 2 în legislația națională, prin adoptarea Legii privind modificările și completările la Legea privind securitatea cibernetică.
- Emiterea de instrucțiuni/manuale/orientări clare pentru sectorul alimentar cu privire la alinierea acestuia la cerințele cadrului actualizat de securitate cibernetică.

* * *

Versiunea oficială a Documentului este în limba engleză, în timp ce la nivel național, în România și Bulgaria, va fi publicată în limbile oficiale ale acestor țări, respectiv română și bulgară.