



**Centrul de inovare digitală pentru o societate mai inteligentă, mai
sigură și mai durabilă**

Descriere tipologie servicii

Servicii de Consultanță

Denumire Serviciu	Descriere Serviciu
Analiza datelor cu privire la amenințări avansate persistente	Testarea vulnerabilității la un atac cibernetic prelungit și țintit, în care un intrus obține acces la rețea și rămâne nedetectat pentru o perioadă extinsă de timp.
Optimizarea portofoliului de aplicații	Audit al aplicațiilor în raport cu procesul organizațional; Optimizare bazată pe indicatori cantitativi.
Validare concept / Demonstratori virtuali	Analiza cazului de utilizare; Definirea specificațiilor; Modelare; Simulare; Optimizarea parametrilor; Evaluarea nivelului de investiții; Evaluarea productivității integrate a ciclului de viață.
Consultanță pentru achiziții publice de sisteme digitale complexe	Audit; Definirea specificațiilor și a indicatorilor de performanță (KPI-uri); Formularea părții tehnice a caietului de sarcini și a bugetului necesar; Asistență în analiza ofertelor.
Testarea în cadrul unui spațiu cibernetic simulat	Un spațiu cibernetic este un mediu tehnologic controlat și interactiv, unde angajații învață cum să detecteze și să atenueze atacurile ciberetice folosind același tip de echipament pe care îl au la locul de muncă. Poligonul simulează cele mai grave atacuri posibile asupra infrastructurii IT, rețelelor, platformelor software și aplicațiilor.
Raportarea gestionării riscurilor ciberetice	Elaborarea documentației și a bunelor practici pentru gestionarea riscurilor de securitate cibernetică, inclusiv fluxul de la identificarea, analizarea, evaluarea și abordarea amenințărilor de securitate cibernetică ale organizației. Acțiunea principală de luat în considerare: Dezvoltarea unor politici și unelte robuste pentru evaluarea riscului furnizorilor; Identificarea riscurilor emergente, cum ar fi noile reglementări cu impact

	asupra afacerii; Identificarea punctelor slabe interne, cum ar fi lipsa autentificării cu doi factori; Atenuarea riscurilor IT, posibil prin programe de formare sau noi politici și controale interne; Testarea posturii generale de securitate; Documentarea gestionării riscului furnizorilor și a securității pentru examinări regulatorii sau pentru a liniști clienții potențiali.
Monitorizarea vulnerabilităților de securitate cibernetică	Implementarea senzorilor software încorporați într-o cutie hardware pentru a monitoriza atacurile cibernetice și a furniza rapoarte despre vulnerabilități. Senzorii vor fi montați în sistem pentru mai multe luni. Datele vor fi colectate într-un centru central pentru analiză. Se vor efectua analize individuale și generale.
Arhitectura digitală a întreprinderii	Dezvoltarea DEA folosind Standardele și Metodele TOGAF și Archimate
Informații despre amprenta digitală	Raportul de Inteligență Digitală Footprint caută informații disponibile deschis care ar putea facilita un atac cibernetic, o încălcare a datelor sau un prejudiciu PR asupra afacerii. Raportul și sfaturile ajută organizația să se pregătească pentru necunoscut. Include Raportul de Inteligență Open-Source Țintit, adunând informații relevante, contextuale despre afaceri și angajați, acoperind atât Web-ul Deschis, cât și Dark Web-ul, analiza bazată pe risc și recomandări pentru atenuarea problemelor identificate, conferință telefonică pentru a discuta constatările relevante și zonele cheie de risc.
Investigații de securitate digitală	Acest serviciu va fi atribuit organizațiilor care vor solicita ajutor cu informații în instanță sau pentru identificarea comportamentului necorespunzător al unor angajați în termeni de securitate a informațiilor. Serviciul va consta în descoperirea și interpretarea datelor electronice pentru a păstra orice dovadă în cea mai originală formă posibilă, în timp ce efectuează o investigație structurată prin colectarea, identificarea și validarea informațiilor digitale pentru a reconstrui evenimentele trecute. Serviciul va include o serie de pași: Identificarea: găsirea dovezilor, notând unde sunt stocate; Conservarea: izolarea, securizarea și păstrarea datelor. Acest lucru include prevenirea persoanelor de a manipula posibil dovezile; Analiza: reconstruirea

	fragmentelor de date și tragerea concluziilor pe baza dovezilor găsite; Documentarea: crearea unui înregistrării tuturor datelor pentru a recrea scena crimei; Prezentarea: rezumarea și tragerea unei concluzii.
Parcurs de succes în inovația digitală	Călătoria inovației digitale este setul de acțiuni despre inițiere (declanșatoare, identificarea oportunităților, luarea deciziilor), dezvoltare (proiectare, dezvoltare, adoptare), implementare (instalare, întreținere, formare, stimulente) și exploatare (maximizarea randamentelor, valorificarea sistemelor/datelor existente pentru noi scopuri). În acest serviciu, accentul va fi pe asistarea IMM-urilor pentru a proiecta și dezvolta fie un nou sistem de informații, personaliza o soluție existentă sau adopta o soluție digitală preexistentă astfel încât să colecteze date din procesele sale în cloud și să le utilizeze cu modele de inteligență artificială pentru îmbunătățirea unor KPI-uri. O altă situație este de a asista IMM-urile să convertească un produs sau serviciu clasic într-unul care încorporează tehnologii digitale conduse de inteligența artificială. Accentul nu va fi doar pe tehnologie, ci va lua în considerare toate aspectele procesului de inovație și toate dimensiunile: fonduri, echipă, tehnologie, model de afaceri, proprietate intelectuală, client (piață).
Demararea și evaluarea parcursului transformării digitale	Realizarea analizei maturității digitale folosind șablonul și modelul de evaluare de la JRC
Consultanță pentru Strategia de Transformare Digitală	Proiectarea unui plan detaliat pentru utilizarea soluțiilor digitale în vederea îmbunătățirii aspectelor fizice ale afacerii (sau proceselor publice) pe întreg lanțul valoric.
Răspuns la incidente cibernetice	Proiectarea unui plan de răspuns la incidente, constând dintr-un set de unelte și proceduri pe care echipa de securitate le poate folosi pentru a identifica, elimina și recupera de la amenințările de securitate cibernetică. Planul de răspuns la incidente este conceput pentru a ajuta organizațiile să răspundă rapid și uniform la orice tip de amenințare cibernetică externă. Serviciul va livra strategia de răspuns la incidente a organizației și modul în care aceasta susține obiectivele de afaceri; Rolurile și responsabilitățile implicate în răspunsul la incidente; Procedurile pentru fiecare fază a procesului de răspuns

	la incidente; Procedurile de comunicare în cadrul echipei de răspuns la incidente, cu restul organizației și cu părțile interesate externe; Cum să înveți din incidentele anterioare pentru a îmbunătăți postura de securitate a organizației.
Evaluare digitală profundă, analiza riscului, plan de acțiune	Audituri amănunțite pe toate dimensiunile sistemului IT, analiză SWOT, propuneri de proiecte, prioritizare, estimare bugetară
Evaluarea securității sistemelor de control industrial	Sistemele de control industrial se concentrează în mod specific pe procesele industriale sau automatizarea („Tehnologia Operațională” sau „SCADA” sau „Sistemele Cibernetic-Fizice” sau PLC-uri sau RTU-uri sau HMI-uri). Securitatea ICS se referă la protecția sistemelor de control industrial împotriva amenințărilor din partea atacatorilor cibernetici. Serviciul va evalua: Inventarul și detectarea activelor; Gestionarea vulnerabilităților; Protecția și detectarea intruziunilor în rețea; Detectarea și răspunsul la nivelul punctelor terminale; Gestionarea patch-urilor; Managementul utilizatorilor și accesului.
Strategie Teritorială Integrată pentru Sate Inteligente	Un grup de sate din proximitate geografică sunt asistate în proiectarea strategiei lor integrate pentru un teritoriu inteligent. De obicei, satele au provocări similare și nu dispun de resurse pentru a dezvolta aceste strategii independent. Serviciul va acoperi aproximativ 4 grupuri de sate cu 5 comune/grupuri. Strategia Teritorială Integrată pentru Sate Inteligente presupune participarea localnicilor la îmbunătățirea condițiilor lor economice, sociale sau de mediu, cooperarea cu alte comunități, inovație socială și dezvoltarea strategiilor pentru sate inteligente. Tehnologiile digitale pot fi aplicate în multe aspecte ale vieții și muncii în zonele rurale. Conceptul de sat inteligent include de asemenea adoptarea soluțiilor inteligente atât în sectorul public, cât și în cel privat, într-o gamă largă de domenii politice, cum ar fi îmbunătățirea accesului la servicii, dezvoltarea lanțurilor scurte de aprovizionare cu alimente, dezvoltarea surselor de energie regenerabilă, administrare mai inteligentă, agricultură inteligentă, comunități rezistente

	la schimbările climatice, educație inteligentă, telemedicină, acces la internet.
Servicii de consultanță Pentest	Acest serviciu analizează rezistența securității rețelei folosind metode de exploatare a vulnerabilităților. Testarea de penetrare identifică lacunele de securitate în infrastructura IT imitând un atacator. Acesta ajută la asigurarea că configurația rețelei și gestionarea patch-urilor sunt la zi. Serviciile de testare de penetrare evaluează de asemenea rețeaua organizației, aplicațiile, punctele finale și încercările interne/externe de a infiltra punctele de securitate. Oferă rapoarte complete care conțin informații despre punctele potențial slabe de securitate și zonele vulnerabile în sistemele de email, tuneluri VPN, firewall-uri, routere, servere web și alte dispozitive de rețea.
Serviciu de consultanță pentru modelarea proceselor pentru Automatizarea Proceselor Robotice (RPA)	Proiectul de automatizare a proceselor necesită modelarea proceselor ca o condiție prealabilă. În RPA, roboții sunt creați și sunt făcuți să efectueze sarcini obișnuite într-o rutină de 24/7 și sunt folosiți pentru a scala numerele, geografiile, limbile etc. Ei sunt de asemenea îmbogățiți cu AI (Inteligență Artificială) și sarcini de gândire cognitivă (CT), ceea ce face necesar ca roboții să cunoască traseul de la un capăt la altul, astfel încât AI și CT să fie eficiente și rapide.
Selecție și asistență contractuală pentru robotică	Există multe tehnologii robotice pentru procesele de fabricație. IMM-urile sunt de obicei influențate de integratori și de tehnologia de utilizat, dar acest lucru vine în multe cazuri cu diverse capcane pe parcursul ciclului de viață al investiției. Acest serviciu este dedicat ajutorării IMM-urilor să abordeze această problemă într-un mod sistematic, luând în considerare atât aspectele tehnice, cât și pe cele financiare pe durata ciclului de viață al utilizării. De asemenea, sunt asistați în negocierile cu furnizorul de tehnologie pentru a se asigura că oferta este optimă pentru IMM. Include și simularea procesului robotizat astfel încât beneficiarul să înțeleagă mai bine noul context. Acest lucru accelerează procesul de adopție și reduce timpul până la implementare și costurile de implementare.
Strategia Smart City (Oraș Inteligent)	Este o asistență clasică pentru stabilirea unei strategii, cu probleme specifice orașelor inteligente. Va urma

	modelul dovedit al Cluj IT. Va include analiza stării actuale, SWOT, formularea viziunii, formularea strategiei, proiecte, prioritizarea proiectelor, detalii pentru proiectele emblematic, organizarea pentru executarea strategiei. Domeniile acoperite vor fi guvernarea inteligentă, neutralitatea CO2, mediul inteligent, viața inteligentă, educația inteligentă, economia inteligentă, mobilitatea inteligentă, sănătatea digitală, infrastructura inteligentă, siguranța cetățenilor, reziliența, planificarea urbană inteligentă.
Evaluarea securității tehnologiilor inteligente și a Internet of Things (IoT)	Internetul Obiectelor (IoT) crește exponențial, dar securitatea pentru proiectele și implementările IoT rămâne un obstacol pentru multe organizații. O componentă fundamentală de securitate IoT este asigurarea faptului că dispozitivele și serviciile au identități de încredere care pot interacționa în cadrul unor ecosisteme sigure. Certificatele simple nu pot aborda multiplele niveluri de autorizații, roluri și informații necesare acestor medii complexe. Acest serviciu va evalua securitatea cheilor publice asociate cu dispozitivele IoT. De asemenea, evaluează soluțiile de securitate pentru a oferi încredere în conectarea dispozitivelor IoT la cloud. Acest serviciu este destinat IMM-urilor care folosesc dispozitive IoT conectate în fabricație (robotică, PLC-uri, unități de acționare) și/sau automatizare a clădirilor (hală de producție, birouri de inginerie).
Robotică socială - funcții și proiectare arhitectură de proces	Un asistent virtual poate fi proiectat în diferite forme și poate include diverse tehnologii și arhitecturi, inclusiv cazul implementării în producție. Organizațiile se confruntă cu dificultăți în configurarea funcționalităților și setărilor, inclusiv integrarea cu alte sisteme (de exemplu, site web, robot social fizic, aplicație mobilă etc.). Acest lucru crește costurile proiectului. Acest serviciu va asista organizațiile să elaboreze specificațiile pentru un asistent virtual în raport cu provocările menționate mai sus.
Evaluarea securității tehnologice	Protecția datelor ca una dintre cele mai importante responsabilități personale. Încălcările de date aduc un prejudiciu imens de reputație și adesea au un impact negativ de lungă durată. Acest serviciu se concentrează în principal pe securitatea datelor în organizație, inclusiv

	securitatea aplicațiilor web și mobile, securitatea în cloud (acolo unde este aplicabil), securitatea rețelei și securitatea mobilă. Poate include și evaluarea riscului IT pentru a determina nivelul acceptabil și nivelul real al riscului, un test simplu de penetrare și audit IT.
Asistență tehnică pentru punerea în funcțiune a echipamentelor inteligente	Punerea în funcțiune include diverse activități care au loc după instalarea echipamentelor. În timpul punerii în funcțiune a instalației, se efectuează teste pentru a demonstra că un component sau subsistem instalat funcționează conform proiectării. Punerea în funcțiune operațională include teste pentru a demonstra că componentele sau subsistemele funcționează într-o manieră integrată pentru a atinge funcționalitatea generală a sistemului. O punere în funcțiune eficientă este critică pentru realizarea beneficiilor echipamentului nou. Pe măsură ce multe facilități trec la tehnologii inteligente, acest proces necesită și mai multă diligență. Acest serviciu va ajuta IMM-urile pentru asistență tehnică în cazul celulelor de fabricație robotică sau automatizare cu PLC-uri sau instalarea soluțiilor cloud sau alte sisteme IT complexe. În cazul organismelor publice, acest serviciu va oferi asistență tehnică pentru migrarea datelor în cloud sau pentru alte sisteme IT complexe.
Studii de fezabilitate tehnică pentru sisteme bazate pe tehnologie digitală	Elaborarea studiului de fezabilitate tehnică conform reglementărilor românești pentru achizițiile publice.

Servicii de Formare Profesională

Denumire Serviciu	Descriere Serviciu
Marketing Digital (Workshop)	Marketingul digital este marketingul bunurilor și serviciilor prin intermediul tehnologiilor digitale. Marketingul digital include, de asemenea, promovarea serviciilor și produselor folosind publicitatea display, telefoanele mobile și alte media digitale. Acest serviciu este livrat în format de atelier, unde participanții vor învăța cum funcționează

	mediul digital și cum trebuie să-și configureze propriul ecosistem de canale și cea mai eficientă strategie pentru a atrage cât mai mulți vizitatori și cumpărători pe pagina lor web.
Cyber Security Defender	Gestionarea conturilor de utilizator; Configurarea securității aplicațiilor și a sistemului de operare; Securitatea datelor și confidențialitatea; Securitatea rețelei; Analiza malware-ului; Codare securizată; Politici de securitate cibernetică
Securitate Cibernetică pentru Toți [nivelul 1]	Introducere în securitatea cibernetică, termeni și concepte, autentificarea cu parolă, recunoașterea și evitarea atacurilor de tip phishing, amenințările malware, GDPR
Securitate Cibernetică pentru Toți [nivelul 2]	Clasificarea evenimentelor cibernetică; Actorii amenințărilor și motivațiile lor, Ingineria socială, Refuzul serviciului, Hacking-ul serverelor web, Hacking-ul aplicațiilor web, Hacking-ul rețelelor wireless, Hacking-ul platformelor mobile, Politici de securitate cibernetică (notă: pot apărea ajustări)
Arhitect Întreprindere Digitală	Provocări pe agenda de management, Paradigma ingineriei întreprinderii, Definirea arhitecturii întreprinderii, Aplicarea arhitecturii întreprinderii, Metoda de dezvoltare a arhitecturii, Cadru de capacitate a arhitecturii, Metoda ArchiMate, Construirea unei capacități de EA, Cele mai bune practici
Manager Transformare Digitală	Introducere în Industria 4.0; Internetul Industrial; Etapele de maturitate; Societatea 5.0; Economia circulară; Introducere în transformarea digitală; Transformarea afacerilor digitale; Cauzele perturbării și transformării; Transformarea digitală și experiența clientului; Strategia de Transformare Digitală; Configurarea Culturii și Proceselor Organizației Digitale; Transformarea digitală în diverse industrii (sectorul public, sănătate, fabricație)
Securitatea Rețelelor Industriale	Comutare și monitorizare; Alocarea adreselor în rețeaua de producție; Funcțiile de rutare și firewall; Rețele de fabricație separate prin VLAN; Traducerea Adreselor de Rețea (NAT); Rețele Private Virtuale (VPN); Comunicare criptată; Autorizare și control al accesului; Scalabilitate prin concepte de grup și rol; Funcționarea unei

	Infrastructuri cu Chei Publice (PKI); Manipularea certificatelor digitale.
Securitate Clădiri Inteligente	Introducere în automatizarea clădirilor; Sisteme de monitorizare și control pentru clădiri; Sistemul de iluminat; Sistemele de încălzire/răcire, ventilație și climatizare; Sisteme de securitate și siguranță; Tehnologiile de comunicație utilizate în automatizarea clădirilor; Dependințe ale sistemelor; Integrarea sistemelor; Standardele utilizate în implementarea instalațiilor; Proiectarea sistemelor de monitorizare și control; Implementarea sistemelor de monitorizare și control; Tehnologiile Internet of Things și utilizarea lor în automatizarea clădirilor; Automatizarea clădirilor pentru Orașul Inteligent; Studii de caz
Robotică Inteligentă pentru industrie [pachetul B]	Robotică inteligentă pentru fabricație este o tehnologie robotică industrială care cuprinde roboți industriali și/sau roboți mobili autonomi și/sau brațe robotice colaborative și/sau asistenți virtuali inteligenți (chatboți) care pot, de asemenea, colabora cu ființele umane, învăța din mediul/experiența lor și își rafinează sau modifică acțiunile în consecință. Robotică inteligentă pentru fabricație permite Inteligenței Artificiale (AI) și Internetului Obiectelor (IoT) să personalizeze experiența utilizatorului, să crească eficiența și să îmbunătățească productivitatea. Acest curs include programarea roboților ABB și coboților ABB, aplicații client-server prin TCP/IP sau utilizarea PLC-ului ca intermediar între client și server, conectarea robotului în cloud, colectarea datelor în cloud, analiza datelor cu ML, interacțiunea cu mediul cu sisteme de viziune și AI, comunicarea cu utilizatorii prin cloud și aplicații mobile.
Robotică Inteligentă pentru industrie [pachetul C]	Robotică inteligentă pentru fabricație este o tehnologie robotică industrială care include roboți industriali și/sau roboți mobili autonomi și/sau brațe robotice colaborative și/sau asistenți virtuali inteligenți (chatboți) capabili să colaboreze cu ființele umane, să învețe din mediul/experiența lor și să își rafineze sau modifice acțiunile în consecință. Robotică inteligentă pentru fabricație permite Inteligenței Artificiale (AI) și Internetului Obiectelor (IoT) să personalizeze experiența utilizatorului, să sporească eficiența și să îmbunătățească productivitatea. Acest curs include programarea roboților Motoman și Fanuc și a coboților UR, aplicații client-server

	prin TCP/IP sau utilizarea PLC-ului ca intermediar între client și server, conectarea robotului în cloud, colectarea datelor în cloud, analiza datelor cu ML, interacțiunea cu mediul prin sisteme de viziune și AI, comunicarea cu utilizatorii prin cloud și aplicații mobile.
Robotică Inteligentă pentru Sisteme de Produse-Servicii [pachetul B]	Introducere în robotică inteligentă specifică pentru sisteme de produs-serviciu (PSS), acoperind concepte de bază și aplicații. Prezentarea diferitelor tipuri de roboți (industriali, de servicii, mobili autonomi, exoschelete, drone) și rolul lor în cadrul unui sistem PSS. Bazele programării roboților și automatizării: Învățarea limbajelor de programare și a interfețelor utilizate în robotică. Utilizarea Inteligenței Artificiale și a IoT în robotică: O introducere în modul în care AI și IoT pot îmbunătăți funcționalitatea roboților în cadrul PSS. Principii de design pentru interacțiunea om-robot: Cum să se creeze interfețe eficiente și intuitive între roboți și utilizatorii umani. Aplicații practice și studii de caz: Examinarea cazurilor reale de utilizare a robotică inteligentă în diverse sectoare industriale. Aspecte de securitate și confidențialitate în robotică: Înțelegerea importanței securității datelor și a confidențialității în sistemele PSS.
Robotică Inteligentă pentru Sectorul Public	Robotică inteligentă pentru sectorul public include tehnologie robotică ce cuprinde roboți sociali și/sau roboți de servicii și/sau roboți mobili autonomi și/sau drone și/sau asistenți virtuali inteligenți (chatboți) și/sau brațe robotice colaborative care pot, de asemenea, colabora cu ființele umane, învață din mediul/experiența lor și își rafinează sau modifică acțiunile în consecință. Robotică inteligentă permite Inteligenței Artificiale (AI) și Internetului Obiectelor (IoT) să personalizeze experiența utilizatorului, să sporească eficiența și să îmbunătățească productivitatea. Focalizarea acestui curs va fi pe înțelegerea arhitecturii chatboților și modul în care pot fi implementați în sistemele de e-guvernare, precum și posibilitățile de utilizare a roboților sociali pentru relații publice. De asemenea, va include exerciții pentru dezvoltarea diferitelor aplicații de PR în sectorul public folosind kioscuri-robot și roboți sociali.

**Specializare în Digitalizare pentru
Sectorul Public**

Consecințele strategice și politice ale digitalizării; Relația dintre tehnologie, proces și schimbări organizaționale; Exemple de digitalizare în organizații de stat și municipale; Legătura între perspectiva valorii publice și efectele digitalizării; Rolul platformelor digitale, cum ar fi rețelele sociale, în procesele democratice; Comunicarea bazată pe tehnologie ca parte integrantă a strategiei de comunicare a conducerii și a proceselor decizionale politice; Exemple și experiențe din diverse organizații din sectorul public; Exemple de arhitecturi digitale în diverse organizații publice.

Servicii de accelerare a investițiilor

Denumire Serviciu	Descriere Serviciu
Consultanță sprijin pentru investiții Administrație Publică	Implementarea unui set de servicii integrate care facilitează accesul la finanțare pentru entități publice pentru proiecte în domeniul investițiilor tehnologice, digitalizării și inovației