ELECTROCENTRALE BUCUREȘTI S.A.
Splaiul Independenței nr. 227, cod poștal 060041, sector 6, București
Tel.: +4021.275.11.03, Fax: +4021.275.14.05
office@elcen.ro, www.elcen.ro
C.U.I.: 15189596, R.C.: J40/1696/2003

ELECTROCENTRALE BUCURESTI S.A.
Nr. 48872/15.10.2026

APROBAT
Director Directia Management si Securitate
SEBASTIAN MARIAN DEACONESCU

Caiet de sarcini pentru servicii de proiectare în vederea realizării unui sistem electronic de securitate integrat CTE Bucuresti Sud

Serviciile de proiectare tehnică la faza Proiect Tehnic și Detalii de Execuție (PT + DE), pentru sistemul electronic de securitate integrat al CTE Bucuresti Sud va cuprinde următoarele subsisteme:

- supraveghere video cu funcții de analiză video;
- control acces;
- detecție la efracție;
- modernizare sistem iluminat exterior;
- dispecerat central de monitorizare;

Cerințele din caietul de sarcini sunt obligatorii, iar nerespectarea acestora în totalitate conduce la respingerea ofertei. Ofertanții vor prezenta un angajament sub semnătura administratorului societății, din care să rezulte capacitatea de a presta serviciile de proiectare care fac obiectul prezentului caiet de sarcini pentru obiectivul precizat în Anexa nr. 1, odată cu intrarea în vigoare a contractului.

Cuprinsul caietului de sarcini

1. Date generale
2. Cerințe privind protecția informațiilor clasificate
3. Obiectul, scopul și cerințele generale ale contractului
4. Descrierea obiectivelor și datele de intrare
5. Cerințe privind arhitectura și funcționalitățile sistemului electronic de securitate integrat
6. Modalitățile de prestare a serviciilor de proiectare
7. Conținutul documentației de proiectare
8. Condiții de prestare a serviciilor de proiectare
9. Durata contractului, valoarea estimată și alte date contractuale
10. Avizarea și recepția documentației
11. Norme de securitatea muncii, PSI, situații de urgență și protecția mediului
12. Dispoziții finale și precizări
13. Modul de prezentare a propunerii tehnice și financiare

Anexele parte intergată din caietul de sarcini sunt:

1 – Lista obiectivelor cu adresele poștale;
2 – Liste de cantități estimate pe categorii de subsisteme;
3 – analiza de risc la securitate fizică;
4 – Extras neclasificat din Studiul de fezabilitate;
5 – Lista specialiștilor solicitați;
6 – Anexa de securitate;

- 6.1 Lista personalului autorizat care va avea acces la informații clasificate secrete de serviciu;
- 6.2 Lista locurilor de execuție a activităților în care se utilizează informații clasificate;
- 6.3 Caiet de sarcini privind protectia informatiilor clasificate;

7 – Formularul propunerii financiare.

Cap. 1. Date generale

1.1. Societatea Electrocentrale București S.A., cu sediul în Splaiul Independenței nr. 227, sector 6, București, are ca principal obiect de activitate producerea și vânzarea de energie electrică pentru Sistemul Energetic Național și de energie termică pentru alimentarea populației de pe raza Municipiului București.

1.2. Din structura organizatorică a societății fac parte următoarele obiective: CTE București Sud, CTE București Vest, CTE Grozăvești cu trei puncte de lucru și Sediul executiv ELCEN, precum și CTE Progresu cu un punct de lucru, amplasate pe teritoriul Municipiului București și al județului Ilfov;

1.3. Specificul activității, importanța și valoarea instalațiilor existente impun implementarea unui sistem electronic de securitate integrat, care să permită reducerea costurilor cu personalul de pază și, în același timp, creșterea nivelului de securitate prin mijloace electronice și analiză video. Soluția tehnico-economică a fost aprobată de Consiliul de Administrație pe baza Studiului de fezabilitate „Sistem electronic de securitate (sistem video de monitorizare integrat, cu componenta pază perimetrală și control acces) Electrocentrale București SA".

1.4. Prezentul caiet de sarcini privește exclusiv serviciile de proiectare tehnică, faza Proiect Tehnic și Detalii de Execuție (PT + DE), inclusiv piesele desenate. Furnizarea echipamentelor, execuția lucrărilor și punerea în funcțiune a sistemului se vor realiza ulterior, prin procedură separată, pe baza documentației elaborate în cadrul prezentului contract. Serviciile de pază umană, patrulare și intervenție nu fac obiectul prezentei proceduri.

1.5. Cadrul legal principal aplicabil:

- Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, republicată, cu modificările și completările ulterioare, inclusiv O.U.G. nr. 37/2026;
- H.G. nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003, cu modificările și completările ulterioare;
- Legea nr. 10/1995 privind calitatea în construcții, republicată, cu modificările și completările ulterioare;
- H.G. nr. 907/2016 privind etapele de elaborare și conținutul-cadru al documentațiilor tehnico-economice aferente obiectivelor/proiectelor de investiții finanțate din fonduri publice;
- Legea nr. 307/2006 privind apărarea împotriva incendiilor, cu modificările și completările ulterioare;
- Legea nr. 182/2002 privind protecția informațiilor clasificate, H.G. nr. 585/2002 și H.G. nr. 781/2002;
- Regulamentul (UE) 2016/679 privind protecția datelor cu caracter personal și Legea nr. 190/2018;
- Legea nr. 99/2016 privind achizițiile publice și H.G. nr. 394/2016.

Cap. 2. Cerințe privind protecția informațiilor clasificate

2.1. Prestatorul trebuie să dețină, pe toată perioada de valabilitate a contractului, un funcționar de securitate și o structură de securitate proprie, în conformitate cu prevederile Legii nr. 182/2002 privind protecția informațiilor clasificate, cu modificările și completările ulterioare, a Standardelor Naționale de Protecție a Informațiilor Clasificate în România, aprobate prin H.G. nr. 585/2002, și a H.G. nr. 781/2002 privind protecția informațiilor secrete de serviciu.
2.2. Documentația de proiectare elaborată în cadrul contractului (PT + DE) conține informații ce urmează a fi clasificate. Prestatorul are obligația să se asigure că toate persoanele care, în virtutea principiului „nevoii de a cunoaște", vor avea acces la respectivele informații vor deține autorizații de acces la informații clasificate nivel „Secret de serviciu". Informațiile și documentele, precum și nivelul de clasificare vor fi menționate în anexa de securitate, care face parte integrantă din contract (Anexa nr. 6).
2.3. Elaborarea, multiplicarea, transmiterea, păstrarea și predarea documentației se realizează cu respectarea regimului juridic prevăzut de lege pentru informațiile clasificate.
2.4. Pe lângă documentația clasificată, prestatorul va elabora un extras neclasificat al proiectului (caiete de sarcini, liste de cantități, specificații tehnice), obținut prin anonimizarea datelor sensibile, care să poată fi pus la dispoziția ofertanților în procedura de achiziție pentru furnizare și execuție.
2.5. Pentru o înțelegere completă a activităților ce urmează a fi desfășurate, ofertanții au posibilitatea să viziteze obiectivele și să consulte documentele aferente (analize de risc la securitatea fizică, planuri de pază, planșe cu dispunerea echipamentelor electronice de securitate existente etc.) la sediul autorității contractante. Vizitarea tuturor obiectivelor se va finaliza cu întocmirea unui proces-verbal de vizitare.
2.6. Vizitarea obiectivelor se va efectua a7pe baza unei solicitări transmise de ofertanți pe adresa de email stipulată în fișa de date; data și ora exactă se stabilesc de comun acord. La prezentarea pentru vizită, operatorii economici vor prezenta autorizațiile de acces la informații clasificate nivel „Secret de serviciu" ale tuturor persoanelor care vor avea acces la documente clasificate.

Cap. 3. Obiectul, scopul și cerințele generale ale contractului

3.1. Obiectul contractului constă în prestarea serviciilor de proiectare tehnică, faza Proiect Tehnic și Detalii de Execuție (PT + DE), pentru sistemul electronic de securitate integrat al obiectivului din Anexa nr. 1, inclusiv dispeceratul local de monitorizare. Cerințele sunt formulate unitar, iar documentația PT + DE se elaborează pe CTE Bucuresti Sud și cuprinde următoarele subsisteme:

a) supraveghere video cu analiză video și detecție perimetrală;
b) control acces cu automatizare și management al vizitatorilor, inclusiv recunoașterea numerelor de înmatriculare;
c) detecție și alarmare la efracție;
d) monitorizarea sistemelor de detecție și alarmare la incendiu în cadrul unei platforme unice;
e) reablitarea sistemului de iluminat existent, necesar funcționării supravegherii video și eficienței pazei;
f) dispeceratul central de monitorizare și management centralizat, dispeceratele locale și punctele de vizualizare;
g) infrastructura de rețea, de transmisie și de alimentare electrică aferentă.

3.2. Scopul contractului este obținerea unei documentații complete, care să permită: obținerea avizelor prevăzute de lege, inclusiv avizul organelor de poliție; organizarea procedurii de achiziție pentru furnizarea echipamentelor și execuția lucrărilor; execuția lucrărilor fără completări de

proiectare. Sistemul proiectat urmărește „sigilarea" perimetrului și controlul strict al accesului, reducerea costurilor cu personalul de pază și creșterea nivelului de securitate prin mijloace electronice și analiză video.

3.3. Nu fac obiectul contractului: furnizarea echipamentelor, execuția lucrărilor, punerea în funcțiune, mentenanța și exploatarea sistemului, serviciile de pază, patrulare, monitorizare-intervenție și transport valori.

3.4. Obiective primare. Serviciile de proiectare au ca obiective primare:

a) asigurarea, prin soluțiile proiectate, a securității instalațiilor, echipamentelor, bunurilor și persoanelor din cadrul obiectivelor;

b) controlul accesului în obiective în conformitate cu prevederile legale în vigoare și procedurile ELCEN, în scopul împiedicării sustragerilor de orice fel și a pătrunderii ilegale a persoanelor străine;

c) proiectarea pe baza documentelor și informațiilor primite de la Autoritatea Contractantă (Studiul de fezabilitate, analizele de risc la securitatea fizică, planurile de pază, listele de cantități și fișele tehnice);

d) asigurarea calității serviciilor de proiectare prin utilizarea unor tehnologi moderne, a unor platfome software deschise;

3.5. Garanția de bună execuție. Pentru garantarea calității și realizării în termenul stabilit, se prevede o garanție de bună execuție de 5% din valoarea contractului, fără TVA, constituită prin una dintre următoarele modalități:

a) virament bancar în contul beneficiarului;

b) instrumente de garantare emise în condițiile legii: scrisoare de garanție emisă de o instituție de credit din România sau din alt stat; asigurare de garanții emisă fie de o societate de asigurări care deține autorizație de funcționare emisă în România sau într-un alt stat membru al Uniunii Europene și/sau este înscrisă în registrele publicate pe site-ul Autorității de Supraveghere Financiară, fie de o societate de asigurări dintr-un stat terț, printr-o sucursală autorizată în România de Autoritatea de Supraveghere Financiară. Instrumentul de garantare, prezentat în original, va prevedea plata sumelor reclamate de beneficiar necondiționat și irevocabil, la prima cerere, oricând pe durata de valabilitate, fără nicio formalitate suplimentară, până la concurența sumei garantate. Valabilitatea instrumentului trebuie să depășească cu minim 30 de zile durata contractului și se prelungește corespunzător dacă contractul nu se finalizează în această perioadă;

Cap. 4. Descrierea obiectivelor și datele de intrare

4.1. Proiectarea se realizează pentru CTE Bucuresti Sud, la care se adaugă dispeceratul local de monitorizare. Ultima coloană arată dacă, după implementarea sistemului, obiectivul rămâne cu pază fizică permanentă, conform Studiului de fezabilitate; numărul punctelor locale de vizualizare se stabilește în PT, în funcție de dispozitivul final de pază.

Obiectiv	Adresă	Suprafață (mp)	Porți de acces	Sisteme existente	Pază permanentă după implementare
H. CTE București Sud	Str. Releului nr. 2B, sector 3	325.276	4 (persoane, auto, CFR)	Kit de panică la poarta principală	Da

4.2. Kiturile de panică și sistemele antiefracție existente sunt conectate în prezent la un dispecerat de monitorizare și intervenție, proiectul va prevedea integrarea lor în sistemul nou.

4.3. Limita de perimetru se află la nivelul gardului exterior al obiectiv.
4.4. Datele de intrare puse la dispoziție de Autoritatea Contractantă sunt:
a) Studiul de fezabilitate, etapele 1 și 2, extras neclasificat în Anexa nr. 4;
b) Liste de cantități estimate pe categorii de subsisteme Anexa nr. 2;
c) analizele de risc la securitatea fizică al obiectivului Anexa nr. 3 (planul de paza este consultabil la sediul Autorității Contractante)
4.5. Datele de intrare se completează de proiectant prin relevee proprii în fiecare obiectiv, conform Cap. 6.

Cap. 5. Cerințe privind arhitectura și funcționalitățile sistemului electronic de securitate integrat

Cerințele din prezentul capitol sunt minimale și trebuie acoperite integral de soluția proiectată, acestea derivă din Studiul de fezabilitate și din cerințele Autorității Contractante.

5.1. Principii de proiectare

5.1.1. Strategia de securitate este „sigilarea" perimetrului și controlul strict al accesului în zonele și spațiile de interes. Sistemul asigură funcția de protecție, dar și funcția de suport, prin generarea de indicatori de performanță, statistici și alerte.
5.1.2. Detecția la nivelul perimetrului se realizează pe 100% din perimetru, pentru 100% din timp și la 100% din parametri, exclusiv prin mijloace tehnice. Resursa umană reprezintă doar varianta de rezervă, pentru situații deosebite și pentru o perioadă limitată (ex.: până la repararea sau înlocuirea unui echipament defect).
5.1.3. Soluția proiectată trebuie să îndeplinească următoarele cerințe de specialitate:

- detecția timpurie, la nivelul perimetrului, prin mijloace automatizate și calificate;
- reacția rapidă și calificată, dimensionată situației;
- existența unei soluții de rezervă pentru orice situație în care sistemul nu funcționează conform specificațiilor;
- trasabilitatea fiecărei activități (ex.: armare/dezarmare, intervenție), în vederea alocării eficiente a răspunderii;
- managementul specializat al activităților;
- generarea de date suport pentru companie (statistici, alerte) și de indicatori de performanță care să permită identificarea timpurie a situațiilor neconforme sau potențial periculoase;
- reducerea costurilor.

5.1.4. Sistemul se proiectează pe conceptul de securitate bazată pe date, cu operatorul uman ca decident final: fluxuri de lucru predefinite care filtrează automat alarmele false și corelează evenimentele; înregistrarea ireversibilă a oricărei schimbări de stare, modificări de parametri și acțiuni umane; alocarea automată și transparentă a răspunderii pe lanțul dispecer – agent – manager.
5.1.5. Specificațiile tehnice din PT se formulează prin caracteristici funcționale și de performanță. Se vor prefera echipamente și platforme care utilizează protocoale și interfețe deschise, standardizate, care asigură interoperabilitatea și independența față de un anumit furnizor.
5.1.6. Infrastructura și platformele sistemului sunt proprietatea ELCEN. Firma de pază se conectează ca utilizator, prin interfețe și drepturi definite de ELCEN, astfel încât schimbarea prestatorului de pază să nu necesite modificarea proiectului.
5.1.7. Sistemul trebuie să fie scalabil și să permită integrări ulterioare, inclusiv prin interfețe de programare (API) documentate.

5.2. Arhitectura de monitorizare și managementul centralizat

5.2.1. Sistemul proiectat trebuie să fie integrat, administrarea acestuia trebuie să se poată realiza dintr-o platformă software unică, cu management centralizat și alocare dinamică a resurselor. Toate subsistemele (supraveghere video, control acces, efracție, monitorizarea detecției la incendiu, comanda iluminatului, starea echipamentelor) raportează într-o platformă de management centralizat, cu management centralizat al alarmelor și al sistemelor implementate în ansamblul lor.

5.2.2. Monitorizarea alarmelor și a imaginilor live se realizează în timp real, pe trei niveluri:

a) **Dispeceratul local și punctele de vizualizare de la posturile de pază** – se păstrează și se integrează în sistemul central; preiau monitorizarea obiectivului la indisponibilitatea dispeceratului central (pauză, lipsă de conexiune). Postul de la poarta principală monitorizează camerele zonei de acces, tratează cazurile deosebite (ex.: număr de înmatriculare citit greșit) și comandă de la distanță celelalte puncte de acces dinspre exterior;

c) **Dispecerul propriu al firmei de pază** – principalul utilizator operațional al sistemului; are acces în timp real la alarme și la imaginile live de la toate obiectivele, cu drepturi definite pe roluri, printr-o conexiune securizată și segregată (pct. 5.8).

5.2.3. Evenimentele se transmit simultan către toate nivelurile de monitorizare. Proiectul va prevedea căi de transmisie principale și de rezervă, cu supravegherea continuă a disponibilității lor, având ca referință seria de standarde SR EN 50136.

5.2.4. Proiectul va defini regulile de tratare a evenimentelor între cele trei niveluri: preluare, confirmare, escaladare și închidere, fără dublă tratare și cu alocarea automată a răspunderii.

5.2.5. Posturile de operare vor asigura cel puțin: vizualizare live și redare; comenzi de zoom și orientare a camerelor mobile; căutare inteligentă în înregistrări; afișarea automată a imaginilor asociate unei alarme; registru electronic de evenimente și de tură; notificarea echipajelor de intervenție și a persoanelor desemnate de ELCEN (șeful de obiectiv, responsabilul cu paza, inginerul șef); acces de la distanță securizat pentru reprezentanții beneficiarului, inclusiv de pe dispozitive mobile.

5.2.6. Sistemul va măsura automat și va raporta cel puțin: timpul de preluare a evenimentului, timpul de reacție (prima intervenție la fața locului), timpul de rezolvare și timpul total de nefuncționare a sistemelor, comparabil cu nivelul de serviciu contractat cu furnizorii.

5.2.7. Kiturile de panică și sistemele antiefracție existente (Cap. 4) se integrează în sistemul nou și se monitorizează pe toate cele trei niveluri.

5.3. Supraveghere video și detecție perimetrală

5.3.1. Detecția accesului neautorizat la nivelul perimetrului se realizează prin camere video cu funcții de analiză video (detecția formei umane și a vehiculelor, trecerea unei linii virtuale, intruziunea într-o arie), care alertează automat dispecerul și îi permit validarea vizuală a alarmei. Zona de detecție se setează la limita de proprietate, astfel încât alertarea să se producă în momentul pătrunderii.

5.3.2. Soluțiile tehnice eligibile, conform Studiului de fezabilitate, sunt:

- a) camere video cu un obiectiv, infraroșu și alertă audio, cu detecție tipică la distanțe de până la 50–60 m;
- b) camere video cu obiectiv dublu, infraroșu și alertă audio, pe tronsoanele de perimetru fără obstacole (elemente constructive, copaci, instalații, trasee de țevi).

Camerele vor putea fi prevăzute cu difuzoare pentru adresarea la distanță a persoanelor detectate.

5.3.3. Sistemele de detecție perimetrală independente (infraroșu, microunde, gard inteligent) și camerele termale nu se utilizează ca soluție generală, pentru motivele prezentate în Studiul de fezabilitate. Camerele termale pot fi propuse punctual, pe linii drepte de perimetru aflate la minim 10 m de căile interioare de circulație, numai cu justificare tehnico-economică.
5.3.4. Pentru fiecare zonă supravegheată, PT va stabili nivelul de performanță necesar (detecție, observare, recunoaștere, identificare) și va justifica prin calcul acoperirea și amplasarea camerelor.
5.3.5. Funcțiile de analiză video și de licențiere care se vor specifica în PT, evidențiate separat pe tip de sistem, sunt cel puțin: detecție perimetrală bazată pe inteligență artificială; recunoașterea numerelor de înmatriculare; detecția atributelor vehiculelor; clasificarea țintelor om/vehicul cu filtrarea alarmelor false; analiză video pentru persoane și vehicule; detecție de mișcare cu clasificarea țintelor pe toate canalele; redare și căutare inteligentă; trecere linie virtuală, intruziune, intrare/ieșire din regiune.
5.3.6. Funcția de recunoaștere facială se proiectează numai acolo unde există un temei legal și pe baza unei evaluări a impactului asupra protecției datelor, conform Regulamentului (UE) 2016/679.
5.3.7. Perioada de stocare a înregistrărilor video va fi de minimum 20 de zile, conform legislației în vigoare. PT va dimensiona capacitatea de stocare prin calcul.
5.3.8. PT va prevedea semnalizarea zonelor supravegheate video, conform legislației privind protecția datelor cu caracter personal.

5.4. Control acces cu automatizare și management al vizitatorilor

5.4.1. Soluția de control acces este sistemul cu automatizare a accesului și management al vizitatorilor, conectat online, care gestionează independent toate punctele de acces, pe fluxuri distincte, fără a necesita intervenția personalului de securitate decât în cazurile atipice sau la alerte, inclusiv de la distanță. Interfonul se poate utiliza doar ca echipament suplimentar, pentru comunicarea cu dispecerul sau ca element de captare a datelor. Un sistem de management al parcărilor se acceptă numai dacă nu folosește consumabile și are funcționalități de corelare a datelor între locații.
5.4.2. Sistemul va asigura:

- autentificarea persoanelor și a autovehiculelor, atât la intrare, cât și la ieșire;
- autorizarea accesului pe baza unor parametri specifici (program de lucru, punct de acces etc.);
- auditarea, prin înregistrarea jurnalelor operațiunilor de acces;
- control multistratificat: pe bază de roluri; pe bază de atribute (ex.: purtarea echipamentului individual de protecție); obligatoriu, cu reguli stricte, pentru punctele de acces din exterior și zonele cu grad mare de criticitate (dispecerat, spații cu documente clasificate);
- fluxuri individuale și gestionarea distinctă a angajaților, vizitatorilor și furnizorilor, inclusiv acces în regim self-service;
- acționarea de la distanță a echipamentelor (porți, bariere, turnichete) pentru punctele de acces neasistate de personal;
- interfețe de programare (API) documentate, pentru dezvoltări sau integrări ulterioare.

5.4.3. Componentele sistemului vor fi: sistemul de management al identității (înrolare și administrare utilizatori); elementele de captare a datelor (cititoare de diverse tehnologii, tastaturi, ecrane tactile, camere de recunoaștere a numerelor de înmatriculare); controlerele de acces, amplasate obligatoriu în zona protejată; elementele de blocare (bariere, turnichete, electromagneți etc.); componentele de control și management centralizat.

5.4.4. Componenta de gestionare a vizitatorilor trebuie să prezinte dovada legală că poate înlocui registrul pe hârtie prevăzut de legislație (certificare, aprobare sau aviz al autorităților competente). Sistemul de control acces gestionează posesorii de carduri (angajații), iar registrul electronic certificat gestionează vizitatorii.

5.5. Detecție și alarmare la efracție

5.5.1. Gradul de securitate al sistemelor de alarmare la efracție se stabilește pe baza analizei de risc la securitatea fizică.

5.6. Monitorizarea sistemelor de detecție și alarmare la incendiu

5.6.1. PT va prevedea preluarea în platforma de management centralizat și afișarea pe toate nivelurile de monitorizare a semnalelor de alarmă, defect și stare de la centralele de detecție și alarmare la incendiu din obiectiv.
5.6.2. Proiectantul va inventaria, prin relevee, centralele de detecție la incendiu existente și va stabili soluția de interfațare (contacte, protocol de comunicație), fără a afecta funcționarea și conformitatea acestora cu Normativul P118/3-2015 și SR EN 54.

5.7. Sistemul de iluminat

5.7.1. Proiectul tehnic tratează obligatoriu sistemul de iluminat al perimetrului, al punctelor de acces și al zonelor de interes, ca necesitate absolută pentru funcționarea analizei video și pentru asigurarea unui serviciu de pază eficient.
5.7.2. PT va realiza releveul iluminatului existent și va stabili, pe zone, nivelurile de iluminare necesare, corelate cu performanța camerelor (inclusiv funcționarea în infraroșu) și cu nivelurile de detecție, observare, recunoaștere și identificare de la pct. 5.3.4, având ca referință SR EN 12464-2.
5.7.3. Soluția de iluminat va evita orbirea camerelor și poluarea luminoasă, va utiliza corpuri de iluminat cu eficiență energetică ridicată și va permite comanda automată (programare, senzori crepusculari) și comanda din platforma centralizată, inclusiv aprinderea zonelor la declanșarea unei alarme.
5.7.4. PT va prevedea alimentarea și protecția circuitelor de iluminat, precum și elementele de susținere (stâlpi, console, fundații), cu detaliile de execuție aferente.

5.8. Rețea de date, transmisie și securitate cibernetică

5.8.1. Sistemul de securitate va funcționa pe o rețea dedicată, segmentată și separată de rețeaua de birou a beneficiarului.
5.8.2. PT va dimensiona lățimea de bandă necesară între obiective, dispeceratul central, dispeceratele locale și dispeceratul firmei de pază, inclusiv fluxurile video pentru vizualizarea de la distanță, și va stabili necesarul de conectivitate.
5.8.3. Măsurile minime de securitate a datelor, care se vor detalia în PT, sunt:

- confidențialitate: criptarea datelor în tranzit (canale private virtuale, protocoale securizate pentru camere și controlere) și în repaus, cel puțin pentru comunicațiile din afara rețelei locale; aplicarea principiului privilegiului minim (fiecare operator vede doar camerele necesare rolului său);
- integritate: restrângerea drepturilor utilizatorilor, copii de siguranță și jurnale detaliate de utilizare a platformelor;
- disponibilitate: segmentarea rețelei, redundanța componentelor critice (servere cu preluare automată la defect) și monitorizarea continuă a stării echipamentelor;

- răspundere: eliminarea conturilor generice, autentificarea multi-factor pentru accesul la zonele sensibile și jurnale de audit care înregistrează cine, ce modificare a făcut și din ce valoare în ce valoare.

5.8.4. Conexiunea dispeceratului firmei de pază se proiectează securizat și segregat: canal dedicat criptat, autentificare multi-factor, conturi nominale, drepturi limitate la rolul operațional și jurnal de audit.

5.8.5. PT va ține seama de cerințele de securitate cibernetică aplicabile beneficiarului, inclusiv cele rezultate din transpunerea Directivei (UE) 2022/2555 (NIS2).

5.9. Alimentare electrică

5.9.1. PT va proiecta alimentarea electrică a tuturor echipamentelor, cu surse neîntreruptibile și, unde este necesar, surse de rezervă, astfel încât sistemul să funcționeze la căderea alimentării de bază. Autonomia minimă se stabilește în PT, pe baza analizei de risc și a cerințelor legale aplicabile.

5.10. Mentenanță și exploatare

5.10.1. PT va cuprinde instrucțiunile de exploatare și mentenanță, cu un program recomandat: mentenanță semestrială în locațiile nefuncționale sau în conservare și trimestrială în locațiile funcționale, având în vedere mediul industrial.

5.10.2. PT va stabili lista stocului tampon pentru echipamentele cu impact semnificativ și predispuse la defectare (ex.: routere, camere perimetrale, brațe de barieră) și va formula cerințele de nivel de serviciu pentru viitorul contract de mentenanță (timp de intervenție de maxim 24 de ore).

5.10.3. PT va descrie scenariile de rezervă pentru situațiile de nefuncționare parțială sau extinsă a sistemului, ca bază pentru planurile de contingență ale beneficiarului.

Cap. 6. Modalitățile de prestare a serviciilor de proiectare

6.1. Proiectarea se realizează pe baza datelor de intrare de la pct. 4.4, completate cu relevee proprii. Proiectul tehnic va avea la bază analiza de risc la securitatea fizică a fiecărui obiectiv.

6.2. Serviciile de proiectare cuprind următoarele activități:

1. preluarea și analiza datelor de intrare;
2. releveul fiecărui obiectiv: perimetru, porți și căi de acces, iluminat existent, sisteme de securitate existente, centrale de detecție la incendiu, trasee de cabluri, puncte de alimentare, spații tehnice;
3. evaluarea riscurilor specifice fiecărei locații și corelarea soluției cu analiza de risc la securitatea fizică;
4. stabilirea configurației sistemelor, prin alegerea tipurilor de echipamente pe criterii funcționale și de performanță, fără referire la mărci;
5. elaborarea unei soluții de principiu pentru fiecare obiectiv și pentru dispeceratul central, supusă aprobării beneficiarului înainte de detaliere;
6. elaborarea PT + DE pe fiecare obiectiv și a proiectului dispeceratului central;
7. întocmirea și susținerea documentației pentru obținerea avizului organelor de poliție, conform H.G. nr. 301/2012;
8. verificarea tehnică de calitate a proiectului de către verificatori de proiecte atestați, pentru cerințele aplicabile;

6.3. Cantitățile din Anexa nr. 2 sunt determinate la faza de studiu. Proiectantul le poate majora, cu justificare tehnică; reducerea lor se face numai cu justificare tehnică și cu acordul scris al beneficiarului.
6.4. Predarea documentației se face pe obiectivul CTE Bucuresti Sud.
6.5. Pe durata contractului, prestatorul participă la ședințe de lucru periodice cu reprezentanții beneficiarului și transmite rapoarte de progres.

Cap. 7. Conținutul documentației de proiectare (PT + DE)

7.1. Documentația se elaborează conform conținutului-cadru al proiectului tehnic de execuție prevăzut de H.G. nr. 907/2016, cu particularitățile proiectelor de sisteme de securitate prevăzute de H.G. nr. 301/2012, și cuprinde, pentru fiecare obiectiv, piesele de mai jos.
7.2. **Piese scrise:**

- memoriu tehnic general și memorii pe specialități: supraveghere video și analiză video, control acces, efracție, iluminat, rețea și transmisie, alimentare electrică, dispecerat;
- evaluarea riscurilor specifice și corelarea soluției cu analiza de risc la securitatea fizică;
- breviare de calcul: acoperire video și niveluri de performanță, stocare, lățime de bandă, iluminat, alimentare și autonomie, căderi de tensiune;
- matricea de integrare și interfețe: evenimente, protocoale, priorități și reguli de tratare între subsisteme și cele trei niveluri de monitorizare;
- cerințele de securitate cibernetică și protecția datelor, inclusiv elementele necesare evaluării impactului asupra protecției datelor;
- caiete de sarcini pentru execuția lucrărilor și pentru furnizarea echipamentelor, cu specificații tehnice neutre (caracteristici minime);
- liste de cantități de lucrări și de echipamente, pe obiecte și categorii de lucrări;
- deviz general și devize pe obiect;
- programul de control al calității execuției, cu fazele determinante;
- procedurile de testare, recepție și punere în funcțiune;
- instrucțiunile de exploatare și mentenanță și lista stocului tampon;
- măsurile de securitate și sănătate în muncă pentru execuție;
- extrasul neclasificat prevăzut la pct. 2.4.

7.3. **Piese desenate:**

- plan de încadrare în zonă și plan de situație, cu limita perimetrului;
- planuri de amplasare a echipamentelor: camere cu câmpurile vizuale și zonele de detecție, cititoare, bariere, turnichete, senzori, corpuri de iluminat, difuzoare;
- scheme bloc și scheme de principiu pentru fiecare subsistem și pentru sistemul integrat;
- schema rețelei de date (topologie, segmentare);
- trasee de cabluri și canalizații;
- scheme de alimentare electrică (tablouri, surse neîntreruptibile);
- planurile dispeceratului central și ale dispeceratelor locale (amplasarea posturilor de operare și a ecranelor);
- detalii de execuție pentru toate elementele care nu pot fi executate fără detaliere: montaj camere și senzori, stâlpi, console, fundații, treceri și protecții.

7.4. Documentația se predă în limba română, semnată și ștampilată, în numărul de exemplare pe suport hârtie prevăzut la pct. 9.3 și în format electronic, atât editabil (desene, documente, tabele), cât și PDF, cu respectarea regimului informațiilor clasificate.

Cap. 8. Condiții de prestare a serviciilor de proiectare

8.1. Activitatea de proiectare a sistemelor tehnice de securitate este strict reglementată și se realizează de societăți licențiate de Inspectoratul General al Poliției Române (I.G.P.R.). Ofertanții vor face dovada că dețin licența de funcționare T pentru activitățile de proiectare, instalare, modificare sau întreținere a componentelor sau sistemelor de alarmare împotriva efracției.

8.2. Ofertanții vor deține codul CAEN 8020 – Activități de servicii privind sistemele de securizare.

8.3. Ofertantul va prezenta o echipă care să conțină cel puțin următorii experți principali, cu responsabilitățile, cerințele minime și documentele doveditoare din Anexa nr. 5: manager de proiect (1 persoană), proiectant coordonator sisteme de securitate (1 persoană), proiectant sisteme de securitate (2 persoane) și expert instalații electrice (1 persoană). Ofertantul va prezenta informații privind modul de asigurare a avizelor I.G.P.R. pentru personalul calificat, conform art. 80 din H.G. nr. 301/2012.

8.4. Pe lângă licența de la pct. 8.1, ofertantul (respectiv membrul asocierii sau subcontractantul care prestează partea de servicii corespunzătoare) va face dovada că deține, în termen de valabilitate la data depunerii ofertei:

a) autorizație emisă de Inspectoratul General pentru Situații de Urgență pentru proiectarea sistemelor și instalațiilor de semnalizare, alarmare și alertare la incendiu;

b) atestat emis de Autoritatea Națională de Reglementare în Domeniul Energiei de tip C1A, pentru proiectarea de linii electrice aeriene sau subterane cu tensiunea nominală de 0,4 kV ÷ 20 kV, posturi de transformare cu tensiunea nominală superioară de cel mult 20 kV, stații de medie tensiune, precum și partea electrică de medie tensiune a stațiilor de înaltă tensiune;

c) certificate pentru sistemul de management al calității conform SR EN ISO 9001, sistemul de management al securității informației conform SR EN ISO/IEC 27001 și sistemul de management de mediu conform SR EN ISO 14001, în versiunile în vigoare, emise de organisme de certificare acreditate. Autoritatea Contractantă acceptă certificate echivalente emise de organisme stabilite în alte state membre, precum și alte dovezi privind măsuri echivalente, conform art. 195 din Legea nr. 99/2016;

d) un sistem intern de protecție a informațiilor clasificate secrete de serviciu, organizat conform H.G. nr. 781/2002, în corelare cu cerințele de la Cap. 2 și pct. 8.6.

8.5. Ofertanții (inclusiv toți membrii unei asocieri, terții susținători și subcontractanții) vor face dovada că dețin o politică privind protecția datelor cu caracter personal.

8.6. Ofertanții (ofertant unic, toți membrii unei asocieri, terții susținători, subcontractanții) vor prezenta dovada că dețin Plan de prevenire a scurgerii de informații clasificate aprobat de Serviciul Român de Informații, prin numărul și data planului și numărul și data adresei de aprobare. La solicitarea Autorității Contractante, acestea vor fi prezentate în condițiile legii.

8.7. Responsabilitatea instruirii, a prelucrării normelor legislative și a echipării cu mijloace de securitate și sănătate în muncă revine exclusiv prestatorului, care va face dovada deținerii de personal anume desemnat pe această linie.

8.9. Rolul de responsabil de contract și de interfață cu Autoritatea Contractantă este îndeplinit de managerul de proiect.

8.10. Experții principali pot fi înlocuiți numai în condițiile din Anexa nr. 5 și ale art. 162 alin. (1) lit. b) din H.G. nr. 395/2016, cu persoane care îndeplinesc cel puțin aceleași cerințe minime.

Cap. 9. Durata contractului, valoarea estimată și alte date contractuale

9.1. Durata contractului este de 90 de zile de la data semnării contractului.

9.2. Serviciile se prestează în următorii pasi:

Pasul	Conținut	Termen
1	Preluarea datelor de intrare, relevee, soluții de principiu pe obiectiv și pentru dispeceratul local	Termenul contractual este de 90 de zile
2	PT + DE pe obiectiv, predate eșalonat conform pct. 6.4	
3	Verificarea tehnică de calitate și recepția documentației	10 zile de la data acceptării documentației fără observații

9.3. Documentatia va fi in doua exemplare in format fizic.

Cap. 10. Avizarea și recepția documentației

10.1. Proiectantul întocmește și depune documentația în vederea obținerii avizului organelor de poliție, conform normelor metodologice aprobate prin H.G. nr. 301/2012.

10.2. Proiectul se verifică de verificatori de proiecte atestați, pentru cerințele aplicabile; referatele de verificare fac parte din documentația predată.

10.3. Recepția documentației se face la finalizarea serviciilor conform contractului, de către comisia desemnată de ELCEN, pe bază de proces-verbal. Observațiile comisiei se remediază de proiectant fără costuri suplimentare.

10.4. Proiectantul răspunde, conform Legii nr. 10/1995, pentru calitatea documentației și remediază fără costuri suplimentare erorile sau omisiunile de proiectare constatate pe parcursul execuției.

Cap. 11. Norme de securitatea muncii, PSI, situații de urgență și protecția mediului

11.1. Personalul prestatorului își desfășoară activitatea în obiectivul CTE Bucuresti Sud (relevee, vizite, ședințe) în conformitate cu prevederile Legii nr. 319/2006 privind securitatea și sănătatea în muncă, H.G. nr. 1425/2006, H.G. nr. 1091/2006 și H.G. nr. 1146/2006, cu modificările și completările ulterioare.

11.2. Accesul personalului prestatorului în obiective se face numai după efectuarea unui instructaj pe linie de securitate și sănătate în muncă, situații de urgență și protecția mediului, de către personalul de specialitate al beneficiarului, consemnat într-un proces-verbal semnat de beneficiar și de prestator, și cu respectarea procedurilor de acces ELCEN.

11.3. Convenția privind delimitarea răspunderilor pe linie de securitate și sănătate în muncă, situații de urgență și protecția mediului este obligatorie și se semnează de beneficiar și prestator odată cu semnarea contractului.

11.4. Pe timpul activităților desfășurate în incinta obiectivelor, personalul prestatorului respectă prevederile Legii nr. 307/2006 privind apărarea împotriva incendiilor, ale Ordinului M.A.I. nr. 163/2007 privind Normele generale de apărare împotriva incendiilor și ale Legii nr. 481/2004 privind protecția civilă, cu modificările și completările ulterioare.

11.5. Personalul prestatorului va evita producerea oricăror evenimente cu efecte nocive asupra mediului sau asupra sănătății personalului și va respecta prevederile O.U.G. nr. 195/2005 privind protecția mediului; prestatorul răspunde de eventualele impacturi negative rezultate din activitatea sa.

11.6. Prestatorul este obligat să-și însușească și să respecte politica, procedurile și reglementările ELCEN privind calitatea, mediul, securitatea și sănătatea în muncă, situațiile de urgență și PSI.
11.7. PT va cuprinde măsurile de securitate și sănătate în muncă necesare pe durata execuției, conform H.G. nr. 300/2006 privind cerințele minime de securitate și sănătate pentru șantierele temporare sau mobile.

Cap. 12. Dispoziții finale și precizări

12.1. Propunerea financiară va cuprinde costul serviciilor de proiectare al obiectivului, conform formularului din Anexa nr. 7.
12.2. Nedetalierea tuturor elementelor de cost duce la declararea ofertei ca inacceptabilă. Nu se acceptă formulări de genul „Alte cheltuieli", fără o detaliere exactă și fără alocarea unui cost pentru fiecare element prezentat în calculație.
12.3. Autoritatea Contractantă nu va accepta justificarea prețului prin invocarea facilităților prevăzute de Legea nr. 76/2002 privind sistemul asigurărilor pentru șomaj și stimularea ocupării forței de muncă, întrucât acestea nu dovedesc în sine posibilitatea de a beneficia de ajutor de stat, iar luarea lor în considerare ar încălca principiul tratamentului egal. Nu se acceptă nici fundamentarea prețului pe subvenții, scheme de minimis sau alte reduceri temporare care nu pot fi justificate pe întreaga durată a contractului.
12.4. Facturarea se face la finalizarea contractului, după recepția documentației aferente, pe baza procesului-verbal de recepție.
12.5. Termenul de plată al facturilor este de 30 de zile de la data incarcarii acesteia in SPV (Spatiul Privat Virtual).
12.6. Criteriul de atribuire este cel mai bun raport calitate-preț.
12.7. Documentația elaborată devine proprietatea ELCEN, care o poate utiliza pentru avizare, achiziția furnizării și execuției, execuție, exploatare și mentenanță. Prestatorul nu poate utiliza sau divulga în alte scopuri informațiile obținute în executarea contractului.

Cap. 13. Modul de prezentare a propunerii tehnice și financiare

13.1. Propunerea financiară

13.1.1. Ofertantul elaborează propunerea financiară astfel încât să furnizeze toate informațiile solicitate cu privire la prețuri, tarife și alte condiții financiare și comerciale legate de obiectul contractului, completând formularul din Anexa nr. 7.
13.1.2. Prețul include toate costurile serviciilor, precum și cele implicite ce decurg din executarea contractului: forța de muncă, relevee și deplasări, verificarea tehnică de calitate a proiectului, asigurările, împreună cu riscurile, răspunderile și obligațiile ce decurg din contract.
13.1.3. Prețurile trebuie să fie rezultatul liberei concurențe și să poată fi justificate.
13.1.4.Ofertantul indică, motivat, care informații din propunerea financiară sunt confidențiale, clasificate sau protejate de un drept de proprietate intelectuală, în conformitate cu art. 70 din Legea 99 si art.129 din HG 394.
13.1.5. Ofertele financiare aparent neobișnuit de scăzute, respectiv sub 80% din valoarea estimată a contractului, conform art. 136 alin. (4) din H.G. nr. 395/2016, vor fi justificate de ofertanți. Comisia de evaluare va solicita clarificări conform art. 222 din Legea nr. 99/2016 și art. 142 din HG 394 poate cere, fără ca lista să fie exhaustivă, documente privind modul de organizare și metodele de lucru, nivelul de salarizare al personalului și costurile implicate de echipamentele și programele utilizate.

13.1.6. Propunerea financiară are caracter obligatoriu, din punctul de vedere al conținutului, pe toată perioada de valabilitate stabilită de Autoritatea Contractantă și asumată de ofertant.

13.2. Propunerea tehnică

13.2.1. Pentru a fi considerată conformă, propunerea tehnică trebuie să îndeplinească toate cerințele minime obligatorii din caietul de sarcini. Ofertantul va indica faptul că a ținut cont de obligațiile referitoare la condițiile de muncă și protecția muncii prevăzute de actele normative în vigoare.

13.2.2. Propunerea tehnică va cuprinde cel puțin:

- metodologia de proiectare: realizarea releveelor, evaluarea riscurilor, elaborarea soluțiilor de principiu, integrarea celor trei niveluri de monitorizare, abordarea securității cibernetice și a protecției datelor;
- organizarea echipei și alocarea specialiștilor pe obiective și specialități;
- modul de asigurare a protecției informațiilor clasificate pe durata contractului;

13.2.3. **Ofertele care se limitează la a confirma faptul că vor presta toate activitățile solicitate, fără să prezinte concret modul în care le vor realiza, vor fi considerate neconforme.**

13.2.4. **Nu se admit oferte alternative.** Nerespectarea prevederilor caietului de sarcini atrage, după caz, excluderea, descalificarea ofertanților sau respingerea ofertelor.

13.2.5. Documentele se prezintă în limba română; cele redactate în altă limbă vor fi însoțite de traduceri autorizate. Autoritatea Contractantă poate solicita informații suplimentare considerate semnificative pentru evaluarea propunerii tehnice.Anexe

- Anexa nr. 1 – Lista obiectivelor cu adresele poștale
- Anexa nr. 2 – Liste de cantități estimate pe categorii de subsisteme, determinate prin Studiul de fezabilitate
- Anexa nr. 3 – Analizele de risc la securitatea fizică
- Anexa nr. 4 – Extras neclasificat din Studiul de fezabilitate
- Anexa nr. 5 – Lista experților principali solicitați
- Anexa nr. 6 – Anexa de securitate:
  - 6.1 Lista personalului autorizat care va avea acces la informații clasificate secrete de serviciu;
  - 6.2 Lista locurilor de execuție a activităților în care se utilizează informații clasificate;
  - 6.3 Caiet de sarcini privind protectia informatiilor clasificate;
- Anexa nr. 7 – Formularul propunerii financiare

Sef Serviciu ICSSU
George Stefan MISAILA

Elaborat
Costel COBÂRLIE

ANEXA 1

Lista obiectivelor cu adresele poștale

Nr. crt.	Societatea Electrocentrale București S.A.	Adresa obiectiv
1	CTE BUCUREȘTI SUD	Str. Releului nr. 2B, Sector 3, București

Anexa 2

Liste de cantități estimate
pe categorii de subsisteme, determinate prin
Studiul de fezabilitate la **CTE București SUD**

Structura sistemului de supraveghere video

Nr. Crt.	Denumire Echipament	Specificatii echipament	Cantitate
1	Camera video exterior (perimetru)	Bullet, IP, 5MP, lentila 3.6 mm, IR 50 m, cu soft de analiza human detection	71
2	Camera video exterior (ansamblu)	Bullet, IP, 4MP, lentila 2.8 mm, IR 40 m	13
3	Camera video PTZ	Speed dome, IP, 4MP, 4.8 mm, IR 150 m	4
4	Camera video interior	Dome, IP, 2MP, 2.8 mm, IR 15 m	6
5	Camera video LPR	LPR, IP, 4MP, 8-32mm, IR 100 m	3
6	Inregistrator video digital de retea	64 canale	2
7	HDD	12TB, special pentru supraveghere video	8
8	HDD	4TB	1
9	Switch IP	32 canale	2
10	Switch IP	8 porturi RJ 45 si 2 de fibra optica SFP	2
11	Switch IP	8 porturi POE si 2 uplink pentru camerele de interior	1
12	Cutie distributie	500m x 400m x 200m	20

13	Sursa neintreruptibila de tensiune	UPS	4
14	Cablu FTP	CAT 6	6.000 m
15	Fibra optica	8 fire-10 fire-12 fire-24 fire	3.500 m
16	Stalpi	4-6m	9
17	Dotare tablouri exterior	Sina DIN tip omega montaj echipamente	20
18	Dotare tablouri exterior	Priza DIN montaj in tablou exterior pe sina	20
19	Dotare tablouri exterior	Prelungitor 5-8 porturi schuko, lungime 2-3 metri	20
20	Dotare tablouri exterior	UPS 600-800 VA	20
21	Dotare tablouri exterior	siguranta unipolara, montaj pe sina din, 6-10A	20
22	Dotare tablouri exterior	switch 6-8 porturi RJ45 POE + 2-4 porturi FO SFP + sursa alimentare switch	20
23	Dotare tablouri exterior	modul SFP lungime de unda Tx1550nm/Rx1310nm sau lungime de unda Tx1310nm/Rx1550nm, gigabit	40
24	Dotare tablouri exterior	caseta sudura, material ABS, 12/24 fibre	20
25	Dotare tablouri exterior	accesorii montaj, mufe RJ45 si FO + accesorii FO si montaj cutie	20
26	Speaker IP + card micro SD	Difuzare fisier audio sau flux audio in timp real, nivel maxim presiune sunet 120dB	20
27	Cablu de curent	Cablu 3x2.5 electric armat cupru rezistent uz industrial si ingropat	100
28	Suduri si alte lucrari FO		1
29	Accesorii montaj cabluri si FO	Spre exemplu : Cleme de ancorare tip pană, cleme universale tip ODWAT, cleme de întindere profesionale, cleme de susținere cu inserție de cauciuc, cârlige în formă de J,	97

		amortizoare de vibrații, console metalice, bandă din oțel inoxidabil, catarame de strângere, șuruburi cu ochet, suporturi pentru rezerva de cablu, casete de joncțiune etanșe, tuburi spiralate de protecție.	
30	Accesorii montaj stalpi	Spre exemplu : Buloane, conexspanduri, ciment gata preparat, suruburi, piulite, sapatura	9
31	Rack metalic echipamente + accesorii	Capacitate 42U, montare pe podea, standard 19 inch, dimensiuni 600 mm (latime) x 800 mm (adancime) x 2055 mm (inaltime) + tavi echipamente, prelungitoare, ventilatoare, bari de alimentare, organizator de cabluri	2
32	Monitor NVR + suport	Monitor FHD 32 inch, rezolutie 1920x1080 + suport perete VESA	2
33	Tub flexibil tip Copex / Pat Cablu / Tub PVC	Necesar mascare cabluri unde nu se poate traseu aerian	1200
34	Router internet monitorizare video	8-12 porturi Gigabit si 2-4 porturi SFP	2
35	Doze metalice camere video	Cutie de jonctiune (doza legaturi) metalica pentru camere IP	97
36	Patch panel	Patch panel pentru fibra optica cu sina glisanta 24 porturi FO LC / SC + accesorii pigtail	2
37	Antena transmisie semnal wireless	Wireless bridge cu distanta transmisie wireless pana la 5 km, rata transmisie max. 867 Mbps	0
38	Material consumabil si neprevazut	Spre exemplu : Suruburi, piulite, intinzatoare metalice / accesorii, etc.	97
39	Calculator statie client pentru monitorizare video	Spre exemplu (similar sau superior) : i7 + RTX 4060 + 32GB RAM + 512 GB / 1 TB SSD NVMe M.2 + 1x Port Gigabit Ethernet + Windows 11 PRO	2
40	Monitor statie client	Monitor FHD 32 inch, rezolutie 1920x1080 + suport perete VESA	4
41	Manopera		
42	Alte materiale		

Structura sistemului control acces

Nr. Crt.	Denumire Echipament	Specificatii echipament	Cantitate
1.	Yala electromagnetica	Putere retentie 280kgf, Alimentare selectabil 12Vcc/550mA, 24Vcc/330mA	3
2.	Amortizor hidraulic	Deschidere pana la 135° Greutate: 1000g	3
3.	Buton exit	Functionare: 3 fire - normal inchis/normal deschis Tensiune de aplicare: 36Vcc, 3A	3
4.	Cititor de carduri	Capacitate: 3 000 cartele/coduri (4-6 cifre) 10.000 evenimente Distanta de citire: 3-6 cm	3
5.	Bariere auto	Putere 300W, 230 V Dimensiune bara 6 metri	3
6.	Turnicheti	Bidirectionali, 230 V, distanta trecere 550 mm	4
7.	Semafor	Rosu-Verde, 2 lumini LED, 24V, TLHTC2-24	2
8.	Modul I/O	Modul adresabil inteligent I/0, input-output	2
9.	Mini PC	Unitate de programare si diagnosticare	2
10.	Bucla inductiva	Detector single, bucla inductiva, pentru prezenta autoturisme la sisteme de parcare, sensibilitate reglabila, (24V)	1
11.	Fotocelule reflective	Compatibil cu orice automatizare de poarta, Alimentare la 24V CC	4
12.	Interfon	SPL 92dB, noise reduction	1
13.	Motor automatizare poarta	20 m, 1200 Kg, 230 VAC	1
14.	Limitator cursa poarta	Limitator cursa poarta culisanta	2
15.	Cremaliera	Metal galvanizat, 1m, 8mm grosime	10

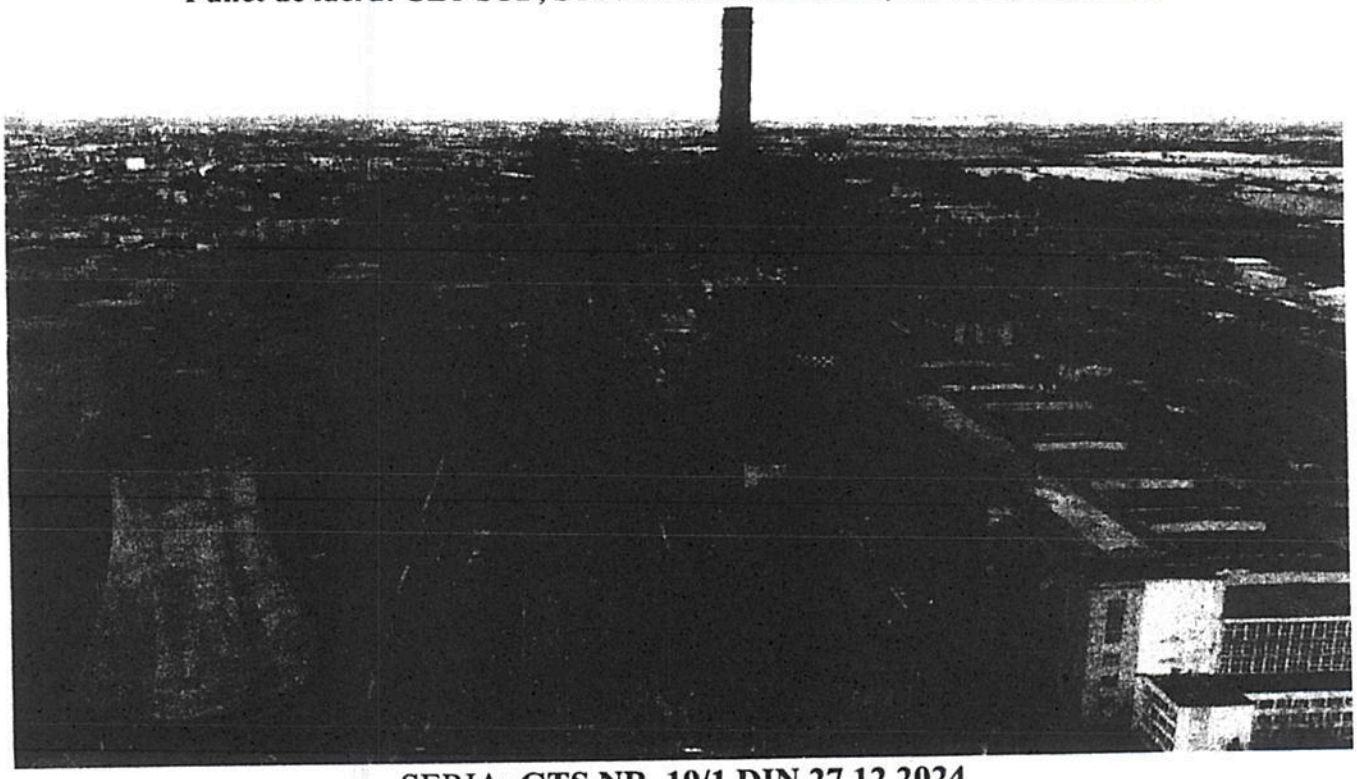
16.	Suport L/Z electromagnet	Suport de montaj pentru yala electromagnetica	3
17.	Alimentator semafor	Alimentator dedicat pentru semafoare	2
18.	Butoane de urgenta	Buton de deblocare de urgenta, contact NC/NO	3
19.	Cablu bucla inductiva	Cablu dedicat pentru bucla inductiva	100
20.	Cablu FTP	CAT 6	900
21.	Cablu de curent	Cablu 3x2.5 electric armat cupru rezistent uz industrial si ingropat	500
22.	Accesorii montaj cabluri si FO	Spre exemplu : Cleme de ancorare tip pană, cleme universale tip ODWAT, cleme de întindere profesionale, cleme de susținere cu inserție de cauciuc, cârlige în formă de J, amortizoare de vibrații, console metalice, bandă din oțel inoxidabil, catarame de strângere, șuruburi cu ochet, suporturi pentru rezerva de cablu, casete de joncțiune etanșe, tuburi spiralate de protecție.	10
23.	Tub flexibil tip Copex / Pat Cablu / Tub PVC	Necesar mascare cabluri unde nu se poate traseu aerian	300
24.	Material consumabil si neprevazut	Spre exemplu : Suruburi, piulite, intinzatoare metalice / accesorii, etc.	10
2	Manopera		
2	Alte materiale		
2	Total licente (48 luni)		

S.C. GUARD TRAINING SYSTEM S.R.L.
Bucuresti, Sectorul 3, Bdul. Liviu Rebreanu Nr.46 - 58
CUI 31278512; J40/2429/25.02.2013
E-mail: guard.training.system@gmail.com; Telefon: +40 0758 251101

INTRARE ELCEN
NR. ..... din 12.2024
Ex: _1_ / _2_

ELECTROCENTRALE BUCUREȘTI S.A.
SPLAIUL INDEPENDENȚEI 227; BUCUREȘTI
IEȘIRE Nr. 6828
Ziua 07 Luna 02 Anul 2025
-8-

RAPORT DE EVALUARE
SI TRATAREA RISCURILOR LA SECURITATEA FIZICĂ
pentru
S.C. ELECTROCENTRALE BUCURESTI S.A.
Punct de lucru: CET SUD, STR. RELEULUI nr. 2B, Sector 3, Bucuresti



SERIA: **GTS NR. 19/1 DIN 27.12.2024**

Evaluator de risc la securitatea fizica
MĂDĂLIN TEPOR
R.N.E.R.S.F. – 901/2015

IMPORTANT:
Vă rugăm să aveti in vedere că analiza de risc la securitate fizică se revizuiește obligatoriu în următoarele situații:
- LA FIECARE 3 ANI, pentru corelarea cu dinamica parametrilor interni și externi care generează și/sau modifică riscurile de securitate fizică a locatiei;
- IN CEL MULT 60 DE ZILE de la producerea unui incident de securitate;
- IN CEL MULT 30 DE ZILE de la modificarea caracteristicilor arhitecturale,funcționale sau a obiectului de activitate.

S.C. GUARD TRAINING SYSTEM S.R.L.
Bucuresti, Sectorul 3, Bdul. Liviu Rebreanu Nr.46 - 58
CUI 31278512; J40/2429/25.02.2013
E-mail: guard.training.system@gmail.com; Telefon: +40 0758 251101

AM PRIMIT ORIGINALUL RAPORTULUI DE EVALUARE,
GRILA DE EVALUARE SI ANEXELE.
S.C. ELECTROCENTRALE BUCURESTI S.A.

BUCURESTI
27.12.2024
Exemplar nr.1/2

SCRISOARE DE TRANSMITERE

Catre:

S.C. ELECTROCENTRALE BUCURESTI S.A.
Domnului DIRECTOR GENERAL
Claudiu-Ionut CRETU-SARBU

Va transmitem anexat Analiza de Risc la securitatea fizicii a obiectivului, realizata conform Contractului de prestari servicii nr. 146 din 16.12.2024.

Lucrarea identifica amenintarile si vulnerabilitatile care pot pune in pericol viata, integritatea corporala sau libertatea persoanei ori care pot aduce prejudicii bunurilor si valorilor detinute de beneficiar, in scopul determinarii impactului si evaluarii riscurilor de securitate si in baza careia se stabilesc masurile necesare pentru limitarea sau eliminarea acestora.

Contractul de prestari servicii este inregistrat in *Registrul de evidenta al contractelor* evaluatorului cu nr. 146 din 16.12.2024.

Inspectia In teren, actualizarea si documentarea raportului cu date necesare s-au realizat in data de 20.12.2024, in prezenta d-lor CIOABA LIVIU – seful Sectiei Dragomiresti si SEBASTIAN TATU – responsabil securitate ELCEN.

Grila de evaluare specificii obiectului de activitate al unitatii beneficiare s-a completat naplicatia electronica a paginii web a Inspectoratului General al Politiei Romane. Data de referinta pentru care sunt valabile toate calculele, analizele si estimarile efectuate, este de 23.12.2024.

In baza datelor, calculelor efectuate, a ipotezelor si conditiilor limitative, valorile medii sunt prezentate in raport ca fiind valori orientative.

Administrator
SC GUARD TRAINING SYSTEM SRL
Mădălin Tepor

S.C. GUARD TRAINING SYSTEM S.R.L.
Bucuresti, Sectorul 3, Bdul. Liviu Rebreanu Nr.46 - 58
CUI 31278512; J40/2429/25.02.2013
E-mail: guard.training.system@gmail.com; Telefon: +40 0758 251101

DECLARATIE DE CONFORMITATE

Prin prezenta declaraţie de conformitate se confirmă faptul că:

- prezentarea faptelor din raport sunt corecte, analizate şi reflectă realitatea şi pertinenţa cunoştinţelor evaluatorului;

- analizele şi concluziile sunt limitate numai la ipotezele şi condiţiile limitative prezentate în raport;

- evaluarea a fost efectuată în conformitate cu prevederile legale în vigoare;

- evaluatorul are experienţă în ceea ce priveşte evaluarea riscurilor de securitate prezentate în raport;

- raportul a fost elaborat pe baza studiilor, calculelor şi aprecierilor expertului, fără a apela la un sprijin din partea altor persoane calificate în acest sens.

Evaluator de risc la securitatea fizică
MĂDĂLIN TEPOR

Administrator
SC GUARD TRAINING SYSTEM SRL

Mădălin Tepor

S.C. GUARD TRAINING SYSTEM S.R.L.
Bucuresti, Sectorul 3, Bdul. Liviu Rebreanu Nr.46 - 58
CUI 31278512; J40/2429/25.02.2013
E-mail: guard.training.system@gmail.com; Telefon: +40 0758 251101

DECLARATIE DE CONFIDENTIALITATE

Confirm că oferta a fost realizată cu obiectivitate şi profesionalism şi cu respectarea totală a principiilor şi prevederilor legale.

În numele S.C. GUARD TRAINING SYSTEM S.R.L. mă angajez să realizez obligaţiile noastre cu obiectivitate şi corectitudine.

În numele S.C. GUARD TRAINING SYSTEM S.R.L. mă angajez să păstrez deplină confidenţialitate asupra informaţiilor pe care le voi primi, să nu le utilizez decât pentru elaborarea documentaţiilor realizate pentru beneficiarul de proiect de la care am primit informaţiile şi să nu divulg aceste informaţii şi nici documentaţiile elaborate unei terţe părţi.

În numele societatii mă angajez ca după încheierea activităţilor să nu păstrez copii ale informaţiilor primite şi ale documentaţiilor realizate.

Mă angajez să iau toate măsurile necesare pentru ca toţi membrii echipei implicate în realizarea activităţilor de consultanţă să respecte prevederile din prezenta declaraţie.

Declar că sunt conştient că orice încălcare a acestor angajamente conduce la sancţiuni pecuniare aplicabile S.C. GUARD TRAINING SYSTEM S.R.L.

Evaluator de risc la securitatea fizică
MĂDĂLIN TEPOR

ADMINISTRATOR
SC GUARD TRAINING SYSTEM SRL

Mădălin Tepor

Cuprins

1. Premisele Evaluarii 7
1.1. PRECIZARI 7
1.2. BIBLIOGRAFIE: 7
1.3. TERMENI SI DEFINITII: 8
2. Nominalizarea unitatii, obiectul de activitate al acesteia si scopul evaluarii 8
2.1. Denumirea unitatii analizate: 8
2.2. Datele de identificare: 9
2.3. Obiectul de activitate: 9
2.4. Încadrarea unității conform Instrucțiunea MAI Nr. 9 din 01.02.2013 9
2.5. Scopul evaluarii: 10
3. Amplasarea geografica a unitatii, vecinatati, cai de acces, alti factori externi cu impact asupra activitatii unitatii 10
3.1. Amplasarea obiectivului: 10
3.2. Caracteristici si amenajari: 11
3.3. Sisteme de alimentare cu energie electrica si iluminat: 12
3.4. Factori externi cu impact asupra activitatii unitatii: 13
4. Cadrul organizational intern, politici si responsabilitati privind securitatea fizica a unitatii 13
4.1. Detalierea sistemului securitatii fizice in cadrul obiectivului : 14
4.2. Centralizarea masurilor de securitate existente: 17
5. Identificarea infractiunilor asociate riscurilor potentiale care se pot manifesta in obiectiv, corelarea categoriilor de risc cu sursele acestora si sferele de impact in care se pot produce .. 19
6. Analizarea si estimarea riscurilor la securitatea fizica 20
6.1. SCALA DE MASURARE IMPACT/PROBABILITATE 20
6.2. MATRICEA DE EVALUARE A RISCURILOR: 21
6.3. RISCUL DE OMOR SI VATAMARE CORPORALA 21
6.4. RISCUL DE FURT 22
6.5. RISCUL DE TALHARIE 23
6.6. RISCUL DE DISTRUGERE 24
6.7. VIOLAREA SEDIULUI PROFESIONAL 26

7. Stabilirea masurilor suplimentare de tratare a riscurilor si a costurilor estimate pentru implementarea acestora 27

8. Concluziile finale ale raportului 31

Clauza de nepublicare: 32

9. Anexe 33

9.1. Anexa 1 Grila de evaluare 33

1. Premisele Evaluarii

1.1. PRECIZARI

In conformitate cu prevederile legale prevazute de H.G. nr. 301/2012 privind normele metodologice de aplicare a Legii nr. 333/2003 referitoare la paza obiectivelor, bunurilor, valorilor si protectia persoanelor, a Instructiunilor M.A.I. nr. 9 din 01.04.2013 privind efectuarea analizelor de risc la securitatea fizica a unitatilor la **S.C. ELECTROCENTRALE BUCURESTI S.A.** se întocmeste de către dl. MĂDĂLIN ȚEPOR, in calitate de evaluator de risc la securitatea fizica inscris in RNERSF pozitia 1469.

Analiza de Risc se desfăsoară în baza Contractului de prestări servicii nr.___ din ___.12.2024 (**ANEXAT**).

Grila in baza careia s-a facut evaluarea se regaseste in **Anexa nr.1** a prezentului raport de evaluare. Evaluarea obiectivului a fost facuta in baza grilei specifice prevazuta in Anexa nr. 12 – (Grila de evaluare a nivelului de risc pentru unitati care nu trebuie sa indeplineasca cerinte minimale), in conformitate cu Instructiunile MAI nr. 9 din 01.02.2013.

1.2. **BIBLIOGRAFIE:**

Elaborarea raportului de evaluare si tratare a riscurilor la securitatea fizica a fost realizat in baza prevederilor legale descrise in:

- Articolul nr. 2 din Hotararea 301/2012 - Normele de aplicarea a Legii 333/2003 privind paza obiectivelor, bunurilor, valorilor si protectia persoanelor;
- Instructiunile MAI nr. 9 din 01.02.2013 privind efectuarea analizelor de risc la securitatea fizica a unitatilor ce fac obiectul HG 301/2012.
- Coeficientii de criminalitate pentru **municipiul Bucuresti** in anul 2023.
- Coeficientii de criminalitate zonali la nivelul **sectorului 3** in anul 2023.

Alte documente standardizate:

- SR ISO 31000:2010 Managementul riscului - Principii si linii directoare;
- SR EN 31010:2010 Managementul riscului - Tehnici de evaluare a riscului;
- Seria de standarde Sisteme de management al calitatii (SR EN ISO 9001:2008);
- Seria de standarde SR EN 50131 - Sisteme de alarma. Sisteme de alarma impotriva efractiei si jafului armat;
- Standarde europene sau na\ionale de ce1ificare a mijloacelor de protectie mecanofizica (unitati de depozitare de securitate, vitraje, tamplarie).

Documentele studiate care au stat la baza elaborarii „Raportului de evaluare si tratare a riscurilor la securitatea fizica", sunt:

- Informatii generale;
- Planurile de situatie sau schitele spatiilor/punctelor de lucru pentru care se face evaluarea;
- Planul de Paza;
- Contractul de monitorizare si interventie la obiectiv;
- Ghidul de inteviu pentru Analiza de risc la securitatea fizica – 10 pagini

1.3. TERMENI SI DEFINITII:

- ***securitate fizica***– starea de fapt in care riscul determinat de factorii de amenintare si vulnerabilitatile care pot pune in pericol viata, integritatea corporala sau libertatea persoanei ori pot aduce prejudicii valorilor detinute de unitati, se situeaza la un nivel acceptabil;
- ***amenintare*** – factor intern sau extern ce are capacitatea de a exploata vulnerabilitatea unei unitati prin acte sau fapte ce creeaza dezechilibre ori instabilitati si genereaza stari de pericol asupra vietii, integritatii corporale sau libertatii persoanelor ori valorilor detinute;
- ***vulnerabilitate*** – caracteristica a arhitecturii, implementarii sau operarii activitatii unei entitati, prin care aceasta este expusa distrugerii, agresiunii ori disfunctionalitatii in fata unei amenintari.
- ***analiza de risc la securitatea fizica***– tehnica analitica folosita pentru a se identifica amenintarile si vulnerabilitatile care pot pune in pericol viata, integritatea corporala sau libertatea persoanei ori care pot aduce prejudicii valorilor detinute de unitati, in scopul determinarii impactului si evaluarii riscurilor de securitate si in baza careia se stabilesc masurile necesare pentru limitarea sau eliminarea acestora;
- ***incident de securitate*** - evenimentul produs, avand o evolutie necontrolata, care genereaza efecte distructive asupra securitatii fizice a unei unitati si care necesita o actiune imediata pentru restabilirea situatiei anterioare;
- ***masuri de securitate*** – componenta de baza a unei solutii de securitate, corespunzatoare uneia sau mai multor amenintari si vulnerabilitati identificate conform analizei de risc;
- ***mecanisme de securitate*** – solutii care cuprind mai multe masuri de securitate, care functioneaza conform unor scenarii predefinite, pentru securizarea unuia sau mai multor obiective, atunci cand sunt amplasate in acelasi perimetru;
- ***sisteme de securitate*** - solutii la nivel de sistem pentru unitati cu multiple obiective de securitate distribuite geografic in locatii diferite;
- ***parametrii interni si externi care genereaza si/sau modifica riscurile la securitatea fizica a unitatii*** – contextul care poate cuprinde, dar nu se limiteaza la:

a) mediul cultural, social, politic, de reglementare, financiar, tehnologic, economic, natural si concurential, la nivel international, national, regional sau local;
b) factorii cheie si tendintele cu impact asupra obiectivelor organizatiei;
c) relatiile cu partile interesate, perceptiile si valorile acestora.

2. Nominalizarea unitatii, obiectul de activitate al acesteia si scopul evaluarii

2.1. Denumirea unitatii analizate:

ELECTROCENTRALE BUCURESTI este persoană juridică română, societate pe acţiuni. ELCEN a fost înfiinţată în decembrie 2002, ca filială a S.C. Termoelectrica S.A., prin reorganizarea acestei societăţi comerciale. În prezent, Ministerul Energiei este principalul acţionar al companiei, deţinând 97,51% din acţiuni, restul acţiunilor fiind deţinute de SNGN Romgaz (2,49%).

Obiectul de activitate al companiei îl reprezintă producţia, transportul, distribuţia, dispecerizarea şi vânzarea energiei termice, dar şi producţia şi vânzarea energiei electrice. ELCEN este cel mai mare producător de energie termică din România (40%) şi din Bucureşti (90%). Din punct de vedere al producţiei de energie electrică, ELCEN asigură aproximativ 4% din cota de piaţă la nivel naţional, potrivit raportoartelor ANRE privind piaţa de energie, publicate pentru anul 2023.

ELCEN are în componenţă patru termocentrale şi o uzină de reparaţii în Bucureşti. Puterea electrică instalată în centrale este de 586.25 MW, iar puterea termică de 1736.38 Gcal/h. Centralele au în componenţă

grupuri energetice în cogenerare şi agregate energetice de vârf (CAF-uri, cazane cu apă fierbinte). În 2023, cantitatea de energie electrică totală produsă a fost de 1.827,781 TWh, în timp ce cantitatea de energie termică livrată a fost de 3.514,808 Tcal.

2.2. Datele de identificare:

- Denumire societate: **S.C. ELECTROCENTRALE BUCURESTI S.R.L.** (Anexa 2)
- Sediul social situat in: Splaiul Independentei nr. 227, Sector 6, Bucuresti
- Punctul de lucru situat in: **CET SUD**, Str. Releului nr. 2B, sector 3, Bucuresti
- Cod unic de inregistrare societate: RO 15189596
- Numar de ordine in Registrul Comertului: J40/1696/2003

2.3. Obiectul de activitate:

In conformitate cu codul **CAEN 3511, obiectul de activitate principal al companiei este *"Producția de energie electrică "***.

In cadrul obiectivului angajatii isi desfasura activitatea cu program L-V, 08.00 – 16.30, precum si cu program de tura, pe 3 schimburi permanente de cate 8 ore.

Terenul si cladirea sunt proprietatea ELCEN.

Conform declaratiilor reprezentantului legal, nu exista litigii cu privire la acestea.

2.4. Încadrarea unității conform Instrucțiunea MAI Nr. 9 din 01.02.2013

In conformitate cu HG 1486/2005, electrocentrale Bucuresti nu face parte din obiectivele de interes strategic. Conform lege 225/ 2018 pentru modificare OUG 98/2010 privind identificare si desemnare Infrastructuri Critice Nationale (ICN), Anexa LISTA sectoarelor, subsectoarelor infrastructurii critice naționale/infrastructurii critice europene (ICN/ICE)" obiectivele ar putea fi incadrade la ICN.

..1.1. Lista sectoarelor ICN

Nr. crt.	Sectorul	Subsectoare
1	Energetic	1.1.Energie electrică, inclusiv nuclear-electrică – capacități și instalații pentru producere, depozitare stocare, rețele de distribuție și transport; 1.2. Petrol și derivate petroliere – capacități și instalații pentru extracție producție, rafinare, tratare, depozitare stocare, distribuție și transport prin conducte, terminale; 1.3. Gaze naturale și derivate din gaze naturale – capacități și instalații pentru extracție producție, rafinare, tratare, depozitare stocare, distribuție și transport prin conducte, terminale; 1.4. Resurse minerale.

Incadrarea din punct de vedere al Anexei 1 din H.G. 301/2012: Evaluarea de risc va fi efectuata folosind (grila nr.12). Conform art 8 si 8'1 masurile de Securitate minimale:

Cerințele minime pentru unitățile de interes strategic

a) sistemul de alarmare la efracție va asigura detecție perimetrală la nivelul gardului de protecție a obiectivului, pentru semnalarea pătrunderii neautorizate către personalul de pază aflat în serviciu;

b) obiectivul se protejează prin asigurarea pazei fizice.

Articolul 8^1

Unitățile și instituțiile de interes public trebuie să prevadă sisteme de supraveghere video pe căile de acces, holuri și alte zone cu risc ridicat, detecție a efracției pe zonele de expunere sau depozitare valori și control

acces, prin personal sau echipamente

Concluzii: Electrocentrale Bucuresti nu se incadreaza la nici o categorie de unitate pentru care sunt prevazute masuri minimale de Securitate.

2.5. Scopul evaluarii:

Prezentul raport de evaluare si tratare a riscurilor la securitatea fizica a fost elaborat in scopul identificarii, analizei si a stabilirii masurilor de tratare a riscurilor la securitatea fizica asociate obiectivului evaluat.

Obiectivele evaluarii riscurilor la securitatea fizica constau in realizarea unei constientizari a potentialelor amenintari de securitate fizica si a efectelor lor pentru obiectivul analizat in vederea asigurarii:

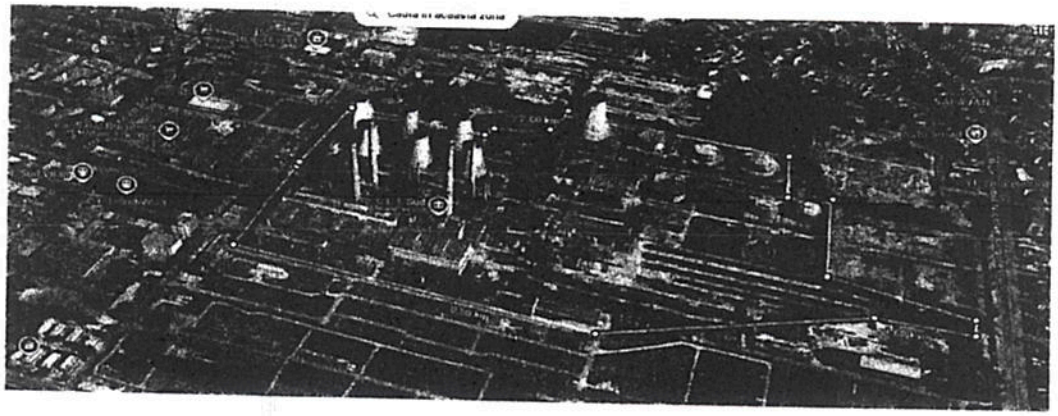
- Identificarii amenintarilor si vulnerabilitatilor care pot pune in pericol viata, integritatea corporala sau libertatea persoanei ori care pot aduce prejudicii valorilor detinute;
- Determinarii impactului si evaluarii riscurilor de securitate ;
- Informarii conducerii obiectivului, personalului acestuia si autoritatilor publice;
- Nivelului minim de securitate prevazut de legislatia in vigoare;
- Alinierii la cerintele legale in materie;
- Stabilirii masurilor necesare pentru limitarea sau eliminarea riscurilor de securitate;
- Unei avertizari timpurii care sa contribuie atat la bunastarea companiei cat si a angajatilor si clientilor sai, protejandu-i si consolidandu-i reputatia.
- **Din punct de vedere al obiectului de activitate si conform art.14 alin. (1) din instructiunea MAI 9/2013, locatia intra in categoria unitatilor pentru care se aplica grila de evaluare a riscului la securitatea fizica prevazuta in anexa la HG 301/2012 pentru a se incadra in nivelul de risc acceptabil respectiv grila 12.**

3. Amplasarea geografica a unitatii, vecinatati, cai de acces, alti factori externi cu impact asupra activitatii unitatii

3.1. Amplasarea obiectivului:

CET SUD se afla amplasat intre str. Releului si bd. Nicolae Grigorescu, la marginea de sud a cartierului Salajan pe partea dreapta pe sensul de deplasare dinspre centura Bucuresti spre centrul orasului, intr-un spațiu larg delimitat si împrejmuit cu gard de beton pe 2 laturi cu inaltimea de 2 metri si suprainaltare de sarma ghimpata de aprox. 40 cm iar pe celelalte 2 laturi cu gard de plasa pe stalpi metalici intr-o zona cu obiective pazite.

Detalii privind pozitia imobilului sunt prezentate in plansa foto obtinuta prin intermediul aplicatiei "Google maps".



VECINATATI

Unitatea este invecinata:

- NORD –ZONA REZIDENTIALA;
- SUD – UNITATI ECONOMICE - TRANSELECTRICA;
- EST – UNITATI ECONOMICE;
- VEST – UNITATI ECONOMICE – ICMENERG.
  - Din punct de vedere al vecinătăților, obiectivul ELECTROCENTRALE BUCURESTI – CET SUD se poate considera a nu fi o unitate izolata, avand ca vecinatati alte obiective păzite, pe o raza de maxim 50 m.

Conform datelor IGPR pe anul 2023, nivelul de criminalitate in sectorul 3 este „**RIDICAT**" (**110,51%**), in Bucuresti inregistrand un nivel „**RIDICAT**" (**1114,80%**).

3.2. Caracteristici si amenajari:

Se impune mentiunea ca prezentul raport de evaluare vizeaza CTE BUCURSTI SUD, ce se intinde pe o suprafata de aproximativ 323.000 mp, respectiv un complex de imobile compus din:

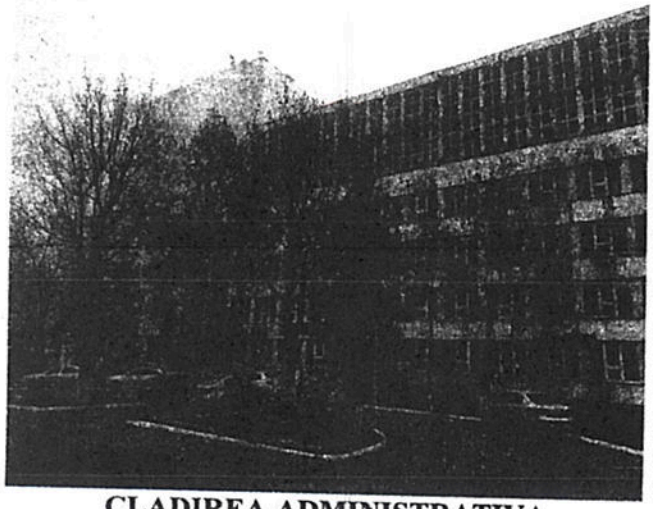
- **CORP CLADIRE C1 – BLOC ADMINISTRATIV** – cladire cu 6 nivele, executata din cadre de beton si cadre metalice, cu destinatie: birouri (administratie, camera serverelor, arhiva), spatii functionale, având 3 cai de acces cu usi duble batante, prevazute cu incuietori mecanice (incuietori tip YALE).
- **7 TURNURI DE RACIRE, STATIE DE POMPE TERMOFICARE**
- **3 POSTURI TRAFO 20KW**
- **STATIA DE POMPARE GAZ METAN**
- **DEPOZITE DE ECHIPAMENTE SI MATERIALE**
- **LINII SI REMIZA CFU;**
- Teren dispus in perimetrul obiectivului, inchis pe 2 laturi cu gard din placi prefabricate din beton (2m), completat in partea superioara cu sârmă ghimpată, iar pe celelalte 2 laturi cu gard de plasa de sarma montata pe stalpi metalici si cu suprainaltare de sarma ghimpata..

Obiecitvul dispune de 5 căi de acces, după cum urmează:

1. **1 cale de acces principala** auto si pietonala, amplasată in str. Releului, prevazuta cu poarta metalica cu bariera si post de paza si control acces.
2. **1 cale de acces** amplasată in vecinatatea blocului administrativ;

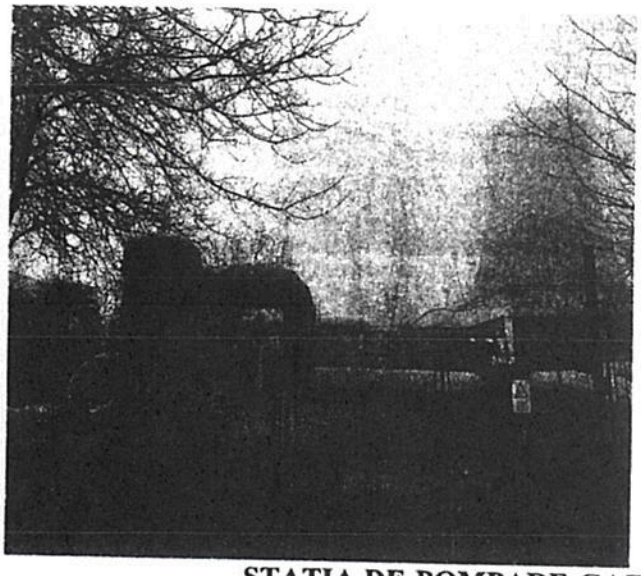
3. **2 cai de acces CFU** situate pe spatele obiectivului, **din care una este nefunctionala**;
4. **1 cale secundara** in vecinatatea CFU – **destinată accesului personalului TRANSELECTRICA.**

FOTO nr. 1



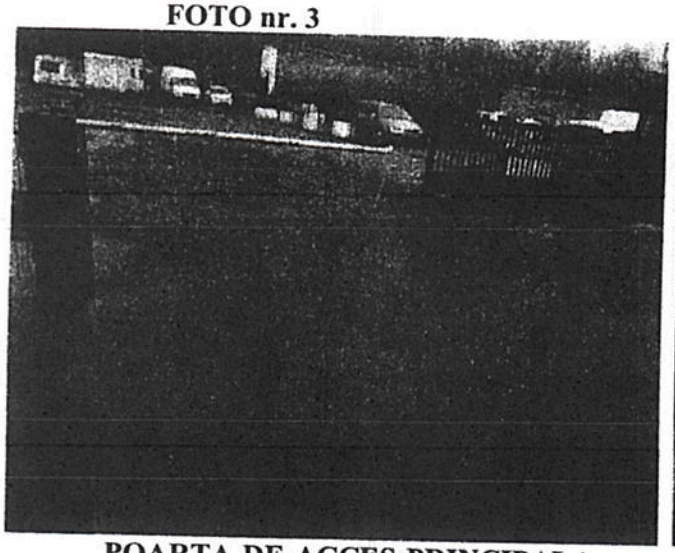
CLADIREA ADMINISTRATIVA METAN

FOTO nr. 2



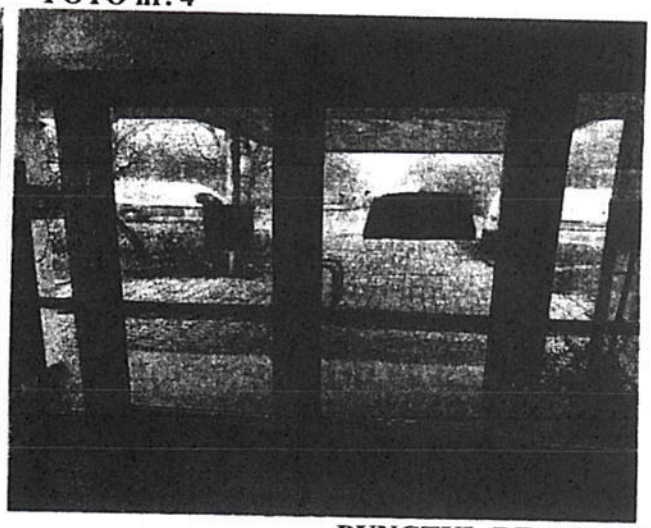
STATIA DE POMPARE GAZ

FOTO nr. 3



POARTA DE ACCES PRINCIPALA PERSONAL

FOTO nr. 4



PUNCTUL DE ACCES

3.3. Sisteme de alimentare cu energie electrica si iluminat:

Obiectivul este racordat la sistemul public de alimentare cu energie electrica de la reteaua publică. Unitatea dispune de un grup electrogen care sa asigure continuitatea functionarii sistemelor de securitate in ipoteza survenirii unor caderi de tensiune. Sistemul de iluminare perimetrala este nefunctional, existand lampi functionale doar pe interior in zona pompelor.

FOTO nr. 5



STALP DE ILUMINAT LATURA DE VEST

FOTO nr. 6



ZONA PERIMETRALA LATURA DE NORD

3.4. Factori externi cu impact asupra activitatii unitatii:

Din categoria factorilor externi cu impact asupra activitatii unitatii putem nominaliza:

a) Factori externi care tin de amplasament

- Caracteristicile unitatii din punct de vedere al vecinatatilor se incadreaza la categoria **industriale si comerciale.**
- Obiectivul se afla in vecinatatea fata de o artera intens circulata atat de autovehicule cat si de pietoni, acest lucru face ca obiectivul sa fie incadrat intr-**o zona cu trafic intens.**
- Posibilitatea de fuga/disimulare este incadrata ca fiind **rapida** intrucat pe o distanta de 25 m fata de zona de acces in obiectiv au fost identificate minim 3 directii de parasire a obiectivului.

b) Factori externi care tin de functionalitate

Conform declaratiilor angajatilor, caderile de tensiune sunt rare. Obiectivul se afla intr-o cladire ce dispune de grup electrogen cu declansare automata sau de un ansamblu UPS-uri care sa asigure alimentarea cu energie electrica a sistemelor vitale.

c) Factori externi care tin de infractionalitatea locala/zonala

Conform raportului de evaluare al activitatii din anul 2023 al IGPR mentionat in bibliografie, infractionalitatea contra persoanelor si patrimoniului, concludenta pentru obiectivul evaluat, se prezinta astfel: **coeficientul de criminalitate** la nivelul **municipiului Bucuresti** este 1114,80 - **ridicat,** iar la nivelul **sectorului 3** este **110,51 - ridicat,** conform datelor din bibliografie.

4. Cadrul organizational intern, politici si responsabilitati privind securitatea fizica a unitatii

Conceptul de securitate fizica organizat in cadrul obiectivului este constituit dintr-un ansamblu integrat de masuri organizatorice, cuprinzand sisteme tehnice de securitate dar si de ordin procedural, care au ca scop realizarea unui sistem unitar si coordonat al securitatii fizice a unitatii. In prezent, securitatea fizica a intregului obiectiv se asigura astfel:

a) Prin resurse externe:
   - Firma de paza
b) Prin resurse interne:
   - Administrator;
   - Responsabilitatile privind asigurarea securitatii fizice in obiectiv sunt indeplinite de: Administratorul societatii.

- Politici si proceduri privind securitatea fizica: a fost constatata existenta unui cadru procedural intern privind regulile si responsabilitatile angajatilor pe securitatea fizica (acces angajati, mod actiune in caz de jaf, suspiciuni furt, gestiune chei acces etc), dar angajatii nu si-au asumat aceste prevederi procedurale si nu s-a putut stabilii prin documente daca angajatii au fost instruiti cu privire la diferite situatii de urgenta (atac armat,talharie,furt).
- Conducerea SOCIETĂȚII intenționează sa aloce resursele necesare, pentru fiecare etapa a procesului de management, si stabilirea mecanismele de comunicare si raportare cu părțile externe interesate (societatea prestatorac a unor servicii de securitate, politia, pompieri, ISU,etc.).
- In cadrul obiectivului sunt organizate, in mod planificat, intalniri de informare si instruire, atat cu întregul personal al unitatii, cu personalul cu atribuții specific domeniului securității pesonalul societăților colaboratoare (delegate, conducători auto) Conducerea SOCIETĂȚII a dispus ca masurile de prevenire sa fie revizuite si corectare situația in care s-ar produce un incident /eveniment de securitate sau o modificare a parametrilor inițiali.
- Pentru a se asigura ca intregul proces de management al riscului este eficient si susține performanta instituției, indicatorii de performanta privind asigurarea securității sunt revizuiti periodic, este masurat progresul in raport cu prevederile planului si abaterea de la acesta.
- S-a avut in vedere stabilirea si menținerea unor proceduri pentru identificarea posibilelor riscuri si situații de urgenta si a pregătirii răspunsului adecvat in fiecare caz. De asemenea, procedurile răspund cerinței de prevenire si reducere a efectelor asupra angajatilor si mediului, asociate acestor urgente.

4.1. Detalierea sistemului securitatii fizice in cadrul obiectivului :

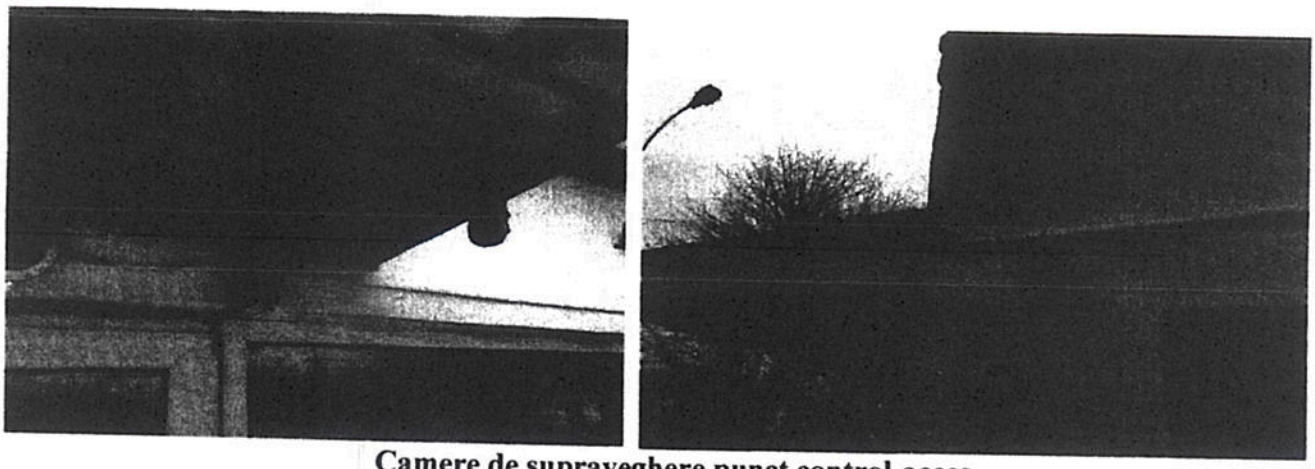
Conceptul de securitate fizica in cadrul obiectivului analizat vizeaza urmatoarele componente:

A. Subsistemul TVCI
B. Servicii de securitate cu personal uman
C. Transport valori
D. Mijloace de protectie mecano-fizica
E. Instalare si mentenanta sisteme tehnice
F. Proceduri de securitate si politica de awareness

A) Subsistemul de supraveghere video

La momentul evaluarii obiectivul dispune de sistem de supraveghere video compus dintr-un numar necunoscut de camere de supraveghere video de diverse modele, din care functioneaza maxim 3, conform declaratiilor personalului, dar nu pot fi vizualizate decat pe telefoanele personale ale unor angajati. Aspectul poate fi de gravitate ridicata, avandu-se in vedere incalcarea tuturor reglementarilor in materie de securitate, precum si cele privind prelucrarea si protectia datelor cu caracter personal.

FOTO nr. 7 **FOTO nr. 8**



Camere de supraveghere punct control-acces

Un sistem de supraveghere video performant este obligatoriu pentru aceasta categorie de obiectiv si trebuie instalat astfel incat sa asigure complet intreg perimetrul si poartile de acces, trebuie sa asigure inregistrare continuua timp de 20 de zile consecutiv, iar calitatea imaginilor sa pemita recunoasterea trasaturilor fetei persoanei. Salvarea imaginilor se va realiza in dispeceratul centralizat al ELCEN, iar DVR-urile vor fi asigurate cu UPS-uri care sa asigure functionarea inca min. 30 de minute din momentul intreruperii alimentarii cu energie electrica a echipamentelor.

AA) Subsistemul de semnalizare si alarmare la efractie

Exista un buton de panica conectat prin communicator gprs la firma de paza, care asigura interventia in caz de armare buton. Butonul se afla in postul de control acces la dipozitia agentului de securitate

AAA) Subsistemul de control acces

NU exista.

Se impune instalarea sistemelor tehnice de securitate si conectarea acestora intr-un dispecerat centralizat de monitorizare, intocmirea proiectului tehnic al sistemelor de securitate si depunerea lui spre avizare la unitatea de politie competenta teritorial.

B) Paza umana

Începând cu data de 29.04.2024, activitatea de paza umana este asigurată de catre personalul specializat al firmei S.C. INTEGRA GUARD SRL, str. Dumbraveni nr. 4D, sector 4, Bucuresti, in baza Contractului de prestari servicii nr. 234 din 2024 incheiat intre parti (**ANEXAT**).

In conformitate cu contractul si conform plan de paza, pus la dipozitie, 1334/2016 dispozitivul de paza este constituit din 9 posturi de paza permanente, din care un post inarmat, la punctul de control acces in unitate la care se adauga un post de 8 ore, Sef de obiectiv.

Referitor la acest aspect precizam ca posturile de paza, se afla la distante mari intre ele, fara legatura de vedere directa, fiind imposibila chiar si cooperarea in cazul unei situatii de risc major. Mai mult decat atat personalul de paza nu are posibilitati de observare a intregului perimetru al obiectivului datorita imposibilitatii de deplasare in proximitatea gardului.

Dispozitiv de securitate

Post	Program	Dispunere si Descriere	Responsabilitati
Sef Obiectiv	8 ore	Intrarea prinicpala	Control, supervizare, instruire
Postul 1	24 ore	Post fix, permanent, situat in latura de vest, in cladirea intrarii principale in obiectiv, la poarta de acces nr 1.	Control acces personal si vizitatori, precum si control acces mijloce auto
Postul 2	24 ore	Post mobil, permanent, situat in latura de vest, in cabina metalica pe foisor, in vecinatatea statiei de electroliza	Supraveghere si patrulare in zona de responsabilitate cuprinsa intre postul 1 intrarea prinicpala si jonctiunea cu postul 3 turnul de racire nr 7
Postul 3	24 ore	Post mobil, permanent, situat in latura de nord, in cabina metalica pe foisor, in vecinatatea turnului de racire nr 7	Supraveghere si patrulare in zona de responsabilitate cuprinsa intre postul 2 statia de gaze si postul 4, podul de peste estacata de termoficare
Postul 4	24 ore	Post mobil, permanent, situat in latura de est, in cabina metalica pe foisor, in vecinatatea estacatei de termoficare	Supraveghere si patrulare in zona de responsabilitate cuprinsa intre postul 3, podul peste estacata de termoficare si jonctiunea cu postul5- rampa de descarcare pacura
Postul 5	24 ore	Post mobil, permanent, situat in latura de est, in cabina metalica pe foisor, la poarta de acces mijloace CFU nr 4	Supraveghere si patrulare in zona de responsabilitate cuprinsa intre postul 4, poarta de acces 3 si jonctiunea cu postul 6, la capatul rampei de descarcare a pacurii cladire CTG. Executa si control acces mijloace CFU
Postul 6	24 ore	Post mobil, permanent, situat in latura de sud, in cabina paza situata la poarta de acces nr 5, mijloace auto	Misiune de control acces si patrulare in zona de responsabilitate cuprinsa intre jonctiunea cu postul de paza 5, racorduri cale ferata rampa descarcare pacura, aleea de acces in depozitele de materiale si supraveghere cele doua porti de acces exterioare ale platformei depozitului si jonctiunea cu postul de paza 7, gospodaria de ulei
Postul 7	24 ore	Post fix,mobil, permanent, situat in latura de sud, in cladirea administrativa a Uzinei de Mentenanta	Misiune de control acces a personalului in cladirea administrativa (700-1500) si supraveghere si patrulare (1500-700) in zona de responsabilitate cuprinsa intre jonctiunea cu postul de paza 5, aleea de acces reparatii electrice pana la poarta prinicpala de acces din fata Uzinei de Mentenanta
Postul 8	24 ore	Post fix, mobil, permanent, situat in cladirea CTG	Supraveghere si patrulare in zona de responsabilitate cuprinsa intre platforma de parcare auto, exteriorul cladirii CTG, pana la statia de pacura si jonctiunea cu postul 7 zona de acces depozitul de materiale
Postul 9	24 ore	Sef Tura, Post fix, permanent, situat in latura de vest, in cladirea intrarii principale in obiectiv, la poarta de acces nr 1.	Control acces personal si vizitatori, precum si control acces mijloce auto

C) Transportul valorilor

In cadrul unitatii analizate NU se efectueaza tranzactii cu numerar.

D) Mijloace mecano-fizice

Usi metalice necertificate antiefractie si antiincendiu pentru zonele de depozitare si usi de termopan la celelalte incaperi.

E) Instalare si mentenanta sisteme tehnice

La momentul evaluarii in cadrul obiectivului **NU erau montate sistemele de securitate.**

F) **Proceduri de securitate si politica de awareness**

Procedurile de securitate reprezinta o componenta si un element important din managementul securitatii, scopul acestor proceduri fiind acela de a reglementa toate activitatile si fluxurile administrative si operationale cu scopul de a prevenii sau a gestiona intr-un mod cat mai performat incidentele de securitate.

Procedurile de securitate se impart in mai multe categorii si ating valente diverse dupa cum urmeaza:

- **Proceduri administrative**
  - Modul in care se realizeaza accesul in unitate.
  - Modul in care se realizeaza angajarea
  - Modul in care se controleaza si evalueaza angajatii
- **Proceduri operationale**
  - Modul in care se utilizeaza sistemul antiefractie (cine, cum si cand armeaza/dezarmeaza sistemele antiefractie)
  - Modul in care se utilizeaza sistemul de control acces (drepturile de acces, periodicitatea actualizarii drepturilor de acces)
  - Modul in care se utilizeaza sistemul de supraveghere video (cine, cum si in ce scop utilizeaza sistemul de supraveghere video)
  - Modul de utilizare a altor sisteme de Securitate
- **Proceduri de fizica**
  - Business impact analysis
  - Business continuity plan/contigent plan
  - Proceduri de securitate cibernetica
  - Modul de acces si protectie a retelelor.
  - Modul de protectie a terminalelor (politica de parolare, frecventa schimbare parole)
- **Proceduri in cazuri de urgenta**
  - Modul de actiune in caz de incendiu
  - Modul de actiune in caz de calamitati naturale
  - Modul de actiune in cazul unui atac terrorist

Procedurile de securitate si activiatea de awareness respectiv de instruire recurenta este nu numai un elemet important de reducere a incidentelor de securitate, este si o obligatie legala prevazuta in legislatia in vigoare respectiv Art. 2 din H.G. nr. 301/2012.

In cadrul obiectivului evaluat s-a constatat existenta unor proceduri de lucru de securitate care au fost insusite de catre personalul angajat.

Zonele functionale:

Potrivit datelor colectate de la fata locului, zonele functionale determinate privind protectia prin sistemele tehnice de securitate existente, a mijloacelor de protectie mecano-fizice, in cadrul obiectivului analizat, conform prevederilor H.G. nr. 301/2012, sunt:

A. Zona de acces:

Intrarea in obiectiv este controlata de agentul de paza de la postul nr. 1 care aplica prevederile legale privind accesul in obiectiv.

Accesul in curtea se face pe o poarta metalica prevăzută cu bariera (vezi foto de mai sus).

Intrucat pe o raza de 25 m fata de intrarea principala exista numeroase cai de acces care fac posibila parasirea zonei in cel putin 3 directii diferite de deplasare (ganguri, pasaje, pasarele), se considera ca posibilitatea de disimulare/fuga este ridicata.

Conform procedurilor interne, zona va fi supravegheata pe timpul zilei de catre angajatii care vor desfasura activitati in cadrul obiectivului si de catre agentul de securitate, fiind totodata monitorizata video.

B. Zona perimetrala

Obiectivul se afla intr-un areal in care sunt amplasate si alte societati cu masuri de securitate implementate (Transelectrica) si beneficiază de limita perimetrala pe latura de SUD.

Evaluatorul apreciaza negativ asigurarea securității locatiei analizate prin servicii de paza organizate si lipsa sistemelor electronice.

Iluminatul stradal asigura s i iluminatul intrarii in obiectiv, obiectivul are un sistem de iluminare pe intreaga zona perimetrala.

Conform procedurilor interne, zona perimetrala va fi supravegheata pe timpul zilei de catre angajatii care vor desfasura activitati in cadrul obiectivului si de catre agentul de securitate.

C. Zona de tranzactionare NU exista - nu se lucreaza cu numerar.

D. Zona de depozitare reprezinta spatiul special amenajat pentru pastrarea In siguranta a valorilor monetare s i a bunurilor: depozitul pentru materia prima, echipamente si piese, constituite de numeroase magazii asigurate cu usi metalice si lacate.

Unitatea nu dispune de seif.

E. Zona de expunere NU exista, nu se prezinta/expun bunuri si valori pentru public.

F. Zona de transfer NU exista, si nu este necesara avand in vedere lipsa de numerar.

G. Zona de procesare NU exista, si nu este necesara avand in vedere lipsa de numerar.

H. Zona echipamentelor de securitate exista, dar este necorespunzatoare. Usa nu este asigurata cu sistem de control-acces, echipamentele nu sunt asigurate si incuiate, oricine putand interveni asupra lor, nu exista UPS-uri pentru asigurarea continuitatii functionarii in cazul intreruperii alimentarii cu energie electrica, nu exista BACK-UP tehnic in alt mediu.

4.2. Centralizarea masurilor de securitate existente:

Zona	Descriere	Paza umana	Mecano fizic	Sistem Efractie	Control acces	CCTV	Turguard	Proceduri
Zona de Acces 1	cale de acces principala auto si pietonala, amplasată in str. Releului, prevazuta cu poarta metalica cu bariera si post de paza si control acces.	post de paza permanent	Poarta de acces metalica	buton de panica conectat GPRS	bariera	da	nu	da

Zona de Acces 2	cale de acces amplasată in vecinatatea blocului administrativ;	post de paza permanent	Poarta de acces metalica	nu	nu	nu	nu	da
Zona de Acces 3	cale secundara in vecinatatea CFU – destinată accesului personalului TRANSELECTRICA.		Poarta de acces metalica	nu	nu	nu	nu	da
Zona de Acces 4	cale de acces CFU situate pe spatele obiectivului	post de paza permanent		nu	nu	nu	nu	da
Zona de Acces 5	cale de acces CFU situate pe spatele obiectivului nefunctionala			nu	nu	da	nu	da
Zona de Acces 6	Acces cladire administrativa	post de paza 700-1500	nu	nu	nu	da	nu	da
Zona de Perimetru	Perimetru de aproximativ 2500 metri	da	gard din beton	nu	nu	nu	nu	da
Zona de tranzacţionare	nu exista							
Zona de depozitare	nu sunt valori monetare insa sunt valori materiale depozitate	nu	Usi metalice necertificate antiefractie si antiincendiu	nu	nu	nu	nu	da
Zona de expunere	nu exista							
Zona de transfer	nu exista							
Zona de procesare	nu exista							
Zona echipamentelor de securitate	nu sunt definite	nu	nu	nu	nu	nu	nu	nu
Zona de tranzactii cu	nu exista							

automate bancare								
Alte zone de important a cu regim securitate ridicat	nu sunt definite							

5. Identificarea infractiunilor asociate riscurilor potentiale care se pot manifesta in obiectiv, corelarea categoriilor de risc cu sursele acestora si sferele de impact in care se pot produce

Potrivit intentiei legiuitorului, prin cele 2 acte normative care stau la baza prezentei evaluari, HG 301/2012, respectiv Instructiunile MAI nr. 9/2013, s-a urmarit identificarea si tratarea riscurilor care, prin potentialul lor de manifestare ,periculozitate si consecinte, vizeaza urmatoarele categorii de infractiuni prevazute de Codul Penal.

Asadar toate riscurile care se pot manifesta in cadrul obiectivului vor fi tratate prin prisma consecintelor prevazute de codul penal.

Pentru simplificarea identificarii se vor aborda grupele principale de infractiuni savarsite cu intentie care aduc atingere integritatii persoanelor si patrimoniului

Identificarea riscurilor si a zonelor functionale stabilite din prezentul raport in care riscurile determinate se pot produce:

Categorie de risc	Sursa de risc	Producere pe zonele functionale
Omorul	Conflictele individuale, circumstantele infractiunilor de furt, talharie sau distrugere	Zona de acces, zona perimetrala, zona echipamentelor de securitate
Vatamarea corporala	Conflictele individuale, circumstantele infractiunilor de furt, talharie sau distrugere	
Furtul	Lipsa sau ineficienta masurilor tehnice si procedurale adecvate pentru protectia fizica Lipsa sau ineficienta pregatirii pe linia securitatii Nivelul de criminalitate local	Zona de acces, zona perimetrala, zona echipamentelor de securitate
Talharia	Lipsa sau ineficienta masurilor tehnice si procedurale adecvate pentru protectia fizica Lipsa sau ineficienta pregatirii pe linia securitatii Nivelul de criminalitate local	Zona de acces, zona perimetrala, zona echipamentelor de securitate

Distrugerea intentionata	Actiuni de razbunare ale angajatilor sau clientilor	Zona de acces, zona perimetrala, zona echipamentelor de securitate
Violarea sediului profesional	Insuficienta sau ineficienta masurilor de control acces si perimetral	Zona de acces, zona perimetrala, zona echipamentelor de securitate

6. Analizarea si estimarea riscurilor la securitatea fizica

Analizarea riscurilor identificate a fost efectuata prin prisma parametrilor interni si externi care genereaza si/sau modifica riscurile la securitatea fizica a companiei, respectiv:

- Mediul cultural, social, de reglementare, financiar, tehnologic, natural si concurential, la nivel national, regional sau local;
- Factor cheie cu impact asupra securitatii fizice a obiectivului;
- Prevederile legislative;
- Principiilor de organizare si reglementarilor interne ale companiei;
- Principiilor de management a riscurilor.

Riscurile identificate conform declaratiei beneficiarului cat si a inscrisurilor studiate nu au generat vreun incident in ultimul an in obiectiv.

Metoda folosita pentru evaluarea riscurilor identificate a fost HAZOP (hazard and operability study), conform notiunilor din standardul SR-EN 31010. adoptat si implementat ASRO ca si standard national la data de 24 decembrie 2010

Estimarea riscurilor la securitatea fizica s-a efectuat prin incadrarea obiectivului in grila de evaluare si cuantificarea gradului de risc prevazute in grila specifica din Instructiunile MAI Nr. 9/2013, care constituie Anexa 1 la prezentul raport.

Riscurile identificate au fost estimate in matricea de la pct. 6.3, pe baza calculului dintre probabilitatea de manifestare a unui risc si coeficientul de impact al acestuia, folosind urmatoarele scale:

6.1. SCALA DE MASURARE IMPACT/PROBABILITATE

Risc	Interpretare	Clasificare
Impact mare/ Probabilitate mare	**Foarte mare** **Sunt cele mai mari riscuri carora întreprinzatorii trebuie sa le acorde o atentie deosebita.**	**A**
Impact mare/ Probabilitate medie Impact mediu/ Probabilitate mare	**Mare** **Aceste riscuri au fie o probabilitate mare de aparitie, fie un impact semnificativ**	**B**
Impact mediu/ Probabilitate medie	**Mediu** **Exista o sansa medie ca riscurile unui impact sesizabil sa apara.**	**C**
Impact mediu/ Probabilitate scazuta	**Mic** **Aceste riscuri pot aparea în unele situatii si au un impact scazut sau mediu.**	**D**

Impact scazut/ Probabilitate medie		
Impact scazut/ Probabilitate scazuta	**Neglijabil** **Sunt riscuri cu probabilitate mica de aparitie si cu un impact scazut. De aceea pot fi neglijate.**	E

6.2. MATRICEA DE EVALUARE A RISCURILOR:

CRITERIU		IMPACT		
		Scazut (nesemnificativ, trebuie doar notat)	**Mediu** (impact rezonabil, necesita monitorizare)	**Mare** (va avea un impact semnificativ)
PROBABILITATEA	**Scazuta** (putin probabil sa se întample)	E	D	
	Medie (se poate produce la un moment dat)	D		
	Mare (probabil se va produce)			A

Ca urmare a datelor obtinute din observatiile facute la fata locului, a datelor furnizate de catre reprezentantul Beneficiarului, a identificarii masurilor de securitate existente in obiectiv, a reglementarilor interne cu privire la securitatea fizica, precum si din stabilirea factorilor de context extern, se apreciaza urmatoarele valori pentru fiecare categorie de risc:

6.3. RISCUL DE OMOR SI VATAMARE CORPORALA

CRITERIU		IMPACT		
		Scazut (nesemnificativ, trebuie doar notat)	**Mediu** (impact rezonabil, necesita monitorizare)	**Mare** (va avea un impact semnificativ)
PROBABILITATEA	**Scazuta** (putin probabil sa se întample)	E	D	

	Medie (se poate produce la un moment dat)	D		
	Mare (probabil se va produce)			A

Avand in vedere faptul ca unitatea dispune de unele sisteme electronice de securitate in prezent necorespunzatoare tehnic, dar dispune de un contract de paza cu o firma specializata, iar posibilitatea de "disimulare/fuga este scazuta credem ca probabilitatea producerii infractiunii de omor si vatamare corporala este scazuta.

Totodata, intrucat datele cu privire la infractiunea de omor si vatamare corporala, indiferent de formele acesteia, nu conduc catre procente ingrijoratoare pentru zona locatiei, precum si pedepsele aspre prevazute de lege, conduc la concluzia ca, desi impactul unei asemenea fapte ar fi de un nivel critic, totusi coroborarea cu probabilitatea foarte redusa de intamplare il incadreaza la un indice valoric **E** pentru obiectiv, ceea ce reprezinta o valoare minima pentru acest tip de risc.

BARIERE CARE PREVIN CAUZA:

- Existența unor mecanisme și sisteme tehnice privind securitatea fizică, echipamente care au impact psihic descurajant asupra majorității potențialilor agresori;
- Existența personalului de intervenție;
- Existența unei posibilități de solicitare a ajutorului.

FACTORI CARE DETERMINĂ CREȘTEREA RISCURILOR ȘI EFECTELOR

- Lipsa instruirii adecvate a personalului propriu în domeniul securității fizice
- Lipsa capacității de intervenție a personalului
- Personalul propriu și cel de intervenție este depășit numeric și din punct de vedere al capacității de ripostă.
- Nu există forțe de sprijin sau acestea nu pot ajunge în timp optim
- Sistemele electronice de protecție sunt defecte sau nu fiincționează în parametrii normali

BARIERE CONTRA CONSECINȚELOR:

- Blocarea atacului;
- Instruirea personal propriu în vederea acordării primului ajutor;
- Existența trusei de prim ajutor;
- Păstrare confidențialitate în raport cu mass-media.

Nu in ultimul rand, un element determinant este reprezentat si de faptul ca nu au fost inregistrate astfel de infractiuni.

In concluzie, **se impun masuri suplimentare** pentru tratarea acestui tip de risc.

Se recomanda si instruirea personalului cu privire la acest risc si modul de actiune in situatii de urgenta.

6.4. RISCUL DE FURT

CRITERIU	**IMPACT**		
	Scazut	**Mediu**	**Mare**

		(nesemnificativ, trebuie doar notat)	(impact rezonabil, necesita monitorizare)	(va avea un impact semnificativ)
PROBABILITATEA	Scazuta (putin probabil sa se întample)	E	D	
	Medie (se poate produce la un moment dat)	D		
	Mare (probabil se va produce)			A

Zona vulnerabila pentru riscul de furt o reprezinta zona perimetrala , precum si zona de depozitare unde exista valori care pot fi sustrase atat de persoane din afara, cat si de proprii angajati.

Per ansamblu, tinand cont de necoroborarea masurilor de protectie de ordin tehnic, uman si procedural, de faptul ca NU exista un cadru supravegheat video, desi exista un contract de paza, precum si de faptul ca au existat tentative de furt de aproximativ 1000 kg cupru in anul 2024, concluzionez ca riscul asociat infractiunii de furt este inacceptabil, fiind incadrat la un indice valoric **A.**

BARIERE CARE PREVIN CAUZA:

-Existența, supravegherea, proceduri de acces și efectuarea de control al angajaților la ieșirea din unitate;

- Existența unui management de specialitate care să realizeze și implementeze măsuri și proceduri de securitate, care să asigure auditul de securitate fizică;
- Efectuarea unui control eficient;
- Recrutarea și angajarea unui personal integru;
- Motivarea personalului de securitate.

FACTORI CARE DETERMINĂ CREȘTEREA RISCURILOR FURTULUI:

- Colaborare între angajați și pază pentru realizarea furtului
- Infractorii atacă și imobilizează personalul societății

BARIERE CONTRA CONSECINȚELOR:

- Existența personalului instruit și capabilități necesare preintampinarii furturilor;
- Blocarea tentativei de furt și recuperarea bunurilor;
- Existența unei capacități de prevenire, de protecție și ripostă (intervenție, sisteme mecanofizice, electronice, etc)

De asemenea, mentionez ca **se impun masuri suplimentare** pentru tratarea acestui tip de risc in afara de cele mentionate la cap VI. Se recomanda reinstruirea angajatilor privind procedurile pentru prevenirea acestor riscuri.

6.5. RISCUL DE TALHARIE

CRITERIU	IMPACT		
	Scazut	Mediu	Mare

		(nesemnificativ, trebuie doar notat)	(impact rezonabil, necesita monitorizare)	(va avea un impact semnificativ)
PROBABILITATEA	Scazuta (putin probabil sa se întample)	E	D	
	Medie (se poate produce la un moment dat)	D		
	Mare (probabil se va produce)			A

BARIERE CARE PREVIN CAUZA: avand in vedere faptul ca societatea dispune de un contract de paza cu o firma specializata, ca NU exista un sistem de supraveghere video instalat, iar posibilitatea de disimulare/fuga este greoaie se apreciaza ca probabilitatea producerii infractiunii de talharie este scazuta.

FACTORI CARE POT DETERMINA CREȘTEREA RISCURILOR ȘI EFECTELOR:

- Lipsa instruirii adecvate a personalului propriu în domeniul securității fizice;
- Lipsa capacității de intervenție a personalului;
- Personalul propriu și cel de intervenție este depășit numeric și din punct de vedere al capacității de ripostă;
- Nu există forțe de sprijin sau acestea nu pot ajunge în timp optim;
- Sistemele electronice de protecție nu exista sau nu fiincționează în parametrii normali.

Desi, per ansamblu, tinand cont de coroborarea masurilor de protectie de ordin tehnic si procedural, precum si de faptul ca nu au fost inregistrate in obiectiv astfel de evenimente, desi impactul ar fi mare, probabilitatea este scazuta si concluzionez ca riscul asociat infractiunii de talharie este acceptabil, fiind incadrat la un indice valoric C.

BARIERE CONTRA CONSECINȚELOR:

- Blocarea atacului;
- Instruire personal propriu în vederea acordării primului ajutor;
- Existența trusei de prim ajutor;
- Păstrare confidențialitate în raport cu mass-media.

In concluzie, **se impun masuri suplimentare** pentru tratarea acestui tip de risc.

Se recomanda reinstruirea personalului cu privire la acest risc.

6.6. RISCUL DE DISTRUGERE

CRITERIU	IMPACT		
	Scazut	Mediu	Mare

		(nesemnificativ, trebuie doar notat)	(impact rezonabil, necesita monitorizare)	(va avea un impact semnificativ)
PROBABILITATEA	Scazuta (putin probabil sa se întample)	E	D	
	Medie (se poate produce la un moment dat)	D		
	Mare (probabil se va produce)			A

Avand in vedere specificul obiectivului si anume ca nu exista bunuri de valoare insemnata amplasate pe zonele publice, iar distrugerea celor existente prezumam ca, fapta poate fi din culpa si nu conduce la o ingrijorare majora.

BARIERE CARE PREVIN CAUZA: avand in vedere faptul ca societatea dispune de un contract de paza cu o firma specializata, ca NU exista un sistem de supraveghere video instalat, iar posibilitatea de disimulare/fuga este greoaie se apreciaza ca probabilitatea producerii infractiunii de distrugere este scazuta.

FACTORI CARE POT DETERMINA CREŞTEREA RISCURILOR ŞI EFECTELOR:

- Lipsa instruirii adecvate a personalului propriu în domeniul securităţii fizice;
- Lipsa capacităţii de intervenţie a personalului;
- Personalul propriu şi cel de intervenţie este depăşit numeric şi din punct de vedere al capacităţii de ripostă;
- Nu există forţe de sprijin sau acestea nu pot ajunge în timp optim;
- Sistemele electronice de protecţie sunt defecte sau nu funcţionează în parametrii normali.

Desi, per ansamblu, tinand cont de coroborarea masurilor de protectie de ordin tehnic si procedural, precum si de faptul ca nu au fost inregistrate in obiectiv astfel de evenimente, desi impactul ar fi mare, probabilitatea este scazuta si concluzionez ca riscul asociat infractiunii de distrugere este acceptabil, fiind incadrat la un indice valoric **C**.

BARIERE CONTRA CONSECINŢELOR:

- Blocarea accesului neautorizat in zona de depozite;
- interzicerea accesului persoanelor aflate sub influenta alcoolului;
- evacuarea persoanelor turbulente.

In concluzie, **se impun masuri suplimentare** pentru tratarea acestui tip de risc.

Se recomanda reinstruirea personalului cu privire la acest risc.

Din coroborarea posibilitatii de producere cu nivelul de impact asupra organizatiei, precum si pe baza faptului ca in ultimul an nu au fost inregistrate astfel de evenimente, acest risc se incadreaza la un indice valoric **E** pentru obiectiv, ceea ce reprezinta o valoare **acceptabila** pentru acest tip de risc.

6.7. VIOLAREA SEDIULUI PROFESIONAL

CRITERIU		IMPACT		
		Scazut	Mediu	Mare
		(nesemnificativ, trebuie doar notat)	(impact rezonabil, necesita monitorizare)	(va avea un impact semnificativ)
PROBABILITATEA	Scazuta (putin probabil sa se întample)	E	D	
	Medie (se poate produce la un moment dat)	D		
	Mare (probabil se va produce)			A

Avand in vedere faptul ca exista proceduri speciale de securitate pentru acces, cat si faptul ca exista un sistem de supraveghere video pentru personalul care acceseaza obiectivul, apreciem ca acest tip de risc nu conduce la o ingrijorare majora.

BARIERE CARE PREVIN CAUZA:

- Existența procedurilor de lucru și implementarea lor;
- Instruire, conștientizare, responsabilizare și sancționare angajați;
- Respectarea normelor legale de utilizare a echipamentelor si dispozitivelor electronice, calculatoarelor, imprimantelor si faxurilor, mediilor de stocare;
- Implementarea instrumentelor de protecție.

FACTORI CARE DETERMINĂ CREȘTEREA RISCURILOR EXPLOATĂRII NECORESPUNZATOARE A ECHIPAMENTELOR

-Lipsa de pregătire sau pregătire necorespunzatoare a personalului;
-Neglijenta si superficialitate in munca;
-Indisciplina si insubordonare;
-Folosirea de echipamente neverificate sau neautorizate.

Vulnerabilitățile speciale identificate pot fi înlăturate prin:

-motivarea personalului;
-instruirea corespunzătoare a personalului și verificarea activităților desfășurate de către acesta.

Din coroborarea posibilitatii de producere cu nivelul de impact scazut si un nivel de probabilitate medie asupra organizatiei acest risc se incadreaza la un indice valoric **D** pentru obiectiv, ceea ce reprezinta o valoare **acceptabila** pentru acest tip de risc.

In concluzie, **se impun masuri suplimentare** pentru tratarea acestui tip de risc.

Se recomanda si instruirea personalului cu privire la acest risc si modul de actiune in situatii de urgenta.

7. Stabilirea masurilor suplimentare de tratare a riscurilor si a costurilor estimate pentru implementarea acestora

Nr. Crt	TIP	Zone	Descriere măsură	Detalii măsură	Cost
1	Procedural	General	Refacere si resupunere spre avizare a planului de paza	Planul de paza aprobat in 2016, in baza evaluarii de risc cu masurile consemnate nu reflecta realitatea din teren iar masurile nu au fost implementate conform cu evaluarea de risc. Recomandam ca postul de paza inarmat din actualul contract si plan de paza sa fie transformat in post de paza neinarmat.	0
2	Procedural	General	Reevaluarea riscurilor de Securitate la schimbarea configuratiei sistemului de Securitate, a arhitecturii spatiului sau in cazul unui incident de securitate	ori de cate ori apar incidente de securitate sau modificari de structura	0
3	Procedural	General	Redactarea unei proceduri de verificare periodică a înregistrărilor stocate pe inregistratoarele sistemului de supraveghere video	Va fi desemnată o persoană care să fie instruită de instalatorul sistemului CCTV.	0
4	Procedural	General	Individualizarea codurilor de acces pentru persoanele autorizate.	Se execută de către societatea care asigură întreținerea sistemului. Codurile se vor schimba la fiecare trimestru cf. HG301/2012 Anexa 7, Art. 11	0
5	Mecanofizice	Zona de perimetru	Defrisarea vegetatiei pe intreaga zona perimetrala si evacuarea acesteaia din obiectiv;	Asigurarea unei vizibilitati bune agentului de patrulare si camerelor dar si vizibilitate din exterior a locatiei.	conform oferta sau resurse interne

6	Mecanofizice	Zona de perimetru	Repararea gardului pe intreaga zona perimetrala;	Asigurarea integritatii perimetrului prin masuri mecanofizice si intarzierea unor eventuale tentative de patrundere prin efractie	conform oferta sau resurse interne
7	Mecanofizice	Zona de perimetru	Repararea si punerea in functiune a sistemului de iluminat perimetral	Asigurarea unei vizibilitati bune agentului de patrulare si camerelor dar si vizibilitate din exterior a locatiei.	conform oferta sau resurse interne
8	Mecanofizice	Zona de acces	Instalarea panourilor de avertizare: "Acces interzis", "Obiectiv protejat", "Zona supravegheata video 24h/24h"	Respectarea cerintelor legale cu privire la obiectivele monitorizate video si efractie	conform oferta sau resurse interne
9	Sisteme de securitate	Zona de perimetru	Proiect de securitate prin firma autorizata	Se va contracta o firma autorizata pentru elaborare proiect tehnic de securitate	6500 lei

10	Sisteme de securitate	Zona de perimetrala	Sistem CCTV perimetral minim 50 camere, de exterior cu ir de minim 60 metri, si functii de detectie perimetrale (intrare in perimetru) dvr/nvr si monitor de vizualizare/monitorizare camere in postul de acces, cu asigurarea cerintelor legale de stocare. Datorita lunigimi perimetrului numarul de camere si tipul de camere trebuie stabilite prin un proiect tehnic, Folosirea cladirilor inalte pentru instalare camere tip speed dome pentru monitorizare generala curti si perimetre. Alertele perimetrale sa fie semnalizate in postul de acces/ monitorizare cctv atat vizual prin pop up pe monitor cat si sonor prin sistemul audio PC sau sursa externa gen sirena/ difuzoare externe	Se va contracta o firma avizata pentru instalare sistem CCTV. Sistemul trebuie sa alerteze in caz de efractie un operator local sau un operator din un centru operational de securitate. Sistemul trebuie sa acopere in totalitate perimetrul 2500 m. Echipamentele sa fie conectate la o sursa alternativa gen UPS in caz de caderi de tensiune	150000lei
11	Sisteme de securitate	Zone de acces	Sistem CCTV pentru monitorizare acces cu minim 6 camere, de exterior cu ir de minim 40 metri, si functii de detectie auto, persoane (intrare in perimetru) dvr/nvr si monitor de vizualizare/monitorizare camere in postul de acces, cu asigurarea cerintelor legale de stocare. Recomandarea daca se doreste si registru electronic este de a se instala camere tip LPR pentru intrarile auto	Se va contracta o firma avizata pentru instalare sistem CCTV acces. Sistemul va fi monitorizat de un operator local sau un operator din un centru operational de securitate.	20000lei
12	Sisteme de securitate	Alte zone in interiorul perimetrului	Sistem CCTV pentru monitorizare accese in cladirile administrative, centru de comanda, statie de pompare, statie gaze, statie de hidrogen,statie tratate ape, puncte trafo	In baza proiectului elaborat, si functie de numarul cladirilor, aceselor in cladiri alte informatii relevante se va contracta firma autorizata pentruinstalare sistem cu respectare cerintelor legale	de determinat in baza proiectului si ofertelor

13	Sisteme de securitate	Zona echipamentelor de securitate	Alegerea unei zone pentru a pozitiona echipamentele de securitate	constituirea unei zone unde sa fie pozitionate centralele de efractie, pcurile unde sunt instalate softuri, nvruri pentru sistem cctv alte echipamente de securitate, care trebuiesc protejate fizic cu cheie si sau sisteme de securitate de control acces si detectie la efractie	0
14	Sisteme de securitate	Zona echipamentelor de securitate	Alegerea unei zone pentru a pozitiona echipamentele de securitate	Montarea unei camere cctv pentru monitoriza intrare in zona, sau instalarea uneui sistem de acces control	1000 lei
15	Sisteme de securitate	General	Sistem acces control, accese bloc cladire administrativa, cladire de comanda, alte zone de interes	Implementarea pentru toate accesele in cladirile aflate pe perimetru a unui sistem de acces control	25000 lei
16	Sisteme de securitate	General	Mentenanta sisteme de securitate	Contractarea unei firme licentiate pentru a asigura mentenanta periodica a sistemelor de securitate	15000 lei anual
17	Masuri de Securitate U	Zona de acces si perimetrala	Mentinere dispozitivul de paza actual pana la implementarea altor masuri de securitate: 9posturi de paza fixe, permanente (24 ore/zi), din care un post la punctul de control acces dotat cu buton de alarma, la care se adauga un post de 8 ore un post de Sef de obiectiv.	Conform plan de paza si consemnelor generale si particulare	conform contract

	ma na				

Evaluarea implementării masurilor de tratare a riscurilor este orientativa si presupune o estimare a evaluatorului pe baza preturilor medii ale unor astfel de masuri. Costul final al implementării depinde de soluția tehnica decisa de BENEFICIAR, calitatea si prețul echipamentelor instalate, complexitatea lucrărilor, lungimea cablurilor, furnizorul ales si negocierea BENEFICIARULUI cu acesta.
Aceasta evaluare a costurilor nu tine loc de studiu de fezabilitate sau oferta comercial si nu implica cu nimic evaluatorul;

Deoarece scopul final al analizei de risc este acela de a găsi un echilibru economic între impactul riscului asupra organizației și costurile de punere în aplicare a măsurilor de prevenire și protecție, considerăm că măsurile propuse în prezentul raport sunt suficiente în condițiile actuale de mediu, adaptate locației și tipului de activitate desfășurată în unitate.

Beneficiarul, conform normelor legale în vigoare, are obligația să implementeze, în termen de 60 de zile de la primirea documentației, măsurile menționate în Raport. Concluziile prezentate de către evaluator sunt valabile la data prezentată în raport și pe perioada în care condițiile specifice nu suferă modificări care pot afecta opiniile estimate.

Recomandarile evaluatorului prezentate mai sus sunt cerințe minimale, beneficiarul poate suplimenta echipamentele de securitate în vederea cresterii gradului de acoperire a perimetrului monitorizat.

Dupa finalizarea implementarii sistemelor de securitate din masuri, recomandam analiza atributiilor posturilor de paza actuale si modalitatea in care atributiile au fost inlocuite total sau partial prin sisteme de securitate, pentru a determina necesarul dispozitvului de paza umana (mentinerea sau diminuarea dispozitivului).

8. Concluziile finale ale raportului

Implementarea masurilor dispuse in cap.VI sunt necesare pentru obtinera gradului de securitate a obiectivului si scaderea procentajului riscurilor identificate.

La completarea grilei de evaluare acolo unde exista criterii in grila care nu au corespondent in realitate se va acorda punctaj minim, respectiv:

- ✓ 2,2,1 Compartiment operator
- ✓ 2,2,2 Dotare ghișeu de lucru cu clienții
- ✓ 2,3,1 Amplasare și dotare
- ✓ 2,5,1 Trasee de manipulare interioară numerar
- ✓ 2,5,2 Puncte de transfer către exterior
- ✓ 2,6,1 Amplasare
- ✓ 2,9,3 Semnalizare forțare seif
- ✓ 2,12,3 Transporturi valori

Dupa implementarea masurilor exact cum au fost dispuse de evaluator, riscurile vor fi diminuate rezultand un punctaj ponderat de **54,80 %** fara paza umana si rezultand un nivel de **risc acceptabil**.

Clauza de nepublicare:

A. concluziile sunt valabile la data efectuării analizei și sunt asumate de evaluator;

B. concluziile își păstrează valabilitatea în măsură în care condițiile specifice nu suferă modificări structurale, tehnice tehnologice, operaționale sau de altă natură;

C. confidențialitatea raportului;

D. obligativitatea înregistrării documentului după asumare de către beneficiar.

Din punct de vedere al cerintelor prevazute de Legea 333/2003 privind paza obiectivelor, bunurilor, valorilor si protectia persoanelor, de HG 301/2012 privind normele de aplicare a Legii 333/2003 si de Instructiunile MAI Nr.9/2013 obiectivul are un concept de protectie fizica eficient si care asigura indeplinirea cerintelor minimale de securitate prevazute de lege.

Evaluator autorizat:
SC GUARD TRAINING SYSTEM SRL

MĂDĂLIN TEPOR

Administrator
SC GUARD TRAINING

MĂDĂLIN TEPOR

Am luat la cunostinta si imi asum consecintele prezentului raport de evaluare:
DIRECTOR GENERAL
S.C. ELECTROCENTRALE BUCUREȘTI S.A.

Claudiu-Ionut CRETU-SARBU

IMPORTANT:
Vă rugăm să aveti in vedere că **analiza de risc la securitate fizică se revizuiește obligatoriu** în următoarele situații:

- **LA FIECARE 3 ANI,** pentru corelarea cu dinamica parametrilor interni și externi care generează și/sau modifică riscurile de securitate fizică a locatiei;
- **IN CEL MULT 60 DE ZILE** de la producerea unui incident de securitate;
- **IN CEL MULT 30 DE ZILE** de la modificarea caracteristicilor arhitecturale,funcționale sau a obiectului de activitate.

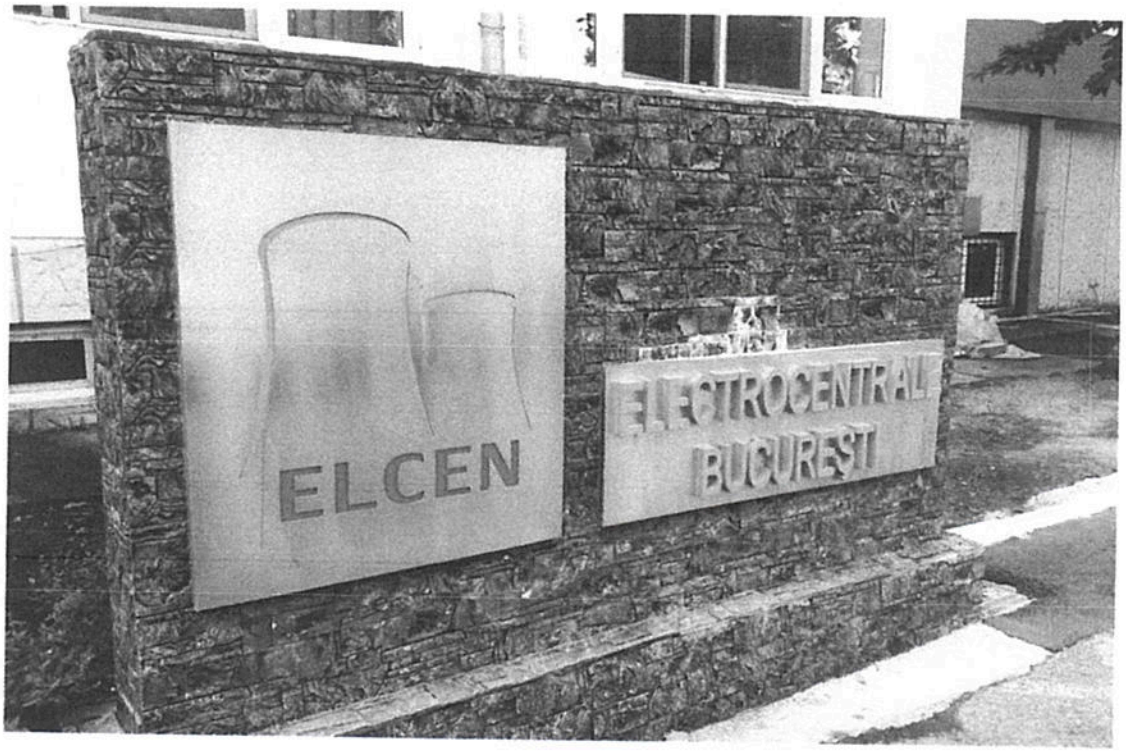
ETAPA 1

Anexa 4

SRA - SECURITY RISK ADVISOR SRL
Intrarea Dusului nr. 2G, parter, biroul 4, Sector 6, Bucuresti
ONRC: J2019008692405, CUI: RO-41343693

STUDIU DE FEZABILITATE

Sistem electronic de securitate
(sistem video de monitorizare integrat, cu componenta paza perimetrala si control acces) Electrocentrale Bucuresti SA



Beneficiar: Electrocentrale Bucuresti SA

Faza: Studiu de Fezabilitate - etapa 1

Contract: 150 din 2026

CUPRINS

1. Informatii generale privind obiectivul de investitii 4
1.1. Denumirea obiectivului de investitii 4
1.2. Ordonator principal de credite/investitor 4
1.3. Ordonator de credite (secundar/tertiar) 4
1.4. Beneficiarul investitiei 4
1.5. Elaboratorul studiului de fezabilitate 4
2. Analiza soluțiilor tehnice posibile pentru implementarea sistemului electronic de securitate 4
2.1. Cerinte si strategia de asigurare a securitatii 4
2.1.1. Strategia de securitate 4
2.1.2. Cerinte de specialitate 5
2.2. Descrierea din punct de vedere tehnic, constructiv, functional-arhitectural si tehnologic 6
2.2.1. Perimetru 6
2.2.2. Acces 10
2.2.3. Paza 14
2.2.4. Monitorizare 16
2.2.5. Interventie rapida 17
2.2.6. Mentenanta 18
2.2.7. Managementul securitatii 18
2.2.8. Date 20

1. Informatii generale privind obiectivul de investitii

1.1. Denumirea obiectivului de investitii

Sistem electronic de securitate (sistem video de monitorizare integrat, cu componenta paza perimetrala si control acces) Electrocentrale Bucuresti SA.

1.2. Ordonator principal de credite/investitor

Electrocentrale Bucuresti SA

1.3. Ordonator de credite (secundar/tertiar)

Nu este cazul

1.4. Beneficiarul investitiei

Electrocentrale Bucuresti SA

1.5. Elaboratorul studiului de fezabilitate

Proiectant general: SRA Security Risk Advisor SRL

2. Analiza soluțiilor tehnice posibile pentru implementarea sistemului electronic de securitate

2.1. Cerinte si strategia de asigurare a securitatii

2.1.1. Strategia de securitate

Cea mai performanta strategie in acest tip de situatii este „sigilarea" perimetrului si controlul strict al accesului in zonele si spatiile de interes.

Acest lucru presupune implementarea unor sisteme de securitate si redimensionarea unora dintre serviciile existente, respectiv contractarea unor servicii specifice asa cum sunt detaliate la punctul 3.3.

Strategia vizeaza in mod special asigurarea functiei de protectie a securitatii dar nu exclude functia de suport prin care sa generam diferiti indicatori de performanta, statistici sau alerte.

Strategia cuprinde si o serie de cerinte specifice (de specialitate) care ghideaza atat modul de configurare a solutiilor, cat si selectarea tehnologiilor care prezinta cel mai mare beneficiu pentru scenariul considerat.

De asemenea, trebuie precizat ca in cazul locatiilor foarte mici, nu se justifica existenta a doua variante / scenarii de asigurare a securitatii, tocmai datorita dimensiunii care nu permite variatii foarte mari ale solutiei fara o crestere semnificativa a costurilor. In general, implementarea unor solutii alternative mizeaza pe capabilitati mai avansate, cu costuri mai mari, dar pentru care exista un "break even" din punct de vedere financiar, atunci cand un anumit volum este atins. Spre exemplu, folosirea unor camere cu rezolutie mai mare si cu lentita diferita, poate scadea numarul de camere insa acestea presupun cresterea capacitatii de procesare la nivelul serverului. Prin urmare, este necesar sa existe un anumit numar de camere inlocuite prin noul sistem astfel incat sa fie acoperit acest cost suplimentar de procesare in conditii de eficienta economica.

2.1.2. Cerinte de specialitate

Orice solutie de securitate implementata la nivelul centrului logistic trebuie sa indeplineasca urmatoarele cerinte:

	detectia timpurie (la nivelul perimetrului) prin mijloace automatizate si calificate
	reactia rapida, calificata (prin personalul de paza propriu) si dimensionata situatiei (prin folosirea de resurse externe suplimentare in cazuri deosebite).
	existenta unei solutii de rezerva pentru orice tip de situatie in care sistemul nu functioneaza conform specificatiilor
	trasabilitate pe fiecare activitate realizata (ex: armare/dezarmare, interventie etc.) in vederea alocarii eficiente a raspunderii
	managementul specializat al activitatilor
	generarea de date suport pentru companie (ex: statistici, alerte)
	generarea de indicatori de performanta care sa permita identificarea timpurie a situatiilor neconforme sau potential periculoase, a bottle neck-urilor etc
€	reducerea costurilor

2.2. Descrierea din punct de vedere tehnic, constructiv, functional-arhitectural si tehnologic

Solutia tehnica presupune o combinatie de sisteme (hardware si software) si servicii pentru realizarea scopului propus de "sigilare" a perimetrului si control strict al accesului din exterior pe proprietate.

Descrierea si analiza elementelor constitutive ale solutiilor este realizata in capitolele urmatoare, cu precizarea ca diferenta intre scenarii este data de modul in care combinam solutiile de detectie la nivelul perimetrului, cu cele de control al accesului.

2.2.1. Perimetru

Protectia perimetrului se bazeaza pe realizarea detectiei pe 100% din perimetru, pentru 100% din timp si la 100% din parametri. Din acest motiv, singura optiune considerata este detectia realizata prin mijloace tehnice.

Resursa umana reprezinta in acest caz doar varianta de rezerva (ex: defectarea unei camere) ce poate fi dispusa in zona de interes pentru suplinirea lipsei detectiei tehnice. Acest lucru trebuie privit insa ca o solutie de rezerva ce trebuie folosita in situatii deosebite si pentru o perioada limitata de timp (ex: pana la repararea / inlocuirea echipamentelui).

Limita de perimetru din obiectivele analizate se afla la nivelul gardului exterior, cu o singura exceptie, respectiv cladirea administrativa (sediul central) unde o latura a cladirii (dinspre strada Portocalelor) reprezinta limita de proprietate.

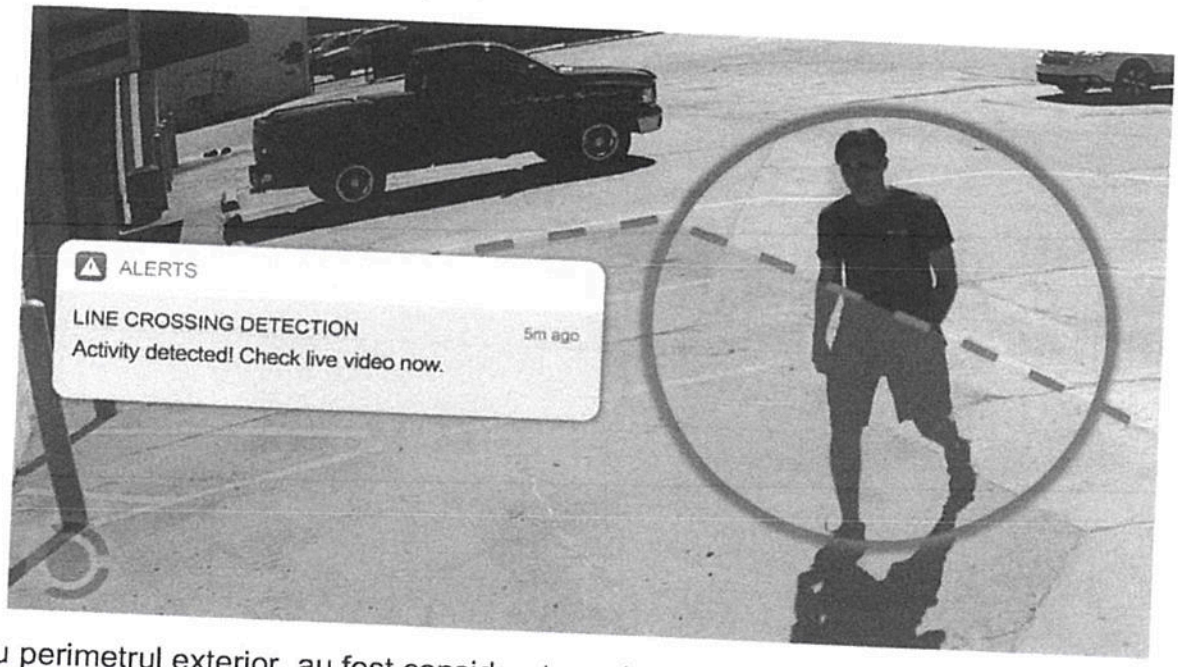
Specificul in cazul cladirii administrative este ca limita de perimetru include ferestre ce pot constitui o cale de acces neautorizat in interiorul proprietatii protejate. Pentru protejarea acestui tip de perimetru se va implementa un sistem de detectie a efractiei clasic, prevazut cu senzori de geam spart si senzori de miscare cu tehnologie duala, care sa alerteze personalul de paza aflat in serviciu.

Sistemele video inteligente permit detectia automata a formei umane si alertarea in situatia in care omul intersecteaza o arie sau o linie virtuala.

Sistemul se auto-monitorizeaza si efectueaza detectia in mod automat, alertand dispecerul din centrul de monitorizare. In acest fel, este posibil ca un singur dispecer sa monitorizeze un numar mare de locatii si camere de supraveghere video.

Acest mod de organizare al detectiei este mult superior celui clasic, in care un dispecer are in fata un numar de monitoare, fiecare afisand un numar de camere video. Practic, dispecerul de monitorizare fie nu are suficiente detalii pentru a detecta o situatie suspecta (pentru ca imaginile sunt prea mici), fie poate monitoriza un numar redus de camere (respectiv acele imagini de dimensiune mare care intra in campul sau vizual).

Este important de mentionat ca, prin setarea zonei de detectie la limita de proprietate, alertarea se realizeaza la momentul accesului neautorizat in perimetru ceea ce inseamna ca timpul de interventie foarte scurt nu ofera infractorilor suficient timp pentru a opera. In acest interval redus de timp, infractorii trebuie sa ajunga pana la zona de interes, sa patrunda in acea zona, sa sustraga marfa / materiale / etc. si sa paraseasca zona cu bunurile respective, fapt ce este practic imposibil.



Pentru perimetrul exterior, au fost considerate mai multe solutii, dupa cum urmeaza:

SISTEME DE DETECTIE PERIMETRALA

Se poate realiza prin tehnologii diferite precum infrarosu, microunde sau gard inteligent. Problema principala a acestui sistem este ca el detecteaza un eveniment de un anumit tip (ex: intreruperea unei raze infrarosu sau deformarea unui camp electromagnetic) si, in lipsa unui sistem de supraveghere video, genereaza extrem de multe alarme.

Acest sistem a fost descalificat ca solutie tehnica din urmatoarele motive:

- Genereaza un numar foarte mare de alerte si au posibilitati limitate de filtrare a alertelor false (ex: daca mai multe raze sunt interupte simultan sau daca deformarea campului electromagnetic depaseste o anumita valoare);
- Calitatea alarmelor este slaba prin comparatie cu alte sisteme (ex: sistemele video inteligente detecteaza forme si nu dau alerte la animale etc.);
- Necesita validare video a alarmelor;
- Creste nivelul de complexitate pentru ca necesita integrare cu sistemul de supraveghere video;
- Creste costurile deoarece folosirea unui sistem separat de detectie este mai scump decat folosirea unei licente de analiza video prin care se face detectia.

CAMERE VIDEO TERMALE

Camerele video termale analizeaza imaginile in spectru termic si genereaza alerte daca identifica persoane in zona de interes. Aceste camere au marele avantaj de a realiza o detectie mai buna la distante mari (chiar si la peste 800 metri). Prin urmare, folosirea unor astfel de camere ar reduce necesarul de echipamente, accesorii si lucrari.

Totusi, si aceasta tehnologie a fost descalificata din urmatoarele motive:

- Camerele termale nu pot oferi informatii cu privire la persoana respectiva (ex: daca este angajat care efectueaza o lucrare sau daca este o persoana neautorizata);
- Chiar daca aceste camere ofera si imagini in spectru vizual normal ce ar putea fi folosite de un dispecer pentru validarea alarmelor, distanta mare la care se face detectia in regim termic face imposibila validarea pe intreaga zona de detectie din motive de rezolutie sau luminozitate (seara sau noaptea devine practic imposibil sa stabilesti cine e persoana detectata);
- Singurul mod de a realiza validarea este de a folosi multe camere in spectru vizual normal pentru distante mai mici sau cateva camere speed dome (PTZ), astfel incat dispecerul sa poata interpreta corect imaginea, ceea ce invalideaza rationamentul initial de reducere a numarului de camere;
- Defectiunea unei camere video termale genereaza vulnerabilitati pe o zona mare ce nu pot fi suplinite de un singur agent de securitate, tocmai datorita distantelor, prin urmare creste costul suplimentar al scenariului de rezerva, fie prin folosirea unei resurse suplimentare (care genereaza un cost suplimentar punctual), fie prin reducerea moderata a dispozitivului actual de paza (care genereaza o reducere mai mica decat ceea ce este maxim posibil), tocmai pentru a putea acoperi nevoile de securitate in astfel de situatii.

In concluzie, desi detectia termica este o tehnologie valida, ea este pretabila mai ales pentru spatii largi unde accesul persoanelor nu este permis (ex: infrastructura de cai ferate, zone de protectie sanitara, etc.). Tehnologia ar putea fi folosita in cateva locuri (ex: linii ale perimetrului drepte si la o distanta de minim 10 metri de caile interioare de circulatie), insa aceste oportunitati sunt extrem de reduse si ar introduce un nivel de complexitate al solutiei care nu se justifica prin avantajele generate.

CAMERE VIDEO CU UN OBIECTIV SI INFRAROSU

Camerele de supraveghere video clasice, care lucreaza in regim normal pe timp de zi, respectiv cu infrarosu in conditii de luminozitate scazuta, reprezinta solutia ideala si tehnologia de baza folosita in majoritatea proiectelor de securitate.

In cadrul prezentului studiu de fezabilitate, aceasta tehnologie a fost selectata ca fiind una din cele 2 scenarii conforme si eligibile in raport cu obiectivele propuse deoarece:

- Realizeaza o detectie foarte buna (in general la distante de pana la 50-60 metri) prin folosirea unor functii de analiza video specifice (ex: cross-line si human detection);
- Permite dispecerului sa observe zona de interes si sa recunoasca persoanele care au generat alerta si in acest mod sa valideze / invalideze alerta;
- Indisponibilitatea imaginilor de la o camera (sau de la un cluster de camere cum ar fi in situatia in care se strica un router) genereaza o vulnerabilitate mai mica ce poate fi usor acoperita de un agent de securitate.

Desi numarul mai mare de echipamente implica un cost initial mai mare, diferenta de cost apare o singura data si nu este mare in valoare absoluta. In plus, costurile de reparatii sunt mai mici iar configuratia sistemului presupune ca un agent de securitate poate suplini lipsa imaginilor in majoritatea cazurilor, nefiind nevoie de resursa suplimentara (si costuri suplimentare asociate).

CAMERE VIDEO CU OBIECTIV DUBLU SI INFRAROSU

Diferenta fata de solutia anterioara este ca fiecare camera de acest tip este pravazuta cu doua lentile (de obicei una cu unghi mai deschis pentru zone apropiate si cealalta cu unghi mai ingust pentru distante mai lungi).

Acest tip de camera poate acoperi o distanta mai mare decat camerele cu un singur obiectiv si realizeaza detectia in spectru vizual normal pe o distanta mai mare. Pactic avem 2 camere intr-una singura ceea ce scade costul total de achizitie.

Avantajele sunt aceleasi cu cele de la solutia anterioara, cu singura diferenta ca in acest caz scade costul initial cu instalarea si ulterior cu mentenanta acestora.

Din punct de vedere al dezavantajelor as preciza doar faptul ca ele nu pot fi folosite pe intreaga lungime a perimetrului pentru ca ar putea fi obturate de elemente constructive, copaci, instalatii, trasee de tevi etc.

In concluzie, aceasta este la randul ei o solutie acceptabila din perspectiva studiului de fezabilitate pentru ca ofera toate datele necesare pe linie de detectie si alertare la nivelul perimetrului, respectiv validarea alertelor, la un pret mai mic decat solutia anterioara.

2.2.2. Acces

Implementarea sistemului de control al accesului strict este o componenta critica a strategiei de securitate. Mecanismele de control al accesului cuprind o gama larga de tehnici, cum ar fi:

- **Autentificarea -** verificarea identitatii persoanelor sau autoturismelor atat la la check-in, cat si la check-out;
- **Autorizarea -** validarea accesului pe baza de parametri specifici (program de lucru, punct de acces, etc.);

- **Auditare -** inregistrarea de loguri specifice operatiunilor de acces.

Controlul eficient al accesului necesita o abordare multistratificata, care sa permita diverse elemente de control, cum ar fi:

- **RBAC (Role-Based Access Control)**: alocarea de permisiuni pe baza de roluri de utilizatori;
- **ABAC (Attribute-Based Access Control)**: ia in considerare parametri suplimentari cum ar fi utilizarea de echipamente personale de protecție (ex: casca);
- **MAC (Mandatory Access Control)**: folosit pentru punctele de acces din exterior si eventual in anumite zone cu grad mare de criticalitate (dispecerat, documente clasificate, etc.) pentru a implementa reguli stricte de acces bazate pe criterii multiple.

Din perspectiva datelor, accesul poate fi împărțit în 3 componente majore:

- **Access registration (DATA)**: colectarea datelor necesare pentru inregistrarile de acces (in/out);
- **Access validation (LOGIC)**: acordarea sau respingerea dreptului de acces pe baza unui set de conditii;
- **Access transaction (ACTION)**: initiaza o serie de actiuni (automatizate) cum ar fi deschiderea unei bariere, deblocarea unui turnichet sau electromagnet, afisarea unui mesaj, activarea unui semafor, trimiterea unei notificari sau actualizarea unor date.

Actualizarea si implementarea unei proceduri de acces este necesara pentru a delimita zonele si regulile de acces. Practic, tipul de conditii de acces care trebuie implementate depinde de o serie de factori care includ elemente precum: tipul de activitate (ex: acces angajati, acces vizitatori, acces de urgenta), tipul de punct de acces (pietonal sau auto), tipul de persoana (angajat, partener sau vizitator), etc.

Din punct de vedere al componentei, sistemele de control acces contin:

- Sistem de managementul al identitatii (pentru inrolare / management utilizatori);
- Inputuri / Elemente de captare a datelor (ex: cititoare cu diverse categorii si tehnologii, tastaturi, ecrane tactile, camere video LPR, etc.) prin care se preiau datele;
- Controler acces (creierul sistemului amplasat in mod obligatoriu in zona protejata) - contine regulile si logica de acces si este responsabil pentru luarea deciziilor si emiterea de comenzi;
- Elemente de blocare a accesului (ex: bariera, turnichet, electromagnet, etc.);
- Elemente de control si management centralizat (optional) - permit controlul la distanta al echipamentelor pentru sistemele conectate.

In cazul de fata, alegerea solutiei corecte pentru gestionarea accesului trebuie sa tina cont de urmatorii factori principali:

- asigurarea unui nivel optim de control si trasabilitate pentru fiecare scenariu de acces;
- optimizarea maxima a costurilor (in special in cazul punctelor de acces cu trafic redus / ocazional);
- actionarea la distanta a echipamentelor (ex: deblocarea unei porti, deschiderea unei bariere) care permite o reducere mai mare a numarului de posturi de paza;
- asigurarea unor functii de suport pentru personalul de securitate in cazul posturilor de acces neasistate de personal (ex: automatizare, detectia fraudei de acces, etc.).

In acest sens au fost considerate analizate 4 solutii, dupa cum urmeaza:

INTERFON

Interfonul, ca solutie de acces de sine statoare, poate fi folosit doar daca detine certificare pentru sisteme de control acces (ex: SR EN 50133).

Chiar si asa, este o solutie de nivel inferior celorlalte solutii de acces analizate, nepotrivit pentru o locatie de interes public.

Interfonul poate fi insa folosit ca un echipament suplimentar pentru comunicare la distanta (ex: cu un dispecer al ELECTROCENTRALE BUCURESTI SA) sau cu un element periferic al sistemului de control acces (respectiv un element de captare a datelor).

SISTEM DE PARKING MANAGEMENT

Acest sistem are o aplicabilitate limitata (pentru parcarile cu acces din exterior) si poate fi operat independent de sistemul de control al accesului.

Totusi, desi este un sistem valid din punct de vedere tehnic si al conformitatii cu cerintele legale, este o optiune respinsa in cadrul studiului din urmatoarele motive:

- atata timp cat nu se percep bani pentru folosirea accesului, sistemul de control acces poate indeplini aceleasi functii ca si cel de parking si nu este nevoie de un alt sistem;
- este mai scump decat sistemele de control acces in majoritatea situatiilor deoarece, in mod clasic, foloseste elemente in miscare (ex: imprimanta care printeaza ticketul de parcare) care necesita mentenanta sau care presupun folosirea de consumabile;
- ar putea face ca datele sa fie gestionate separat, printr-o baza de date distincta si necorelata cu celelalte date de acces;
- nu permite "by default" functionalitati "cross-site", respectiv corelarea datelor dintre sisteme, fiind necesare integrari.

Daca in cadrul procedurii de achizitie va exista un ofertant care propune un sistem de parking management care nu foloseste consumabile si care are asigurate functionalitati "cross-site", atunci sistemul trebuie acceptat ca fiind unul valid din punct de vedere al cerintelor tehnice.

SISTEM CONTROL ACCES STAND-ALONE

Acestea sunt sistemele clasice de control acces, larg raspandite la nivelul societatii civile si al institutiilor de stat, si reprezinta o solutie acceptabila daca prezinta certificarile necesare pentru astfel de sisteme (ex: ISO 50133).

Sistemele stand-alone functioneaza local, fara sa existe nevoia de conectare la internet sau la furnizori de cloud. Este preferabil insa ca sistemele sa poata fi conectate online pentru:

- Managementul centralizat al sistemului (ex: modificare utilizatori, program de lucru, reguli de acces, etc.);
- Acordarea dreptului de acces la distanta (ex: deschiderea barierei, deblocarea turnichetului), in special pentru locatiile cu trafic redus / ocazional unde alocarea unui agent de securitate nu se justifica din punct de vedere economic.

Un neajuns semnificativ al acestui sistem este faptul ca pentru accesul persoanelor necunoscute (ex: furnizori, vizitatori, etc.) este necesara fie validarea accesului pentru toate operatiunile de intrare/iesire in/din locatie, fie alocarea de carduri de vizitatori pentru perioada in care acestia sunt prezenti in locatie, indiferent daca vorbim de o vizita de scurta durata (ex: vizitatori) sau de lunga durata (ex: contractori care efectueaza lucrari pentru anumite perioade de timp).

SISTEM CONTROL ACCES CU AUTOMATIZARE ACCES SI MANAGEMENT VIZITATORI

Componenta de automatizare a accesului si management al vizitatorilor reprezinta un upgrade al sistemelor de control acces stand-alone, in sensul ca presupune primirea de date din exterior. Prin urmare, aceste sisteme sunt intotdeauna conectate si online.

Din perspectiva tehnica, aceste sisteme prezinta cele mai mari avantaje:

- Reguli de validare a accesului setate in functie de rezident;
- Fluxuri de acces personalizate in functie de tipul de acces si rezident (tin cont de regulile de validare personalizate);
- Sistemul ia decizii singur pentru diferite scenarii, in functie de setarile efectuate;
- Nu necesita interventia personalului de securitate decat din perspectiva cazurilor atipice sau a alertelor.

Un sistem din aceasta categorie actioneaza independent, pe fluxuri distincte si variate, fara a fi nevoie de interventie umana, ceea ce il face un instrument ideal pentru a reduce si mai mult numarul de posturi de paza.

Singurul dezavantaj al acestui sistem este costul suplimentar pentru locatiile de dimensiuni mici, respectiv acele locatii cu un dispozitiv de paza redus numeric (1-2 posturi).

Pentru locatiile de dimensiuni mari sau cu multe puncte de acces, acest sistem este ideal deoarece poate gestiona toate punctele de acces in mod independent si nu este nevoie sa asiguram posturi de paza redundante si nici sa ocupam timpul unui post pentru a trata toate situatiile in care cineva este prezent la punctul de acces si solicita dreptul de a intra in / iesi din locatie.

2.2.3. Paza

Dispozitivul de paza este constituit din unul sau mai multe posturi de paza care au sarcini diverse. Aceste posturi pot fi impartite in mai multe categorii si pot fi inlocuite integral / partial de sisteme, dupa cum urmeaza:

Tip	Scenariu actual	Scenariul alternativ
Perimetru	Detectia accesului neautorizat la nivelul perimetrului se face prin agenti de securitate amplasati in posturi de paza perimetrala care efectueaza patrulari pe zona de interes. Performanta detectiei este in general slaba, mai ales in contextul caracterului critic al obiectivelor.	Se realizeaza prin camere video inteligente cu functii de analiza video (cross-line si human detection). Acopera 100% din zona alocata pentru 100% din timp la parametri maximi de performanta. Sunt influentate de conditiile climatice si se pot defecta.
Acces	Personalul de paza realizeaza operatiunile de inregistrare, validare si acordare al accesului pentru toti vizitatorii, dar si pentru angajati in anumite conditii (ex: invoiri) sau contractori.	Sistemul este intotdeauna automatizat, pe baza de cartela pentru angajati, respectiv pe baza de reguli specifice si coduri de acces pentru non-angajati. Sistemul lucreaza independent si nu necesita interventie umana decat in cazuri speciale. Poarta principala de acces trebuie sa fie in continuare deservita de un agent de securitate care va controla la distanta toate celelalte puncte de acces dinspre exterior.
Monitorizare	Monitorizarea video live exista doar in CET-uri si se realizeaza local, de catre un agent de paza cu rol de dispecer.	Sistemele conectate online permit monitorizarea la distanta de catre un singur dispecer, dar si monitorizarea locala de catre unul dintre agentii din dispozitivul de paza (posibil chiar de catre postul

Tip	Scenariu actual	Scenariul alternativ
		de la punctul principal de acces ca urmare a faptului ca interventiile pe zona de acces sunt limitate). La modul ideal, dispeceratul central este responsabil de functia de monitorizare, iar monitorizarea locala se face prin cumul, de catre un agent de securitate, pe momente punctuale (ex: pauza dispecer central, lipsa conectivitate la dispeceratul central, etc.).
Reactie	Fiecare post actioneaza pe zona de responsabilitate si poate beneficia de ajutorul altor agenti de securitate, sub coordonarea sefului de tura sau de obiectiv.	Este necesar ca la nivelul CET-urilor sa existe posturi de paza mobile pentru a asigura o reactie imediata. In cazul in care forta de raspuns nu este suficienta, precum si in cazul locatiilor de mici dimensiuni care sunt deservite in prezent de 1-2 posturi de paza, trebuie angajata forta de raspuns suplimentara / externa, respectiv servicii de interventie rapida.
Conducere	Legea obliga la constituirea unui post de sef de tura pentru toate dispozitivele de paza care cuprind mimim 12 de persoane. Acest sef de tura asigura managementul de prima linie, operational, timp de 24 ore/zi. Managementul general, relationarea cu autoritatile, etc., sunt asigurate de seful de obiectiv.	Majoritatea dispozitivelor de paza ar putea fi redimensionate astfel incat sa fie sub pragul pentru care este necesar seful de tura. Conducerea operationala in cazul producerii unor incidente de securitate va fi asigurata de catre dispecerul care monitorizeaza sistemul de supraveghere video. In continuare, seful de obiectiv trebuie pastrat, atat pentru nevoi pe linie administrativa, cat si pentru relationarea cu autoritatile si Electrocentrale Bucurest SA.
Altele	N/A	N/A

Trebuie precizat ca fiecare obiectiv din categoria CET ar trebui sa aiba in componenta cel putin urmatoarele posturi:

- **Acces** - un post de acces la punctul principal de acces acesta avand posibilitatea sa monitorizeze camerele video de pe zona de acces si sa trateze cazurile deosebite (ex: numar inmatriculare citit gresit);
- **Monitorizare** - nu este necesar un post dedicat la nivelul obiectivului deoarece agentul din punctul de acces poate face prin cumul activitatea, cu conditia de a avea dotarea necesara;
- **Perimetru** - nu este necesar nici un post pe perimetru deoarece detectia se face in mod automat;
- **Interventie** - este necesar ca fiecare locatie sa aiba 1 sau 2 posturi mobile, eventual dotate cu mijloc de interventie rapida (ex: scooter, ATV, auto de serviciu) in functie de dimensiunea obiectivului si timpul de interventie estimat pana la cel mai indepartat punct de pe perimetru. Acest post va acoperi si situatiile deosebite aparute pe linia perimetrului (ex: camere defecte) sau la nivelul punctelor de acces (ex: automatizare nefunctionala sau camere LPR defecte, etc.);
- **Sef de tura** - necesar doar acolo unde dispozitivul depaseste 12 persoane si poate fi unul dintre posturile mobile.

Planurile de contingenta pe linie de securitate fizica trebuie sa prevada si situatii cu totul speciale (ex: sisteme nefunctionale in proportie insemnata si pentru o perioada de timp semnificativa), motiv pentru care ar trebui bugetate un numar de ore suplimentare care vor fi sau nu folosite, in functie de situatia din teren. Un astfel de necesar nu poate fi estimat, dar apreciem ca un numar de 6000 ore/an ar trebui sa fie acoperitoare.

Contractul cu firma de prestari servicii de paza ar trebui sa prevada obligativitatea asigurarii surplusului de personal pentru situatii deosebite in termen de maxim 12 ore.

2.2.4. Monitorizare

Din punct de vedere al monitorizarii, este recomandat ca serviciul sa fie organizat astfel:

- Un post permanent de monitorizare (dispecer central), cu sarcini de monitorizare ale tuturor locatiilor;
- Dispecer de monitorizare local care sa preia monitroizarea in anumite momente (ex: pauza de masa dispecer central, lipsa conexiune la internet, etc.).

Dispecerul central poate asigura singur functia de monitorizare pentru toate locatiile tinand cont de urmatoarele elemente:

- Sistemul filtreaza alertele false si genereaza un numar relativ mic de alerte intr-un interval de 24 ore care pot fi usor tratate de o singura persoana;

- Standardul IGPR pentru dispeceratele de efractie este de 1 dispecer pentru primele 1500 de obiective si cate 1 dispecer suplimentar pentru fiecare 1000 de obiective suplimentare (Electrocentrale Bucuresti SA este mult sub aceste valori, chiar daca vom considera fiecare camera ca fiind echivalentul unui obiectiv);
- Sistemul este capabil sa invete si sa se adapteze datorita functiilor de AI ceea ce inseamna ca in timp numarul de alarme false va fi si mai mic;
- Daca numarul de alarme este mult prea mare in anumite momente, atunci pot fi folositi dispecerii locali pentru a degreva dispecerul central de anumite locatii astfel incat sa poata fi eficient.

In ceea ce priveste dispecerul local, conform analizei noastre nu este necesar a se infiinta un post de monitorizare local dedicat din urmatoarele considerente:

- Exista deja monitorizare centralizata ceea ce inseamna ca necesarul de monitorizare local este limitat pe zona de acces si pe situatiile de indisponibilitate a monitorizarii centrale (ex: lipsa conexiune, pauza de masa dispecer central);
- Chiar si in cazul in care dispecerul local ar trebui sa preia monitorizarea obiectivului pentru o perioada mai indelungata (ex: pentru cateva zile sau chiar saptamani), sistemul se automonitorizeaza si ridica alerte iar dispecerul va trata alertele punctual (le va califica ca fiind false sau reale si va coordona raspunsul in caz de alerta reala);
- Gestionarea accesului este la randul ei automatizata iar agentul de securitate va trata strict exceptiile sau situatiile deosebite de unde rezulta ca incarcarea sa va fi limitata, cu exceptia unor momente punctuale (ex: schimb de tura) cand ar trebui sa beneficieze de suport din partea posturilor mobile.

2.2.5. Interventie rapida

In privinta interventiei rapide avem 2 situatii distincte: cea pentru obiectivele unde nu exista servicii de paza, respectiv cea pentru obiectivele unde exista astfel de servicii.

Pentru locatiile de mici dimensiuni, unde nu exista servicii de paza, este necesar a se contracta interventie rapida externa pentru a asigura un raspuns adecvat in cazul aparitiei unui incident real de securitate.

Pentru celelalte locatii, respectiv cele care au servicii de paza (cum ar fi CET-urile), interventia se va face cu personalul din dispozitivul propriu de paza si, daca acest lucru este insuficient, se va apela la interventia rapida externa (similar cu obiectivele mici), respectiv la serviciul SNUAU - 112 (Sistemul National Unic pentru Apeluri de Urgenta) pentru cazurile cu adevarat speciale.

2.2.6. Mentenanta

Schimbarea paradigmei de securitate pune un accent foarte mare pe componenta tehnica, aceasta fiind prima veriga in lantul logic de protectie deoarece prin intermediul sistemelor tehnice de securitate se face detectia cazurilor potential periculoase. Functionarea

necorespunzatoare a sistemelor creeaza brese in sistemul de protectie, ceea ce reprezinta vulnerabilitati care ar putea fi exploatate de elemente interesate cu impact asupra companiei sau publicului larg.

Prin urmare, este imperios necesar ca aceste sisteme sa functioneze la parametri optimi iar intreruperile sa fie de foarte mica durata. Pentru asigurarea unui nivel optim, se recomanda implementarea urmatoarelor masuri:

- Efectuarea mentenantei semestriale in locatiile nefunctionale / in conservare, respectiv trimestriale in toate locatiile functionale, avand in vedere mediul industrial in care sunt amplasate echipamentele;
- Asigurarea unui stoc tampon / de rezerva cu echipamentele care ar putea produce un impact semnificativ si care sunt pretabile sa se defecteze usor (ex: router, camere video de perimetru, camere video perimetrale, brat bariera);
- Asigurarea unui SLA de maxim 24 ore pentru furnizorul de servicii de mentenanta (termenul fiind si cel prevazut de legislatia in vigoare pentru interventia initiala on site);
- Asigurarea bugetului de paza suplimentar prevazut la subcapitolul de paza si care ar putea fi folosit in situatii deosebite.

2.2.7. Managementul securitatii

Noul concept de securitate poate fi definit ca "data driven security" ceea ce inseamna ca se bazeaza pe date pe care le genereaza prin infrastructura proprie, precum si prin activitatile curente ale personalului de securitate.

Impactul este unul semnificativ si necesita redesenarea cadrului organizatoric intern astfel incat sa tina cont de si sa fie aliniat cu aceasta noua strategie. Am impartit functia de management al securitatii intr-o componenta de reglementare (guvernanta) si una de operatii (management operational).

GUVERNANTA

Arhitectura de guvernanta propusa integreaza tehnologia avansata cu factorul uman critic (**Human in the Loop**), fiind sustinuta de trei piloni fundamentali care asigura eficienta operationala si conformitatea:

1. Automatizarea si Orchestrarea Raspunsului

Prin utilizarea unor fluxuri de lucru (workflows) predefinite, sistemul filtreaza automat "zgomotul" (alarmele false) si coreleaza evenimente disparate. Automatizarea nu elimina operatorul, ci ii livreaza acestuia doar incidentele calificate care necesita atentie, reducand oboseala decizionala si timpii de reactie. In acest sens, trebuie create politici si proceduri (sau modificate cele actuale), astfel incat modul de actiune si raspuns sa plece de la realitatile noului sistem de protectie.

2. Trasabilitatea Totală (Audit Trail)

Intr-un sistem guvernat prin date, nimic nu este efemer. Orice schimbare de stare a unui senzor, orice modificare a parametrilor de sistem si, crucial, orice actiune umana, este inregistrată ireversibil. Această trasabilitate granulara transforma investigatia post-incident dintr-o presupunere intr-o analiza factuala.

3. Alocarea Raspunderii (Accountability)

Principiul *Human in the Loop* este eficient doar daca responsabilitatea este clar definita. Tehnologia semnaleaza anomalia, dar guvernanta impune cine trebuie sa reactioneze si in ce interval de timp (SLA). Sistemul digitalizeaza lantul de comanda: dispecerul care preia alarma, agentul care se deplaseaza in teren si managerul care valideaza inchiderea incidentului sunt toti parti ale aceluiasi sistem integrat de monitorizare si raspuns / reactie. Astfel, alocarea raspunderii este automata si transparenta, eliminand ambiguitatea in cazul unor brese de securitate.

In concluzie, adoptarea guvernantei in contextul Data-Driven Security asigura faptul ca sistemul de securitate fizica este auditabil, predictibil si capabil sa ofere o imagine operatională clara, unde tehnologia amplifica capabilitatile umane, iar omul ramane decidentul final informat.

MANAGEMENTUL OPERATIONAL

Din punct de vedere al activitilor concrete, distingem doua niveluri separate de management, respectiv:

- Front line management - asigurat de personalul din dispozitivul de paza in cadrul activitatii curente si in conformitate cu sarcinile alocate prin consemnul particular din planul de paza, respectiv procedurile de lucru interne;
- Supervisory management - asigurat de managerul de securitate care are rolul de a asigura performanta optima a fiecarei componente a sistemului de protectie (uman, tehnic, procedural) si de a trata cazurile deosebite (incidente de securitate, performanta necorespunzatoare, etc.).

Pentru masurarea performantei, managerul de securitate trebuie sa dezvolte indicatori de performanta si instrumente adecvate pentru masurarea acestor indicatori. Spre exemplu, este recomandat sa fie masurati indicatori precum:

- **Awarness time** - timpul care a trecut de la producerea unui eveniment relevant pe linie de securitate si pana cand acesta a fost preluat de personalul desemnat spre rezolvare;



- **Reaction time** - timpul care s-a scurs din momentul in care a fost sesizat evenimentul si pana cand a avut loc prima interventie on site (acolo unde este necesara o astfel de interventie);
- **Resolve time** - timpul care a trecut de la momentul in care un incident a fost sesizat si pana cand acesta a fost rezolvat;
- **Downtime** - timpul total de nefunctionare al sistemelor care ar trebui comparat cu un SLA asumat contractual cu furnizorii de servicii.

2.2.8. Date

Intr-o arhitectură *Data-Driven Security*, datele (fluxuri video, log-uri de acces, evenimente generate de sisteme) devin cel mai valoros activ. Integritatea sistemului de securitate fizica depinde in mod critic de masurile de igiena cibernetica implementate. Guvernanta datelor trebuie să adreseze cele patru dimensiuni cardinale ale securitatii informatiei (CIA + A), fiecare avand riscuri specifice si contramasuri obligatorii, conform celor descrise mai jos:

1. Confidentialitate (Confidentiality)

- **Riscul asociat: Data Breach (Acces neautorizat la date)** - aceasta implica expunerea datelor cu caracter personal (GDPR) sau a celor sensibile pentru securitate cum ar fi date privind functionarea sistemelor, amplasarea senzoristicii, parametrii de functionare, loguri, etc.
- **Masuri minimale** - implementarea criptarii datelor atat in tranzit (VPN, HTTPS/TLS pentru camere si controlere), cat si in repaus (stocare criptata), cel putin pentru comunicarea din afara retelei locale. Aplicarea stricta a principiului *Least Privilege* (fiecare operator vede doar camerele necesare rolului sau).

2. Integritate (Integrity)

- **Riscul asociat: Alterarea Datelor (Tampering/Corruption)** - acesta este un risc critic in investigatii deoarece o persoana interesata ar putea sterge sau modifica date pentru a ascunde o fapta (mascarea urmelor);
- **Masuri minimale:** Restrangerea drepturilor utilizatorilor, generarea de backup-uri si colectarea de loguri cat mai detaliate cu privire la modul de utilizare al platformelor.

3. Disponibilitate (Availability)

- **Riscul asociat: DDoS (Denial of Service) / Sabotaj** - sistemul poate deveni indisponibil ca urmare a unor actiuni rau intentionate care vizeaza intreruperea comunicarii intre senzorii din teren si serverul central, generarea unui flux mare de date cu scopul de a bloca capacitatea de procesare, etc;

- **Masuri minimale:** Segmentarea retelei (VLAN dedicat strict securitatii, separat de reteaua office), redundanta hardware (servere de failover) si monitorizarea continua a starii de sanatate a dispozitivelor (heartbeat monitoring).

4. Raspundere (Accountability)

- **Riscul asociat: Repudierea (Repudiation)** - riscul ca un operator sau administrator sa nege efectuarea unei actiuni critice (ex: "Nu eu am dezactivat alarma"), iar sistemul sa nu poata dovedi contrariul din cauza folosirii conturilor comune;
- **Masuri minimale** - eliminarea conturilor generice (ex: "admin", "user1"), implementarea Autentificarii Multi-Factor (MFA) pentru accesul la zonele sensibile si jurnale de audit care inregistreaza cine, ce modifcare a facut, respectiv din ce valoare in ce valoare.

In concluzie, convergenta dintre securitatea fizica si cea cibernetica este totala. Protectia datelor generate de sistemele de securitate nu este doar o cerinta IT, ci o conditie operațională obligatorie pentru validitatea si legalitatea intregului lant de securitate.

Anexa nr. 5

Lista experților principali solicitați

Ofertantul trebuie să prezinte o echipă care să conțină cel puțin următorii experți principali.
Proiect similar. Pentru toți experții, prin proiect similar se înțelege un proiect în cadrul căruia s-a proiectat un sistem de securitate integrat care a inclus: infrastructură hardware și software specifică, echipamente de comunicații, sistem de vizualizare de tip video wall, platformă software de management video (VMS), analiză video ca parte a sistemului de securitate, precum și dimensionarea unui dispecerat.

1. Manager de proiect – 1 persoană

Responsabilități principale:

- organizează și asigură bunul mers al activităților desfășurate de echipa contractantului în cadrul proiectului;
- asigură interfața cu persoanele care participă la execuția contractului din partea Autorității Contractante, cu care colaborează pe întreaga durată a contractului pentru armonizarea solicitărilor acesteia cu soluțiile tehnice propuse de ceilalți experți;
- răspunde de managementul contractului conform metodologiei agreate cu Autoritatea Contractantă, respectiv de planificarea, monitorizarea, controlul și încheierea contractului;
- asigură coordonarea echipei de implementare a contractului;
- menține și aplică managementul riscurilor și procedurile de asigurare a calității;
- alocă resursele astfel încât contractantul să răspundă optim necesităților, constrângerilor și obiectivelor Autorității Contractante;
- asigură elaborarea proceselor-verbale de recepție, a rapoartelor de activitate și a celorlalte documente de raportare a progresului.

Cerințe minime:

- studii superioare absolvite cu diplomă de licență în unul din domeniile telecomunicațiilor, electronicii, radiocomunicațiilor, automaticii, calculatoarelor, ingineriei electrice sau într-un domeniu similar;
- certificat profesional în management de programe sau management de proiecte, probat prin diplomă/certificat recunoscut național sau internațional ori alte documente care dovedesc certificarea;
- experiență generală: minimum 5 ani;
- experiență specifică: participarea în cel puțin trei proiecte similare, în care să fi desfășurat activități similare poziției pentru care este propus.

2. Proiectant coordonator sisteme de securitate – 1 persoană

Responsabilități principale:

- coordonează întreaga echipă tehnică, cu alocarea sarcinilor pe fiecare membru;
- asigură resursele pentru executarea serviciilor de proiectare cuprinse în specificațiile tehnice;
- coordonează elaborarea și validarea soluției tehnice, a arhitecturii de sistem, a documentației de proiectare și a specificațiilor tehnice aferente componentelor;
- asigură corelarea și integrarea activităților echipelor de software, hardware, comunicații, securitate, instalații și infrastructură;
- urmărește respectarea standardelor, normativelor, reglementărilor și bunelor practici aplicabile;

- gestionează modificările tehnice, analizează impactul acestora asupra soluției, termenelor, resurselor și livrabilelor și formulează recomandări managerului de proiect;
- întocmește rapoartele tehnice cerute de proiect sau de managerul de proiect.

Cerințe minime:

- studii superioare absolvite cu diplomă de licență în unul din domeniile telecomunicațiilor, electronicii, radiocomunicațiilor, automaticii, calculatoarelor, ingineriei electrice sau într-un domeniu similar;
- certificat profesional privind competențele de inginer/proiectant sisteme de securitate, acreditat de Ministerul Educației Naționale, probat prin diplomă/certificat recunoscut național sau internațional ori alte documente doveditoare;
- certificat profesional privind competențele de manager de securitate, acreditat de Ministerul Educației Naționale, probat în același mod;
- aviz I.G.P.R. în conformitate cu Legea nr. 333/2003, actualizată;
- experiență generală: minimum 5 ani;
- experiență specifică: participarea în cel puțin trei proiecte similare, în care să fi desfășurat activități similare poziției pentru care este propus.

3. Proiectant sisteme de securitate – 2 persoane

Responsabilități principale:

- efectuează releveele în obiective și colectează datele necesare proiectării: perimetru, puncte de acces, sisteme de securitate existente, centrale de detecție la incendiu, trasee de cabluri, spații tehnice;
- elaborează, sub coordonarea proiectantului coordonator, soluțiile de principiu și documentația PT + DE pentru supravegherea video și analiza video, detecția perimetrală, controlul accesului și managementul vizitatorilor, detecția la efracție, integrarea monitorizării detecției la incendiu și dispeceratele;
- stabilește amplasarea echipamentelor și nivelurile de performanță ale supravegherii video (detecție, observare, recunoaștere, identificare) și realizează breviarele de calcul pentru acoperire, stocare și lățime de bandă;
- elaborează planurile de amplasare, schemele bloc, schemele de principiu și detaliile de execuție pentru subsistemele de securitate;
- definește integrarea subsistemelor în platforma de management centralizat, regulile de transmitere și tratare a evenimentelor pe cele trei niveluri de monitorizare și măsurile de securitate cibernetică aferente;
- proiectează soluțiile pentru echipamentele amplasate în zone cu pericol de atmosferă explozivă, cu respectarea cerințelor specifice;
- elaborează caietele de sarcini, specificațiile tehnice neutre și listele de cantități pentru subsistemele de securitate;
- întocmește documentația pentru avizarea de către organele de poliție, conform H.G. nr. 301/2012, și o susține împreună cu proiectantul coordonator;
- răspunde observațiilor verificatorilor de proiecte și ale comisiei tehnico-economice a beneficiarului și operează modificările necesare.

Responsabilitățile se pot împărți între cei doi proiectanți pe subsisteme sau pe obiective, conform organizării prezentate în propunerea tehnică.

Cerințe minime:

- studii superioare absolvite cu diplomă de licență în unul din domeniile telecomunicațiilor, electronicii, radiocomunicațiilor, automaticii, calculatoarelor, ingineriei electrice sau într-un domeniu similar;
- certificat profesional privind competențele de inginer/proiectant sisteme de securitate, acreditat de Ministerul Educației Naționale, probat prin diplomă/certificat recunoscut național sau internațional ori alte documente doveditoare;
- aviz I.G.P.R. în conformitate cu Legea nr. 333/2003, actualizată;

- electrician autorizat ANRE, grad minim IIA, care conferă dreptul de proiectare a instalațiilor electrice cu orice putere instalată tehnic realizabilă, la o tensiune nominală mai mică de 1 kV;
- atestat privind capacitatea de proiectare a instalațiilor în spații industriale cu pericol de atmosferă explozivă, emis de INSEMEX;
- experiență generală: minimum 5 ani;
- experiență specifică: participarea în cel puțin trei proiecte similare, în care să fi desfășurat activități similare poziției pentru care este propus.

4. Expert instalații electrice – 1 persoană

Responsabilități principale:

- efectuează releveul instalațiilor electrice existente în obiective: puncte de alimentare, tablouri, rețele, iluminat existent, instalații de legare la pământ;
- proiectează alimentarea electrică a tuturor echipamentelor sistemului de securitate: tablouri, circuite, surse neîntreruptibile și surse de rezervă, cu stabilirea autonomiei;
- proiectează sistemul de iluminat al perimetrului, al punctelor de acces și al zonelor de interes, corelat cu cerințele supravegherii video, inclusiv comanda automată și comanda din platforma centralizată;
- realizează breviarele de calcul pentru instalațiile electrice: bilanț de puteri, dimensionarea cablurilor și a protecțiilor, căderi de tensiune, calcule luminotehnice;
- proiectează instalațiile de legare la pământ și de protecție împotriva supratensiunilor și a trăsnetului pentru echipamentele exterioare (stâlpi, console, camere);
- elaborează traseele de cabluri și canalizații și detaliile de execuție pentru stâlpi, fundații și treceri;
- asigură corelarea soluțiilor electrice cu instalațiile existente și cu cerințele de exploatare ale centralelor, inclusiv în zonele cu pericol de atmosferă explozivă;
- elaborează caietele de sarcini, specificațiile tehnice și listele de cantități pentru lucrările de instalații electrice și iluminat;
- răspunde observațiilor verificatorilor de proiecte și ale comisiei tehnico-economice a beneficiarului și operează modificările necesare.

Cerințe minime:

- studii superioare absolvite cu diplomă de licență în unul din domeniile telecomunicațiilor, electronicii, radiocomunicațiilor, automaticii, calculatoarelor, ingineriei electrice, energetic sau într-un domeniu similar;
- electrician autorizat ANRE, grad minim IIIA, care conferă dreptul de proiectare a instalațiilor electrice cu orice putere instalată tehnic realizabilă, la o tensiune nominală mai mică de 20 kV;
- experiență generală: minimum 5 ani;
- experiență specifică: participarea în cel puțin trei proiecte similare, în care să fi desfășurat activități similare poziției pentru care este propus.

5. Condiții referitoare la calificarea experților

5.1. Prestatorul va prezenta în ofertă informații privind modul de asigurare a execuției tuturor operațiunilor în conformitate cu reglementările legale în ceea ce privește avizele I.G.P.R. pentru personalul calificat, conform art. 80 din H.G. nr. 301/2012.

5.2. Pentru fiecare expert principal, ofertanții vor prezenta în propunerea tehnică:

- CV în format Europass;
- copii ale documentelor care demonstrează îndeplinirea cerințelor privind studiile, expertiza și experiența specifică: diplome de studii, certificări în termen de valabilitate la data depunerii ofertei, alte diplome relevante; recomandări emise de beneficiarul final al proiectului, semnate sau contrasemnate de autoritatea contractantă ori de beneficiarul privat în calitate de beneficiar final, sau alte documente edificatoare din care să reiasă activitățile desfășurate și experiența specifică similară;

- declarație de disponibilitate semnată de persoana propusă, dacă aceasta nu este angajată a ofertantului.

5.3. Autoritatea Contractantă își rezervă dreptul de a verifica exactitatea informațiilor și a dovezilor furnizate, de a solicita alte documente sau informații care să clarifice experiența echipei propuse și de a contacta beneficiarii finali ai proiectelor prezentate, pentru confirmare.
5.4. Nu se acceptă îndeplinirea cerințelor minime aferente unui expert prin cumul de către mai multe persoane.
5.5. Experții principali semnează declarații individuale de disponibilitate pe întreaga perioadă de derulare a contractului, în două exemplare, unul pentru contractant și unul pentru Autoritatea Contractantă.
5.6. Autoritatea Contractantă poate solicita înlocuirea experților principali pe perioada derulării contractului, pe baza unei cereri scrise, motivate și justificate, dacă apreciază că un membru al personalului prestatorului este ineficient sau nu își îndeplinește sarcinile la nivelul cerințelor stabilite. Înlocuirea respectă prevederile art. 162 alin. (1) lit. b) din H.G. nr. 395/2016.
5.7. Toate costurile generate de înlocuirea experților principali sunt în sarcina exclusivă a prestatorului. Dacă un expert principal nu este înlocuit imediat, Autoritatea Contractantă poate solicita desemnarea unui înlocuitor temporar sau alte măsuri care să compenseze absența. Autoritatea Contractantă nu efectuează nicio plată pentru perioada absenței expertului principal sau a înlocuitorului acestuia, termenul de plată decalându-se corespunzător.
5.8. Experții nerezidenți pot prezenta certificările și autorizările corespunzătoare emise în țara de rezidență, în copie, însoțite de traducerea autorizată în limba română.

Anexa 6

ANEXĂ DE SECURITATE

LA CONTRACTUL NR. _____ din _____

1. Data întocmirii: _____

2. Beneficiar (Contractor) : _____, cu adresa/sediul în Bucureşti, str. _____, înregistrată la Registrul Comerţului sub nr. _____, C.U.I.: _____, reprezentată prin director general _____.

3. Contractant: _____, adresa/sediul în _____, înregistrată la Registrul Comerţului sub nr. _____, cod fiscal _____, cont virament nr. _____, deschis la _____, reprezentată prin _____.

4. Perioada de derulare a prevederilor anexei de securitate:

- început: intră în vigoare după semnarea acesteia de către reprezentanţii autorizaţi ai părţilor contractante.

- sfârşit: după predarea tuturor documentelor clasificate puse la dispoziţie de contractor sau generate de contractant.

5. Nivelul de clasificare a parţilor contractului, conform art. 203, din H.G.R. 585/2002 , este „SECRET DE SERVICIU"

6. Anexe:

- Anexa nr. 1 - Lista personalului autorizat, aparţinând contractantului/subcontractantului, care va avea acces la informaţii clasificate ce vor fi utilizate în derularea contractului.

- Anexa nr. 2 - Lista locurilor de execuţie a activităţilor în care se utilizează date şi informaţii clasificate.

- Anexa nr. 3 - Caietul de sarcini privind protecţia informaţiilor clasificate.

BENEFICIAR **CONTRACTANT**

Director general _____ _____

VIZAT

Şeful Structurii de Securitate _____ *Funcţionar de securitate* _____

NOTĂ: În cazul subcontractării unor activităţi protejate, este obligatoriu ca şi aceste contracte să conţină anexe de securitate care să fie avizate şi aprobate de responsabilul de contract al părţii contractoare.

Anexa nr. 6.1

LISTA PERSONALULUI AUTORIZAT,
APARȚINÂND _____, CARE VA AVEA ACCES LA INFORMAȚII CLASIFICATE SECRETE DE SERVICIU, CE VOR FI UTILIZATE ÎN DERULAREA CONTRACTULUI.

Nr. crt.	Numele și prenumele	Funcția	Autorizația de acces la IC SSv	
			Seria și nr.	Perioada de valabilitate
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

**Această listă va fi actualizată permanent, iar modificările vor fi notificate părții contractoare.*

VIZAT

Șeful Structurii de Securitate _____ *Funcționar de securitate* _____

Anexa nr. 6. 2

LISTA LOCURILOR DE EXECUȚIE A ACTIVITĂȚILOR ÎN CARE SE UTILIZEAZĂ DATE ȘI INFORMAȚII CLASIFICATE

A. Locurile de desfășurare a activităților de documentare:				
Nr. crt.	**Categorii de personal/nr.persoane**	**Activitățile/Informațiile necesar a fi protejate**	**Nivel de secretizare**	**Observații**
1	- Ingineri de specialitate - Tehnicieni	- Planul de dispunere a echipamentelor .....; - Shema bloc si conexiuni pentru	Secret de serviciu	1. În zona administrativa de la sediul SC _____ Bucuresti, str. _____ 2. În zona administrativă, in locația unde sunt instalate echipam., desemnată de catre beneficiarul de exploatare, prin gestionarul de documente clasificate al acestuia
B. Locul unde se pastrează informații clasificate				
Nr. crt.	**Categorii de personal/nr.persoane**	**Activitățile/Informațiile necesar a fi protejate**	**Nivel de secretizare**	**Observații**
2	- Gestionar documente clasificate	- Planul de dispunere a echipamentelor pentru .....; - Shema bloc si conexiuni pentru	Secret de serviciu	În zona administrativa de la sediul SC _____
C. Locul unde se întrebuințează sistemele de prelucrare automată a datelor				
Nr. crt.	**Categorii de personal/nr.persoane**	**Activitățile/Informațiile necesar a fi protejate**	**Nivel de secretizare**	**Observații**
3	- Ingineri de specialitate - Tehnicieni	Proiectare/stocare - oferta tehnică și financiara - planuri/scheme/detalii de execuție (daca este cazul)	Secret de serviciu	În zona administrativa de la sediul SC _____

**Această listă va fi actualizată permanent, iar modificările vor fi notificate părții contractoare.*

VIZAT

Șeful Structurii de Securitate _____ *Funcționar de securitate* _____

Anexa nr 6.3

CAIETUL DE SARCINI
PRIVIND PROTECȚIA INFORMAȚIILOR CLASIFICATE

1. Obiectul caietului de sarcini îl constituie asigurarea protecției informațiilor clasificate secret de serviciu ce urmează a fi gestionate pe parcursul derulării prezentului contract.

2. Activitățile ce urmează a fi desfășurate în derularea prezentului contract presupun accesul la informații clasificate secret de serviciu. Divulgarea neautorizată a unor astfel de informații poate aduce prejudicii _____ și beneficiarului de exploatare.

2.1. Activități ce presupun acces la informații clasificate

Nr. crt.	**Denumirea activităților**	**Nivelul de clasificare al informațiilor**	**Observații**
1.	Transportul documentelor clasificate	Secret de serviciu	
4.	Managementul documentelor clasificate	Secret de serviciu	

2.2. Lista clasificărilor de securitate (LCS)

Nr. crt.	**Descrierea succintă a conținutului documentului/ Nr. înregistrare document**	**Nivelul de clasificare**	**Observații**
1.	Planul de dispunere a echipamentelor pentru .....;	Secret de serviciu	
2.	Shema bloc si conexiuni pentru extindere sistem	Secret de serviciu	
3.	Planuri/scheme/detalii de execuție (daca este cazul)	Secret de serviciu	
4.	Oferta tehnică și financiara (daca este cazul)	Secret de serviciu	

2.3. Informațiile clasificate, puse la dispoziție pentru documentare de către beneficiar precum și cele generate de contractant, indiferent de formă sau suport fizic, se vor gestiona în zone administrative conform reglementărilor în vigoare.

2.4. Nivelul de clasificare al informațiilor și măsurile de protecție al acestora ce fac obiectul prezentului caiet de sarcini nu pot fi modificate, iar respectivele informații diseminate decât cu acordul contractorului.

2.5. Beneficiarul va gestiona informații în format electronic/ fizic secret de serviciu doar în cadrul Sistemului Informatic propriu acreditat de prelucrare automată a datelor.

3. Obligațiile beneficiarului:

a. desemnează o persoană din cadrul SC _____ responsabilă cu implementarea și supervizarea măsurilor de securitate legate de contract;

b. notifică în timp util, către Beneficiar, numarul de înregistrare al Programului Propriu de Prevenire a Scurgerii de Informații Clasificate, avizat de Autoritatea Desemnată de Securitate;

c. menține permanent legătura cu Structura de Securitate a _____ și cu reprezentantul beneficiarului de exploatare în vederea asigurării faptului că toate informațiile clasificate gestionate în cadrul contractului vor fi protejate corespunzător;

d. păstrează evidența angajaților implicați în derularea contractului, care au fost autorizați să aibă acces la informații clasificate;

e. interzice accesul la informațiile clasificate gestionate în cadrul contractului acelor persoane ce nu au fost autorizate în conformitate cu legislația în vigoare;

f. respectarea principiului „necesității de a cunoaște" în ceea ce privește diseminarea informațiilor clasificate gestionate în cadrul contractului;

g. comunică Structurii de Securitate a _____ și reprezentantului beneficiarului de exploatare orice încălcări sau posibile încălcări ale măsurilor de securitate, acte de sabotaj ori activități subversive, orice informații care pot genera neîncredere față de angajat, orice schimbări ale acționariatului sau managementului firmei, orice schimbări care afectează statutul de securitate al firmei;

h. notifică în timp util, către Beneficiar, orice modificare survenită în Anexa nr. 7.1 si Anexa nr. 7.2 a prezentului document;

i. nu va utiliza, fără acordul Structurii de Securitate a _____, informațiile clasificate ce i-au fost încredințate sau care sunt generate pe parcursul derulării contractului, decât pentru scopul specific al contractului;

k. stabilește și apoi implementează proceduri coerente privind măsurile de securitate necesare în ceea ce privește accesul, manipularea, transmiterea și stocarea informațiilor clasificate și asigură disponibilitatea, confidențialitatea și integritatea acestora.

l. va returna Structurii de Securitate a _____ PS toate informațiile și materialele clasificate ce i-au fost încredințate sau care sunt generate pe parcursul derulării contractului sau sub-contractului (inclusiv suporții de informație care au fost utilizați pentru gestionarea informațiilor clasificate), cu excepția cazurilor în care acestea au fost distruse cu acordul Structurii de Securitate a _____ sau păstrarea a fost autorizată de către aceasta. Informațiile și materialele clasificate vor fi returnate într-o perioadă de timp ce va fi stabilită de reprezentantul Structurii de Securitate a _____.

6. Contractul se execută în condițiile respectării prevederilor H.G.R. nr. 585/2002 și H.G.R. nr. 781/2002 iar accesul la informații clasificate secrete de serviciu este permis numai după notificarea, către Beneficiar, a numarului de înregistrare al Programului S.C. _____ de Prevenire a Scurgerii de Informații Clasificate, avizat de Autoritatea Desemnată de Securitate;

VIZAT

Șeful Structurii de Securitate _____ *Funcționar de securitate* _____

Anexa 7

Formularul propunerii financiare

Nr. Crt.	Denumirea serviciului	Cantitate	Prețul unitar fără TVA	Prețul Total fără TVA	Prețul Total cu TVA
		Cpl.	RON	RON (Col.2 x Col.3)	RON (Col.4 x 1.21)
0	1	2	3	4	5