SCHEMA PER LA CERTIFICAZIONE DI

OT CYBER SECURITY EXPERT

Rev.	Data	Motivazione	Convalida	Approvazione
0	31.03.2021	1° emissione	*Presidente CSI/Schema*	*Amministratore Delegato*

1. SCOPO E CAMPO DI APPLICAZIONE

Questo documento ha lo scopo di regolare i rapporti intercorrenti tra CEPAS, che opera quale organismo di certificazione del personale, e le persone fisiche che richiedono la certificazione volontaria di terza parte delle proprie competenze in qualità di "OT Cyber security expert secondo lo standard IEC 62443".
La certificazione si applica alla persona fisica che ne fa richiesta; non è quindi applicabile ad aziende/organizzazioni.
Per lo svolgimento dell'attività di certificazione, CEPAS effettua, a propria scelta, la valutazione diretta dei candidati oppure si avvale di Organismi di Valutazione esterni da essa selezionati, qualificati e approvati, secondo Procedura PG70, in quanto provvisti di adeguati locali, attrezzature, strumentazione e personale tecnico per lo svolgimento delle attività tenuti sotto controllo da parte di CEPAS. Può essere approvato un numero illimitato di organismi di valutazione.

2. PROFILO DELLA FIGURA PROFESSIONALE

L'OT cyber security expert, indipendentemente dalla tipologia di clienti (persona, gruppi, organizzazioni) e dai contesti di intervento eroga l'attività sia in forma di libero professionista che di risorsa interna alle organizzazioni. La diffusione della figura è prevalente nei settori di produzione in qualunque campo ove vi siano delle reti di comunicazione dedicate ai sistemi e processi di produzione.

La diffusione della figura di OT cyber security expert sta diventando sempre maggiore date le evoluzioni del settore produttivo. Con l'avvento della filosofia Industria 4.0 tutte le macchine ed i sistemi di produzione devono poter essere interconnessi, integrati e telemanutenuti. Questo fa sì che gli aspetti di security legati a minacce e vulnerabilità dei sistemi e dei dispositivi di automazione diventino sempre più un punto aperto e che deve essere affrontato.

Si rende pertanto necessario che esista una figura, esattamente come già esiste per i sistemi ICT, che abbia in carico la gestione del rischio di cyber attacco direttamente sul mondo della produzione, e sia in grado di valutare, intervenire e mitigare il rischio oltre che le conseguenze di eventuali attacchi. Sul piano professionale, l'esperto deve avere una chiara competenza relativamente ai sistemi di automazione industriale, con particolare conoscenza delle diverse architetture utilizzate nei vari ambiti industriali (DCS, PLC, SCADA, ecc.) e delle tematiche relative alla comunicazione industriale (fieldbus seriali e Ethernet based).

L'OT cyber security expert deve dimostrare di possedere le competenze relative alle seguenti attività legate alla security di un sistema di automazione industriale (IACS = Industrial Automation and Control System): valutazione del rischio, identificazione dei perimetri e dei conduit, definizione di strategie di protezione, definizione dei Security Level (SL) target per ciascun Functional Requirement (FR) del sistema, implementazione delle procedure e dei sistemi necessari a raggiungere e mantenere il SL target ipotizzato.
Le competenze da dimostrare sono:
Conoscenza del panorama normativo nazionale ed internazionale
Competenze di automazione industriale

- Architetture di sistema
- Apparati di rete
- Fieldbus seriali (Profibus)
- Fieldbus Ethernet based (Profinet, Modbus TCP, ecc.)

Valutazione del rischio

- Raccolta, comprensione e definizione dei dati relativi al sistema
- Suddivisione del sistema in aree funzionali
- Identificazione delle minacce e delle vulnerabilità
- Stima del rischio

Suddivisione del sistema in sottosistemi ed identificazione dei passaggi (conduit)

- Quali protocolli e dati sono ammessi
- Quali dispositivi sono ammessi

Definizione dei Security Level

- Sulla base del risk assessment stabilire gli SL per ciascun FR
- Identificazione dei requirements da implementare

Procedure e policies

- Definizione delle procedure e policies aziendali atte a raggiungere il SL target

Attività di campo

- Progettazione, realizzazione di un sistema di protezione adeguato al SL target

3. IMPEGNI DI CEPAS E DEI CANDIDATI

CEPAS concede libero accesso ai propri servizi ai candidati richiedenti, senza discriminazione di alcun tipo, riconosce l'importanza dell'imparzialità nella certificazione e svolge le proprie attività con obiettività, evitando ogni conflitto d'interesse.
In particolare CEPAS si vincola a non utilizzare come esaminatori per la valutazione del candidato coloro che abbiano effettuato formazione allo stesso sulle tematiche oggetto del presente schema. Il vincolo è esteso anche agli esaminatori degli eventuali organismi di valutazione qualificati. Tutte le funzioni coinvolte nel processo di certificazione sono vincolate al rispetto del Codice Etico del gruppo Bureau Veritas, disponibile sul sito www.cepas.it
La certificazione è rilasciata a seguito della positiva valutazione di ciascun candidato basata sui risultati dell'esame.

Il candidato inviando la richiesta di certificazione a CEPAS aderisce allo schema di certificazione e ne accetta, sottoscrivendole, tutte le fasi del processo di valutazione, certificazione e registrazione descritte in seguito.
Per ottenere e mantenere la certificazione, il richiedente deve rispettare e documentare l'applicazione di tutti i requisiti applicabili della/delle normative di riferimento per la certificazione, dei requisiti aggiuntivi definiti da CEPAS e dagli eventuali organismi di accreditamento, nonché le prescrizioni del presente documento e di quelli in esso richiamati.
I candidati sono tenuti a rispettare le norme di comportamento al fine di tutelare la sicurezza delle persone e delle cose.

4. RIFERIMENTI

Tutti i riferimenti a Leggi, Norme e documenti CEPAS non datati richiamati nel presente documento si intendono nella loro ultima edizione vigente

- UNI CEI EN ISO/IEC 17024 "Requisiti generali per gli organismi che eseguono la certificazione delle persone";
- IEC62443-1-1, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
- IEC62443-2-1, Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program
- IEC62443-2-3, Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment
- IEC62443-2-4, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers
- IEC62443-3-1, Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems
- IEC 62443-3-2: Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design
- IEC62443-3-3 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
- IEC62443-4-1 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements
- IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components;
- Presente schema di certificazione

5. TERMINI E DEFINIZIONI

Candidato: richiedente che possiede i prerequisiti specificati ed è stato ammesso al processo di certificazione
Commissario d'esame: persona che ha la competenza per condurre un esame e, ove tale esame richieda un giudizio professionale del candidato, per valutarne i risultati
Competenza: capacità di applicare conoscenze ed abilità al fine di conseguire i risultati prestabiliti
Esame: attività che fanno parte della valutazione, che permettono di misurare la competenza di un candidato mediante uno o più mezzi quali prove scritte, orali, pratiche od osservazione diretta, come definiti nello schema di certificazione.
Strutture: centro di esame, o Organismo di Valutazione, qualificato dall'OdC nel quale si svolgono esami di certificazione sotto il controllo e secondo specifiche procedure dell'OdC
Valutazione: processo che permette di valutare se una persona possiede i requisiti dello schema di certificazione

Certification Process Review (CPR): fase interna di revisione del processo di certificazione per consentire l'emissione del certificato.

6. RICHIESTA DI CERTIFICAZIONE

Possono accedere all'esame i candidati che siano in possesso di tutti i seguenti pre-requisiti e ne facciano richiesta come di seguito riportato:

Titolo di studio	Formazione	Esperienza lavorativa
Diploma di istruzione secondaria superiore *(N.B. Sono accettati tutti i titoli, corsi e diplomi riconosciuti equipollenti a quelli italiani, ai sensi delle vigenti disposizioni di legge)*	Partecipazione a corsi, convegni, webinar relativi a security industriale, automazione industriale, protocolli industriali su base ethernet, industria 4.0" della durata di almeno 48 ore negli ultimi 3 anni con i contenuti indicati in Allegato 1/A	Esperienza lavorativa specifica documentata pari a 3 anni maturata in modo continuativo nel ruolo di responsabile o all'interno di un team sulle tematiche ICT che abbia consentito di acquisire conoscenze e competenze del settore di riferimento *oppure* Esperienza lavorativa specifica documentata pari a 3 anni maturata in modo continuativo nel settore dell'automazione industriale

Documenti da consegnare a CEPAS (o all'ODV)	- Modulo MD08 "Richiesta ammissione esame e contratto di certificazione delle competenze" compilato e sottoscritto - Allegati in esso richiesti Sottoscrivendo il modulo MD08, il canddato ne accetta le condizioni economiche, le condizioni generali del contratto e quelle previste dal presente schema di certificazione. Nel caso non sia il richiedente a farsi carico delle quote di certificazione e di mantenimento, sarà sua cura far apporre, nel suddetto modulo, firma e timbro dell'azienda o persona a cui intestare le fatture.
Durata e contenuti del contratto	Il contratto di certificazione ha durata triennale e comprende le attività necessarie per il rilascio e il mantenimento della certificazione, dettagliate nel presente schema.

Nel caso la richiesta di certificazione non possa essere accolta, CEPAS ne comunicherà al richiedente le ragioni motivate.

7. PROCESSO DI VALUTAZIONE

La valutazione di idoneità del Candidato, ai fini del rilascio della certificazione CEPAS, avviene attraverso la sequenza, temporale e vincolante, di ciascuna delle seguenti fasi:

Fase	Finalità
Valutazione della documentazione prodotta dal Candidato	Accertare il possesso dei requisiti richiesti dallo Schema
Esame di certificazione, come definito nel successivo paragrafo 8	Valutazione delle conoscenze, abilità e competenze, eseguita dalla Commissione di Esame
CPR - Certification Process Review	Riesame interno della documentazione e dei risultati d'esame
Approvazione della proposta di certificazione da parte del Technical Manager	Rilascio del certificato e iscrizione al Registro CEPAS pubblicato su www.cepas.it

Qualora l'esito di una qualsiasi delle suddette fasi sia negativo, viene interrotto il processo di valutazione e informato il Candidato. Per proseguire nell'iter di certificazione sarà necessario risolvere prima le carenze riscontrate, entro i tempi indicati da CEPAS.
Di tutte le certificazioni rilasciate, viene data periodica comunicazione al CSI - Comitato CEPAS per la Salvaguardia e l'Imparzialità.

8. PROCESSO DI ESAME

Ammissione all'esame	Sono ammessi a sostenere l'esame di certificazione tutti coloro che, avendo presentato richiesta attraverso il modulo MD08 e documentato il possesso dei requisiti minimi richiesti, sono stati dichiarati idonei.
Finalità dell'esame	Valutazione delle conoscenze e delle abilità del candidato, come indicate nel presente schema. I Commissari sono responsabili della valutazione delle prove d'esame del Candidato e rispondono a CEPAS per tutte le attività di valutazione.
Pianificazione e gestione dell'esame	Le sessioni di esame sono pianificate e gestite da CEPAS, o dagli OdV approvati in accordo alla procedura CEPAS PG70. La lista dei Candidati all'esame e l'elenco della documentazione presentata dagli stessi è preventivamente verificata dagli esaminatori.
Luogo e data dell'esame	L'esame si svolge nelle località, nelle date e secondo il programma comunicati da CEPAS (o dall'OdV) ai candidati. Nel caso di esami da remoto, ai candidati vengono preventivamente comunicate la piattaforma utilizzata e le relative modalità di collegamento
Obblighi del candidato, prima dell'inizio della sessione d'esame	- esibire un documento di identità valido, - firmare il foglio presenze, - firmare per accettazione le "Condizioni generali di vendita" e l'"Informativa Privacy" - presentare evidenza di pagamento della quota prevista per la partecipazione all'esame

8.1 ARGOMENTI D'ESAME E CRITERI DI VALUTAZIONE

Gli argomenti d'esame vertono sulle conoscenze e abilità, come descritti nell'Allegato 1 .
L'esame prevede tre prove: due prove scritte e una prova orale.

Prova	Modalità e finalità	Tempo massimo	Punteggio massimo	Soglia minima
Prima Prova scritta	test a risposta chiusa con 40 domande con 3 risposte di cui 1 sola è quella esatta (sono escluse le risposte vero/falso);	60 minuti	40 punti	24 punti
Seconda prova scritta	caso studio (approfondimenti sulla disciplina e sulle migliori pratiche di cybersecurity) per la valutazione delle abilità	120 minuti	40 punti	24 punti
Prova orale	Approfondimento di eventuali incertezze riscontrate nella prova scritta e/o pratica e/o per approfondire il livello delle conoscenze acquisite dal candidato	20 minuti	20 punti	12 punti

Il superamento dell'esame prevede la **soglia minima** del 70% del punteggio massimo conseguibile.
Durante lo svolgimento delle prove scritte d'esame, i Candidati possono consultare testi di legge non commentati, previa autorizzazione dell'esaminatore, ma non possono usare telefoni cellulari, né scambiare informazioni con altri candidati. Il mancato rispetto di tali prescrizioni è causa di interruzione dell'esame stesso.
Al termine dell'esame la Commissione comunica al candidato l'esito della stessa e le eventuali aree di miglioramento da sviluppare durante la validità della certificazione.

8.2 ESAMINATORI e OSSERVATORI

L'esame è condotto da esaminatori CEPAS in possesso dei requisiti minimi indicati nell'Allegato 2, qualificati da CEPAS o da un suo OdV approvato. Essi sono tenuti a mantenere la riservatezza sulle prove di esame, attenersi a criteri di oggettività

nella valutazione, comunicare eventuali legami e rapporti e interessi in conflitto che potrebbero compromettere la loro imparzialità e la riservatezza nello svolgimento delle loro funzioni, rispettare il presente schema.
La Commissione d'esame è costituita da uno o più esaminatori in modo da coprire tutte le competenze richieste per la valutazione.Qualora l'esame sia svolto da un OdV, la Commissione d'esame può essere supervisionata, anche senza preavviso, dal personale CEPAS debitamente autorizzato. Alle sessioni di esame, CEPAS può prevedere la presenza di osservatori propri, degli enti di accreditamento o di eventuali autorità competenti.

8.3 RIPETIZIONE DELL'ESAME

I candidati che non superano l'esame (o una singola prova) possono ripetere l'esame (o la singola prova) nelle sessioni successive, effettuando il pagamento della sola tariffa di ripetizione esame.
Se il candidato non ha superato una delle prove scritte, può sostenere l'esame per la prova non superata in una ulteriore sessione di esame, da svolgersi entro un anno.

9. RILASCIO DELLA CERTIFICAZIONE, ISCRIZIONE AL REGISTRO, INTEGRITA' DEI DATI E PRIVACY

Al Candidato che ha superato positivamente l'esame, in possesso di tutti i requisiti richiesti e in regola con gli aspetti amministrativi, CEPAS rilascia la certificazione, previa delibera positiva dell'Organo deliberante.
Il certificato riporta i seguenti dati:
- nome dell'organismo di certificazione
- nome, cognome, data e luogo di nascita della persona certificata
- numero del certificato
- schema di certificazione e/o norma di riferimento
- data di inizio validità e di scadenza
- firma del responsabile dell'OdC autorizzato.

L'iscrizione nel relativo Registro CEPAS viene effettuata dopo la delibera del certificato; il registro è consultabile sul sito www.cepas.it.
CEPAS, in qualità di titolare, garantisce che il trattamento dei dati dei Candidati alla certificazione avvenga nel rispetto del Regolamento UE 2016/679 e del DLgs 196/2003 modificato dal DLgs 101/2018.
I documenti relativi all'attività di certificazione sono conservati con la massima cura da CEPAS e dagli organismi di valutazione approvati. Le informazioni ottenute dal personale operante per conto di CEPAS, compreso l'organo deliberante, sono soggette al vincolo di riservatezza.

10. MANTENIMENTO ANNUALE (SORVEGLIANZA) E RINNOVO DELLA CERTIFICAZIONE

La validità della certificazione durante il periodo contrattuale dei tre anni (decorrenti dalla data del rilascio del certificato) è soggetta all'esito positivo delle attività di sorveglianza annuale, svolte da CEPAS.

Mantenimento annuale	La persona certificata è tenuta a fornire, con cadenza annuale, un'autodichiarazione, resa ai sensi del DPR 445/2000 (mediante apposita modulistica predisposta da CEPAS), relativa ai seguenti aspetti: - accettazione documenti CEPAS - continuità professionale secondo il profilo/i certificato/i - partecipazione ad attività di aggiornamento pari ad almeno 8 ore, anche in modalità FAD ed e-learning - assenza di reclami o adeguata gestione degli stessi nell'attività specifica Il mantenimento della certificazione è inoltre soggetto al pagamento delle quote annuali previste.
Rinnovo della certificazione	Il certificato è rinnovabile in vista della sua scadenza, in seguito a specifica richiesta e a un nuovo accordo contrattuale. Il rinnovo è possibile, solo nel caso in cui il certificato sia in corso di validità e prevede, in aggiunta ai requisiti richiesti per il mantenimento annuale: - dichiarazione relativa all'attività professionale in corso di svolgimento ed evidenza dei lavori svolti nei 3 anni di durata della certificazione - partecipazione ad attività di aggiornamento sui temi oggetto della certificazione per almeno 24 ore complessive nei 3 anni trascorsi, anche in modalità FAD ed e-learning - elenco di attività svolte nel settore OT cyber security nel triennio (risk assessment, stesura policies e procedure, implementazione di sistemi di sicurezza - assenza di reclami o adeguata gestione degli stessi nell'attività specifica L'iter di rinnovo si deve concludere entro la scadenza del certificato in corso.

Per tutte le altre condizioni relative a mantenimento e rinnovo si rimanda al Regolamento Generale CEPAS (RG01 – par. 2.5, 2.7).

11. SOSPENSIONE, RITIRO E ANNULLAMENTO DELLA CERTIFICAZIONE

CEPAS ha il diritto di sospendere, ritirare o annullare la certificazione in qualsiasi momento della durata del contratto, al verificarsi di una o più delle condizioni riportate di seguito.
A seguito della notifica del provvedimento di sospensione, di ritiro o di annullamento della certificazione, la persona certificata deve sospendere l'utilizzo del certificato, restituendolo a CEPAS.

Sospensione	La certificazione può essere sospesa, per un periodo massimo di 6 mesi, verificandosi una o più di queste condizioni: - violazione di quanto previsto al par. 10; - gravi carenze nell'attività svolta dalla persona certificata, in seguito a reclami, azioni legali ed altre evidenze oggettive; - uso scorretto o ingannevole della certificazione CEPAS; - inadempimento degli obblighi contrattuali di tipo economico assunti per l'iscrizione, lo svolgimento degli esami e il mantenimento del certificato; - richiesta da parte della persona certificata.
Revoca	La certificazione può essere revocata, verificandosi una o più di queste condizioni: - qualora persistano le condizioni che hanno causato la sospensione, nonostante l'attuazione del provvedimento di sospensione. - qualora la gravità del comportamento della persona certificata, suffragata da evidenze oggettive inconfutabili, renda necessario tutelare l'immagine CEPAS con provvedimenti di tipo drastico ed urgente, ricorrendo contestualmente alle vie legali nei confronti della persona certificata.
Annullamento	La certificazione può inoltre essere annullata da CEPAS nel caso in cui la persona certificata faccia espressa richiesta di interrompere il rapporto contrattuale in corso e la comunicazione di disdetta pervenga almeno 3 mesi prima della scadenza annuale. La mancata comunicazione di rinuncia nel termine dei 3 mesi prima della data di scadenza annuale non assolve dal versamento della quota di mantenimento per l'annualità successiva.

CEPAS notifica alla persona certificata le ragioni del provvedimento di sospensione, ritiro o annullamento della certificazione, definendo se applicabile le azioni necessarie a riattivare il certificato e indicano termini e condizioni per l'utilizzo della certificazione.
Il ritiro e l'annullamento della certificazione comportano la risoluzione del relativo contratto con la persona in questione e l'obbligo per quest'ultima di restituire a CEPAS il proprio certificato di conformità, cessando nel contempo ogni riferimento ad esso; a tal proposito si veda il regolamento generale RG01.
La persona certificata può appellarsi ai provvedimenti di sospensione e revoca della certificazione in accordo a quanto stabilito dalle procedure consultabili sul sito www.cepas.it.

12. RECLAMI E RICORSI

CEPAS tratta i reclami e i ricorsi sulle proprie decisioni in merito alla certificazione in accordo agli art. 4 e 5 del Regolamento Generale (RG01) pubblicato sul sito www.cepas.it e che prevedono:

- l'obbligo di registrare e trattare ciascun reclamo o ricorso, confermando al reclamante o ricorrente il ricevimento dello stesso entro tempi stabili,
- l'avvio di un'istruttoria specifica
- la comunicazione della decisione finale al reclamante o ricorrente
- l'adozione, se necessaria, di ogni azione correttiva nel caso il ricorso o il reclamo abbia segnalato una carenza da parte di CEPAS.

Nel caso di reclamo relativo a una persona certificata, la decisione finale può prevedere l'avvio di opportune verifiche presso il cliente. Gli esiti di tali verifiche sono comunicati al reclamante, nel rispetto dei vincoli di riservatezza.

In caso di ricorsi, i costi relativi al ricorso sono a carico di CEPAS se questo è accolto e del ricorrente se il ricorso è respinto.

Per qualunque controversia fra una parte interessata e CEPAS che non risulti risolta con le attività descritte nei casi precedenti (reclami e ricorsi) si deve fare ricorso al Foro competente di Milano.

13. REGOLAMENTO GENERALE PER IL RILASCIO E IL MANTENIMENTO DELLA CERTIFICAZIONE/QUALIFICA DELLE FIGURE PROFESSIONALI, CODICE DEONTOLOGICO E PRESCRIZIONI PER L'USO DEL CERTIFICATO E MARCHIO CEPAS

Le persone certificate e/o in iter di certificazione si impegnano a rispettare il Regolamento generale per il rilascio e il mantenimento della certificazione/qualifica delle figure professionali CEPAS (RG01), il Codice deontologico CEPAS (CD01) e le Prescrizioni per l'uso del certificato e marchio CEPAS (MC01), pubblicati su www.cepas.it .

La certificazione può essere comunicata dalla persona certificata sulla propria carta stampata personale o nel sito personale con il solo riferimento al numero del certificato accompagnato dal nome "CEPAS".

L'uso del marchio CEPAS non è consentito.

ALLEGATO 1

ARGOMENTI DELL'ESAME di CERTIFICAZIONE e DELLA FORMAZIONE SPECIFICA

Area normativa
Principali riferimenti normativi in ambito IEC 62443
Definizione dei ruoli che concorrono alla security secondo la IEC 62443
Definizione di security Level
Definizioni di Functional Requirement
Livelli ed ambiti di applicazione della famiglia IEC 62443
Struttura ed approccio della famiglia IEC 62443
Normativa CEI EN IEC 61158
Area tecnica
Riferimenti del mondo automazione
Modello ISO/OSI e stack di comunicazione Ethernet based
Protocolli di comunicazione real time Ethernet based
Sistema IACS
Minacce
Vulnerabilità
Conseguenze
Struttura di un attacco
Tipi di attacco
Concetto di defense in depth
- Security plan
- Progettazione adeguata di una rete industriale
- Separazione IT/OT
- Segmentazione della rete OT
- Protezione del perimetro
- Device hardening
- Monitoraggio della rete
- Gestione degli aggiornamenti

Area Metodologica
Tecnologie utilizzate per garantire la sicurezza informatica
- Switch gestiti
- Firewall
- VPN
- Antivirus
- IDS/IPS
- Vulnerability scanners

Gli argomenti sono sviluppati in 24 ore suddivise tra lezioni ed esercitazioni. Le esercitazioni, pari ad almeno il 25% del corso, devono essere raccolte, registrate e documentate in modo appropriato.

ALLEGATO 2

PROFILO DELL'ESAMINATORE E DEI DOCENTI DEI CORSI DI FORMAZIONE
Requisiti minimi

Istruzione: Diploma di Istruzione Secondaria Superiore

Conoscenze professionali specifiche: requisiti base sul mondo automazione, requisiti base sui sistemi informatici

Formazione specifica come discente e/o come docente sui temi di cybersecurity di cui all'All. 1

Esperienza lavorativa: Esperienza professionale come tecnico nel mondo automazione o tecnico nel mondo della security IT rilevante e documentabile per almeno 5 anni nel settore di riferimento specifico