



**GARA A PROCEDURA APERTA AI SENSI DEL
D.LGS. 36/2023 E S.M.I., PER LA CONCLUSIONE DI
UN ACCORDO QUADRO PER OGNI LOTTO AVENTE
AD OGGETTO L’AFFIDAMENTO DI SERVIZI
MANAGED SECURITY SERVICES DA REMOTO, DI
GOVERNANCE, ANALISI DEL RISCHIO E
CONTROLLO PER LE PUBBLICHE
AMMINISTRAZIONI (ID 2737)
LOTTE 1 e 2**

**APPENDICE 2 AL CAPITOLATO TECNICO
SPECIALE - PROFILI PROFESSIONALI**

Classificazione Consip: Ambito pubblico



Indice

1.	SCOPO DEL DOCUMENTO	3
2.	INFORMATION SECURITY CONSULTANT SENIOR	7
3.	INFORMATION SECURITY CONSULTANT JUNIOR	10
4.	SECURITY SOLUTION ARCHITECT	13
5.	SCHEMA PER LA PRESENTAZIONE DEI CURRICULA	16

1. SCOPO DEL DOCUMENTO

Il presente documento è redatto sulla base del framework E-CF (European Competence Framework)¹ del Comitato Europeo di Normazione (CEN) e del documento “Competenze Digitali”² emesso da AgID nel dicembre 2019.

Per i profili inseriti dedicati alla sicurezza informatica si fa riferimento, ove applicabile, allo European Cybersecurity Skills Framework Role Profiles (ECSF) di ENISA.

Trattasi di requisiti minimi che dovranno evolversi nel contesto delle migliori professionalità presenti nel settore della cybersicurezza per sostenere la protezione dei perimetri di sicurezza delle PA, a tutela della protezione del Paese.

Le figure professionali necessarie **per lo svolgimento dei servizi di supporto specialistico** dovranno aderire ai profili di seguito descritti.

Il presente documento considera le esigenze di servizi in ambito cybersicurezza espresse sulla base del Piano Triennale per l’informatica nella Pubblica Amministrazione che sulla normativa relativa al perimetro di sicurezza nazionale cibernetica. Ciascun profilo professionale si riferisce a risorse professionali con ampia esperienza, competenza funzionale e tecnica per l’ambito del lotto. Tali competenze dovranno essere costantemente aggiornate all’evoluzione della tecnologia, normativa e organizzativa della cybersicurezza nonché degli standard, delle linee guida e best practices applicabili.

Nel presente documento, e laddove citati nel Capitolato Tecnico Generale e Speciale, ogni riferimento ad attività o metodologie basate sull’adozione di prodotti e ogni riferimento a prodotti vanno intesi in relazione ai prodotti e/o ai componenti di tali prodotti che sono effettivamente adottati per i sistemi informatici gestiti dalla singola Amministrazione.

Le competenze e conoscenze tecniche delle figure che seguono non sono esaustive delle esigenze future. Infatti, le competenze iniziali potranno variare in funzione dell’evoluzione tecnologica e in relazione a ulteriori tematiche, prodotti, sistemi e metodologie che emergeranno durante la validità dell’AQ e dei Contratti Esecutivi, nonché nei casi di cui al paragrafo 10.1 del Capitolato Tecnico Generale. A tal fine, la presente appendice potrà essere aggiornata nel corso della vigenza dell’AQ e dei Contratti Esecutivi, in accordo tra le parti e comunque previa approvazione del Comitato Tecnico.

Per ogni profilo è richiesto il possesso di una esperienza lavorativa minima, che deve essere stata maturata in ambito ICT. Per ogni profilo è richiesto inoltre il possesso di uno specifico titolo di studio oppure di una “cultura equivalente”; la cultura equivalente corrisponde ad una esperienza lavorativa maturata in ambito ICT aggiuntiva rispetto a quella minima indicata nel profilo stesso; l’entità dell’esperienza aggiuntiva necessaria dipende dal titolo di studio posseduto dalla risorsa rispetto a quello richiesto, come sintetizzato nella seguente tabella. In ogni caso, il titolo di studio posseduto

¹ <https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf>

² <https://www.agid.gov.it/it/agenzia/competenze-digitali>

Ad esempio, nel caso in cui fosse richiesta una laurea magistrale in discipline tecnico-scientifiche con esperienza minima maturata in ambito ICT di 10 anni, il possesso di laurea triennale in discipline tecnico-scientifiche richiederebbe esperienza minima di 12 anni (10 + 2).

Si precisa che per lauree in discipline tecnico-scientifiche si intendono le lauree che possono essere ricondotte alle classi di laurea che prevedono, nelle proprie attività formative di base e/o caratterizzanti, uno o più dei settori scientifico disciplinari inclusi nelle aree “scienze matematiche e informatiche” o “ingegneria industriale e dell’informazione”.

Le classi di laurea e i settori scientifico-disciplinari suddetti fanno riferimento alla classificazione fornita dal Ministero dell’Istruzione, Università e Ricerca nell’ambito dei D.M. 16 marzo 2007 e s.m.i. e 4 ottobre 2000 e s.m.i., nonché secondo quanto previsto dai DM. 1648 e 1649 del 19 dicembre 2023 emanati dal Ministero dell’Università e Ricerca.

L’eventuale equiparazione dei diplomi di laurea conseguiti in base ad ordinamenti previgenti è regolata da quanto previsto nel Decreto Interministeriale 9 luglio 2009 (G.U. 7 ottobre 2009 n. 233) e s.m.i..

Per ciascun profilo professionale le competenze, le conoscenze e le abilità indicate nel presente documento devono essere presenti nel complesso delle risorse professionali che il Fornitore può mettere a disposizione dell’Amministrazione per l’erogazione dei servizi e non devono essere interamente possedute da un’unica risorsa. Resta inteso che, al contrario, i titoli di studio (o la cultura equivalente) e l’esperienza lavorativa pregressa dovranno essere posseduti da ciascuna risorsa. Per le certificazioni valgono le regole indicate in corrispondenza di ciascun profilo professionale.

È facoltà dell’Amministrazione dettagliare le proprie esigenze dettagliando le competenze/conoscenze/abilità relativamente a quelle indicate per ciascun profilo nell’ambito del presente documento.

Le certificazioni possedute dalle risorse per ciascun ruolo dovranno essere mantenute aggiornate e in corso di validità per tutta la durata contrattuale e dovranno essere allineate all’evoluzione del prodotto/tecnologia a cui si riferiscono.

Il Piano dei Fabbisogni dell’Amministrazione sarà corredato dalla descrizione del contesto IT tecnologico e applicativo attuale e futuro di riferimento. Nell’ambito del Piano Operativo predisposto dal Fornitore, saranno declinati i profili professionali in coerenza con l’ambiente di riferimento.

Permane in ogni caso l’obbligo per il Fornitore di erogare i servizi richiesti anche a fronte di significative variazioni del contesto tecnologico, adeguando le conoscenze del personale impiegato nell’erogazione dei servizi o inserendo nei gruppi di lavoro risorse con skill adeguato, fermo restando quanto previsto nel presente documento.

I curriculum vitae delle figure professionali da impiegare nei vari servizi dovranno essere resi disponibili alla Amministrazione secondo quanto previsto dal presente documento, rispettando lo schema di CV Europeo riportato in calce al presente documento o diversi template indicati dall’Amministrazione. In ogni caso, dovranno essere particolarmente dettagliate le



competenze/conoscenze/esperienze tecniche al fine di verificare la corrispondenza con i requisiti minimi, gli eventuali requisiti migliorativi offerti e il contesto dell'Amministrazione.

2. INFORMATION SECURITY CONSULTANT SENIOR

Titolo del profilo	INFORMATION SECURITY CONSULTANT SENIOR
Riferimento profilo ECSF	Chief Information Security Officer
Descrizione sintetica	Figura professionale di riferimento per attività e progetti relativi all'attuazione della strategia di cybersicurezza dell'organizzazione per garantire la sicurezza e la protezione dei sistemi, servizi e asset digitali.
Missione	<ul style="list-style-type: none"> • Attuare la strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cybersicurezza e il resto del personale operativo. • Controllare il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. • Attuare misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione. • Identificare e risolvere i problemi di cybersicurezza e anticipare le possibili minacce, esigenze e le sfide future.
Principali Task	<ul style="list-style-type: none"> • Valutare e migliorare la postura di sicurezza dell'organizzazione. • Analizzare e implementare politiche di sicurezza informatica certificazioni, standard, metodologie e framework di cybersicurezza. • Analizzare leggi, regolamenti e normative in materia di sicurezza informatica, comprendere gli obblighi e le misure che impongono e realizzare le azioni che consentano di rispettarli. • Implementare una strategia di cybersicurezza. • Progettare, applicare, monitorare e revisionare periodicamente il sistema di gestione della sicurezza delle informazioni (ISMS) direttamente o guidando risorse in outsourcing. • Attuare un piano di cybersicurezza. • Comunicare, coordinare e cooperare con gli stakeholder interni ed esterni all'organizzazione. • Controllare le reti dell'organizzazione per rilevare violazioni della sicurezza e indagare quando si verifica. • Elaborare documentazione e reportistica relativa a violazioni di sicurezza. • Realizzare progetti in ambito continuità operativa. • Adottare standard di sicurezza e best practices per l'organizzazione.

Competenze e-CF assegnate	A.7.	Competenze e-CF assegnate	A.7.
	B.3.	Testing	B.3.
	B.5.	Produzione di documentazione	B.5.
	C.4.	Gestione del problema	C.4.
	D.1.	Sviluppo della strategia per la Sicurezza informatica	D.1.
	E.3.	Gestione del rischio	E.3.
	E.8.	Gestione della sicurezza dell'informazione	E.8.
	E.9.	Governance dei sistemi informativi	E.9.
Conoscenze	<ul style="list-style-type: none"> • Policy e procedure di cybersicurezza. • Standard, metodologie e framework di cybersicurezza. • Raccomandazioni e buone pratiche di cybersicurezza. • Leggi, regolamenti e normative della cybersicurezza. • Framework delle certificazioni relative alla cybersicurezza. • Pratiche di Ethical hacking. • Modelli di misurazione della maturità relativi alla cybersicurezza. • Standard, metodologie, processi e framework relativi al Risk management. • Pratiche e principi di mitigazione del rischio cyber. • Standard in materia di sicurezza dei sistemi informativi (ad esempio ISO 27001, ISO 27002, ISO 15408, ISO 22399, ISO 22301, OWASP, OSSTMM) e principali standard di sicurezza (ITSEC, ISO27001). • Metodologie e processi in ambito continuità operativa. • Network security (firewall, web application firewall, IPS, Network access control). • Security events (SIEM, SOAR, IDS, End Point). • Sistemi ISMS in accordo con la norma ISO 27001. • Normativa in materia di privacy. 		
Abilità	<ul style="list-style-type: none"> • Essere in grado di coordinare figure professionali Junior. • Essere in grado di redigere documentazione a supporto dei processi di compliance rispetto alle normative applicabili (ad esempio Studio di fattibilità per la continuità operativa, documentazione relative alla gestione degli incidenti informatici, analisi post-mortem). • Essere in grado di eseguire assessment tecnologici per l'identificazione degli strumenti e degli asset atti a garantire la Cyber Resilience. • Essere in grado di definire piani di Disaster Recovery. 		

	<ul style="list-style-type: none"> • Essere in grado di governare/gestire attività di patching (no implementazione) • Essere in grado di redigere documentazione tecnica e di progetto. • Essere in grado di gestire i rischi per la sicurezza delle informazioni e implementazione di nuovi modi per proteggere i sistemi informatici e le reti delle organizzazioni. • Essere in grado di gestire gli avvisi di sicurezza. • Essere in grado di individuare e correggere i difetti nei sistemi e nelle reti di computer.
Certificazioni	<p>Possesso di almeno una delle seguenti certificazioni aggiornate all'ultima release disponibile:</p> <ul style="list-style-type: none"> • Certified Information Security Manager (CISM). • Certified information systems security professional (CISSP). • Certified Ethical Hacker (CEH). • Certified Information Systems Auditor (CISA). • Certified Information Privacy Professional (CIPP). • CompTIA Security+. • Lead Auditor ISO 27001. <p>per almeno il 60% delle risorse (arrotondato all'unità superiore) previste per il singolo Contratto esecutivo.</p>
Titolo di studio	Laurea magistrale specialistica in materie tecnico-scientifiche o cultura equivalente.
Esperienza lavorativa	Minimo 10 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 5 nella funzione.

3. INFORMATION SECURITY CONSULTANT JUNIOR

Titolo del profilo	INFORMATION SECURITY CONSULTANT JUNIOR		
Riferimento profilo ECSF	Chief Information Security Officer		
Descrizione sintetica	Figura professionale di riferimento per attività e progetti correlati alla strategia di cybersicurezza dell'organizzazione alla sua implementazione per garantire la sicurezza e la protezione dei sistemi, servizi e asset digitali.		
Missione	<ul style="list-style-type: none"> • Contribuire all'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location). • Controllare il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. • Attuare misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione. 		
Principali Task	<ul style="list-style-type: none"> • Collaborare nella valutazione della postura di sicurezza dell'organizzazione. • Implementare politiche di sicurezza informatica, certificazioni, standard, metodologie e framework di cybersicurezza. • Analizzare leggi, regolamenti e normative in materia di sicurezza informatica, comprendere gli obblighi e le misure che impongono e collaborare alle azioni che consentano di rispettarli. • Collaborare nello sviluppo e implementazione di una strategia di cybersicurezza. • Monitorare periodicamente il sistema di gestione della sicurezza delle informazioni (ISMS). • Supportare la risoluzione dei problemi di cybersicurezza. • Collaborare alla definizione di un piano di cybersicurezza. • Comunicare e cooperare con gli stakeholder interni ed esterni all'organizzazione. • Controllare le reti dell'organizzazione per rilevare violazioni della sicurezza. • Collaborare alla elaborazione di documentazione e reportistica relativa a violazioni di sicurezza. • Collaborare a progetti in ambito continuità operativa. 		
Competenze e-CF assegnate	A.7.	Competenze e-CF assegnate	A.7.
	B.3.	Testing	B.3.

	B.5.	Produzione di documentazione	B.5.
	C.4.	Gestione del problema	C.4.
	D.1.	Sviluppo della strategia per la Sicurezza informatica	D.1.
	E.3.	Gestione del rischio	E.3.
	E.8.	Gestione della sicurezza dell'informazione	E.8.
	E.9.	Governance dei sistemi informativi	E.9.
Conoscenze	<ul style="list-style-type: none"> • Policy e procedure di cybersicurezza. • Standard, metodologie e framework di cybersicurezza. • Raccomandazioni e buone pratiche di cybersicurezza. • Leggi, regolamenti e normative relative alla cybersicurezza. • Framework delle certificazioni relative alla cybersicurezza. • Pratiche di Ethical hacking. • Modelli di misurazione della maturità relativi alla cybersicurezza. • Standard, metodologie, processi e framework relativi al Risk management. • Pratiche e principi di mitigazione del rischio. • Standard in materia di sicurezza dei sistemi informativi (ad esempio ISO 27001, ISO 27002, ISO 15408, ISO 22399, ISO 22301, OWASP, OSSTMM) e principali standard di sicurezza (ITSEC, ISO27001). • Metodologia e processi in ambito continuità operativa. • Network security (firewall, web application firewall, IPS, Network access control). • Security events (SIEM, SOAR, IDS, End Point). • Sistemi ISMS in accordo con la norma ISO 27001. • Normativa in materia di privacy. 		
Abilità	<ul style="list-style-type: none"> • Essere in grado di redigere documentazione a supporto dei processi di compliance rispetto alle normative applicabili (ad esempio Studio di fattibilità per la continuità operativa, documentazione relative alla gestione degli incidenti informatici, analisi post-mortem). • Essere in grado di redigere documentazione tecnica e di progetto. • Essere in grado di gestire attività di patching (no implementazione). • Essere in grado di elaborare studi di sistemi e delle reti di computer per la valutazione dei rischi per determinare come migliorare le politiche e i protocolli di sicurezza. • Essere in grado di elaborare studi di sistemi e delle reti informatiche, incluso il processo di valutazione dei rischi di sicurezza. 		

	<ul style="list-style-type: none">• Essere in grado di correlare tra i cambiamenti dei sistemi informatici e gli attacchi informatici.• Essere in grado di gestire i rischi per la sicurezza delle informazioni e implementazione di nuovi modi per proteggere i sistemi informatici e le reti delle organizzazioni.
Certificazioni	N/A
Titolo di studio	Laurea triennale in materie tecnico-scientifiche o cultura equivalente.
Esperienza lavorativa	Minimo 3 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 2 nella funzione.

4. SECURITY SOLUTION ARCHITECT

Titolo del profilo	SECURITY SOLUTION ARCHITECT
Riferimento profilo ECSF	Cybersecurity Architect
Descrizione sintetica	Figura professionale che si occupa della progettazione di soluzioni sicure, sviluppa la documentazione relativa all'architettura delle soluzioni e delle infrastrutture.
Missione	<ul style="list-style-type: none"> • Progettare, costruire, eseguire test e implementare i sistemi di sicurezza all'interno della rete IT di un'organizzazione. • Progettare un'architettura di rete sicura al fine anticipare tutte le potenziali mosse e tattiche che eventuali attaccanti possono utilizzare per ottenere l'accesso non autorizzato al sistema informatico.
Principali Task	<ul style="list-style-type: none"> • Condurre l'analisi dei requisiti di cybersicurezza. • Definire le specifiche architeturali e funzionali delle soluzioni di cybersicurezza. • Rendere resiliente l'architettura per evitare "Single Point Of Failure" (SPOF). • Analizzare i sistemi in essere per identificare soluzioni di cybersicurezza efficaci. • Progettare nuovi sistemi e architetture tenendo conto dei requisiti imposti dalle norme relative alla cybersicurezza e dalla privacy rispettando il principio della Security and Privacy by Design. • Guidare e collaborare con chi si occupa operativamente dell'implementazione e con il personale Information Technology (IT) e Operational Technology (OT). • Proporre architetture di cybersicurezza. • Selezionare specifiche, procedure e controlli appropriati nel contesto dell'organizzazione. • Coordinare l'integrazione delle soluzioni di cybersicurezza. • Analizzare le configurazioni e le regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, SOAR, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi Cloud oriented per la sicurezza). • Identificare soluzioni tecnologiche e organizzative da porre in essere per ottimizzare e migliorare le configurazioni di infrastrutture ICT.

	<ul style="list-style-type: none"> • Adottare tecnologie per la sicurezza IT, soprattutto in ambito sicurezza cloud. • Adottare tecniche di correlazione eventi, progettazione di regole di correlazione e tuning sistemi. 	
Competenze e-CF assegnate	A.5. Competenze e-CF assegnate	A.5.
	A.6. Disegno delle applicazioni	A.6.
	B.1. Sviluppo delle applicazioni	B.1.
	B.3. Testing	B.3.
	B.6. Ingegneria dei sistemi	B.6.
	C.2. Supporto alle modifiche/evoluzioni del sistema	C.2.
	D.1. Sviluppo della strategia per la Sicurezza informatica	D.1.
	E.8. Gestione della sicurezza dell'informazione	E.8.
	E.9. Governance dei sistemi informativi	E.9.
Conoscenze	<ul style="list-style-type: none"> • Raccomandazioni e buone pratiche relative alla cybersicurezza. • Standard, metodologie e framework relative alla cybersicurezza • Requisiti di analisi relativi alla cybersicurezza. • Ciclo di vita dello sviluppo software sicuro. • Modelli di riferimento e di integrazione per le architetture di sicurezza. • Tecnologie, soluzioni e controlli relativi alla cybersicurezza. • Rischi, minacce, vulnerabilità e tendenze relative alla cybersicurezza. • Requisiti di compliance a regolamenti, normative e buone pratiche. • Procedure legacy di cybersicurezza. • Privacy-Enhancing Technology (PET). • Standard, metodologie e framework relativi alla Privacy by Design; • Algoritmi di cifratura. • Pratiche e principi relativi ai controlli degli accessi. • Framework delle certificazioni relative alla cybersicurezza. • Regole tecniche e delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza). 	
Abilità	<ul style="list-style-type: none"> • Essere in grado di comprendere l'infrastruttura IT, le relazioni tra i differenti sistemi e componenti infrastrutturali al fine di individuare 	

	<p>problematiche architetture che ne potrebbero compromettere la sicurezza.</p> <ul style="list-style-type: none"> • Essere in grado di analizzare le configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, SOAR, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza). • Essere in grado di verificare l'efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture IT. • Essere in grado di utilizzare sistemi di correlazione eventi, di progettazione regole di correlazione e di tuning di sistemi di analisi eventi. • Essere in grado di utilizzare sistemi di autenticazione, sistemi di Identity & Access Management con esperienza di integrazione.
Certificazioni	<p>possesso di almeno una delle seguenti certificazioni:</p> <ul style="list-style-type: none"> • Certified information systems security professional (CISSP). • Certified Information Systems Security Architecture Professional (CISSP-ISSAP). • Certified Information Systems Security Engineering Professional (CISSP-ISSEP). • CompTIA CySA+. <p>per almeno il 60% delle risorse (arrotondato all'unità superiore) previste per il singolo Contratto esecutivo.</p>
Titolo di studio	<p>Laurea magistrale specialistica in materie tecnico-scientifiche o cultura equivalente.</p>
Esperienza lavorativa	<p>Minimo 6 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 3 nella funzione</p>

5. SCHEMA PER LA PRESENTAZIONE DEI CURRICULA

Di seguito viene presentato lo schema che il fornitore dovrà utilizzare per la compilazione dei curriculum vitae. Si sottolinea che nella redazione dei contenuti dovranno essere privilegiati gli aspetti di interesse per la fornitura e che orientativamente il documento non dovrà superare le 3 pagine.

Nominativo	<i>(Inserire il Cognome e il Nome della risorsa)</i>		
Ruolo	<i>(Inserire il Ruolo attualmente ricoperto dalla risorsa)</i>		
Figura professionale	<i>(Indicazione del ruolo assegnato alla risorsa in funzione delle figure professionali richieste nel capitolato tecnico).</i>		
Servizio/attività	<i>(Fornire l'indicazione del servizio/attività per cui viene proposta la risorsa in relazione agli ambiti definiti nel Capitolato Tecnico)</i>		
Conoscenze	<i>(Fornire una breve descrizione del profilo professionale in termini di conoscenze/competenze e di aree chiave in cui la risorsa ha maturato esperienze significative)</i>		
Principali Esperienze Lavorative	<i>(Indicare le esperienze più significative per la gara in oggetto e comprovanti le competenze richieste nell'Appendice 2, a partire dalla più recente, fornendo una breve descrizione delle attività svolte, del ruolo ricoperto, della durata del progetto. E' necessario suddividere le esperienze per anno e per settore (Es: Pubblica Amministrazione, Bancario, Telecomunicazioni))</i>		
	Settore	Data inizio- Data fine	Esperienze
Competenze Tecniche	<i>(Indicare le competenze specifiche di cui si è in possesso)</i>		
Specializzazioni	<i>(Indicare eventuali specializzazioni, master, ecc.)</i>		
	Anno	Titolo	Descrizione

Certificazioni	<i>(Indicare eventuali certificazioni)</i>		
	Anno	Titolo	Descrizione
Istruzione	<i>(indicare i titoli di studio)</i>		
Lingue	<i>Per ogni lingua straniera, indicare il grado di conoscenza, dove:</i> 1 -in grado di leggere 2 - in grado di leggere e scrivere 3 - in grado di leggere, parlare e scrivere in maniera più che comprensibile 4 - fluente sia nello scritto che nell'orale 5 - madrelingua - (native language)		
	Lingue	Grado di conoscenza	
Principali pubblicazioni	<i>(indicare le principali pubblicazioni)</i>		