

Allegato 4 – Scheda sintetica di presentazione dei percorsi formativi per l'Upskilling e Reskilling

Presentazione dell'offerta di percorsi di formazione ai fini della costituzione del Catalogo dell'offerta formativa GOL

SINTESI

A.1 Tipologia di Percorso di riferimento nell'ambito del Programma GOL:

UPSKILLING

RESKILLING

A.2 Area di formazione di riferimento (*con riferimento alle aree di manifestazione per cui si è stati selezionati con DD 1018 del 12.08.2022)

1 Efficienza energetica

2 Mobilità sostenibile

3 Nuove tecnologie della vita

4 Nuove tecnologie per il Made in Italy

5 Tecnologie innovative per i beni e le attività culturali -Turismo

6 Tecnologie della informazione e della comunicazione

A.3 Titolo del percorso formativo

La sicurezza informatica

A.4. Inquadramento livello EQF

6

A.5 Settore economico professionale (SEP) (fare riferimento al SEP prevalente) con riferimento all'articolazione dell'Atlante del Lavoro e delle Qualificazioni

14 – Servizi digitali

A.6 Area/aree di attività (ADA) con riferimento all'articolazione dell'Atlante del Lavoro e delle Qualificazioni

ADA.14.01.18 Sviluppo della Strategia per la Sicurezza Informatica
ADA.14.01.22 Gestione della Sicurezza dell'Informazione

A.7 Classificazione ISTAT CP 2011

2.1.1.5.4 Specialisti in sicurezza informatica

A.8 Classificazione ISTAT ATECO 2007

62.02.00 Consulenza nel settore delle tecnologie dell'informatica
62.03.00 Gestione di strutture e apparecchiature informatiche hardware - housing (esclusa la riparazione)
62.09.01 Configurazione di personal computer
63.11.30 Hosting e fornitura di servizi applicativi (ASP)

A.9 Articolazione del riferimento professionale per Unità di Competenza

Macroprocesso	Unità di competenze
Produrre beni/Erogare servizi	Analisi dei rischi per la sicurezza dei sistemi hardware e software
	Monitoraggio della sicurezza di sistemi hardware e software

A.10 Descrizione delle singole Unità di Competenza (U.C.)

Macroprocesso	Unità di competenze
Titolo UC	Analisi dei rischi per la sicurezza dei sistemi hardware e software
Macroprocesso di riferimento	Produrre beni/Erogare servizi
Descrivere l'Unità di Competenza e indicare il repertorio regionale di riferimento	Individuare ed analizzare i rischi per la sicurezza dei sistemi hardware e software Repertorio degli standard professionali della Regione Basilicata
Risultato atteso	Rischi per la sicurezza dei sistemi hardware e software individuati ed analizzati

Conoscenze minime	<ul style="list-style-type: none"> ▪ Inglese tecnico per l'informatica ▪ Normativa in materia di protezione dei dati trattati con sistemi informatici ▪ Normativa in materia di sicurezza informatica e relativa certificazione ▪ Principali tecniche di attacco alla sicurezza informatica ▪ Sicurezza dei sistemi e delle reti informatiche
Abilità minime	<ul style="list-style-type: none"> ▪ Analizzare le minacce rilevate ▪ Individuare eventuali bug o imperfezioni nelle applicazioni ▪ Individuare eventuali vulnerabilità' di sistemi hardware e software ▪ Predisporre report sui livelli di sicurezza dei sistemi ▪ Predisporre report sull'attività svolta ▪ Progettare e applicare test di valutazione delle vulnerabilità' mirato ai sistemi operativi e/o alle reti e/o ai data base ▪ Simulare le fasi di un attacco al sistema

Macroprocesso	Unità di competenze
Titolo UC	Monitoraggio della sicurezza di sistemi hardware e software
Macroprocesso di riferimento	Produrre beni/Erogare servizi
Descrivere l'Unità di Competenza e indicare il repertorio regionale di riferimento	<p>Gestire le operazioni di monitoraggio della sicurezza di sistemi hardware e software</p> <p>Repertorio degli standard professionali della Regione Basilicata</p>
Risultato atteso	Sistemi hardware e software sicuri ed in efficienza
Conoscenze minime	<ul style="list-style-type: none"> ▪ Categorie di malware ▪ Documenti di business continuity ▪ Sicurezza dei sistemi e delle reti informatiche ▪ Sistemi identity management system (ims) ▪ Tecniche di benchmarking ▪ Tecniche di disaster recovery
Abilità minime	<ul style="list-style-type: none"> ▪ Adottare le opportune contromisure in caso di attacco alla sicurezza del sistema informativo (hardware e software) ▪ Controllare il rispetto delle misure di sicurezza progettate * gestire le regole di firewall ▪ Individuare ed eliminare malware (spyware, backdoor, trojans, ecc.) ▪ Monitorare e bloccare il traffico interno ed esterno che costituisca una potenziale minaccia alla sicurezza del sistema informativo ▪ Monitorare ed interpretare log (server, dispositivi di rete, applicazioni, ecc.)

	<ul style="list-style-type: none"> ▪ Riconoscere e bloccare attacchi denial of service ▪ Ripristinare integrità', funzionamento e livello di sicurezza in seguito ad una violazione tentata o riuscita della sicurezza del sistema informativo ▪ Testare il funzionamento dei piani di business continuity e disaster recovery ▪ Utilizzare sistemi identity management system (ims) ▪ Utilizzare tecniche e sistemi di crittografia e cifratura
--	---

A.11 Destinatari del percorso formativo –eventuali requisiti di accesso

Indicare puntualmente eventuali requisiti di ammissione dei partecipanti in relazione al titolo di studio e/o ad altre conoscenze/competenze richieste.

Destinatari del percorso formativo

Percettori di ammortizzatori sociali in costanza e in assenza di rapporto di lavoro (NASPI e DIS-COLL), i percettori di reddito di cittadinanza, i lavoratori fragili o vulnerabili (giovani NEET con meno di 30 anni), donne in condizioni di svantaggio, persone con disabilità, lavoratori maturi di 55 anni e oltre, altri lavoratori con minori chances occupazionali e con redditi molto bassi.

Requisiti di accesso

Assolvimento da parte dei partecipanti del diritto-dovere di istruzione e formazione.

Per i cittadini stranieri è indispensabile una buona conoscenza della lingua italiana orale e scritta, che consenta di partecipare attivamente al percorso formativo.

I cittadini extracomunitari devono disporre di regolare permesso di soggiorno valido per l'intera durata del percorso

A.12 Durata complessiva del percorso (*distinguere le ore di aula, FAD e tirocinio curricolare*)

80 ore aula

A.13 Articolazione del percorso formativo

N.	Titolo UFC/segmento/ tirocinio curricolare	Denominazione UC di riferimento	Durata (ore)	di cui FAD
1	Le operazioni di analisi dei rischi per la sicurezza dei sistemi hardware e software	Analisi dei rischi per la sicurezza dei sistemi hardware e software	40	
2	Le operazioni di monitoraggio della sicurezza di sistemi hardware e software	Monitoraggio della sicurezza di sistemi hardware e software	40	
Totale			80	

A.14 Tipo di attestazione prevista

ATTESTAZIONE DI MESSA IN TRASPARENZA DEGLI APPRENDIMENTI

QUALIFICAZIONE REGIONALE ex DGR n. 834/2016

ABILITAZIONE

ALTRO (indicare): _____

Eventuali Note:

A.15 Riferimenti del soggetto richiedente l'inserimento della proposta nel Catalogo dell'offerta formativa GOL

Denominazione e ragione sociale	E.N.F.A.P. UMBRIA IMPRESA SOCIALE SRL
Referente	Cognome e nome VALENTINA MELI Tel. 075.5730115 interno 3 Email comunicazione@enfapumbria.com Indirizzo PEC (del soggetto richiedente in cui ricevere eventuali comunicazioni da parte di ARPAL Umbria) enfapumbria@legalmail.it

in partenariato con (compilare se necessario)

Denominazione e ragione sociale	CONFARTIGIANTERNI FORMAZIONE E RICERCA SCARL
Referente	Cognome e nome ALESSANDRA LIPPANTINI Tel. 345 2947903 Email lippantini@confartigianatoterni.it

A.19 Sedi di svolgimento del percorso (fare riferimento esclusivamente alle sedi indicate nelle manifestazioni d'interesse in risposta all'Avviso ex DGR 627/2022)

N. sede	1
Indirizzo	c/o via Bruno Colli n.5/b – 06132 - Perugia (PG)

(ripetere se necessario)

N. sede	2
---------	---

Indirizzo	c/o via Galvani n.11 – 05100 - Terni (TR)
N. sede	3
Indirizzo	c/o CONFARTIGIANTERNI FORMAZIONE E RICERCA via Luigi Casale n.17 – 05100 - Terni (TR)
N. sede	4
Indirizzo	c/o CONFARTIGIANTERNI FORMAZIONE E RICERCA via Luigi Casale n.9 – 05100 - Terni (TR)
N. sede	5
Indirizzo	c/o CONFARTIGIANTERNI FORMAZIONE E RICERCA vicolo Corsica n.2 – 05018 - Orvieto (TR)
N. sede	6
Indirizzo	c/o NEW CONSULTING CORSI & CO SAS, via Flaminia n.19 – 06022 - Fossato di Vico (PG)
N. sede	7
Indirizzo	c/o NEW CONSULTING CORSI & CO SAS, via Piana 1/f-6 – 06061 - Castiglione del Lago (PG)
N. sede	8
Indirizzo	c/o CENTRO EDILE PER LA SICUREZZA E LA FORMAZIONE (CESF), via P. Tuzi n. 11 – 06128 - Perugia (PG)
N. sede	9
Indirizzo	c/o Co.Ge.S.T.A., via delle Acacie n.12 – 05018 - Orvieto (PG)
N. sede	10
Indirizzo	c/o BELT SCHOOL SRL, via Largo Madonna Alta n.6 – 06128 - Perugia (PG)

N. sede	11
Indirizzo	c/o UR UIL UMBRIA, via Luca della Robbia n.59 – 06018 - Città di Castello (PG)
N. sede	12
Indirizzo	c/o UR UIL UMBRIA, Via Pietro Conti n. 29 – 06049 - Spoleto (PG)
N. sede	13
Indirizzo	c/o UR UIL UMBRIA, Via Pacinotti n.34 – 05100 - Terni (TR)
N. sede	14
Indirizzo	c/o CENTRO SERVIZI UIL SRL, Via Fiamenga n. 55/A – 06034 - Foligno (PG)
N. sede	15
Indirizzo	c/o NEW WELD TECHNOLOGY SRL, Via S. di Giacomo n. 8 – 06073 - Corciano (PG)
N. sede	16
Indirizzo	c/o CASSA EDILE DI MUTUALITÀ E ASSISTENZA DI TERNI, Via S. di Garofoli n. 15 – 05100 - Terni (TR)
N. sede	17
Indirizzo	c/o CONFARTIGIANTERNI SERVIZI SRL, Via Tiberina n. 75 – 06059 - Todi (PG)
N. sede	18
Indirizzo	c/o ARTIGIANSERVIZI SRL, Via Antonio da Sangallo n. 17/B – 06034 - Foligno (PG)
N. sede	19
Indirizzo	c/o LEVITA SRL, Via A. Monteneri n. 43 – 06129 – Perugia (PG)