MINISTERO DELLA DIFESA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE DEGLI ARMAMENTI
II REPARTO COORDINAMENTO AMMINISTRATIVO
Servizio Analisi dei costi di produzione industriale e Benchmarking

Indirizzo Postale**:** Via di Centocelle 301 - 00175 Roma
Posta Elettronica: sgd@sgd.difesa.it
Posta elettronica certificata: sgd@postacert.difesa.it
PdC: F.A. Dott.ssa Rosa Maria GIANFICO
Tel. 2030284; posta elettronica: r2servcic1sz@sgd.difesa.it

Allegati: 1 (uno)
Annessi: 1 (uno)

OGGETTO: Verbale di accertamento ed analisi dei costi orari della Ditta **BITCORP S.r.l.** di Milano (MI). D.A. pilota "TELEDIFE". Verifica di conformità n. 3 in data 10/01/2025 di SGD/DNA.

A: ELENCO INDIRIZZI IN ALLEGATO

^^^^^^^^^^^^^^^^^^^^^^^^^

Riferimento: f.n. M_D A009822 REG2024 0027258 in data 20 dicembre 2024 di TELEDIFE (non a tutti).
^^^^^^^^^^^^^^^^^^^^^^^^^

Si invia, in annesso, il verbale redatto da apposita Commissione di accertamento nel rispetto delle indicazioni procedurali previste dalla Direttiva SGD-G-023 "*Analisi dei costi industriali e congruità delle offerte nel settore del procurement militare*" (edizione 2011 e successive AA.VV.), regolarmente approvato da TELEDIFE, con la Verifica di conformità n. 3 in data 10/01/2025 di SGD/DNA.

Si resta a disposizione per fornire ogni ulteriore elemento di dettaglio che si ritenesse utile acquisire.

IL DIRETTORE DEL II REPARTO
Dirig. Dott. Emanuele COLETTI

Allegato

ELENCO INDIRIZZI

STATO MAGGIORE DELLA DIFESA Ufficio Generale Centro Responsabilità Amministrativa	ROMA
STATO MAGGIORE DELL'ESERCITO Ufficio Generale Centro Responsabilità Amministrativa	ROMA
STATO MAGGIORE DELLA MARINA Ufficio Generale Centro Responsabilità Amministrativa	ROMA
STATO MAGGIORE DELL'AERONAUTICA Ufficio Generale Centro Responsabilità Amministrativa	ROMA
COMANDO GENERALE DELL'ARMA DEI CARABINIERI	ROMA
COMANDO GENERALE DELLA GUARDIA DI FINANZA - VII Reparto	ROMA
COMANDO GENERALE DELLE CAPITANERIE DI PORTO	ROMA
MINISTERO DELL'INTERNO – DIPARTIMENTO P.S.	ROMA
MINISTERO DELL'INTERNO -VIGILI DEL FUOCO	ROMA
COMANDO LOGISTICO DELL'ESERCITO	ROMA
COMANDO LOGISTICO DELLA MARINA MILITARE	NAPOLI
COMANDO LOGISTICO DELL'AERONAUTICA MILITARE	ROMA
DIREZIONE DEGLI ARMAMENTI TERRESTRI	SEDE
DIREZIONE DEGLI ARMAMENTI NAVALI	SEDE
DIREZIONE DEGLI ARMAMENTI AERONAUTICI E PER L'AERONAVIGABILITA'	SEDE
DIREZIONE INFORMATICA TELEMATICA E TECNOLOGIE AVANZATE	SEDE
AGENZIA INFORMAZIONI SICUREZZA ESTERNA	ROMA
AGENZIA INDUSTRIE DIFESA	ROMA

e, per conoscenza:

Ditta **BITCORP S.r.l.** e-mail p.e.c.: bitcorp@pec.it	MILANO

8. MANSIONARIO

ATTIVITÀ DIRETTE SPESABILI CON LE TARIFFE ORARIE, ELABORATE NEL PRESENTE VERBALE	
N°	Denominazione attività
1	Sviluppo di nuove teorie per spiegare fenomeni matematico/informatici.
2	Modellizzazione Matematica di algoritmi informatici.
3	Utilizzo di computer per simulare e studiare fenomeni teorici.
4	Conduzione di esperimenti controllati per testare ipotesi scientifiche in ambito cibernetico (IT, OT, IoT).
5	Raccolta e analisi di dati sperimentali per validare teorie matematiche.
6	Creazione di nuovi strumenti e tecniche per misurare e osservare fenomeni nel dominio cibernetico.
7	Indagini mirate a risolvere problemi specifici e a sviluppare nuove tecnologie informatiche e matematiche o migliorare quelle esistenti.
8	Creazione di prototipi e prodotti informatici pilota per testare nuove tecnologie in condizioni reali.
9	Costruzione di modelli preliminari per testare e perfezionare nuovi prodotti informatici.
10	Verifica delle prestazioni e della sicurezza dei nuovi prodotti attraverso test rigorosi validativi.
11	Miglioramento dei processi produttivi in ambito sviluppo software per aumentare l'efficienza e ridurre i costi.
12	Implementazione di tecnologie informatiche avanzate per automatizzare le operazioni di produzione.
13	Integrazione di sensori e dispositivi connessi per monitorare e ottimizzare i processi produttivi IoT.
14	Big Data e Analisi Avanzata dei Big Data.
15	Analisi dei Requisiti di un Software.
16	Creazione di documenti che descrivono i requisiti funzionali e non funzionali di un software.
17	Architettura del Software, ovvero definizione della struttura generale del sistema, inclusi i componenti principali e le loro interazioni.
18	Progettazione Dettagliata: specifica dei dettagli di ogni componente, inclusi i diagrammi UML e le specifiche delle interfacce.
19	Codifica, compilazione e scrittura del codice sorgente utilizzando linguaggi di programmazione appropriati.
20	Controllo del codice di un software per individuare e correggere errori e migliorare la qualità.
21	Test Unitari: verifica delle singole unità di codice per assicurarsi che funzionino correttamente.
22	Test di Integrazione: verifica delle interazioni tra i diversi componenti del sistema.
23	Test di Sistema: verifica del sistema nel suo complesso per assicurarsi che soddisfi i requisiti.
24	Correzione di Bug: risoluzione di problemi e difetti scoperti dopo il rilascio.
25	Test delle reti per identificare vulnerabilità nei protocolli di comunicazione e nei dispositivi di rete.
26	Test delle applicazioni web per trovare vulnerabilità come SQL injection, XSS, ecc.
27	Test delle applicazioni mobili per individuare falle di sicurezza specifiche delle piattaforme mobili.
28	Test delle reti wireless per identificare vulnerabilità nei protocolli di sicurezza Wi-Fi.

ATTIVITÀ DIRETTE SPESABILI CON LE TARIFFE ORARIE, ELABORATE NEL PRESENTE VERBALE	
N°	Denominazione attività
29	Simulazione di attacchi di ingegneria sociale per valutare la consapevolezza della sicurezza tra i dipendenti.
30	Rilevamento e risposta alle minacce attraverso l'uso di tecnologie avanzate come l'intelligenza artificiale.
31	Allestimento architetture Intrusion Detection and Prevention Systems (IDPS), per rilevare e prevenire intrusioni nella rete.
32	Rilevamento e analisi degli incidenti per comprendere la portata e l'impatto.
33	Contenimento dell'incidente, eliminazione delle minacce e recupero delle operazioni normali.
34	Analisi post-incidente, ricostruzione eventi ed eventuale cristallizzazione di evidenze e responsabilità, per migliorare le difese e aggiornare i piani di risposta.
35	Quantum Annealing, orientato alla risoluzione di problemi di ottimizzazione combinatoria.
36	Variational Quantum Eigensolver (VQE), applicazione dell'algoritmo per trovare gli autovalori di Hamiltoniani quantistici.
37	Quantum Approximate Optimization Algorithm (QAOA): applicazione dell'algoritmo per problemi di ottimizzazione approssimativa.
38	Device-Independent QKD: ovvero distribuzione di chiavi quantistiche indipendente dai dispositivi utilizzati.
39	Continuous-Variable QKD: ovvero utilizzo di variabili continue per la distribuzione di chiavi quantistiche.
40	Quantum Secure Direct Communication (QSDC): ovvero modalità di comunicazione sicura diretta senza necessità di chiavi pre-condivise.
41	Quantum Principal Component Analysis (QPCA): Analisi delle componenti principali su computer quantistici.
42	Quantum Boltzmann Machines: Modelli probabilistici per l'apprendimento automatico quantistico.
43	Quantum Generative Adversarial Networks (QGANs): Reti generative avversarie quantistiche.
44	Studio dei principali strumenti quantistici in Cloud: Attività volte all'apprendimento di strumenti quantistici in cloud come D-Wave o di calcolo quantistico in cloud come Rigetti o piattaforme di calcolo tipo l'orientale Alibaba.
45	Deep Learning: Reti neurali profonde per l'apprendimento di rappresentazioni complesse.
46	Transfer Learning: Riutilizzo di modelli pre-addestrati per nuovi compiti.
47	Ensemble Learning: Combinazione di più modelli per migliorare le prestazioni
48	Question Answering: Sistemi di risposta automatica a domande.
49	Speech Recognition: Riconoscimento e trascrizione del parlato.
50	Facial Recognition: Riconoscimento facciale per identificazione e autenticazione.
51	Image Generation: Generazione di immagini realistiche tramite reti generative.
52	Video Analysis: Analisi automatica di contenuti video.
53	Realizzazione di sistemi di automazione assistita mediante AI dove l'utente interagisce con il bot.
54	Realizzazione di sistemi di automazione mediante AI non assistita, che funziona senza intervento umano.
55	Integrazione di AI e RPA per automazione avanzata.
56	Realizzazione piattaforme di machine learning automatizzato.

ATTIVITÀ DIRETTE SPESABILI CON LE TARIFFE ORARIE, ELABORATE NEL PRESENTE VERBALE	
N°	Denominazione attività
57	Impianti di automazione del machine learning.
58	Sviluppo Servizi di AI per la visione artificiale e NLP.
59	Realizzazione di oracoli decentralizzati per smart contract.
60	Realizzazione e gestione di strumenti per lo sviluppo e il testing di smart contract.
61	Allestimento di librerie di smart contract sicuri.
62	Realizzazione di framework blockchain e DLT.
63	Realizzazione di piattaforme BaaS per lo sviluppo di soluzioni blockchain.
64	Realizzazione di App per la gestione di framework blockchain.
65	Esame e attacco su protocolli di crittografia diffusi, come quelli utilizzata dai principali servizi di Instant Messaging.
66	Attacchi a sistemi Pretty Good Privacy (PGP).
67	Attacchi a sistemi TLS, ovvero protocollo di crittografia per la sicurezza delle comunicazioni su internet.
68	Compromissione di Online Certificate Status Protocol (OCSP).
69	Allestimento di librerie PHE: ovvero per crittografia omomorfica parziale.
70	Allestimento di librerie FHE: ovvero di crittografia completamente omomorfica.
71	Realizzazione di Schemi di crittografia omomorfica basato su reticoli.
72	Applicazione del protocollo crittigrafico per SMPC basato su circuiti offuscati.
73	Sfruttamento di vulnerabilità sconosciute e non ancora corrette.
74	Creazione di exploit personalizzati per vulnerabilità specifiche.
75	Raccolte di exploit preconfezionati per sfruttare vulnerabilità comuni.
76	Simulazione di attacchi di phishing per testare la consapevolezza degli utenti.
77	Attacchi di phishing mirati a individui specifici.
78	Creazione di scenari digitali falsi per ottenere informazioni sensibili.
79	Sfruttamento di vulnerabilità nei dispositivi NFC.
80	Realizzazione attacchi Man-in-the-Middle (MitM).
81	Realizzazione attacchi DNS Spoofing mediante reindirizzamento del traffico di rete a server malevoli.
82	Realizzazione attacchi ARP Spoofing mediante manipolazione delle tabelle ARP per intercettare il traffico di rete.
83	Sfruttamento di vulnerabilità nei database per eseguire comandi SQL malevoli (SQL Injection).
84	Inserimento di script malevoli in pagine web (Cross-Site Scripting - XSS).
85	Esecuzione di codice malevolo su server remoti (Remote Code Execution - RCE).
86	Sfruttamento di vulnerabilità nei protocolli di sicurezza Wi-Fi.
87	Sfruttamento di vulnerabilità nei dispositivi Bluetooth.
88	Sfruttamento di vulnerabilità nei dispositivi Bluetooth (in outsourcing strategico).
89	Assistenza tecnica post vendita (SERVICE).

Ore dirette totali vendibili dalla Società:

14.082,84

Gli oneri per la sicurezza incidono sul C.O.M.A. per lo 0,86%

Inquadramento al CCNL Settore COMMERCIO