FONDO PENSIONE CAIMOP
CASSA PREVIDENZA INTEGRATIVA MEDICI OSPEDALITÀ PRIVATA

Invito a offrire per una Società ICT ai fini dell'adeguamento del Fondo pensione CAIMOP al Digital Operational Resilience Act – DORA. Regolamento (EU) 2022/2554

Il Consiglio di Amministrazione del Fondo pensione CAIMOP, iscritto con il numero 1017 all'Albo dei Fondi pensione tenuto da Covip, ha deliberato - in data 15/10/2024 - di procedere alla **selezione di una società**, avente il compito di fornire al Fondo **supporto nell'implementazione di un modello di compliance al Digital Operational Resilience Act – DORA.** (Regolamento (EU) 2022/2554).

In particolare, l'**OGGETTO dell'incarico** riguarda:

a) **l'attività di adeguamento al Regolamento DORA (e stesura del Framework documentale)**, preceduta da una ricognizione iniziale (cd. Gap Analysis) volta a identificare gli ambiti su cui il Fondo Pensione dovrà eventualmente intervenire e con quali modalità;

b) **l'assunzione dell'incarico di Responsabile della Gestione e della Sorveglianza dei rischi informatici**, ai sensi del Regolamento DORA.

A) ADEGUAMENTO AL REGOLAMENTO DORA

Il Regolamento UE 2022/2554 – Digital Operational Resilience Act (anche "DORA"), di seguito anche "Regolamento", avrà piena attuazione dal **gennaio 2025** ed è caratterizzato dall'introduzione di rilevanti novità in materia di **gestione dei rischi informatici** e di **sicurezza delle informazioni e dei modelli operativi digitalizzati**.

Il regolamento prevede una serie di adempimenti che possono essere raggruppati in **5 macro-aree principali**, corrispondenti alle attività che il Fondo Pensione Caimop ha l'esigenza di ricevere:

1. Gestione dei rischi informatici;
2. Gestione degli incidenti informatici;
3. Test di resilienza operativa digitale;
4. Gestione dei rischi informatici derivanti da terzi (servizi ICT);
5. Condivisione delle informazioni.

In considerazione di quanto specificato, si riassumono di seguito i **principali interventi** da svolgere nell'ambito del supporto professionale richiesto:

- Metodologia di gestione del rischio ICT;
- Gestione degli asset ICT;
- Sicurezza ICT;
- Operazioni ICT;
- Acquisizione, sviluppo e gestione dei sistemi ICT;
- Sicurezza fisica e ambientale;
- Risorse umane;
- ICT business continuity.

In sintesi, il Fondo richiede:

- assistenza e consulenza per lo svolgimento delle **attività propedeutiche** alla pianificazione del lavoro al fine di organizzare gli **interventi in coerenza con gli obiettivi del Regolamento**;
- supporto nell'implementazione di un **modello di compliance** al DORA.

B) FUNZIONE DI GESTIONE DEL RISCHIO INFORMATICO

Il Regolamento DORA prevede che si attribuiscano le responsabilità "della gestione e della sorveglianza dei rischi informatici" ad una **funzione di controllo indipendente** di II livello, distinta dalle altre.

Le principali responsabilità della funzione di **gestione e sorveglianza dei rischi ICT** (detta anche, di seguito, "funzione" o "funzione di gestione del rischio informatico"), possono essere sostanzialmente riassumibili in un generale "coordinamento ed esecuzione di tutte le attività necessarie ad attuare il quadro per la gestione dei rischi informatici definito dall'organo di gestione, monitorandone il corretto funzionamento nel continuo".

Più specificamente, i **compiti assegnati alla Funzione** consistono:

a) nel concorrere alla definizione della politica di gestione dei rischi informatici;

b) nell'assicurare che i rischi ICT e di sicurezza siano individuati, misurati, valutati, gestiti, monitorati nonché riportati e mantenuti entro i limiti della propensione al rischio del Fondo;

c) nell'effettuare tutte le attività di controllo necessarie ad assicurare il corretto funzionamento del quadro di gestione dei rischi informatici così come approvato dall' organo di gestione a seguito delle preliminari attività di adeguamento al Regolamento DORA;

d) nel partecipare attivamente nei progetti di modifica sostanziale del sistema informativo e, in particolare, nei processi di controllo dei rischi relativi a tali progetti;

e) nel redigere, con cadenza annuale, la relazione sul riesame del quadro per la gestione dei rischi informatici.

La candidatura dovrà includere una dichiarazione contenente una **proposta di collaborazione** prevedendo l'utilizzo di professionisti con professionalità e competenze di:

- IT audit;
- Sicurezza;
- Risk & Compliance;
- IT Governance;
- ERP Integrity e Segregation of Duty (SOD).

Tale proposta dovrà **almeno contenere** indicazione in relazione a:

- organizzazione del fornitore (struttura e caratteristiche organizzative, esperienze ed eventuali certificazioni);
- la sussistenza di fattispecie di potenziali conflitti di interesse, oltreché per rapporti esistenti con gli organismi di governo e di controllo del Fondo, anche in ragione di attività prestate in favore di soggetti terzi;
- descrizione delle attività e dei *deliverable* in oggetto e di quant'altro ritenuto utile/necessario per il raggiungimento della conformità al DORA da parte del Fondo sulla base di una pianificazione articolata nelle seguenti fasi:
  - Assessment;
  - Gap Analysis;
  - Piano di Azione;
  - Adeguamento framework documentale;
  - Adeguamento Framework applicativo;
  - Esercizio esternalizzato della funzione di gestione del Rischio informatico;
  - Manutenzione periodica dell'impianto;
  - Formazione;
- descrizione delle modalità di esecuzione delle attività e dei *deliverables* di progetto;

- composizione del team di lavoro indicandone un profilo sintetico, le esperienze maturate e la relativa seniority e allegando i curricula delle figure di riferimento;
- stima delle giornate uomo previste nell'ambito di ciascuna fase e loro distribuzione per profilo professionale;
- pianificazione di massima della durata di progetto (inizio/fine);
- condizioni economiche dettagliata per ciascuna fase nonché condizioni di maggior favore per l'esecuzione di più fasi.

Il Fondo Pensione procederà alla valutazione delle candidature pervenute, nell'ambito della quale si riserva di effettuare colloqui di approfondimento. Il Fondo potrà richiedere eventuali chiarimenti ed integrazioni della documentazione trasmessa.

Il Fondo, in esito alle valutazioni, tramite apposita deliberazione da parte del Consiglio di Amministrazione, a suo insindacabile giudizio, sceglierà quali fasi attivare ed il/i soggetto/i aggiudicatari dello specifico incarico dandone comunicazione allo stesso. L'affidamento di tale incarico sarà subordinato e conseguente al buon esito del processo di sottoscrizione del relativo contratto.

La candidatura alla selezione dovrà essere inviata al Fondo **entro il giorno 4 novembre 2024** esclusivamente tramite PEC all'indirizzo caimop@pec.it e l'oggetto dovrà riportare la dicitura "***Selezione società per adeguamento al Regolamento DORA***.".

Si precisa che la presente offerta non comporta per il Fondo alcun obbligo o impegno ad affidare i predetti servizi agli eventuali candidati e per questi alcun diritto nei confronti del Fondo.

Il Fondo, Titolare del trattamento dei dati, tratterà i dati personali acquisiti nel corso del processo di selezione nel pieno rispetto delle disposizioni di cui al Regolamento UE 2016/679.

Il Presidente del Consiglio di Amministrazione

Dott. Mohammad Alkilani