acquedottolucano

Area Sistemi Informativi

Oggetto: "Procedure di Gestione della Sicurezza Informatica di Acquedotto Lucano SpA e certificazione secondo la norma ISO/IEC 27001:2022 e 20017:2015 relativa al Sistema di Gestione della Sicurezza delle Informazioni"

DISCIPLINARE TECNICO DEL SERVIZIO DI SUPPORTO AL MANTENIMENTO DELLA CERTIFICAZIONE ISO/IEC 27001:2022 e 20017:2015 E PER LA FORMAZIONE

Versione n° del	Redatto da	Responsabile	VISTO:
1.0 del 28.03.2025	Giuseppe Petrigliano	Giuseppe Petrigliano	Raffaele Cafarelli
		Firmato digitalmente da: GIUSEPPE PETRIGLIANO Data: 09/10/2025 15:47:18	

Art. 1 Oggetto del servizio

Con riferimento alle esigenze della funzione Sistemi Informativi di Acquedotto Lucano nell'ambito delle attività di gestione della sicurezza delle informazioni, si richiede la presentazione di un'offerta tecnico-economica per la fornitura dei seguenti servizi per la durata di tre anni:

- supporto al rinnovo, al mantenimento e al miglioramento del proprio Sistema di Gestione della Sicurezza dell Informazioni (SGSI) certificato ISO/IEC 27001:2022 e 20017:2015 il cui audit per il rinnovo e il mantenimento da parte dell'ente di certificazione è previsto negli anni 2026, 2027 e 2028;
- supporto all'attività di Vulnerability Assessment/Penetration Test (VA/PT) da parte di fornitore individuato da Acquedotto Lucano con apposito affidamento;
- attività di formazione al personale di Acquedotto Lucano, sia in ambito sia non in ambito, anche mediante l'utilizzo di una piattaforma web, con certificazione dell'avvenuta formazione, sugli argomenti relativi alle procedure SGSI con relativa certificazione ISO 27001 ed al General Data Protection Regulation (GDPR);

Art. 2 Descrizione dei servizi richiesti

Supporto al mantenimento della certificazione ISO/IEC 27001:2022-20017:2015

Acquedotto Lucano S.p.a. ha conseguito la certificazione ISO/IEC 27001:2022 - 20017:2015 relativa alla sicurezza delle informazioni per la funzione aziendale Sistemi Informativi con campo di applicazione definito, attualmente, come "Gestione e Monitoraggio dell'infrastruttura IT utilizzata a supporto dell'erogazione dei servizi interni e dei servizi erogati al cittadino. Gestione di servizi cloud PaaS e SaaS in accordo alle linee guida ISO/IEC 27017:2015" nel cui ambito operano sette risorse di Acquedotto Lucano.
L'attività di supporto deve garantire il mantenimento della certificazione, assicurando la conformità sui seguenti punti:

a) supporto al mantenimento della certificazione, che prevede:
    - revisione ed aggiornamento/ampliamento del Campo di Applicazione del SGSI e del Manuale SGSI;
    - attività derivanti dall'esito dell'ultimo Audit effettuato dall'Ente di Certificazione;
    - revisione della Risk Analysis e del Piano di Trattamento dei Rischi;
    - revisione del Sistema degli indicatori;
    - supporto alle attività di Audit interni e di eventuali terze parti con presenza presso le sedi Acquedotto Lucano interessate. Gli Audit dovranno essere effettuati esclusivamente da risorse certificate Lead Auditor 27001:2022 27017:2015;
    - individuazione degli elementi, in ambito e fuori ambito, che possono concorrere al realizzarsi delle "Non Conformità" (es. contratti di appalto non specifici della funzione Sistemi Informativi con ripercussioni sulla funzione stessa);
    - supporto alla gestione delle "Non Conformità" rilevate;
    - supporto alla attività di redazione e revisione della documentazione;
    - supporto in fase di certificazione;
    - partecipazione e supporto alla stesura del Riesame di Direzione sul SGSI;
    - presenza durante le fasi di verifica da parte dell'ente certificatore;
    - conduzione di audit di seconda parte. L'attività dovrà prevedere 15 audit in modalità remota o, in locale, presso fornitori ubicati nella regione Basilicata.
b) rilevazione, definizione del fabbisogno formativo e relativa formazione:
    - definizione del piano di formazione aziendale;

- verifica/adeguamento/implementazione delle risorse dedicate alla formazione (documenti, video, …);
- progettazione degli eventi formativi attraverso l'uso di una piattaforma di formazione on-line, messa a disposizione dell'aggiudicatario, ed almeno una sessione in aula da realizzarsi presso la sede di Potenza;
- organizzazione degli eventi formativi;
- verifica e valutazione dei risultati, con rilascio di attestazione dell'effettiva erogazione sia alla risorsa sia al responsabile SGSI;
- affiancamento all'implementazione organizzativa post formazione.

Per le attività di formazione, l'aggiudicatario deve:

1. inserire i contenuti formativi previsti (slide, documenti, …) sulla piattaforma web fornita;
2. rendere disponibile l'accesso alla piattaforma di formazione, a tutte le risorse indicate da AL, per 24 mesi dalla data di richiesta di attivazione della formazione;
3. monitorare l'andamento del percorso formativo di ciascuna risorsa intervenendo, su richiesta ed attraverso i servizi di amministrazione della piattaforma, per supportare le risorse durante tutto il loro percorso formativo;
4. creare test di apprendimento con domanda e risposta;
5. rendere disponibile, almeno, un accesso di amministratore di sistema per la verifica ed il monitoraggio del piano di formazione.

L'attività di supporto al mantenimento dovrà terminare, annualmente, trenta giorni prima della visita da parte dell'ente di certificazione, o in altra data concordata con il responsabile SGSI di Acquedotto Lucano S.p.a..

Art. 3 – Durata e importo dell'incarico

Sulla scorta di quanto indicato nel precedente art. 1, la durata del contratto è fissata in 3 (tre) anni decorrenti dalla data di avvio del servizio comunicata dal Responsabile del Procedimento per la fase di esecuzione.
L'importo complessivo a base della gara per il triennio, per l'affidamento del servizio oggetto del presente Capitolato è così suddiviso:

Servizio	Importo	Tipologia
Supporto al mantenimento	39.000 €	Canone
Audit di 2 parte	15.000 €	A consuntivo

pari a € 54.000 oltre IVA.
L'incidenza del costo lavoro è stimato nella misura del 70% dell'importo a base di gara.

Art. 4 – Gruppo di lavoro

L'aggiudicatario, prima della stipula del contratto, dovrà comunicare i componenti del gruppo di lavoro che saranno impegnati nello svolgimento delle attività relative al mantenimento del SGSI/ISO 27001-27017.
Tutti i componenti del gruppo di lavoro dovranno essere in possesso della certificazione Lead Auditor ISO/IEC 27001:2022. Per tali componenti, ai fini della stipula del contratto, dovrà essere prodotta la necessaria documentazione tesa a comprovare il possesso della suddetta certificazione.

Art. 5 – Modalità di erogazione del servizio

Tutte le attività necessarie all'erogazione dei servizi previsti nel presente Disciplinare sono a carico dell'aggiudicatario che avrà cura di provvedere allo spostamento del personale interessato con mezzi propri. Sono a carico dell'aggiudicatario tutte le spese accessorie e necessarie per l'erogazione dei servizi, quali trasporto o spedizione del bene, spese di trasferta del personale, ecc., escluse le spese per l'acquisizione di eventuali licenze o hardware.

Art. 6 – Penali

Inadempienza	Penale
Risorse del Gruppo di Lavoro presenti sul progetto diverse da quelle previste nel Bando di Gara	2.000 euro per ogni risorsa del Gruppo di Lavoro sostituita
Ritardi nella consegna degli avanzamenti rispetto al Piano di Progetto	200 euro per ogni giorno solare di ritardo

Art. 7 – Modalità di fatturazione e di pagamento

La fatturazione per i servizi di supporto per il mantenimento e miglioramento del Sistema di Gestione della Sicurezza dell Informazioni e per le attività di formazione deve avvenire con cadenza trimestrale posticipata.
I pagamenti saranno disposti previo accertamento della regolare esecuzione[1] del servizio rispetto alle condizioni e ai termini stabiliti nel presente Capitolato.
Il pagamento dei corrispettivi sarà effettuato nel rispetto dei termini previsti dal D. Lgs. 231/2002 come modificato ed integrato dal D. Lgs. 192/2012.

Art. 8 – T.U. Sicurezza 81/2008

Tenuto conto di quanto previsto dall'art. 26, comma 3-bis del D. Lgs. 81/2008, non si è reso necessario predisporre il Documento Unico di Valutazione dei Rischi da interferenza (DUVRI), stante la natura intellettuale dei servizi oggetto di gara; conseguentemente l'importo dei costi della sicurezza connessi ai rischi da interferenza è pari a zero.
In ogni caso Acquedotto Lucano, per l'esecuzione delle attività che richiedono la presenza presso i propri locali di personale dell'aggiudicatario, prima dell'accesso fornirà dettagliate informazioni sui rischi specifici esistenti nei propri uffici e sulle misure di prevenzione e di emergenza adottate.

Art. 9 - Sicurezza e riservatezza (NDA) delle informazioni

I servizi forniti dall'aggiudicatario devono essere regolarmente monitorati, riesaminati e registrati e, se necessario, potranno essere condotti periodicamente degli audit.

Gli audit verranno condotti considerando i requisiti previsti dalla famiglia di norme internazionali ISO/IEC 27000 o altri standard relativi ad attività di audit tecnici o di processo focalizzati sugli aspetti di sicurezza delle informazioni (es. Cobit, ENISA, NIST, ecc.).
Gli audit di seconda parte rappresentano lo strumento per garantire uniformità del livello di conformità agli standard di Acquedotto Lucano S.p.a..
A tale scopo:

[1] Si intende regolare esecuzione l'attestazione da parte di Acquedotto Lucano S.p.a. del completamento della fornitura/prestazione dell'aggiudicatario (es. collaudo).

1. Acquedotto Lucano si riserva il diritto di effettuare e l'aggiudicatario si impegna ad acconsentire, ispezioni ed audit presso l'aggiudicatario ed i locali da questi utilizzati, allo scopo di verificarne i processi produttivi, i sistemi di qualità ed ogni altro dato che possa influire sulla corretta e tempestiva esecuzione delle prestazioni contrattuali.
2. l'aggiudicatario si impegna, altresì, su richiesta di Acquedotto Lucano, ad eseguire in conformità alla norma ISO 19011, propri Audit interni ed a svolgere Audit nei confronti dei propri fornitori, ove del caso, per verificare il rispetto di tali requisiti, fornendone le relative evidenze.
3. Acquedotto Lucano si riserva di eseguire, in conformità alla norma ISO 19011, specifici audit allo scopo di verificare la conformità ai requisiti di sicurezza e privacy definiti.

Relativamente ai servizi di cui alla presente Gara, l'aggiudicatario si obbliga a:

- non diffondere o comunicare a terzi o ad altri dipendenti e consulenti, al di fuori di quelli coinvolti nell'erogazione del servizio e il cui elenco viene allegato all'offerta e aggiornato ad ogni sua successiva variazione da comunicare ad Acquedotto Lucano, le informazioni raccolte, i pareri, gli studi relativi effettuati, nonché gli elementi eventualmente resi disponibili da Acquedotto Lucano per lo svolgimento dell'attività progettuale e a utilizzare dette informazioni esclusivamente ai fini del presente incarico, salvo il caso in cui l'Aggiudicatario debba ottemperare ad obblighi di legge o a richieste di Pubbliche autorità alle quali non è possibile opporre un legittimo rifiuto;
- prendere visione ed osservare puntualmente le prescrizioni per la sicurezza dei dati in uso presso Acquedotto Lucano;
- custodire con la massima diligenza tutti i supporti cartacei e/o elettronici acquisiti o prodotti durante lo svolgimento delle attività;
- far rispettare il presente accordo ai propri dipendenti, e/o consulenti che, per esigenze operative, possano avere accesso alle informazioni di cui sopra.

Sono escluse dagli obblighi di riservatezza le informazioni divulgate al pubblico da Acquedotto Lucano stessa ovvero che risultino da documenti ufficiali pubblici.
Gli obblighi di riservatezza restano fermi anche dopo il termine di scadenza del presente incarico, per un periodo di tre anni.
Nel contesto del suddetto incarico l'Aggiudicatario agirà nel ruolo di Responsabile del Trattamento dei dati personali, in maniera circoscritta ai dati personali che sarà chiamata a trattare per lo svolgimento del predetto incarico, ai sensi del Regolamento (UE) 2016/679.

Art. 10 – Revisione prezzi

Sulla base di quanto indicato all'art. 60 del D.Lgs. 36/2023 e dal relativo Allegato II.2-bis, Acquedotto Lucano S.p.a. prevede la revisione prezzi per i contratti di durata pluriennale a partire dal secondo anno contrattuale, sulla base della variazione dell'indice ISTAT 702 "Attività di consulenza gestionale" (CPV 79998000-6 Servizi di assistenza professionale) rispetto alla data del mese di aggiudicazione ed è calcolata in aumento/diminuizione secondo la seguente formula:

Variazione annuale dell'indice ISTAT 702 – 5% x 80% x canone

Stima dell'accantonamento per revisione
In fase di programmazione economica, è stata prevista una stima prudenziale del 5% annuo (Variazione ISTAT 10% - 5% senza considerarne l'80%), ritenuta coerente con l'andamento storico degli indici sopra citati. Tale stima è limitata alle annualità dalla seconda alla terza e soggetta a conguaglio su base ISTAT reale dell'indicatore 702.
I valori stimati sono i seguenti:

Importo annuo base: € 18.000,00
Accantonamento per revisione prezzi (5% su 2 anni): € 900,00 × 2 = € 1.800,00
Totale importo a base di gara per tre anni: € 54.000,00
Totale stimato comprensivo revisione: € 55.800,00 (IVA esclusa)

Collocazione nel quadro economico
L'importo di € 1.800,00 sarà inserito all'interno della voce "Imprevisti e accantonamenti", garantendo la disponibilità delle risorse economiche per eventuali adeguamenti futuri.