Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

CAPITOLATO TECNICO

PER LA FORNITURA DI SERVIZI DI SECURITY OPERATION CENTER, SOC

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

1 OGGETTO, REQUISITI E AMMONTARE DELL'APPALTO 3
1.1 REQUISITI DI PARTECIPAZIONE 3
1.2 DURATA DELL'APPALTO 4
2 SERVIZIO SOC 4
2.1 AMBITO DEL SERVIZIO 5
2.2 PERIMETRO DI RIFERIMENTO 5
2.3 PROCESSI DI GESTIONE 6
2.4 SERVIZI RICHIESTI 7
2.4.1 FASE 1 – SETUP DEL SERVIZIO SOC E ASSESSMENT INIZIALE 7
2.4.2 FASE 2 – SERVIZIO SOC/CSIRT 8
2.4.3 MODALITA' DI EROGAZIONE DEL SERVIZIO 9
2.4.4 APERTURA E GESTIONE DEI TICKET 10
2.4.5 FLUSSO RILEVAMENTO E GESTIONE EVENTI DI SICUREZZA 10
2.4.6 COMUNICAZIONI ISTANTANEE, DI EMERGENZA ED EXTRA-LAVORATIVO 11
2.5 FASE 3 – SUPPORTO SPECIALISTICO 12
2.6 COMPETENZE RICHIESTE PER I SERVIZI SOC 12
3 MODALITÀ DI EROGAZIONE DEL SERVIZIO 14
3.1 RUOLI 14
3.2 DOTAZIONI E STRUMENTAZIONE TECNOLOGICA 14
3.2.1 PIATTAFORMA SIEM E STRUMENTI DI SICUREZZA UTILIZZATI DAL SOC 14
3.2.2 DASHBOARD DI MONITORAGGIO E SISTEMA DI TICKETING 15
3.3 PROCESSI DI GOVERNANCE 15
3.3.1 ALLINEAMENTO SU STATO DEL SERVIZIO (SAL) 16
3.3.2 GESTIONE DELLE PENALI 16
3.3.3 GESTIONE DEI PROBLEMI 16
3.3.4 PROCEDURA DI ESCALATION 17
3.4 VERIFICHE ED ISPEZIONI 17
3.5 DEFINIZIONE E CLASSIFICAZIONE DEGLI EVENTI DI SICUREZZA 18
4 SLA E PENALI 20
5 PRIVACY & RISERVATEZZA 22
6 FATTURAZIONE 22
7 FORMATO DELL'OFFERTA 22
7.1 OFFERTA TECNICA 23
7.2 OFFERTA ECONOMICA 23
8 CRITERIO DI AGGIUDICAZIONE 24

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

1 OGGETTO, REQUISITI E AMMONTARE DELL'APPALTO

Il presente appalto rientra tra i contratti di forniture e servizi che vengono aggiudicati per scopi diversi dall' esercizio delle attività inerenti il settore speciale d'intervento della società (cosiddetti contratti "estranei" al campo di applicazione del codice dei contratti pubblici) e pertanto è regolato dal diritto privato.

Oggetto dell'appalto è la fornitura di servizi di Security Operation Center (SOC) e di supporto specialistico e di assistenza così come descritti nel presente capitolato.

Acque SPA (in seguito la Società) richiede un'offerta tecnico-economica per la fornitura dei servizi sopraccitati.

L'importo complessivo a base di negoziazione, per una durata complessiva di anni 3, è pari a € 450.000 (quattrocentocinquantamila euro) I.V.A. esclusa.

Non saranno ammesse offerte in aumento, né condizionate, né espresse con riserva.

1.1 REQUISITI DI PARTECIPAZIONE

Ai fini della partecipazione alla presente procedura l'Offerente dovrà dimostrare:
1) L'assenza dei motivi di esclusione di cui agli **articoli 94 e seguenti del D.lgs. 36/2023**, attestata mediante **autodichiarazione** sottoscritta dal **legale rappresentante**;
2) l'Iscrizione nel Registro delle Imprese tenuto presso la Camera di Commercio Industria Artigianato e Agricoltura per attività compatibili con l'esercizio delle attività previste nel presente capitolato;
3) un fatturato globale pari ad almeno 900.000,00€ maturato nei migliori tre anni degli ultimi cinque antecedenti alla pubblicazione della gara. Tale requisito deve essere autodichiarato in forma di dichiarazione sostitutiva dell'atto di notorietà;
4) un fatturato specifico per contratti analoghi pari ad almeno 300.000,00€ maturato negli ultimi dieci anni antecedenti alla pubblicazione della gara, di cui almeno uno di importo non inferiore a 200.000,00€ su base annua. Tale requisito deve essere autodichiarato in forma di dichiarazione sostitutiva dell'atto di notorietà;

Inoltre l'Offerente dovrà essere provvisto di:

- un sistema di qualità aziendale certificato in conformità alle norme UNI EN ISO 9001:2015, avente come scopo le attività oggetto del presente appalto. Il relativo certificato deve essere trasmesso in copia conforme all'originale, nella forma di dichiarazione sostitutiva dell'atto di notorietà.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

- un sistema di gestione della sicurezza delle informazioni certificato in conformità alla norma UNI CEI EN ISO/IEC 27001, e lo scopo della certificazione dovrà coprire le attività oggetto del presente appalto (in particolare quelle relative ai servizi SOC/CSIRT). Sarà necessario trasmettere una copia conforme all'originale del relativo certificato, presentata come dichiarazione sostitutiva dell'atto di notorietà.

1.2 DURATA DELL'APPALTO

La durata del contratto è fissata in n. 3 anni a decorrere dalla data di attivazione dei servizi oggetto dell'appalto, indicata in un apposito verbale di inizio delle attività accettato dalle parti.
Alla scadenza del termine, il rapporto contrattuale si estingue, senza necessità di preavviso o disdetta.
Il contratto potrà essere prorogato limitatamente al tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione di un nuovo contraente agli stessi prezzi patti e condizioni di cui al contratto oggetto di proroga; in tal caso l'appaltatore sarà tenuto ad eseguire le ulteriori prestazioni anche per il periodo di proroga.

2 SERVIZIO SOC

Acque intende affidare i servizi di Security Operations Center con l'obiettivo di consolidare e potenziare la propria postura di sicurezza informatica, garantendo la protezione dell'integrità, della disponibilità e della riservatezza dei dati aziendali, nonché la continuità operativa dei processi di business critici. Il servizio mira a fornire una visibilità completa e in tempo reale sullo stato di sicurezza dell'intera infrastruttura IT e OT, abilitando una gestione coordinata e professionale delle minacce informatiche attraverso competenze specialistiche e tecnologie all'avanguardia.

Il SOC sarà chiamato a fornire anche i servizi di Incident Response, e in questo caso, congiuntamente ai referenti individuati all'interno dell'azienda, svolgerà la funzione di CSIRT (Computer Security Incident Response Team).
L'obiettivo è confermare e adeguare la disponibilità di una struttura operativa di tipo SOC/ CSIRT alle attuali esigenze dell'organizzazione e allo stato dell'arte tecnologico.

Il SOC dovrà fornire almeno le seguenti tipologie di servizi:

- **Servizi di monitoraggio e rilevamento continuo**: monitoraggio 24/7 dell'infrastruttura IT e OT per identificare in tempo reale attività anomale e potenziali minacce, analisi

proattiva e gestione continuativa di sistemi e tecnologie di sicurezza, gestione dei dispositivi di sicurezza (Security Device Management).

- **Servizi di analisi e risposta agli incidenti**: attività di investigazione sulle minacce rilevate e prioritizzazione degli eventi, early warning e segnalazione tempestiva di incidenti di sicurezza con analisi puntuale, gestione degli incidenti e risposta coordinata in accordo con il committente, raccolta evidenze inclusa la digital forensics.
- **Servizi proattivi e miglioramento continuo della sicurezza**: integrazione con threat intelligence per la contestualizzazione degli alert, attività di vulnerability assessment e penetration test, threat hunting su base regolare e/o su richiesta, rafforzamento continuo dell'infrastruttura di sicurezza per ridurre la superficie di attacco.
- **Servizi di supporto e reportistica**: generazione di report periodici operativi su assessment strumentali, eventi di sicurezza, incidenti gestiti, vulnerabilità e SLA, oltre ad assistenza tecnica e supporto operativo qualificato.

2.1 AMBITO DEL SERVIZIO

Nel presente paragrafo sono definiti il perimetro di azione, i servizi e tutti gli aspetti a contorno che permetteranno un efficace ed efficiente funzionamento dei servizi richiesti.
L'attuale descrizione è finalizzata alla corretta identificazione del perimetro di applicazione del contratto, fermo restando la naturale evoluzione da un lato delle esigenze aziendali, dall'altro delle nuove soluzioni e tecnologie che potranno essere introdotte all'interno della durata contrattuale.
Tutte le informazioni relative all'ambito di applicazione del servizio sono aggiornate al mese di luglio 2025; si precisa inoltre che all'interno del periodo di setup del servizio saranno forniti in dettaglio tutti i riferimenti relativi agli asset coinvolti ed alle modalità di gestione, i processi e sotto-processi di gestione ed i dettagli sugli attuali strumenti di monitoraggio.

2.2 PERIMETRO DI RIFERIMENTO

Di seguito è pubblicato il cruscotto riepilogativo di massima degli ambiti IT/OT oggetto dei servizi SOC; tale schema rappresenta un'indicazione per l'Offerente del perimetro che dovrà andare a gestire in modo da assicurare un servizio adeguato alle esigenze di Acque.
Si precisa che presso i 2 datacenter sono erogati servizi esposti alla rete pubblica.

	Infrastruttura	Qty.
Oggetti	Sedi Datacenter / centri stella	2
	Sedi periferiche	25

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

	Device Type IT	Qty.
Oggetti	postazioni client Windows	500
	apparati mobili (smartphone/tablet)	350
	Windows Server AD, DNS, DHCP, ESX, Auth	20
	Windows IIS and Web Servers	20
	Windows General Purpose Servers	180
	Linux Servers	50
	Antivirus Servers	2
	Database Servers	10
	Core, Large Firewalls	14
	IDS, IPS, VPN, WAF, DAM, DLP, LB	10
	Routers and Switches & Wireless	100
Eventi	**EPS medi Stimati**	**2000**

	Device Type OT *	Qty.
Oggetti	Windows Server	15
	Periferiche OT	2500

*Non oggetto di monitoraggio diretto da parte del SIEM

2.3 PROCESSI DI GESTIONE

È richiesto all'offerente di proporre i processi utilizzati per l'erogazione del servizio SOC/CSIRT per consentire al Committente di ridurre significativamente i rischi di disservizio nei confronti delle richieste del Business durante la fase di implementazione del Contratto.
Le proposte dovranno essere strutturate andando a dettagliare processi, framework e standard relativi, utilizzati dall'Offerente per soddisfare i servizi richiesti, facendo riferimento laddove possibile agli standard di settore tra cui, a titolo esemplificativo:

- COBIT5;
- ITIL v3/4;
- PRINCE2 e PMP;
- ISO/IEC 27035.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

2.4 SERVIZI RICHIESTI

Di seguito l'elenco delle attività che vanno a comporre i servizi richiesti:

- **Fase 1 – Setup del servizio SOC e Assessment Iniziale**
- **Fase 2 – Servizio SOC**
- **Fase 3 – Supporto specialistico**

2.4.1 FASE 1 – SETUP DEL SERVIZIO SOC E ASSESSMENT INIZIALE

Queste attività sono finalizzate all'avvio del servizio SOC, in continuità rispetto ai servizi SOC già in essere, a partire dall'analisi dello stato attuale di esposizione al rischio dei servizi e delle infrastrutture di Acque SpA, con relative proposte di mitigazione e/o risoluzione.

L'avvio dell'erogazione dei servizi a cura dell'Offerente sarà preceduto da una fase di "setup" che avrà l'obiettivo di:

- permettere all'Offerente di acquisire maggiore conoscenza del contesto tecnologico di Acque (tecniche, strumenti, tecnologie), dell'organizzazione, della funzione Security di Acque S.p.A., nonché delle procedure e prassi operative in essere;
- definire e concordare tra il Committente e l'Offerente le modalità di erogazione dei Servizi in termini di processi, procedure, strumenti e modalità di comunicazione;
- attuare tutte le attività propedeutiche all'avvio dell'erogazione dei servizi da parte dell'Offerente al termine della fase stessa, tra le quali:
    - Assessment iniziale dell'infrastruttura di sicurezza;
    - Definizione dei flussi informativi, dei processi di escalation e di autonomia nella response del SOC;
    - Integrazione, se necessari ai fini dell'erogazione del servizio, di strumenti forniti dal committente con i sistemi di sicurezza esistenti, previa valutazione tecnica; condivisione piattaforme di sicurezza aziendali e perimetro di azione del SOC;
    - Piattaforma SIEM As-a-Service: l'Offerente dovrà mettere a disposizione la propria piattaforma SIEM (Security Information and Event Management) come servizio, inclusi l'hardware, il software, le licenze, gli aggiornamenti, la manutenzione e la gestione completa della stessa. La piattaforma SIEM sarà lo strumento centrale per la raccolta, la correlazione e l'analisi dei log e degli eventi di sicurezza provenienti dalle infrastrutture di Acque. A tale scopo in fase di startup del progetto verrà definita l'architettura necessaria;

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

- Dashboard di monitoraggio SOC e sistema di ticketing: l'Offerente dovrà mettere a disposizione una o più dashboard web dedicate per la visualizzazione in tempo reale dello stato operativo del SOC e al sistema di ticketing;
- Allineamento con la governance Cybersecurity di Acque;
- Creazione account su piattaforme e applicativi aziendali.

Il Setup dei Servizi avrà la durata massima di 90 (novanta) giorni solari.

Al termine del Setup dei Servizi saranno consegnati i seguenti deliverable, i quali una volta confermati da Acque rappresenteranno l'accettazione del setup (collaudo) per la partenza dei Servizi:

- Manuali operativi, procedure, workflow del SOC/CSIRT;
- Documentazione di setup degli ambienti e loro integrazione nel SOC;
- Descrizione metodologica delle attività operative.

I deliverable dovranno essere gestiti come una tantum con possibilità di aggiornamenti su richiesta.
In questo lasso di tempo, verranno gestiti i ticket aperti e le eventuali problematiche che sorgeranno senza l'applicazione di penali eventualmente contrattualizzate (graceful period).

2.4.2 FASE 2 – SERVIZIO SOC/CSIRT

Le attività richieste sono quelle tipiche di un moderno servizio di Security Operations Center (SOC), finalizzate a garantire la protezione continua delle infrastrutture IT e OT, la rilevazione tempestiva degli incidenti di sicurezza, la gestione delle vulnerabilità e il miglioramento continuo della postura di sicurezza aziendale. In particolare, il servizio dovrà coprire almeno i seguenti ambiti:

- Monitoraggio e rilevamento: Attività di monitoraggio proattivo H24/7 delle infrastrutture e dei sistemi IT/OT, con correlazione centralizzata degli eventi tramite piattaforme SIEM o equivalenti, al fine di rilevare tempestivamente attività sospette o malevole.

- Gestione degli incidenti (Incident Handling): Analisi, prioritizzazione e risposta agli eventi di sicurezza rilevati, in coordinamento con i referenti aziendali. In caso di incidente confermato, il SOC assumerà anche il ruolo di CSIRT, provvedendo a:
  - raccolta e conservazione delle evidenze;
  - analisi forense;
  - gestione delle comunicazioni ed escalation;
  - definizione congiunta delle azioni correttive;
  - redazione della documentazione di lesson learned.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

- Threat Intelligence: raccolta, analisi e integrazione di informazioni su minacce emergenti, vulnerabilità zero-day, indicatori di compromissione (IOC), campagne attive. Il servizio dovrà fornire alert tempestivi su eventi rilevanti per il contesto del Committente.

- OSINT (Open Source Intelligence): erogazione di attività di OSINT volte alla raccolta e analisi di informazioni disponibili pubblicamente per identificare potenziali minacce, vulnerabilità o informazioni rilevanti per la sicurezza dell'organizzazione. Tale servizio dovrà essere erogato almeno 1 volta l'anno.

- Vulnerability Management e Penetration Test:
  - Vulnerability Assessment (VA): scansione e analisi dei sistemi e servizi per identificare vulnerabilità note.
  - Penetration test: su richiesta esplicita del Committente e basati sui risultati delle VA.

  Sono richieste almeno 2 VA all'anno.

- Threat Hunting: ricerca proattiva e sistematica di minacce latenti mediante analisi comportamentali avanzate, correlazione di eventi e identificazione di pattern di attacco anomali. L'attività deve essere condotta quotidianamente, tale da garantire l'identificazione tempestiva di minacce persistenti e non rilevate dai sistemi automatizzati.

- Reporting: si richiede la produzione di report operativi su:
  - assessment strumentali (riepilogo e dettaglio, una tantum e post eventuali aggiornamenti);
  - eventi di sicurezza rilevati (mensili);
  - incidenti gestiti (mensili);
  - stato delle vulnerabilità (quadrimestrale);
  - andamento degli SLA (mensili).

I report dovranno essere forniti con la cadenza richiesta secondo i formati concordati con il Committente.

2.4.3 MODALITA' DI EROGAZIONE DEL SERVIZIO

Il servizio SOC H24 dovrà essere erogato prevalentemente in modalità remota, operando dalle sedi dell'Offerente.
Dovrà essere prevista la possibilità di interazione strutturata con terze parti, quali ad esempio il NOC del Committente o altri fornitori tecnologici se necessario.
L'Offerente dovrà garantire la disponibilità continua del servizio H24, 7 giorni su 7, inclusi festivi nazionali, assicurando la copertura di tutti i turni operativi e la presenza di personale qualificato a tutti i livelli.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

Per garantire un'efficace gestione degli eventi e degli incidenti di sicurezza H24, il SOC dovrà essere strutturato su un modello a livelli (Tiers) ben definito. L'Offerente dovrà dettagliare la composizione del proprio team SOC per ciascun livello, includendo il numero di risorse dedicate, le loro certificazioni pertinenti e le competenze maturate.

2.4.4 APERTURA E GESTIONE DEI TICKET

Tutte le comunicazioni formali relative agli allarmi e agli incidenti di sicurezza, incluse le richieste di informazioni o di azioni, dovranno avvenire esclusivamente tramite l'apertura di un ticket dedicato nel sistema di trouble ticketing messo a disposizione dall'Offerente. Il ticket dovrà avere almeno le seguenti caratteristiche:

- **Identificativo Univoco:** Ogni comunicazione formale dovrà generare un ticket con un identificativo univoco e tracciabile.
- **Contenuto dei Ticket:** Il ticket dovrà contenere le seguenti informazioni minime:
  - Identificativo univoco dell'evento/incidente originale;
  - Gravità e priorità (Critico, Alto, Medio, Basso) definite dal SOC;
  - Descrizione chiara dell'evento e dell'impatto potenziale sull'infrastruttura di Acque;
  - Sistema/asset coinvolto e relative informazioni tecniche;
  - Azioni già intraprese dal SOC;
  - Azioni richieste ad Acque o informazioni necessarie per l'ulteriore indagine;
  - Data e ora di apertura e ultimo aggiornamento.
- **Aggiornamenti e Storico:** l'Offerente dovrà garantire che tutti gli aggiornamenti e le interazioni relative al ticket siano registrati e tracciabili nel sistema di trouble ticketing, consentendo ad Acque di consultare e scaricare lo storico completo.

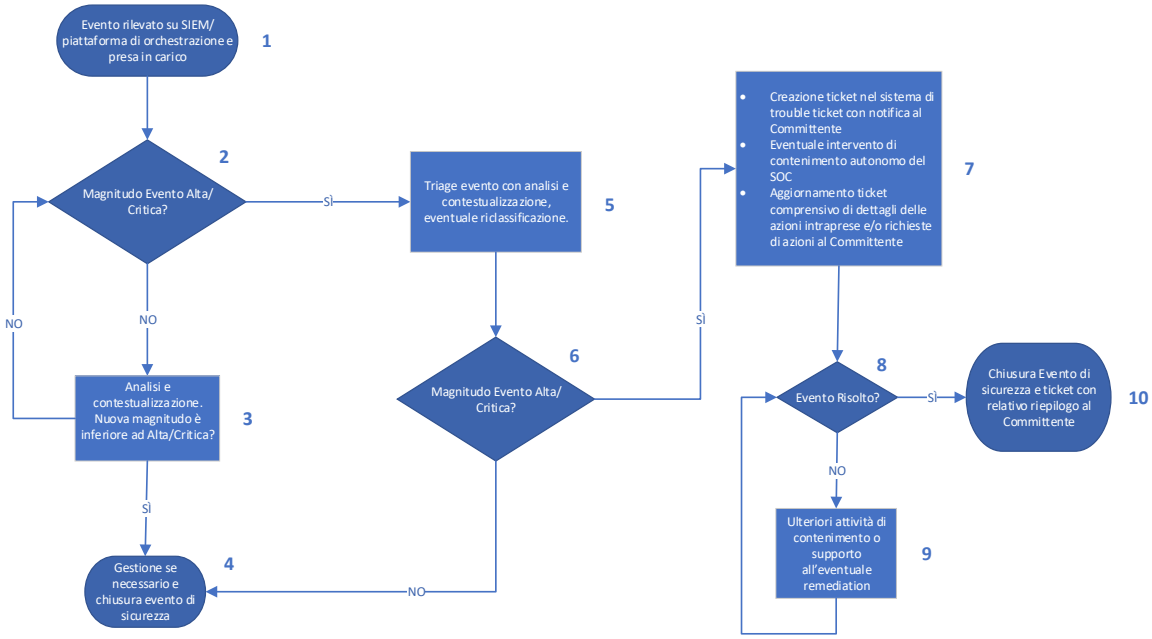
2.4.5 FLUSSO RILEVAMENTO E GESTIONE EVENTI DI SICUREZZA

Viene richiesto al Committente l'adozione del processo operativo per la gestione degli eventi di sicurezza informatica attraverso un flusso strutturato basato sulla valutazione della criticità e dell'impatto degli incidenti rilevati.
Il processo di gestione degli eventi di sicurezza è progettato per garantire una risposta differenziata e proporzionata alle criticità delle minacce rilevate, assicurando tempi di risposta adeguati al livello di rischio identificato e la corretta escalation degli incidenti di sicurezza.
Il flusso operativo si basa su un sistema di decision-making strutturato che prevede valutazioni multiple della magnitudo degli eventi, consentendo percorsi alternativi di gestione in base alla criticità effettiva dell'incidente. La piattaforma SIEM e di orchestrazione costituisce il punto di ingresso centralizzato, mentre il sistema di trouble ticketing garantisce la tracciabilità e la gestione formale degli incidenti confermati.
Il processo implementa una logica di triage progressivo che consente di filtrare efficacemente i falsi positivi e identificare gli eventi di maggiore rilevanza per la sicurezza aziendale. La doppia

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

valutazione della criticità assicura che gli incidenti confermati vengano gestiti attraverso procedure strutturate di contenimento e remediation, con comunicazione tempestiva al Committente degli sviluppi significativi dei soli eventi Alti/Critici.
Il diagramma di flusso allegato illustra graficamente i punti chiave del processo decisionale, evidenziando gli aspetti critici di valutazione, escalation e comunicazione che caratterizzano il servizio SOC.



2.4.6 COMUNICAZIONI ISTANTANEE, DI EMERGENZA ED EXTRA-LAVORATIVO

Le comunicazioni istantanee tramite **telefono o chat/Instant Messaging** (es. piattaforma concordata come Microsoft Teams) dovranno essere riservate esclusivamente ai casi di emergenza o di elevata criticità che richiedono un'azione immediata e coordinata e che non possono attendere l'apertura o l'aggiornamento di un ticket o comunque conseguenti allo stesso.

- **Criteri di Emergenza:** I criteri che definiscono un "caso di emergenza" saranno stabiliti congiuntamente dal Committente e dall'Offerente durante la fase di onboarding, a titolo esemplificativo includeranno:
  - Compromissione attiva di sistemi critici;
  - Attacchi ransomware o eventi con impatto diffuso sull'operatività aziendale;
  - Violazioni di dati con rischio immediato di divulgazione;
  - Qualsiasi evento classificato come "Critico" secondo gli SLA.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

- **Processo di Attivazione:** l'Offerente dovrà indicare numeri di telefono e contatti di chat dedicati per le emergenze, attivi H24/7. Ogni comunicazione di emergenza dovrà essere seguita dall'apertura di un ticket formale per la tracciabilità.
- **Contatti per Orario Extra-Lavorativo:** Per le comunicazioni in orario extra-lavorativo (fuori orario lavorativo, notturno, weekend, festivi nazionali) di Acque, saranno condivisi con l'Offerente i contatti dei referenti interni e le modalità di ingaggio, anche in questo caso dovrà seguire un ticket formale per la tracciabilità.

2.5 FASE 3 – SUPPORTO SPECIALISTICO

Nella fornitura sarà compreso un basket di 200 ore di supporto specialistico, da utilizzare per tutta la durata contrattuale. Le ore saranno utilizzate discrezionalmente da Acque solo in caso di effettiva necessità, e dunque fatturate a consumo previa redazione di verbale di intervento.
Di seguito le attività richieste:

- **Assistenza tecnica qualificata**: supporto su problematiche complesse legate alla sicurezza informatica, gestione di configurazioni avanzate, aggiornamenti critici di sicurezza e risoluzione di malfunzionamenti dei sistemi di protezione;
- **Disponibilità estesa**: servizio disponibile in orari straordinari per attività critiche, interventi di emergenza e supporto su richiesta per situazioni che richiedono competenze tecniche specialistiche;
- **Servizi di consulenza avanzata**: ottimizzazione dell'infrastruttura di sicurezza, supporto per l'implementazione di nuove tecnologie di protezione e supporto per la risoluzione di incidenti complessi che necessitano di expertise avanzate in ambito cybersecurity.

Le attività sopraelencate potranno essere richieste pianificando interventi di supporto in orario lavorativo (lun-ven 8.00 – 18.00) e non lavorativo, erogate da remoto.

Nell'offerta economica l'Offerente dovrà indicare un costo orario. Ad esaurimento del basket potranno essere richiesti gli interventi/giornate dell'Offerente che fatturerà secondo il listino dettagliato nell'offerta economica.
L'Offerente dovrà presentare la dichiarazione delle certificazioni attestanti il profilo professionale dei propri tecnici.

2.6 COMPETENZE RICHIESTE PER I SERVIZI SOC

Le figure professionali che l'Offerente dovrà mettere a disposizione per l'espletamento dei Servizi richiesti dovranno avere un'esperienza maturata e comprovata di almeno 3 anni nel settore di attività di cui al presente capitolato e dovranno godere di caratteristiche in grado di soddisfare i seguenti requisiti:

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

- Laurea o Diploma in discipline tecnico / scientifiche / ingegneristiche;
- Possesso di Certificazione procedurali;
- Possesso di Certificazioni tecniche Cybersecurity, es. OSCP, CCNP Security, Fortinet NSE 8.

Il team di lavoro dovrà possedere una comprovata capacità nello svolgere servizi di:

- Advanced Vulnerability Assessment & Penetration Testing;
- Malware Analysis and Reverse Engineering;
- Deep Web Intelligence;
- Code Review;
- Phishing Campaign;
- Forensics;
- Tailored Early Warning;
- Log Management;
- Security Infrastructure Management and Maintenance;
- Threat Defence;
- Orchestrated Vulnerability Assessment;
- Internal Auditing;
- Regulatory Compliance;
- Organizational Models and Governance DSS;
- ISMS Development and Rollout;
- Risk Analysis and Treatment Plans;
- Cyber Security Enterprise Risk Management;
- Incident Detection, Mitigation, Containment and Response;
- Security Education and Training;
- Proprietary Threat Intelligence;
- Malware analysis logics;
- Legacy for traffic analysis (IT/OT);
- Event Correlation logics (Big Data).

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

3 MODALITÀ DI EROGAZIONE DEL SERVIZIO

3.1 RUOLI

L'Offerente ha il dovere di individuare un modello organizzativo in grado di rispondere in modo efficace ed efficiente alle richieste del Committente.
Si precisa che vista l'importanza che avranno i riferimenti del contratto nominati dall'Offerente, Acque individuerà al suo interno il/i ruolo/i di Service Manager (SMA) del progetto, con la funzione primaria di garantire l'erogazione dei Servizi in linea con i livelli di servizio definiti, contribuire al continuo miglioramento del servizio e gestire gli aspetti contrattuali e di comunicazione fra le parti, tale ruolo dovrà avere necessariamente un alter ego (SMO) con le medesime funzioni lato Offerente.

Il modello organizzativo che l'Offerente dovrà costruire e proporre sarà sotto diretta responsabilità dell'SMO che avrà anche il compito di intervenire con modifiche, adeguamenti o sostituzioni qualora SMA lo richieda. SMO essendo il riferimento del contratto avrà la diretta responsabilità e dovrà garantire la supervisione di tutte le figure professionali utilizzate per l'erogazione di tutti i servizi di tutte le Parti previste dal presente Capitolato.
Il modello organizzativo dovrà altresì garantire la sostituzione tempestiva delle risorse nei casi in cui per motivi di forza maggiore quest'ultime non possano entrare in servizio nell'orario indicato, dandone tempestiva comunicazione.

3.2 DOTAZIONI E STRUMENTAZIONE TECNOLOGICA

Sono a carico dell'Offerente i costi delle dotazioni assegnate al personale, della strumentazione adottata, dei materiali utilizzati, delle attività di trasporto e di ogni altro elemento, strumentale o meno, che si renda necessario per l'erogazione del servizio.

Come precedentemente esplicitato, l'Offerente dovrà mettere a disposizione del committente una piattaforma SIEM, una dashboard di monitoraggio e un sistema di ticketing. Nei prossimi capitoli saranno forniti ulteriori dettagli su ciascuno di questi requisiti.

3.2.1 PIATTAFORMA SIEM E STRUMENTI DI SICUREZZA UTILIZZATI DAL SOC

- Descrizione dettagliata della piattaforma SIEM proposta (marca, modello, architettura, funzionalità, scalabilità, retention dei log).
- Elenco e descrizione degli altri strumenti di sicurezza correlati (ad es. IDS/IPS, Threat Intelligence Platform, SOAR).

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

- Misure di sicurezza e resilienza (ad es. sicurezza logica accessi, backup e DR, HA).

3.2.2 DASHBOARD DI MONITORAGGIO E SISTEMA DI TICKETING

L'Offerente dovrà mettere a disposizione del Committente una o più dashboard web dedicate, sicure e con autenticazione forte, per la visualizzazione in tempo reale dello stato operativo del SOC. Le funzionalità potranno essere implementate in un'unica dashboard integrata o in due dashboard separate (una per il monitoraggio operativo e una per la gestione ticketing), purché garantiscano un'esperienza utente coerente e integrata.
Nel caso di dashboard separate, dovrà essere garantita l'interoperabilità e la correlazione dei dati tra le due interfacce.
Suddette piattaforme dovranno includere, a titolo esemplificativo, le seguenti funzionalità:

- **Panoramica degli Allarmi in Essere:** Visualizzazione aggregata degli allarmi attivi, classificati per gravità, origine e stato di gestione; dovrà essere comunque garantito l'accesso all'interfaccia del SIEM.
- **Stato dei Ticket Aperti:** Dettaglio di tutti i ticket di sicurezza aperti dal SOC e da Acque, inclusi numero ticket, priorità, descrizione, assegnatario, storico delle interazioni e stato di avanzamento.
- **KPI e SLA:** Monitoraggio in tempo reale dei Key Performance Indicators (KPI) e del rispetto dei Service Level Agreements (SLA).
- **Accesso ai Report:** Possibilità di consultare e scaricare la reportistica periodica e ad-hoc.
- **Riferimenti dei tecnici in servizio ed eventuali contatti:** visualizzazione dei tecnici attualmente operativi sul SOC con relativi ruoli e contatti

3.3 PROCESSI DI GOVERNANCE

Di seguito vengono descritti i principali processi di Governance che regolamentano la gestione dei rapporti fra il Committente e l'Offerente.
L'organismo di Governance formato dal/i SM di Acque (SMA) e dal/i SM dell'Offerente (SMO) gestirà i seguenti processi principali:

1. Allineamento su stato del servizio (SAL);
2. Gestione delle penali ;
3. Gestione dei problemi;
4. Procedura di escalation.

Di seguito è descritto ciascun processo in termini di procedure da seguire e coinvolgimento dell'organismo di Governance.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

3.3.1 ALLINEAMENTO SU STATO DEL SERVIZIO (SAL)

SMA e SMO parteciperanno a riunioni mensili di allineamento sullo stato del servizio (SAL), necessari a garantire una collaborazione efficace e un monitoraggio costante delle performance. Durante i SAL, SMO dovrà riportare:

- L'andamento complessivo del servizio erogato, evidenziando le principali attività svolte e i risultati conseguiti nel periodo di riferimento;
- L'analisi dettagliata dei report mensili, inclusi quelli relativi agli eventi di sicurezza rilevati, agli incidenti gestiti e allo stato delle vulnerabilità;
- La valutazione delle performance rispetto agli SLA (Service Level Agreement) e ai KPI (Key Performance Indicators) definiti, con un'analisi degli scostamenti dagli obiettivi e delle relative cause;
- Un riepilogo delle problematiche emerse, delle cause identificate e delle azioni correttive intraprese o pianificate per la loro risoluzione;
- Le attività previste per il periodo successivo, incluse eventuali manutenzioni programmate, aggiornamenti o nuove iniziative, per un allineamento costante sulle priorità.

L'obiettivo di queste riunioni è promuovere un dialogo trasparente e proattivo, consentendo all'organismo di Governance di avere piena visibilità sull'efficacia del servizio SOC e di intervenire congiuntamente per un'ottimizzazione continua.

SMO potrà essere inoltre contattato per richiedere esigenze operative aggiuntive o per l'ingaggio di altre attività di supporto specialistico.

3.3.2 GESTIONE DELLE PENALI

L’erogazione delle attività richieste sarà monitorata tramite la definizione di appositi SLA. Per tale motivo saranno richiesti con cadenza mensile, o con tempistica eventualmente da concordare, report che certifichino il rispetto degli SLA.
Durante il periodo di set-up le penali non verranno applicate, ad eccezione della penale sull’attivazione del servizio che sarà descritta nel capitolo dedicato.
A seguito di violazioni dei LdS (Livelli di Servizio), rilevate ed opportunamente annotate durante i SAL mensili, verranno applicate delle penali, salvo eventuale contestazione. In quest’ultimo caso verrà avviata dal committente la procedura di escalation necessaria; SLA e penali sono descritti nel capitolo 4 del presente capitolato.

3.3.3 GESTIONE DEI PROBLEMI

Entrambe le Parti dovranno essere diligenti e cooperare in modo efficace, efficiente e professionale nella risoluzione di conflitti, problemi o dispute che potrebbero sorgere durante lo

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

svolgimento del contratto o dopo la cessazione dello stesso relativamente ad un qualsiasi aspetto del Contratto.
Al sorgere di un qualsiasi problema, che abbia degli effetti sulle prestazioni concordate e/o che rappresenti impedimento alle attività di Acque, SMO dovrà:

- informare tempestivamente il Responsabile del Servizio di Acque;
- identificare nel minor tempo possibile l'inconveniente e le possibili cause;
- apportare nel minor tempo possibile le correzioni necessarie.

3.3.4 PROCEDURA DI ESCALATION

Le eventuali controversie o inefficienze che dovessero sorgere nel corso dello svolgimento del Contratto in merito all'erogazione del servizio e/o all'interpretazione del Contratto dovranno essere oggetto di un tentativo di soluzione condivisa come segue:

- all'insorgere di una controversia la Parte interessata dovrà comunicare all'Altra l'inconveniente e chiedere l'applicazione della procedura di escalation del problema;
- SMA ed SMO si dovranno riunire al più presto al fine di avviare il processo di analisi della controversia con lo scopo di identificare la soluzione dello stesso.

Qualora non si raggiunga in tempi brevi, ed al massimo entro una settimana, un accordo soddisfacente per entrambe le parti, il problema sarà scalato dalla Committenza.

3.4 VERIFICHE ED ISPEZIONI

Ad Acque sarà consentito, previa richiesta, l'accesso ai locali di erogazione dei servizi SOC/CSIRT, ai soli dati ed informazioni che si renderanno necessarie per l'espletamento delle attività oggetto del contratto, al personale della struttura di monitoraggio incaricato, per lo svolgimento di verifiche ed ispezioni.
Le ispezioni saranno volte alla verifica della validità dei dati relativi alla rendicontazione dei parametri previsti dal contratto per l'erogazione dei servizi (volumi ed effort erogati e livelli di servizio) ed alla conformità di quanto previsto dal contratto e dal Capitolato tecnico. I risultati delle ispezioni saranno trasmessi sotto forma di verbale.
I risultati delle attività di monitoraggio daranno luogo a raccomandazioni emesse periodicamente da parte della struttura di monitoraggio, le quali individuano eventuali Non Conformità e problemi legati alla erogazione dei servizi ed alla gestione del contratto.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

3.5 DEFINIZIONE E CLASSIFICAZIONE DEGLI EVENTI DI SICUREZZA

La presente classificazione costituisce un framework di riferimento esemplificativo e non esaustivo per la categorizzazione degli eventi di sicurezza. Il suo scopo principale è:

- Fornire una base condivisa per l'applicazione degli SLA su eventi classificati come **Alti (Livello 4)** e **Critici (Livello 5)**;
- Stabilire criteri oggettivi e misurabili per la gestione degli incidenti;
- Creare un linguaggio comune tra Committente e Offerente.

La scala di classificazione, attualmente impostata su livelli da 0 a 5 potrà essere rivista e affinata durante la fase di startup del servizio e periodicamente sulla base dell'evoluzione del panorama delle minacce, delle specificità dell'infrastruttura del Committente o della diversa modalità operativa del SOC.

Ogni evento classificato con gravità ALTA (Livello 4) e CRITICA (Livello 5) deve essere immediatamente segnalato al committente. La notifica dovrà avvenire tramite i canali di comunicazione già descritti, indipendentemente dalla necessità di un'azione attiva richiesta al committente stesso. L'obiettivo è garantire la massima visibilità e consapevolezza su eventi di potenziale impatto significativo.

Livello	Denominazione	Descrizione
Livello 5	CRITICO	Attività rilevata che indica una compromissione altamente probabile o già in atto con un potenziale impatto immediato e severo sui sistemi, dati o processi aziendali critici. Richiede un'indagine e un intervento immediati per contenere la minaccia e prevenire o minimizzare danni operativi o perdite significative. Esempi: ransomware, esfiltrazione dati, compromissione Domain Controller/sistemi di backup, APT (Advanced Persistent Threat).
Livello 4	ALTO	Attività sospetta che, se non indagata e mitigata rapidamente, ha un'alta probabilità di evolvere in una compromissione grave o un impatto significativo su sistemi importanti o dati sensibili. Esempi: Tentativi multipli e persistenti di accesso non autorizzato, rilevamento di

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

		malware su endpoint, attività insolite da account privilegiati, traffico di rete inusuale.
Livello 3	MEDIO	Anomalie, violazioni di policy o attività sospette che richiedono un'indagine approfondita per determinarne la natura e il potenziale rischio. Potrebbero indicare un tentativo di attacco preliminare, una vulnerabilità sfruttata o una non conformità che, se non gestita, potrebbe portare a un impatto maggiore. Esempi: Picchi anomali di traffico di rete verso destinazioni insolite o sospette, avvisi multipli di sistemi antivirus su più host, attività di scansione interna o esterna persistente, creazione o modifica anomala di account utente.
Livello 2	BASSO	Tentativi falliti, violazioni minori di policy, o eventi isolati che non indicano un impatto immediato, ma che possono essere indicatori preliminari di attività potenzialmente malevole o di vulnerabilità. Richiedono monitoraggio e un'analisi per pattern ricorrenti. Esempi**:** Tentativi di accesso falliti a sistemi non critici, installazione di software non autorizzato ma senza immediato impatto malevolo, piccoli volumi di traffico non consentito o non classificato.
Livello 1	INFORMATIVO	Eventi di natura informativa che costituiscono indicatori di contesto per la sicurezza aziendale senza rappresentare minacce dirette o immediate.
Livello 0	AUTORIZZATO	Eventi classificati come falsi positivi confermati o attività legittime pre-autorizzate che hanno generato alert ma non costituiscono incidenti di sicurezza. Richiedono solo registrazione per audit trail e possibile tuning dei sistemi di detection.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

4 SLA E PENALI

Servizio	SLA	Penale	Note e Criteri di Misurazione
Presa in Carico evento e Triage di eventi categorizzati con gravità Alta/Critica	Presa in carico evento: 1 ora	5% del canone mensile per ogni violazione	Tutti i tempi sono da considerarsi dalla rilevazione dell'evento sui sistemi preposti del SOC, con categorizzazione dello strumento utilizzato su soglie di criticità Alta/Critica; come riportato nel diagramma di flusso cap. 2.4.5 step 1.
Intervento contenimento per eventi con gravità Alta/Critica	Critica: 1 ora Alta: 2 ora	20% del canone mensile per ogni violazione	Analisi approfondita evento, completamento prime attività operative di contenimento autonome o concordate con il Committente, previa apertura ticket con comunicazione al Committente con tutti i dettagli riportati nel capitolo 2.4.4 "Apertura e Gestione dei Ticket", come riportato nel diagramma di flusso cap. 2.4.5 step 7; verrà considerato il tempo intercorso da fine step 1 a fine step 7.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

Risoluzione evento con gravità Alta/Critica	Critica: 4 ore Alta: 8 ore	5% del canone mensile per ogni violazione	Messa in sicurezza completata e comunicazione delle azioni correttive implementate. Include ripristino della normale operatività. come riportato nel diagramma di flusso cap. 2.4.5 step 10; verrà considerato il tempo intercorso da fine step 7 a fine step 10.
Apertura Ticket del Committente	Presa in carico: 2 ore	5% del canone mensile per ogni violazione	Ticket deve includere numero identificativo, triage secondo standard ITIL (classificazione come incidente, service request, problem, change request), priorità assegnata e conferma di presa in carico. Misurato dalla ricezione della richiesta.
Vulnerability Assessment	30 giorni dalla data di richiesta del committente	5% del canone mensile per ogni violazione	Tempo sospeso per mancanza accessi/autorizzazioni Committente. Include scansioni complete e report dettagliato con raccomandazioni.
Setup Servizio SOC	90 giorni solari dalla firma del contratto	€ 200 per ogni giorno solare di ritardo	La quantità delle penali verrà calcolata al completamento dell'attività di setup.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

5 PRIVACY & RISERVATEZZA

Il fornitore aggiudicatario sarà chiamato, in fase contrattuale, a sottoscrivere tutte le necessarie clausole di riservatezza, NDA, DPIA ove necessarie all'espletamento dei servizi.

6 FATTURAZIONE

I corrispettivi dovuti al Fornitore per la prestazione dei servizi, calcolati sulla base dei prezzi unitari indicati nell'Offerta Economica, saranno fatturati con cadenza bimestrale posticipata.
I bimestri di riferimento dovranno essere inderogabilmente:

- Gennaio/Febbraio;
- Marzo/Aprile;
- Maggio/Giugno;
- Luglio/Agosto;
- Settembre/Ottobre;
- Novembre/Dicembre.

La società, nel corso di validità del contratto, si riserva di chiedere modifiche, senza costi aggiuntivi, al suddetto "piano di fatturazione"; le richieste di modifica avranno effetto dalla successiva fatturazione.

7 FORMATO DELL'OFFERTA

L'Offerente dovrà presentare, oltre a quanto espressamente indicato nel disciplinare di gara:

- un'offerta tecnica;
- un'offerta economica.

Si evidenzia che saranno esclusi i concorrenti che offriranno servizi non aderenti alle caratteristiche obbligatoriamente richieste nel presente documento, ovvero che offrano la prestazione dei servizi con modalità difformi, in senso peggiorativo, da quanto stabilito nel Capitolato Tecnico.

Questa parte del documento illustra i formati dell'Offerta Tecnica ed Economica.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

7.1 OFFERTA TECNICA

Nell' Offerta Tecnica l'Offerente dovrà dichiarare e sottoscrivere esplicitamente la rispondenza dei servizi forniti a quanto richiesto nel presente Capitolato.

Nei capitoli l'Offerente dovrà descrivere e dettagliare la tecnologia e le modalità di prestazione dei servizi. Tutti i servizi (con le loro caratteristiche) che l'Offerente descriverà nell'Offerta Tecnica sono da ritenersi inclusi nell'offerta effettuata. La lunghezza massima ammissibile dell'offerta tecnica è di n. 50 pagine complessive, con l'aggiunta di massimo ulteriori 30 pagine per certificazioni, CV ed eventuali brochure a corredo. La valutazione dell'offerta tecnica sarà effettuata entro i limiti delle 50 pagine suddette, le parti eccedenti non verranno prese in considerazione.

Alla relazione tecnica potrà essere allegata ogni altra documentazione di carattere tecnico; qualora la predetta documentazione dovesse contenere qualsivoglia indicazione (diretta o indiretta) di carattere economico, questa deve essere eliminata, pena l'esclusione dalla Gara.

L'Offerta Tecnica dovrà essere presentata in forma elettronica e cartacea e redatta in lingua italiana.

7.2 OFFERTA ECONOMICA

L'offerta economica presentata deve essere formulata sulla base del fatto che l'Offerente:

- ha preso visione ed accetta integralmente ed incondizionatamente tutte le norme e le clausole contenute nel Capitolato Tecnico;
- ha valutato tutte le circostanze che hanno portato alla determinazione del prezzo di ogni fornitura/servizio proposto.

Dovrà essere inoltre specificato distintamente il prezzo del servizio SOC e il prezzo unitario delle ore di supporto specialistico, indicando chiaramente le tariffe applicabili.
Il prezzo complessivo ai fini del calcolo del punteggio di aggiudicazione sarà determinato dalla somma del prezzo del servizio SOC (comprensivo del SIEM in modalità Saas) e del totale della quotazione delle giornate di supporto specialistico previste.

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

8 CRITERIO DI AGGIUDICAZIONE

L'appalto sarà aggiudicato in considerazione dell'offerta più vantaggiosa da un punto di vista tecnico ed economico.

I criteri di valutazione dell'offerta sono i seguenti:

	Criteri di valutazione	Natura	Peso
1)	Prezzo	Quantitativo	30
2)	Servizio e Modello Organizzativo SOC	Qualitativo	35
3)	Dotazioni e strumentazione tecnologica offerta	Qualitativo	20
4)	Esperienza precedente e prestazioni similari	Qualitativo	15

Criterio 1 – Prezzo (P1 – 30 punti)

Relativamente al criterio 1 del Prezzo, il punteggio da assegnare ad ogni offerta economica sarà individuato applicando la seguente formula:

$$P_{1i}=30*(Pr_b-Pr_i)/(Pr_b-Pr_m)$$

dove,
P_{1i} = punteggio attribuito al concorrente i-esimo relativamente al criterio prezzo.
Pr_b = prezzo a base di negoziazione
Pr_i = prezzo concorrente i-esimo
Pr_m = prezzo minimo offerto dai concorrenti

Criterio 2 - Servizio e Modello Organizzativo SOC (P2 – 35 punti)

Il criterio valuta l'offerta tecnica dell'Offerente in relazione all'organizzazione prevista e alla proposta tecnica rispetto ai servizi richiesti, ovvero:

- organigramma/i aziendale/i specifico e strutturato, contenente la quantità di risorse impiegate, laddove rilevante ai fini della qualità dei Servizi; sono valutate positivamente le offerte che prevedono organigrammi in cui gli addetti ai ruoli fondamentali risulteranno impiegati in modo esclusivo o comunque per la maggior parte del tempo nella gestione delle mansioni inerenti alle attività previste;

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

- la presenza di approcci metodologici strutturati (standard e/o framework) con particolare riferimento alla gestione dei servizi ICT, dei servizi SOC ed alle modalità operative di esecuzione dei lavori;
- procedure operative definite per la gestione operativa, di incidenti e anomalie nelle varie modalità di copertura del servizio e di reperibilità;
- procedure operative definite per la presa in carico dei servizi;
- modalità di gestione e canali di comunicazioni con le strutture della Direzione definite dal Committente;
- deliverables finalizzati alla rendicontazione delle attività svolte e degli obiettivi raggiunti;
- Setup dei servizi SOC;
- Servizio SOC.

L'Offerente si impegna a mantenere il modello organizzativo proposto per tutta la durata contrattuale e, qualora le Parti individuassero e concordassero delle azioni di miglioramento, ad apportare tali modifiche, nel rispetto dei vincoli contrattuali.

Criterio 3 - Dotazioni e strumentazione tecnologica offerta (P3 – 20 punti)

Il punteggio sarà assegnato in base alla qualità, completezza e adeguatezza delle soluzioni tecnologiche proposte per l'erogazione del servizio SOC. In particolare, si valuterà la piattaforma SIEM con relative specifiche tecniche, scalabilità, funzionalità e misure di sicurezza/resilienza presenti. Saranno altresì considerate la qualità e l'integrazione delle dashboard per monitoraggio e ticketing, con attenzione all'esperienza utente, alla sicurezza degli accessi e alla disponibilità di funzionalità operative per il controllo e la gestione degli incidenti. Completa il quadro la valutazione delle dotazioni tecniche fornite al personale operativo. Saranno preferite le soluzioni innovative, coerenti, integrate e adatte alle esigenze del committente.

Criterio 4 - Esperienza precedente e prestazioni similari (P4 – 15 punti)

Il criterio valuta l'offerta tecnica dell'Offerente in relazione alla presenza di esperienza pregressa in lavori similari a quelli richiesti nel presente capitolato tecnico, saranno valutati soltanto i lavori similari, attestati attraverso descrizione delle attività svolte, in numero non inferiore a 5 nell'arco degli ultimi 3 (tre) anni; saranno premiate prestazioni similari per servizi eseguiti in ambito Utilities. L'avvenuto svolgimento di detti lavori dovrà essere riepilogato dall'Offerente mediante un'autodichiarazione contenente il nome del committente, l'oggetto del contratto e l'importo.

ELEMENTI DI VALUTAZIONE

Sarà attribuito un coefficiente pari a 0 (zero) ai singoli criteri:

- in caso di assenza o mancata compilazione della relativa richiesta;

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001

Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

- per soluzioni non pertinenti rispetto agli elementi di valutazione;
- per soluzioni ritenute inadeguate.

CALCOLO DEL PUNTEGGIO COMPLESSIVO

Per tutti criteri di cui sopra, una volta terminata la procedura di attribuzione discrezionale dei punteggi, si procederà ad individuare il punteggio attribuibile a ciascuna offerta tramite la seguente sommatoria:

$$P_i = \sum_k P_{ki}$$

dove,

P_i = punteggio concorrente i-esimo

K = numero dei criteri da 1 a 4

P_{ki} = punteggio del criterio k-esimo del concorrente i-esimo

A parità di punteggio complessivo (Economico più Tecnico) il servizio verrà assegnato al concorrente che avrà totalizzato il punteggio più alto nel criterio di valutazione qualitativa con peso maggiore.

Acque SPA

Il Responsabile Sistemi Informativi
Ing. Francesco Branchitta

Francesco Branchitta
Firmato da
Francesco
Branchitta
il 21/07/2025 alle
13:39:05 CEST

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 - SA 8000
ISO 50001 - ISO 39001
ISO 37001