

Politica per la Sicurezza delle Informazioni

4	03/09/26	F.to I. Binetti	F.to S. Andrisani	F.to P. Lanza P. G. Savino R. Candela L. Rizzo P. Scrimieri	F.to R. Venneri
Rev.	Data	Redazione SECIT	Verifica OSGRU	Approvazione DIRIT LEGLE DICAM DIRSA DIRRU	PREDG



OBIETTIVI

Acquedotto Pugliese, società pubblica in house, è titolare della concessione per il Servizio Idrico Integrato nei comuni della Puglia e in alcuni comuni della Campania.

Acquedotto Pugliese, per conseguire e mantenere nel tempo gli obiettivi prefissati tesi al miglioramento della Sicurezza delle Informazioni come parte integrante dell'attività, mette a disposizione adeguate risorse organizzative al fine di garantire che:

- le informazioni siano accessibili esclusivamente alle persone autorizzate, sia interne che esterne all'azienda, garantendo livelli di servizio e complessità compatibili con i requisiti funzionali dei sistemi interessati;
- siano sempre rispettati i principi di correttezza, liceità e trasparenza, a tutela della riservatezza dei dati personali e dei diritti degli interessati;
- qualunque sia il formato delle informazioni trattate, ne risulti garantita la riservatezza (proprietà per cui l'informazione non è resa disponibile o comunicata ad individui, entità o processi non autorizzati), l'integrità (proprietà che assicura che l'informazione non venga alterata, modificata, cancellata o distrutta senza autorizzazione, sia accidentalmente che intenzionalmente) e la disponibilità (proprietà per cui l'informazione deve essere sempre accessibile ed utilizzabile dagli utenti autorizzati);
- venga effettuato un monitoraggio costante degli asset e delle tecnologie, con particolare riferimento all'identificazione tempestiva di nuove vulnerabilità;
- sia prestata particolare attenzione alle variazioni dei requisiti normativi, contrattuali e alle relative priorità in relazione a nuovi servizi da erogare;
- sia integrata l'analisi dei rischi e delle opportunità considerando, tra i fattori di contesto rilevanti, le implicazioni dei cambiamenti climatici sulle attività aziendali, in linea con l'emendamento 1 della norma ISO/IEC 27001:2022 (AMENDMENT 1: Climate action changes – feb 2024);
- vengano promosse iniziative volte ad affrontare le sfide dei cambiamenti climatici, tra cui:
 - progetti e collaborazioni internazionali che mirino a potenziare la resilienza del servizio idrico attraverso l'adozione di strategie innovative e sostenibili;
 - aggiornamento continuo di un Water Safety Plan per massimizzare la qualità e la sostenibilità dell'acqua anche in condizioni di siccità ed eventi estremi;
 - applicazione della Tassonomia Europea ai sensi dell'art. 8 del Regolamento 2020/852/UE in collaborazione con il **Centro Euromediterraneo sui Cambiamenti Climatici (CMCC)** al fine di valutare i rischi climatici e le vulnerabilità del sistema aziendale, contribuendo alla pianificazione di misure di adattamento proporzionate alle sfide attuali e future.
 - pianificazione ed esecuzione di interventi di risanamento della rete idrica per ridurre le perdite e ottimizzare l'uso delle risorse idriche.
- sia garantita la Business Continuity attraverso interventi mirati, sia di carattere organizzativo che tecnologico e che tali interventi siano definiti, costantemente aggiornati e periodicamente verificati;
- tutto il personale venga addestrato sul tema della Sicurezza delle Informazioni;



- tutto il personale venga informato dell’obbligatorietà delle politiche aziendali e sensibilizzato sulle conseguenze derivanti dalla violazione di tali politiche;
- siano effettuate misurazione per la valutazione delle prestazioni del Sistema di Gestione per la Sicurezza delle Informazioni;
- siano separate le mansioni relative alle attività critiche;
- siano ridotti il più possibile i rischi alla fonte;
- qualsiasi violazione di sicurezza, reale o presunta, venga comunicata ed investigata;
- siano prontamente identificati e gestiti gli incidenti sulla sicurezza ed attivate le autorità competenti, per quelli che hanno impatto su requisiti di legge violati;
- sia evitato l’utilizzo di software non autorizzato;
- siano effettuati riesami periodici del SGSI relativamente a:
 - verifica dell’attualità e dell’efficacia dei controlli applicati per le minacce e le vulnerabilità individuate nel piano del trattamento dei rischi;
 - incidenza dei controlli attuati sull’efficacia gestionale;
 - modifiche apportate alle tecnologie;
 - modifiche normative in materia di sicurezza dei dati e delle informazioni;
 - modifiche apportate alla configurazione dei sistemi rientranti nel SGSI;
 - rivalutazione periodica del rischio.

IMPEGNO DEL MANAGEMENT E RISORSE

Il Management di AQP e la Direzione Innovation & IT Management (DIRIT) condividono gli Obiettivi per la Sicurezza delle Informazioni sopra descritti e supportano pienamente un programma per la sua attuazione e mantenimento.

Al fine di stabilire, attuare, monitorare, aggiornare e migliorare il SGSI, il Management di AQP e DIRIT si impegnano a fornire sufficienti risorse per condurre periodicamente delle analisi ed il trattamento dei rischi per la Sicurezza delle Informazioni.

DIRIT, con il sostegno delle risorse individuate, ed in coerenza con i processi e le metodologie delle Unità Organizzative Risk Management ed Internal Audit:

- identifica una metodologia di valutazione del rischio;
- identifica, analizza e pondera i rischi individuati;
- stabilisce i criteri per l’accettazione dei rischi ed i livelli di rischio accettabili;
- seleziona i controlli da attuare;
- garantisce che siano realizzate le misure di sicurezza identificate nella fase di trattamento dei rischi, attraverso attività di audit, monitoraggio e riesame;
- intraprende azioni correttive assicurandosi che siano raggiunti gli obiettivi prefissati;
- garantisce un processo costante di miglioramento continuo.



APPLICABILITÀ

La presente Politica per la Sicurezza delle Informazioni si applica a tutto il personale AQP, alle aziende Partner, ai Fornitori, Clienti o Terze Parti sotto contratto, coinvolti nel trattamento delle informazioni.

RIESAME

DIRIT verifica periodicamente, con cadenza annuale o nel caso di cambiamenti significativi, l'efficacia del Sistema di Gestione della Sicurezza delle Informazioni ed i requisiti, garantendone sempre l'idoneità, l'adeguatezza e l'efficacia.

COMUNICAZIONE

La presente Politica per la Sicurezza delle Informazioni è trasmessa e resa disponibile ai dipendenti, alle aziende Partner, ai Fornitori, Clienti o Terze Parti sotto contratto quale manifesto di un'alleanza per l'Information Security che favorisca la consapevolezza e l'assunzione di responsabilità individuali.