



acquedotto
pugliese

l'acqua, bene comune

Politica per la sicurezza delle informazioni

2	10/07/23	<i>F.to A. Antonacci</i>	<i>F.to S. Andrisani</i>	<i>F.to P. Lanza P. G. Savino R. Candela L. Rizzo P. Scrimieri</i>	<i>F.to D. Laforgia F. Portincasa</i>
Rev.	Data	Redazione SECIT	Verifica OSGRU	Approvazione DIRIT LEGLE DICAM SATAM DIRRU	Autorizzazione PRCDA DIRGE

NOTA: Il documento firmato è presente nell'archivio di sistema di OSGRU

Pag. 1 a 3

Acquedotto Pugliese S.p.A. con unico azionista Regione Puglia

Via Cognetti, 36 - 70121 Bari - Cap. soc. € 41.385.573,60
C.F. e P.I. 00347000721 - REA C.C.I.A.A. di Bari n. 414092
acquedotto.pugliese@pec.aqp.it - www.aqp.it

AQP
Acquedotto Pugliese





OBIETTIVI

Acquedotto Pugliese, società totalmente partecipata dalla Regione Puglia, è titolare della concessione per il Servizio Idrico Integrato nei comuni della Puglia e in alcuni comuni della Campania.

La Sicurezza delle Informazioni rappresenta un fattore critico di successo su cui viene posta la massima attenzione, sia per le caratteristiche stesse dei servizi (ad alto contenuto di rischio) che per il posizionamento sul mercato scelto dall'organizzazione.

Con lo scopo di contenere tali rischi a livelli accettabili, risulta necessario 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
- qualunque sia il formato delle informazioni trattate, risulti garantita la riservatezza (proprietà per cui l'informazione non è resa disponibile o comunicata ad individui, entità o processi non autorizzati), integrità (proprietà dell'informazione relativa alla salvaguardia dell'accuratezza e della completezza) e loro disponibilità (proprietà per cui l'informazione deve essere accessibile ed utilizzabile previa richiesta di una entità autorizzata)
- venga effettuato un monitoraggio costante nel cambiamento degli asset e della tecnologia, al fine di identificare tempestivamente nuove vulnerabilità
- sia prestata particolare attenzione alle variazioni dei requisiti normativi, contrattuali ed alle relative priorità in relazione a nuovi servizi da erogare
- vengano ottemperati i requisiti previsti in tema di trattamento dei dati personali
- 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 misurazioni 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 autorizzati
- 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 dalla tecnologia (vulnerabilità nuove o modificate, riduzione dei rischi per nuove conoscenze acquisite in base al progresso tecnologico)
 - modifiche apportate alla configurazione dei sistemi rientranti nel SGSI
 - rivalutazione periodica del rischio (a monte ed a valle di qualsiasi azione preventiva).



IMPEGNO DEL MANAGEMENT E RISORSE

Il Management di AQP e la Direzione Information Technology (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:

- 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

APPLICABILITA'

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.