
# Politica di Cybersecurity

Il **Consorzio Venezia Nuova,** concessionario del Ministero delle Infrastrutture e dei Trasporti per la realizzazione degli interventi per la salvaguardia di Venezia e della laguna veneta, allo scopo di garantire l'erogazione del *Servizio Essenziale: Gestione di opere e attrezzature all'interno dei porti, nello specifico "Difesa della laguna veneta delle maree e dall'innalzamento del livello del mare (c.d. acqua alta)";* consapevole della responsabilità che questo ruolo comporta, il Consorzio riconosce l'importanza cruciale della protezione della **sicurezza cibernetica per il raggiungimento dei propri obiettivi** strategici, operativi e per il mantenimento della fiducia dei propri stakeholder.

## 1. Obiettivi della Sicurezza delle Informazioni

Gli obiettivi primari, nonché le principali misure di gestione del rischio ICT di questa Politica sono i seguenti:

1. Implementare e promuovere un **sistema di governance** della sicurezza informatica assicurando una definizione dei ruoli e delle responsabilità, nel rispetto dei principi di accountability e trasparenza, che garantisca la conformità al quadro normativo vigente e agli standard di settore.
2. Garantire la **protezione della riservatezza, integrità e disponibilità** del patrimonio informativo, dei sistemi, delle infrastrutture informatiche e le reti, da eventi intenzionali (violazioni, frodi, ecc.) e non intenzionali (errori umani, fenomeni naturali) per **ridurre al minimo i danni e le interruzioni**; tramite l'individuazione e gestione di rischi ICT, nonché dell'attuazione delle politiche, processi e procedure necessarie.
3. Garantire la **difesa e la resilenza dei sistemi informativi,** attraverso la adozione di un sistema di rilevazione di eventi anomali, incidenti e

vulnerabilità, così come di piano di risposta agli incidenti per ridurre il rischio di attacchi informatici e violazioni della sicurezza.

4. Garantire la **continuità operativa e la resilenza delle infrastrutture critiche**, attraverso il mantenimento della sicurezza dei sistemi informativi e la adozione dei piani di Business Continuity e Disaster Recovery.
5. Garantire che le **terze parti ICT** che collaborino nei processi aziendali abbiano consapevolezza della necessità di garantire **i medesimi oggettivi di sicurezza lungo l'intera catena di approvvigionamento di servizi ICT.**
6. Assicurare che tutte le **normative, regolamenti e standard applicabili** in materia di sicurezza informatica siano soddisfatti in maniera efficace e costante.

Questa politica, quale documentazione ufficiale aziendale, è resa nota e accessibile a tutto il personale tramite il sito web aziendale.

Dipendenti, collaboratori, appaltatori e terze parti sono tenuti a rispettarla e a contribuire attiva e proattivamente alla sicurezza dei sistemi informativi, in linea con i valori fondamentali dell'organizzazione e la missione istituzionale.