CONSORZIO AGRARIO
DI TREVISO E BELLUNO

CYBERSECURITY LEVEL PROFILE

ADOZIONE DEL NIST CYBERSECURITY FRAMEWORK (CSF) 2.0.

Per svolgere le attività necessarie per gestire la sicurezza informatica, CONSORZIO AGRARIO TREVISO E BELLUNO HA ADOTTATO IL FRAMEWORK CSF 2.0.
La scelta di CSF 2.0 si basa sul fatto che questo schema è un approccio globale per la gestione delle contromisure di sicurezza IT necessarie per proteggere le prestazioni delle operazioni.
In particolare, il CSF offre una tassonomia di risultati di sicurezza informatica di alto livello che possono essere utilizzati per comprendere meglio, valutare, dare la priorità e comunicare i loro sforzi di sicurezza informatica.

RISK PROFILE MATURITY LEVEL (CSF TIERS)

L'adozione di CSF 2.0 ha reso possibile ottenere la valutazione del RISK PROFILE MATURITY LEVEL.
In sintesi, si può asserire che CONSORZIO AGRARIO TREVISO E BELLUNO è conforme ai requisiti stabiliti nei livelli di CSF (1 = livello di maturità più basso; 4 = livello di maturità più alto) del NIST CYBERSECURITY FRAMEWORK.
A seconda del TIERS, CONSORZIO AGRARIO TREVISO E BELLUNO è:

- TIER 4 (ADAPTIVE) for CYBERSECURITY RISK GOVERNANCE;
- TIER 4 (ADAPTIVE) for CYBERSECURITY RISK MANAGEMENT.

CYBERSECURITY FRAMEWORK TIERS

CYBERSECURITY RISK GOVERNANCE	CYBERSECURITY RISK MANAGEMENT
TIER 4 - ADAPTIVE	TIER 4 - ADAPTIVE
Esiste un approccio a livello di organizzazione per la gestione dei rischi di cibersicurezza che utilizza politiche, processi e procedure informate sui rischi per affrontare potenziali eventi di cibersicurezza. La relazione tra i rischi di cibersicurezza e gli obiettivi organizzativi è chiaramente compresa e considerata quando si prendono decisioni. I dirigenti monitorano i rischi per la cibersicurezza nello stesso contesto dei rischi finanziari e di altri rischi organizzativi. Il budget organizzativo si basa sulla comprensione dell'ambiente di rischio attuale e previsto e sulla tolleranza al rischio. Le business unit implementano la visione esecutiva e analizzano i rischi a livello di sistema nel contesto delle tolleranze al rischio organizzative. La gestione del rischio di cibersicurezza fa parte della cultura organizzativa. Si evolve da una consapevolezza delle attività precedenti e da una continua consapevolezza delle attività sui sistemi organizzativi e sulle reti. L'organizzazione può tenere conto in modo rapido ed efficiente delle modifiche agli obiettivi aziendali/di missione nel modo in cui il rischio viene affrontato e comunicato.	L'organizzazione adatta le proprie pratiche di cibersicurezza in base alle attività di cibersicurezza precedenti e attuali, comprese le lezioni apprese e gli indicatori predittivi. Attraverso un processo di miglioramento continuo che incorpora tecnologie e pratiche avanzate di cibersicurezza, l'organizzazione si adatta attivamente a un panorama tecnologico in evoluzione e risponde in modo tempestivo ed efficace alle minacce sofisticate e in evoluzione.