Scheda tecnica del corso

Corso di formazione IPDRR – Sicurezza informatica per la gestione delle risorse idriche e ambientali

Costo
780,00 €
Solo esame finale

Codice corso	Durata test	Soglia di superamento	Emissione
IPDRR_CYBER_WAT	60 min	70%	26/08/2026

Executive summary

Il corso di formazione IPDRR fornisce una preparazione operativa sulla protezione dei sistemi digitali impiegati nella gestione delle risorse idriche e ambientali. Il percorso affronta i rischi che interessano reti di acquedotto, impianti di trattamento, depurazione e monitoraggio ambientale, con particolare attenzione all'integrazione tra sistemi informativi IT, tecnologie operative OT, apparati SCADA, PLC, sensori IoT e piattaforme di telecontrollo. I partecipanti imparano a riconoscere minacce e vulnerabilità, classificare gli asset, segmentare le reti, governare gli accessi remoti, proteggere credenziali e dati, gestire aggiornamenti e fornitori, predisporre backup verificati e organizzare la risposta agli incidenti. Il corso collega le misure tecniche alla continuità del servizio, alla sicurezza delle persone, alla tutela dell'ambiente e alla qualità del dato utilizzato per le decisioni operative. Sono inoltre illustrati i principali riferimenti applicabili, tra cui la disciplina NIS2, la resilienza dei soggetti critici, ISO/IEC 27001, IEC 62443, ISO 22301 e gli approcci di gestione del rischio per i servizi idrici. La verifica finale misura la capacità di applicare controlli proporzionati, individuare priorità di intervento e contribuire alla gestione coordinata di eventi cyber in organizzazioni pubbliche e private del settore.

Processo di certificazione

- Registrazione o accesso alla piattaforma Academy.
- Svolgimento esclusivo dell'esame finale del corso. L'eventuale formazione o preparazione può essere svolta esternamente o tramite altri canali.
- Le domande del test richiamano gli obiettivi, le competenze e i contenuti indicati nella presente scheda tecnica.
- Valutazione dell'esito, eventuale validazione e rilascio del certificato secondo le regole applicabili al corso.

Nota importante

Su Academy si sostiene esclusivamente l'esame finale del corso. L'eventuale attività formativa o di preparazione può essere svolta esternamente o tramite altri canali. I quesiti del test richiamano gli argomenti indicati nella presente scheda tecnica e nel programma sintetico del corso.

Programma sintetico

Quadro di riferimento: Direttiva (UE) 2022/2555 NIS2 e D.Lgs. 138/2024; Direttiva (UE) 2022/2557 CER e D.Lgs. 134/2024; Direttiva (UE) 2020/2184 sull'acqua potabile; ISO/IEC 27001:2022 e Amd 1:2024; ISO/IEC 27002:2022; IEC 62443-2-1:2024, IEC 62443-3-2:2020 e IEC 62443-3-3:2013; ISO 22301:2019; ISO 24518:20
Programma: governance del rischio cyber, asset IT/OT, SCADA e IoT, segmentazione, accessi, supply chain, monitoraggio, backup, continuità operativa, risposta agli incidenti e protezione dell'integrità dei dati ambientali.

Descrizione del corso

Il corso sviluppa competenze pratiche per proteggere processi, dati e tecnologie utilizzati nella captazione, potabilizzazione, distribuzione, depurazione, irrigazione, bonifica e nel monitoraggio delle matrici ambientali. L'impostazione integra sicurezza informatica, continuità operativa, sicurezza fisica e tutela ambientale.

Obiettivi formativi

- Comprendere le differenze e le interdipendenze tra ambienti IT e OT.
- Riconoscere minacce, vulnerabilità e scenari di attacco applicabili ai servizi idrici e ambientali.
- Applicare criteri di inventario, classificazione, valutazione del rischio e priorità di trattamento.
- Individuare misure organizzative e tecniche coerenti con la criticità del servizio.
- Contribuire alla gestione degli incidenti, alla continuità operativa e al miglioramento continuo.

Competenze acquisite

- Lettura di un'architettura SCADA/PLC e individuazione dei principali punti di esposizione.
- Segmentazione di rete mediante zone, condotti, DMZ e regole di comunicazione controllate.
- Gestione degli accessi privilegiati, remoti e dei fornitori.
- Protezione di sensori, telemetria, basi dati, sistemi GIS e piattaforme di supervisione.
- Pianificazione di backup, ripristino, monitoraggio, logging e risposta agli incidenti.
- Valutazione dell'impatto di un evento cyber sulla qualità, disponibilità e sicurezza del servizio.

Destinatari

Responsabili e addetti ICT, OT e cybersecurity; gestori del servizio idrico integrato; consorzi di bonifica; enti ambientali; laboratori; tecnici di impianto; responsabili della transizione digitale; responsabili continuità operativa, qualità, ambiente e sicurezza; consulenti e fornitori tecnologici.

Prerequisiti

Conoscenze di base sull'uso dei sistemi informatici e sui processi dell'organizzazione. È utile, ma non obbligatoria, una familiarità con reti, automazione industriale, telecontrollo o gestione ambientale.

Programma

- Servizi idrici e ambientali come infrastrutture e servizi essenziali.
- Governance, ruoli, responsabilità e quadro NIS2/CER.
- Inventario e classificazione di asset, dati, dipendenze e fornitori.
- Architetture IT/OT: SCADA, PLC, HMI, RTU, sensori IoT, GIS e sistemi di laboratorio.
- Analisi del rischio, scenari di minaccia e impatti su salute, ambiente e continuità del servizio.
- Segmentazione, firewalling, DMZ, accessi remoti sicuri e principio del minimo privilegio.
- Gestione delle vulnerabilità, patch, configurazioni, credenziali e dispositivi legacy.
- Logging, sincronizzazione temporale, monitoraggio delle anomalie e conservazione delle evidenze.

- Sicurezza dei dati di misura: integrità, disponibilità, tracciabilità e validazione.
- Backup offline o immutabili, test di ripristino, RTO, RPO e continuità operativa.
- Gestione degli incidenti, comunicazioni, escalation, lezioni apprese ed esercitazioni.
- Supply chain, manutenzione remota e requisiti di sicurezza nei contratti.

Processo di certificazione

- Registrazione o accesso alla piattaforma Academy.
- Svolgimento dell'esame finale relativo al corso selezionato.
- Calcolo dell'esito sulla base delle risposte fornite e della soglia prevista.
- Eventuale validazione amministrativa del risultato.
- Rilascio del certificato o dell'attestazione secondo le regole applicabili.

Modalità Academy

Su Academy si sostiene esclusivamente l'esame finale del corso. La formazione o preparazione può essere erogata esternamente, in presenza, a distanza o tramite altri canali formativi. La scheda tecnica definisce il perimetro degli argomenti valutabili.

Modalità di valutazione

Il test è composto da 30 domande estratte casualmente dalla banca dati del corso. I quesiti richiamano gli argomenti, gli obiettivi e i contenuti della presente scheda tecnica. Le risposte a scelta multipla e vero/falso sono valutate automaticamente; l'esito è soggetto al flusso di validazione previsto dalla piattaforma.

Durata test

60 minuti.

Certificazione / Attestazione

Il superamento richiede almeno il 70% di risposte corrette. Il documento rilasciato attesta il superamento della verifica finale del corso e non implica, salvo espressa indicazione, accreditamenti o riconoscimenti di organismi terzi.

Risultati attesi

Al termine, il partecipante è in grado di riconoscere i principali rischi cyber del settore, proporre controlli proporzionati, contribuire alla protezione dei sistemi IT/OT e supportare la risposta organizzata agli incidenti con attenzione alla continuità dei servizi idrici e alla tutela ambientale.