

CORSO DI CYBER SECURITY · MODULO INFRASTRUTTURE CRITICHE

Sicurezza delle Infrastrutture Critiche

Strategie di Incident Response e Digital Forensics



Obiettivi formativi

01

Inquadrare il servizio idrico integrato come infrastruttura critica e descriverne il contesto tecnologico e organizzativo.

02

Conoscere il quadro normativo applicabile (Direttiva NIS2, D.Lgs. 138/2024, Legge 90/2024, atti attuativi ACN) e i relativi obblighi.

03

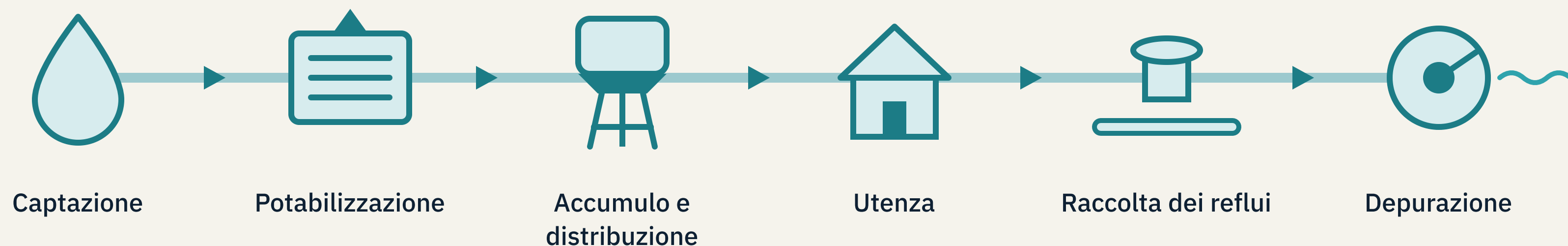
Comprendere la relazione tra governance del rischio, incident response e digital forensics in un gestore di servizi essenziali.

04

Saper impostare la gestione delle prime 72 ore di un incidente, dalla rilevazione alla notifica, preservando le evidenze.

Il servizio idrico integrato

Il gestore del servizio idrico integrato opera in regime di affidamento da parte dell'ente di governo d'ambito e presidia l'intera filiera: captazione, potabilizzazione, accumulo e distribuzione dell'acqua, raccolta delle acque reflue e depurazione.



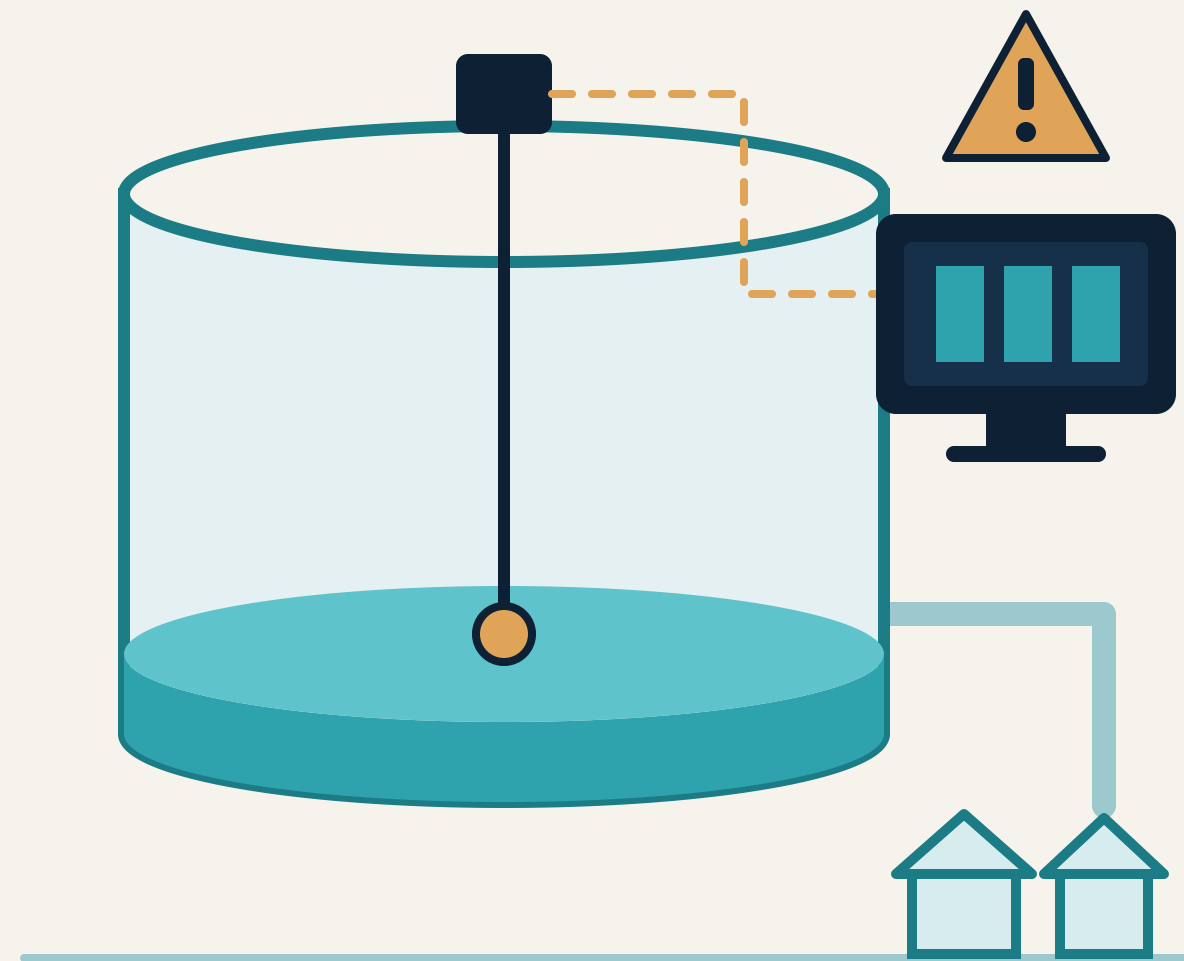
L'interruzione del servizio incide su salute pubblica, strutture sanitarie e attività economiche; per questa ragione la Direttiva NIS2 colloca il settore tra quelli ad alta criticità.

Il contesto tecnologico



Ciascuna interconnessione costituisce un potenziale vettore di accesso: postazioni client, server, macchine virtuali in cloud e canali di assistenza dei fornitori. La superficie d'attacco comprende pertanto l'insieme di tali relazioni.

Lo scenario di riferimento



- 1 Un comando sospetto viene impartito attraverso il sistema SCADA.
- 2 I parametri di processo subiscono una variazione significativa e scatta l'allarme.
- 3 Il sensore di livello di un serbatoio fornisce un dato errato e il segnale viene gestito in modo inadeguato.
- 4 Centinaia di utenti restano privi di acqua per diverse ore: un evento di dinamica elementare che produce un disservizio rilevante.

Il caso Oldsmar (Florida, 2021)

Dinamica dell'evento secondo la ricostruzione iniziale

1. Accesso remoto alla postazione di controllo tramite TeamViewer, con password condivisa, su sistema Windows 7 esposto a Internet senza firewall
2. Modifica del setpoint di idrossido di sodio da 100 a 11.100 ppm
3. L'operatore osserva il cursore muoversi sull'HMI e ripristina immediatamente il valore corretto
4. Nessun impatto sull'utenza: i controlli di processo e le verifiche manuali avrebbero intercettato l'anomalia

Fonti: Pinellas County Sheriff's Office (8 febbraio 2021); Massachusetts DEP, avviso di sicurezza (2021)

SETPOINT DELL'IDROSSIDO DI SODIO

100 → 11.100 ppm

Valore normale e valore impostato sull'HMI durante l'evento

Sviluppi successivi (marzo 2023)

L'ex city manager ha attribuito l'evento a un errore di un dipendente anziché a un attacco informatico; l'FBI non ha reso note conclusioni. Il caso resta istruttivo per le vulnerabilità emerse e per l'incertezza attributiva: senza evidenze forensi acquisite e conservate, la qualificazione dell'evento rimane aperta.

LA DOMANDA GUIDA

Come si interviene nelle prime 24–72 ore dall’evento?

L’efficacia della risposta dipende dalle procedure definite e verificate prima dell’incidente.

Le fonti normative di riferimento

Fonte	Oggetto	Rilevanza per il gestore idrico
Direttiva (UE) 2022/2555 (NIS2)	Livello comune elevato di cibersecurity nell’Unione	Settori «acqua potabile» e «acque reflue» tra i settori ad alta criticità (Allegato I)
D.Lgs. 4 settembre 2024, n. 138	Recepimento della NIS2, in vigore dal 16 ottobre 2024	Responsabilità degli organi di governo, gestione del rischio, notifica degli incidenti, sicurezza della catena di approvvigionamento
Legge 28 giugno 2024, n. 90	Rafforzamento della cybersicurezza nazionale	Segnalazione entro 24 h e notifica entro 72 h al CSIRT Italia per i soggetti pubblici indicati e le relative società in house, incluse le acque reflue

Gli atti attuativi dell’ACN (determinazione n. 164179/2025 sugli obblighi di base; tassonomia degli incidenti pubblicata in G.U. il 17 febbraio 2026) sono esaminati nelle slide seguenti.

La NIS2 e la responsabilità della governance

Responsabilità degli organi di amministrazione

Gli organi di governo approvano le misure di gestione del rischio, ne sorvegliano l'attuazione e ne rispondono: la sicurezza entra formalmente nelle linee di indirizzo societarie.

Soggetti essenziali e importanti

La classificazione segue dimensione e criticità. Le misure di base ACN (det. n. 164179/2025) fissano 37 misure e 87 requisiti per i soggetti importanti, 43 misure e 116 requisiti per quelli essenziali.

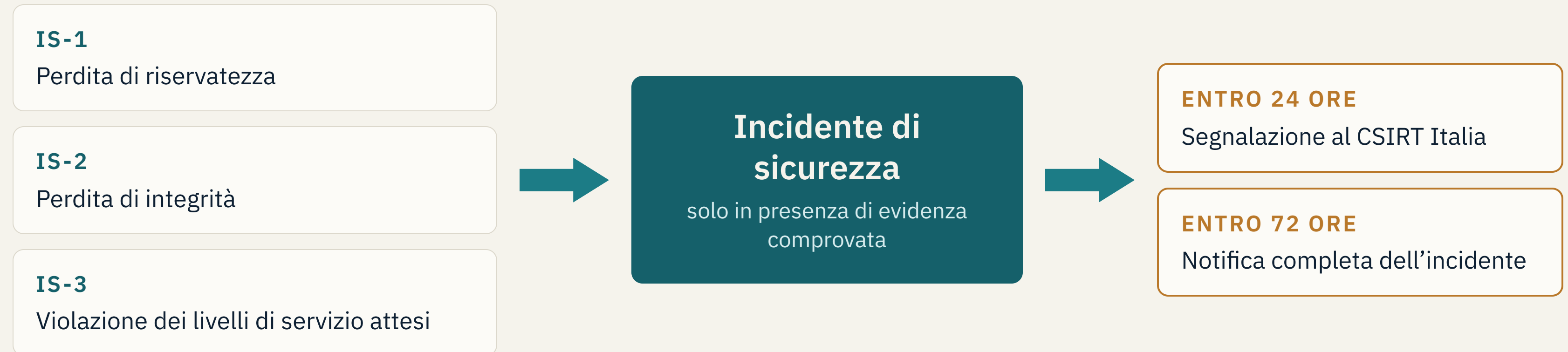
Gestione del rischio documentata e verificata

Piani di continuità operativa, disaster recovery e risposta agli incidenti devono essere redatti, attuati e sottoposti a test periodici, a dimostrazione della conformità.

Sicurezza della catena di approvvigionamento

Il gestore deve verificare, anche mediante audit, i fornitori di servizi e sistemi: la conformità delle terze parti è parte integrante della propria, in un settore con una pluralità di fornitori.

La qualificazione dell'incidente di sicurezza



In assenza di evidenza della perdita di riservatezza o di integrità, ovvero della violazione dei livelli di servizio, l'evento non è qualificato come incidente e non sorge l'obbligo di notifica: la fase di accertamento assume dunque rilievo giuridico, oltre che tecnico.

Fonte: tassonomia degli incidenti ACN ai sensi della Legge 90/2024 (G.U. 17 febbraio 2026)

Gli standard internazionali di riferimento



Gestione della sicurezza e degli incidenti

- ISO/IEC 27001:2022 – sistema di gestione della sicurezza
- ISO/IEC 27035-1:2023 – gestione degli incidenti di sicurezza
- NIST SP 800-61 Rev. 3 (2025) – incident response



Sistemi di controllo industriale e OT

- IEC 62443 – sicurezza dei sistemi di automazione industriale
- IEC 62443-3-3 – requisiti di sistema e security level
- NIST SP 800-82 Rev. 3 (2023) – guida alla sicurezza OT



Digital forensics

- ISO/IEC 27037:2012 – identificazione, raccolta, acquisizione e conservazione delle evidenze digitali
- ISO/IEC 27043:2015 – principi e processi di investigazione
- NIST SP 800-86 (2006) – tecniche forensi nell'incident response

Gli standard forniscono il riferimento metodologico per i piani richiesti dalla NIS2: il sistema di gestione (ISO/IEC 27001), la risposta agli incidenti (ISO/IEC 27035, NIST SP 800-61), la protezione dei sistemi di controllo (IEC 62443, NIST SP 800-82) e il trattamento delle evidenze digitali (ISO/IEC 27037 e 27043).

La letteratura scientifica di riferimento

JOURNAL OF ENVIRONMENTAL ENGINEERING · 2020

A Review of Cybersecurity Incidents in the Water Sector

Hassanzadeh A., Rasekh A., Galelli S.,
Aghashahi M., Taormina R., Ostfeld A.,
Banks M.K. · vol. 146, n. 5

Rassegna di quindici incidenti malevoli
documentati nel settore idrico: le minacce
crescono per frequenza, diversità e
complessità (ransomware, cryptojacking,
minacce interne) e richiedono una difesa
adattiva e cooperativa.

WATER (MDPI) · 2021

A Systematic Review of the State of Cyber-Security in Water Systems

Tuptuk N., Hazell P., Watson J., Hailes S. ·
vol. 13, n. 1, art. 81

Revisione sistematica di 64 studi (2000–
2020): la ricerca si concentra sul
rilevamento di anomalie nei sistemi di
controllo, con scarsa partecipazione
dell'industria e forte crescita dopo il 2015.

IFIP · SPRINGER · 2007

Lessons Learned from the Maroochy Water Breach

Slay J., Miller M. · Critical Infrastructure
Protection, vol. 253, pp. 73–82

Analisi del caso Maroochy Shire (2000):
minaccia interna, assenza di controlli sugli
accessi radio e sui sistemi SCADA;
raccomandazioni organizzative e tecniche
tuttora attuali.

Le due fasi della sicurezza informatica

Fase 1 · Governance e gestione del rischio

1. Adozione di un framework di riferimento (es. NIST CSF) adattato alla realtà del gestore
2. Assessment dello stato dell'infrastruttura e definizione dell'obiettivo di riduzione del rischio
3. Piani documentati: risposta agli incidenti, disaster recovery, continuità operativa
4. Regolamenti interni sull'uso dei dispositivi digitali
5. Verifica periodica dell'attuazione mediante test

Fase 2 · Gestione dell'incidente

1. Attivazione dei protocolli interni e dei ruoli predefiniti
2. Contenimento e valutazione dell'impatto sul servizio
3. Acquisizione delle evidenze e cristallizzazione dei log
4. Comunicazione interna ed esterna e notifica al CSIRT Italia
5. Ripristino del servizio e analisi post-incidente

La qualità della risposta è determinata in larga misura dai processi e dalle procedure definiti nella prima fase.

Continuità del servizio e acquisizione delle prove



L'imperativo della continuità

Nel settore idrico l'obiettivo primario è il ripristino del servizio nel più breve tempo possibile: una struttura ospedaliera non può restare priva di acqua. Ogni scelta tecnica deve ridurre al minimo tale rischio.

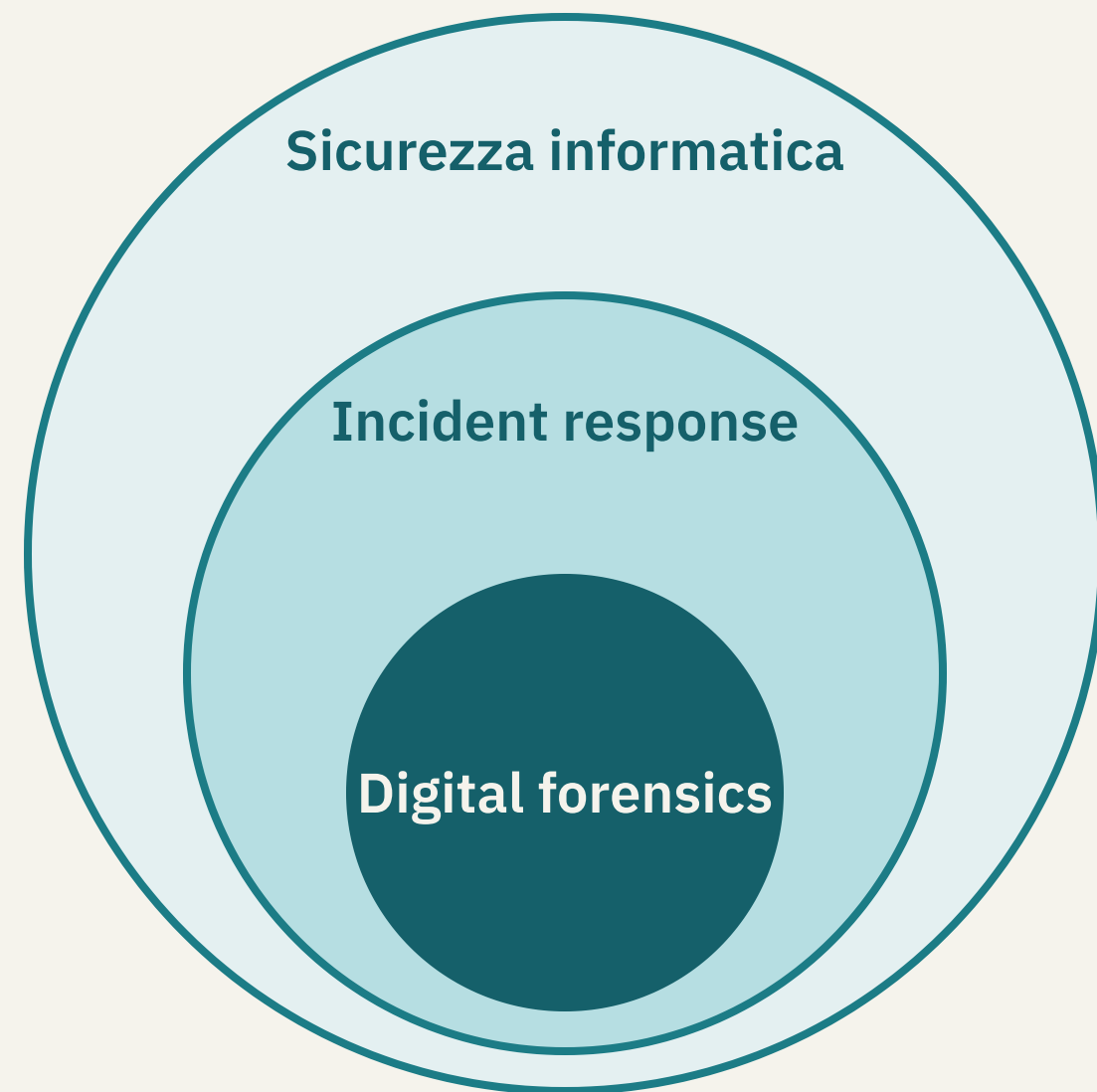


L'imperativo probatorio

La digital forensics richiede l'acquisizione immediata delle evidenze, prima che possano essere alterate o perdute; la memoria volatile, in particolare, non ammette rinvii.

I due obiettivi sono conciliabili soltanto in presenza di processi e procedure definiti ex ante; in loro assenza si perde sul piano della sicurezza o su quello probatorio.

La digital forensics come componente della sicurezza



La digital forensics costituisce un sottoinsieme dell'incident response, a sua volta parte integrante della sicurezza informatica; la sua funzione non si esaurisce nell'ambito giudiziario.

IMPIEGO TRADIZIONALE

Raccolta e cristallizzazione della prova per il contenzioso penale o civile

IMPIEGO ESTESO

Documentazione sistematica della conformità operativa nei confronti di ACN, assicuratori e terzi

La cristallizzazione periodica dell'operato integra le tecniche forensi nelle prassi aziendali e tutela l'organizzazione anche sul piano assicurativo.

I contenuti del piano di risposta agli incidenti

Comunicazioni interne

Struttura legale, DPO, direzione, funzioni operative e struttura informatica: attori da coinvolgere immediatamente.

Comunicazioni esterne

CSIRT Italia (24 h e 72 h), utenti, clienti e fornitori, anche perché l'incidente può originare da un accesso di terzi.

Ruoli e responsabilità

Assegnazione esplicita di compiti e responsabilità, presupposto di ogni comunicazione e decisione tempestiva.

Trasparenza del SOC esterno

Procedure del fornitore chiare e documentate; relazione di merito al referente interno per la sicurezza (CISO o security manager).

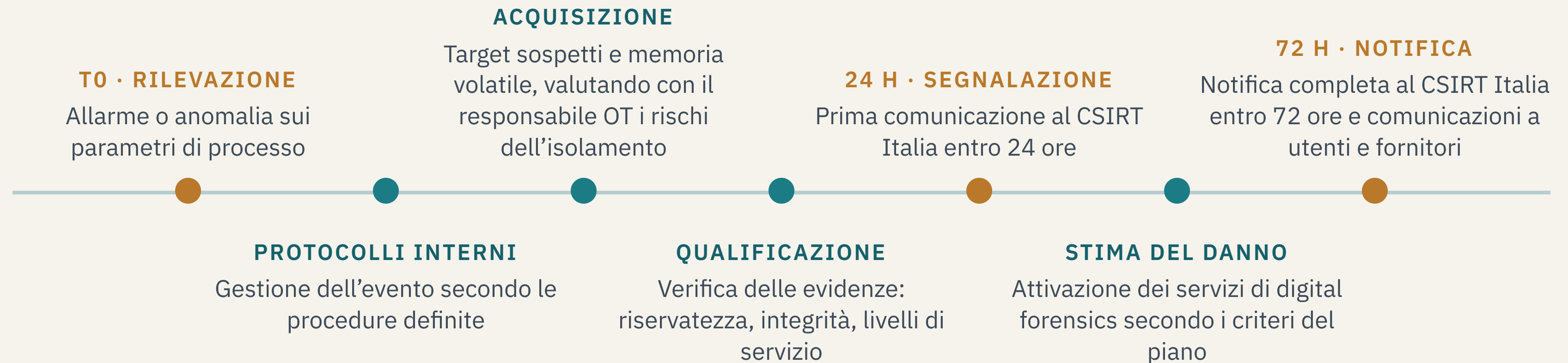
Criteri di attivazione della digital forensics

Servizi contrattualizzati in capitolato e budget approvato dall'organo amministrativo, così da evitare decisioni non pianificate in fase di emergenza.

Esercitazioni e verifiche

Esercitazioni periodiche di risposta, con relazione del referente entro i termini di notifica, per verificare l'applicabilità del piano.

Le prime 72 ore: una cronologia operativa



Le fonti di prova e la ricostruzione degli eventi

Fonti di evidenza

- Log degli apparati di sicurezza (firewall, SIEM, EDR)
- Log delle piattaforme cloud e dei fornitori di servizi
- Registri dei sistemi SCADA, PLC e RTU
- Memoria volatile e immagini dei sistemi sospetti
- Tracciati degli accessi remoti di operatori e fornitori

Principi metodologici

- I log costituiscono la fonte primaria e vanno cristallizzati tempestivamente
- Ai log di fornitori conformi agli standard di settore si riconosce attendibilità, salvo compromissione dell'apparato stesso
- La ricostruzione richiede una super-timeline da fonti eterogenee, anche esterne al gestore
- Attenzione a fusi orari, ritardi di registrazione e specifiche dei fornitori
- Catena di custodia documentata a garanzia dell'integrità delle evidenze

Il caso Oldsmar alla luce del metodo

Evidenza del caso	Principio della lezione	Riferimento
Accesso remoto con password condivisa su sistema esposto a Internet	Governance degli accessi di terze parti e segmentazione della rete	NIS2 (catena di approvvigionamento); IEC 62443 (zone e conduit)
Postazione di controllo con sistema operativo obsoleto (Windows 7)	Obsolescenza del livello OT: messa in sicurezza progressiva	NIST SP 800-82 Rev. 3
Rilevazione da parte dell’operatore e controlli di processo ridondanti	Continuità del servizio: difesa in profondità fisica e digitale	Piano di continuità operativa (NIS2)
Attribuzione pubblica immediata, poi messa in dubbio nel 2023	Qualificazione dell’incidente fondata su evidenze acquisite e conservate	Tassonomia ACN; ISO/IEC 27037
Coinvolgimento tempestivo delle autorità (FBI, Secret Service)	Comunicazioni esterne pianificate e responsabilità definite	Legge 90/2024 (24 h e 72 h); NIST SP 800-61

Altri incidenti di riferimento nel settore idrico

Caso	Vettore	Impatto	Lezione
Maroochy Shire, Australia (2000)	Ex collaboratore con apparati radio e software SCADA sottratti; ripetute intrusioni nel sistema di pompaggio	Sversamento di circa 800.000 litri di liquami in corsi d’acqua e aree pubbliche	Minaccia interna; revoca degli accessi; monitoraggio dei canali radio
Aliquippa (USA) ed Erris (Irlanda), 2023	PLC Unitronics (o rimarchiati) esposti su Internet con password di default; interfacce deturpate	Circa 180 utenti senz’acqua per due giorni (Irlanda); controllo manuale (USA)	Esposizione del livello OT; credenziali di default; avviso CISA AA23-335A
Alto Calore Servizi, Avellino (2023)	Ransomware a doppia estorsione (gruppo Medusa) con esfiltrazione e pubblicazione di dati	Sistemi IT indisponibili per il gestore di 126 comuni (Avellino e Benevento)	Separazione IT/OT; notifica e comunicazione all’utenza; backup e ripristino

Fonti: Slay e Miller (2007); CISA, FBI, NSA, EPA, INCD, Advisory AA23-335A (2023); SecurityWeek (dicembre 2023); comunicazione agli utenti di Alto Calore Servizi (28 aprile 2023). L’attribuzione a CyberAv3ngers è accertata per Aliquippa e ritenuta probabile per Erris.

Le sfide aperte



Obsolescenza tecnologica del livello OT

Investimenti pregressi in PLC e RTU non sono sostituibili nel breve periodo: occorre una messa in sicurezza progressiva anche dei componenti che, per obsolescenza, non soddisfano i requisiti attuali.



Vulnerabilità nei domini IT e OT

Le debolezze interessano entrambi i domini; il mondo OT presenta vincoli di disponibilità che limitano le possibilità di aggiornamento e di isolamento.



Lock-in tecnologico e integrazione

Il principio di resilienza sconsiglia la dipendenza da un unico fornitore; una pluralità di fornitori accresce però la complessità di integrazione dei sistemi.



La sicurezza percepita come costo

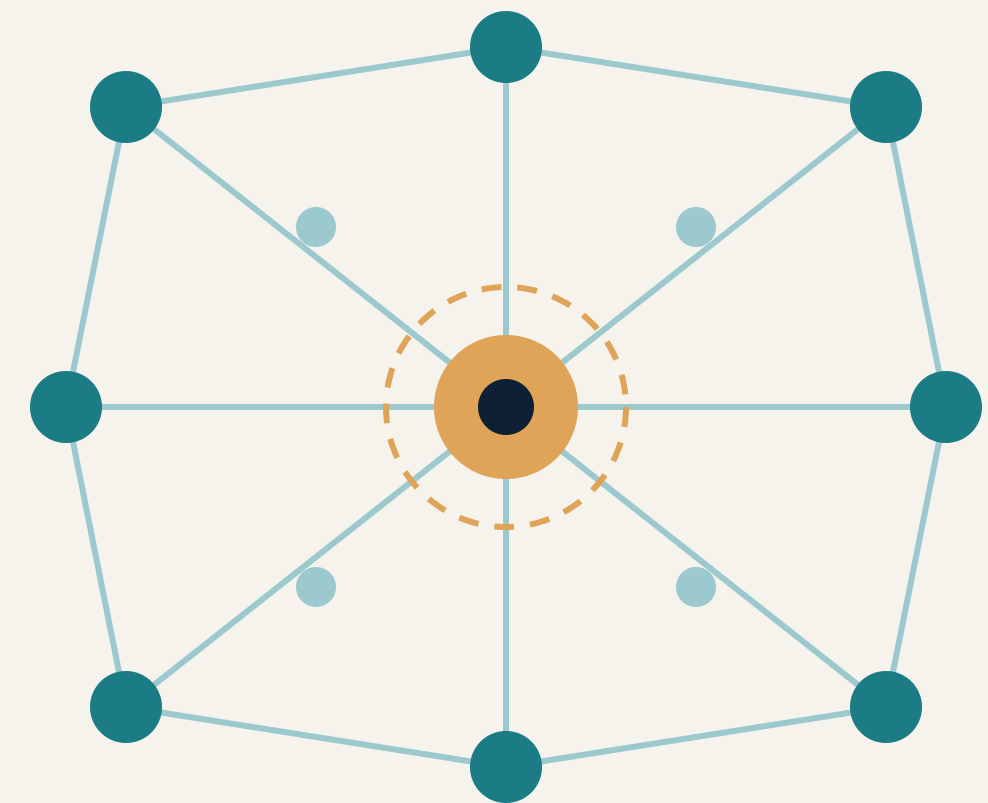
La spesa in sicurezza è raramente letta come vantaggio; la responsabilità introdotta dalla NIS2 costituisce oggi la principale leva di cambiamento.

Intelligenza artificiale e governance della sicurezza

L'automazione dei processi di sicurezza (vulnerability assessment, penetration test, SOC basati su agenti) può ridurre i costi operativi in misura rilevante.

- Governabilità: mantenimento del controllo umano sui processi delegati agli agenti
- Accountability: la responsabilità giuridica resta in capo all'organizzazione
- Supervisione: verifica delle decisioni automatizzate prima della loro esecuzione su impianti critici

La delega di funzioni di sicurezza ad agenti autonomi richiede criteri espliciti di supervisione, verifica e attribuzione delle responsabilità.



Punti chiave della lezione

- 1** Il servizio idrico integrato è un'infrastruttura ad alta criticità ai sensi della NIS2, con un contesto tecnologico eterogeneo e un'ampia superficie d'attacco.
- 2** Il quadro normativo (D.Lgs. 138/2024, Legge 90/2024, atti ACN) responsabilizza la governance e impone piani, misure di base e notifiche entro 24 e 72 ore.
- 3** La governance del rischio precede e determina la qualità dell'incident response: processi e procedure vanno definiti e verificati prima dell'evento.
- 4** La digital forensics è parte integrante della sicurezza: documenta la conformità operativa, oltre a fornire le prove per il contenzioso.
- 5** Nelle prime 72 ore occorre preservare le evidenze (log e memoria volatile), qualificare l'incidente, notificare e attivare servizi forensi già pianificati.

Domande per il seminario

QUESITO 1

In che misura il requisito dell'«evidenza» previsto dalla tassonomia ACN può ritardare la notifica di un incidente reale, e quali rischi ne derivano?

QUESITO 2

Come si concilia, in un impianto OT, l'acquisizione della memoria volatile con l'impossibilità di interrompere il processo industriale?

QUESITO 3

Quali clausole contrattuali dovrebbe prevedere un gestore nei confronti di un SOC esterno per garantire trasparenza e collaborazione forense?

QUESITO 4

Quali condizioni di supervisione e di accountability renderebbero accettabile un SOC gestito da agenti di intelligenza artificiale?

RIFERIMENTI

Fonti e riferimenti normativi

Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (NIS2)

Decreto legislativo 4 settembre 2024, n. 138, recepimento della Direttiva (UE) 2022/2555

Legge 28 giugno 2024, n. 90, disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici

Agenzia per la Cybersicurezza Nazionale, Determinazione n. 164179 del 14 aprile 2025, obblighi di base per i soggetti NIS

Agenzia per la Cybersicurezza Nazionale, tassonomia degli incidenti ai sensi della Legge 90/2024, Gazzetta Ufficiale del 17 febbraio 2026

National Institute of Standards and Technology, Cybersecurity Framework (CSF) 2.0, 2024

RIFERIMENTI

Standard, letteratura e fonti sui casi

Hassanzadeh A., Rasekh A., Galelli S., Aghashahi M., Taormina R., Ostfeld A., Banks M.K. (2020), «A Review of Cybersecurity Incidents in the Water Sector», Journal of Environmental Engineering, 146(5), DOI 10.1061/(ASCE)EE.1943-7870.0001686

Tuptuk N., Hazell P., Watson J., Hailes S. (2021), «A Systematic Review of the State of Cyber-Security in Water Systems», Water, 13(1), 81, DOI 10.3390/w13010081

Slay J., Miller M. (2007), «Lessons Learned from the Maroochy Water Breach», in Critical Infrastructure Protection, IFIP vol. 253, Springer, pp. 73–82

ISO/IEC 27001:2022; ISO/IEC 27035-1:2023; ISO/IEC 27037:2012; ISO/IEC 27043:2015; IEC 62443 (serie), IEC 62443-3-3

NIST SP 800-61 Rev. 3 (2025), Incident Response Recommendations and Considerations for Cybersecurity Risk Management; NIST SP 800-82 Rev. 3 (2023), Guide to Operational Technology (OT) Security; NIST SP 800-86 (2006), Guide to Integrating Forensic Techniques into Incident Response

CISA, FBI, NSA, EPA, INCD (2023), Cybersecurity Advisory AA23-335A, IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities

Caso Oldsmar: Pinellas County Sheriff's Office, conferenza stampa dell'8 febbraio 2021; Massachusetts Department of Environmental Protection, avviso di sicurezza (2021); dichiarazioni dell'ex city manager di Oldsmar (marzo 2023)



GRAZIE PER L'ATTENZIONE

Vincenzo Calabrò

Ingegnere informatico · Analista di cyber security e digital forensics · Docente, relatore e formatore

vincenzocalabro.it



Profilo LinkedIn

linkedin.com/in/vincenzocalabro