

Sicurezza delle Infrastrutture Idriche

Strategie di Incident Response e Digital Forensics

Ing. Gaetano Consalvo
info@gaetanoconsalvo.it

Genova, 16 ottobre 2026 : Informatica forense: il prossimo capitolo è già iniziato

Utility del settore idrico

Gestore del Servizio Idrico Integrato

Definizione

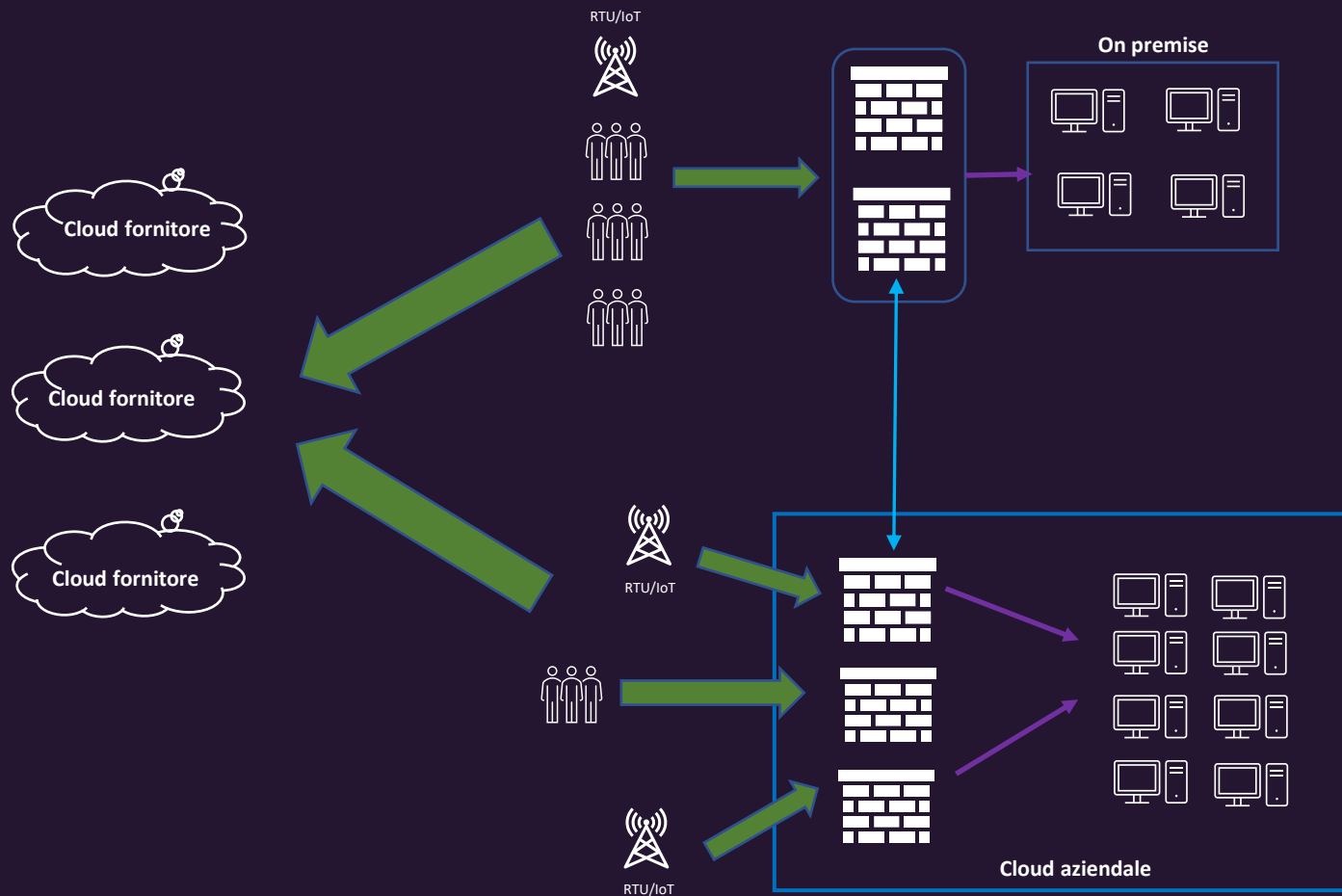
E' un soggetto, pubblico, privato o misto, che gestisce in modo industriale uno o più servizi del **Servizio Idrico Integrato**, cioè le attività pubbliche di: **captazione, adduzione e distribuzione dell'acqua per usi civili, fognatura e depurazione delle acque reflue**, secondo principi di efficienza, efficacia ed economicità.



ACQUEDOTTO
FOGNATURA
DEPURAZIONE

In termini più operativi: è il gestore del servizio idrico, responsabile di acquedotto, fognatura e depurazione

Possibile contesto tecnologico



Possibile Scenario Operativo

COMANDO SOSPETTO IMPARTITO TRAMITE SISTEMA SCADA
(*Supervisory Control and Data Acquisition*)

Allarme di processo: variazione di parametri

Possibile disservizio all'utenza

PRIME 24/72 ORE: COME INTERVENIRE?

Normativa di riferimento: Direttiva NIS 2

L'Italia ha recepito la Direttiva NIS 2 tramite il Decreto Legislativo 4 settembre 2024, n. 138, pubblicato in Gazzetta Ufficiale il 1° ottobre 2024 ed entrato in vigore il 16 ottobre 2024.

Alcuni concetti essenziali per le utility del settore idrico

- Settore ad alta criticità

Acqua potabile e acque reflue rientrano tra i settori ad alta criticità: fornitori/distributori di acqua destinata al consumo umano e imprese che raccolgono, smaltiscono o trattano acque reflue sono inclusi nell'Allegato I del D.Lgs. 138/2024.

- Approccio basato sul rischio

Necessità di identificare rischi cyber su sistemi IT, OT/SCADA, telecontrollo, reti, impianti, sensori, fornitori e dati, adottando misure proporzionate all'impatto sul servizio erogato.

- Governance e responsabilità del management

La sicurezza non è solo compito tecnico: organi direttivi e amministrativi devono approvare, supervisionare e sostenere le misure di gestione del rischio.

Altri concetti essenziali per le utility del settore idrico

- **Continuità del servizio idrico**

backup, disaster recovery, business continuity, piano di risposta agli incidenti di sicurezza informatica.

- **Gestione e notifica degli incidenti**

Gli incidenti significativi vanno gestiti con processi formalizzati e notificati secondo le regole NIS: entro 24h per early warning, 72h per notifica completa.

- **Sicurezza della supply chain**

Vanno governati i rischi di fornitori di manutenzione impianti, software SCADA, cloud, telelettura, laboratori, outsourcing IT, operatori terzi, ecc.

- **Misure tecniche e organizzative minime**

Alcune misure: controllo accessi, MFA, gestione vulnerabilità, logging, formazione, crittografia, segmentazione, monitoraggio, **incident response** e gestione asset.

Incidente di sicurezza informatica

*'un evento che compromette la **disponibilità, l'autenticità, l'integrità o la riservatezza di dati** conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi' – (Art. 2, DECRETO LEGISLATIVO 4 settembre 2024, n. 138)*

Determina del **9 febbraio 2026 dell'AGENZIA PER LA CYBERSICUREZZA NAZIONALE**: il gestore idrico (..servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali), in quanto soggetto di cui all'art. 1, comma 1, della **legge 28 giugno 2024, n. 90**, qualifica gli eventi di sicurezza informatica come incidenti di sicurezza informatica ai fini di segnalazione/notifica, quando:

- Si ha evidenza della perdita di **riservatezza...**
- Si ha evidenza della perdita di **integrità...**
- Si ha evidenza della violazione dei **livelli di servizio** attesi...

Possibili Vettori di minaccia

- Supporti esterni/rimovibili
- Client/server/VM
- E-mail
- Sistemi di trasmissione e acquisizione dati (es. RTU, PLC)
- Sistemi OT (sensori, sistemi di telecontrollo, ecc.)
- sistemi IT (es. sistema gestionale, documentale, ecc.)
- Ecc.

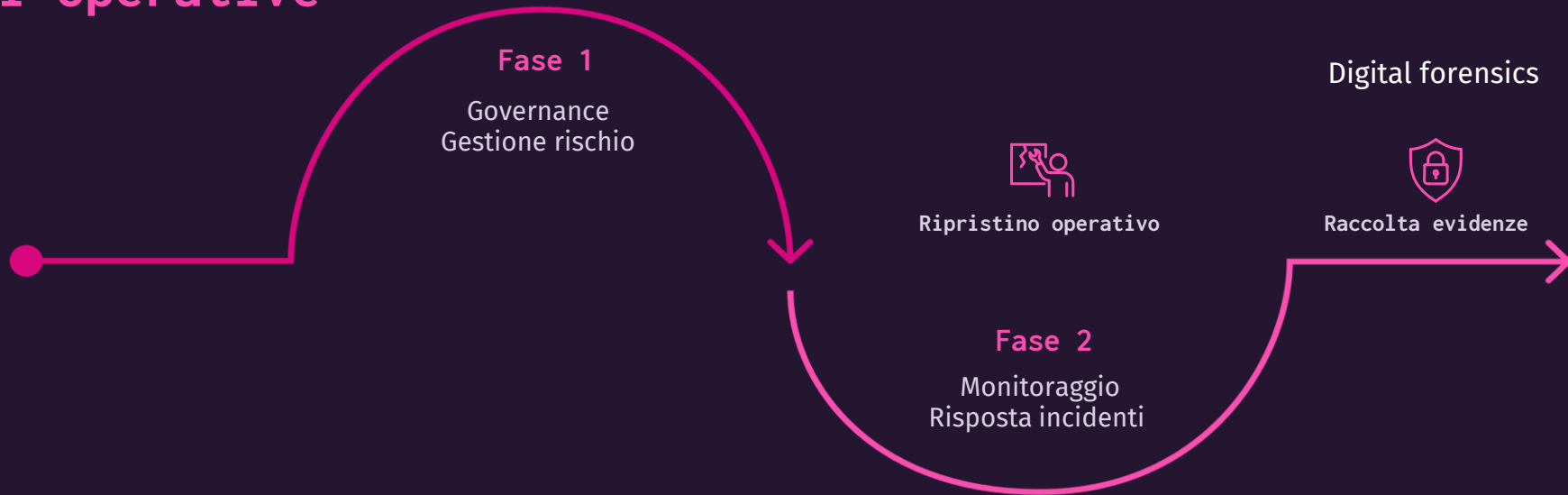
Scenari possibili

- **Compromissione del sistema di controllo industriale (es. attacchi ai sistemi SCADA)**
- **Attacco alla catena di fornitura**
- **Furto**
- **Errore umano voluto/involontario**
- **Cyberattacchi**
- **Ransomware, malware, ecc.**
- **Data breach**
- **Eventi naturali**: danni fisici a infrastrutture a supporto dei sistemi informativi (rete elettrica, sistemi di comunicazione)
- **Attacchi mirati al patrimonio finanziario** (es. phishing)
- Ecc.

SFIDA ATTUALE

- ☐ Costi di gestione
- ☐ Sistemi legacy
- ☐ Superficie d'attacco in rapida espansione
- ☐ Obsolescenza tecnologica
- ☐ Vulnerabilità di sicurezza
- ☐ Difficoltà di integrazione

Fasi Operative



Fase 1: Definizione della strategia di cybersecurity per l'infrastruttura idrica

- Costituzione e formazione team interno all'azienda. Scelta di eventuali partner/strutture operative dedicate (es. SOC)
- Adozione di framework di riferimento: policy e procedure aziendali, *incident response plan* e piano di continuità operativa
- sicurezza della catena di approvvigionamento
- Ricognizione infrastrutturale, applicativa e di processo
- Attività di Cybersecurity Assessment: VA/PT (Vulnerability Assessment e Penetration test)
- Remediation
- Risk Assessment

Incident Response e Digital Forensics

Sicurezza informatica

Incident response

Digital forensics



Le fasi del processo forense (NIST SP 800-86)

1. Raccolta (Collection)
2. Esame (Examination)
3. Analisi (Analysis)
4. Reportistica (Reporting)



Ciclo di vita dell'incident response

(NIST: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>)

(NIST: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf>)

Il processo di *incident response* è composto da 4 fasi (fonte NIST) :

- ✓ **“Preparation”**: predisposizione di policy e misure di sicurezza (processi e procedure)
- ✓ **“Detection and Analysis”**: identificazione e analisi di possibili anomalie
- ✓ **“Containment, Eradication and Recovery”**: gestione dell'incidente e ripristino di sistemi/informazioni.
- ✓ **“Post - Incident Activity”**: analisi di cosa non ha funzionato

Fonte: **NIST Special Publication (SP) 800-86**

Guide to Integrating Forensic Techniques into Incident Response: <https://csrc.nist.gov/pubs/sp/800/86/final>

Piano di risposta agli incidenti

Art. 24, comma 1, del D.Lgs. n. 138/2024 - Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica.

“I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate [...] per prevenire o ridurre al minimo l’impatto degli incidenti per i destinatari dei loro servizi e per altri servizi”.

Per le infrastrutture critiche che garantiscono servizi essenziali, è fondamentale predisporre un Piano di risposta agli incidenti di sicurezza che definisca le azioni da intraprendere in caso di incidente e i ruoli e le responsabilità dei soggetti coinvolti.

Contenuti del Piano

- ❑ Gestione delle comunicazioni interne: ICT, DPO, legale, direzione e funzioni operative
- ❑ Gestione delle comunicazioni esterne: CSIRT Italia, autorità competenti, clienti, utenti, fornitori e media
- ❑ Responsabilità definite: referente cybersicurezza/CSIRT, IT/Cyber Security, comunicazione, privacy, legale, customer care
- ❑ Procedure per detection, analysis, containment, eradication and recovery
- ❑ Criteri di attivazione delle attività di Digital Forensics, per raccogliere e preservare evidenze digitali

Digital Forensics

Quando?

- ☐ Raccogliere prove a supporto di eventuali azioni legali
- ☐ Richieste di risarcimento per i danni subiti dall'azienda
- ☐ Attribuire o escludere responsabilità
- ☐ Dimostrare la compliance alla normativa di settore
- ☐ Ecc.

Perché?

- ☐ Ricostruzione degli eventi
- ☐ Individuare e preservare le prove
- ☐ Garantire la catena di custodia
- ☐ Produrre risultati tecnicamente validi
- ☐ Ecc.

Come?

- ☐ Esiste un piano di risposta agli incidenti specifico per il contesto?
- ☐ Esistono processi e procedure dettagliate?
- ☐ Asset inventory e architettura sono disponibili?
- ☐ Sono presenti strumenti di monitoraggio e difesa?
- ☐ Disponiamo di log dettagliati?
- ☐ Quale impatto hanno i sistemi da acquisire sulla continuità operativa?
- ☐ Ecc.

Chi?

- ☐ Chi si occupa della sicurezza informatica?
- ☐ Esistono figure competenti e formate in ambito cybersecurity?
- ☐ Ecc.

Evidenze

- Log firewall: connessioni in ingresso/uscita, IP sorgente/destinazione, porte, traffico anomalo, accessi remoti, ecc.
- EDR, XDR, antivirus
- Active Directory: logon/logoff, tentativi falliti, creazione/modifica utenti, ecc.
- Log applicativi: accessi alle applicazioni, errori, modifiche dati, attività di utenti privilegiati, ecc.
- Sistemi SCADA, telecontrollo e OT: eventi di accesso, comandi inviati, variazioni di configurazione, allarmi, ecc.
- Accessi fornitori, operatori e terze parti: account esterni, VPN, orari di intervento, attività svolte, eventuali credenziali condivise, ecc.
- Comunicazioni interne ed esterne: email, piattaforme ticket, comunicazioni con fornitori/SOC, ecc.
- Log SIEM: alert, regole violate, timeline SIEM, log disponibili e fonti collegate
- Sistemi client/server compromessi o sospetti
- Sistemi cloud: log Microsoft 365/AWS, accessi amministrativi, audit log, ecc.
- Backup e sistemi di storage

Dall'incidente alla prova digitale

Prime 24/72 ore

Scenario operativo

➤ COMANDO SOSPETTO IMPARTITO TRAMITE SISTEMA SCADA

Allarme di processo: variazione di parametri

- | | |
|--------------------------------|--|
| 1 Rilevazione e analisi | Verifica comando, account, allarmi e storico di processo. Confrontare l'evento con interventi autorizzati, ecc. |
| 2 Contenimento | Limitare accesso remoto sospetto con il responsabile OT, senza compromettere la sicurezza dell'impianto. |
| 3 Acquisizione | Preservare log VPN/firewall, SCADA, SIEM e sistemi interessati (es. PLC/RTU). Cristallizzare le informazioni acquisite |
| 4 Analisi forense | Ricostruire timeline IT/OT/cloud considerando fusi/scarti orari |
| 5 Reporting | Documentare catena di custodia e produrre relazione per management, strutture aziendali, CSIRT e autorità |

0-24 ore:

Capire e mettere in sicurezza, contenere e preservare

- ☐ Attivare struttura IT interna/esterna
- ☐ Confermare evento
- ☐ Preservare log volatili senza spegnere sistemi critici
- ☐ Bloccare/limitare accessi remoti sospetti e account fornitore
- ☐ Acquisire log VPN/firewall, SCADA, SIEM
- ☐ Cristallizzare evidenze (hash, catena custodia, ecc.)
- ☐ Valutare early warning CSIRT

24-72 ore:

Ricostruire e notificare

- ☐ Correlare timeline IT/OT/cloud
- ☐ Validare recovery/ripristino e remediation
- ☐ Preparare notifica completa con evidenze

Ruoli chiave

- SOC o referente cyber
- Responsabile OT/Struttura IT
- DPO e Legale
- Fornitori
- Specialisti di Digital Forensics

Conclusioni



Nelle infrastrutture idriche, investire in sicurezza informatica e in strategie di incident response e digital forensics significa proteggere un'infrastruttura critica e la collettività.



Una strategia efficace di Incident Response e Digital Forensics si costruisce prima dell'incidente, attraverso ruoli chiari, policy aggiornate, procedure definite e strumenti funzionali alla gestione della sicurezza.

La Digital Forensics è un investimento strategico per la resilienza delle infrastrutture idriche, nonché uno strumento fondamentale per ricostruire le cause, individuare i vettori di attacco, valutare gli impatti e supportare le comunicazioni verso le autorità in caso di incidente informatico.

Sfida imminente

Governare l'AI per difendere ciò che è critico

Riferimenti e approfondimenti

- <https://www.acn.gov.it/portale/nis>
- <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022L2555>
- <https://www.gazzettaufficiale.it/eli/id/2025/05/05/25A02717/sg>
- <https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG>
- LINEE GUIDA Per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90. - Agenzia per la cybersicurezza nazionale
- <https://www.acn.gov.it/portale/linee-guida-rafforzamento-resilienza>
- <https://www.acn.gov.it/portale/w/domini-della-cybersicurezza-domini-della-cybersicurezza-assessment-e-testing>
- A. Deane e A. Kraus, The Official (ISC)2 CISSP CBK Reference, 6th edition. Indianapolis: John Wiley and Sons, 2021. M. Chapple, J. M. Stewart, e D. Gibson, (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th ed. Indianapolis: John Wiley and Sons, 2021.
- <https://www.ncsc.gov.uk/collection/vulnerability-management/guidance/carry-out-assessments>
- <https://www.acn.gov.it/portale/w/domini-della-cybersicurezza-asset-management>
- https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework
- <https://www.cybersecurityframework.it/metodologia-assessment>
- <https://www.cybersecurityframework.it/>
- <https://www.acn.gov.it/portale/w/modello-operativo-integrato-di-cybersecurity-governance-introduzione>
- <https://www.isaca.org/resources/cobit>
- <https://www.isaca.org/resources/cobit/cobit-5>
- <https://www.nist.gov/cyberframework>
- <https://www.acn.gov.it/portale/linee-guida-rafforzamento-resilienza>
- <https://rischiocyber.acn.gov.it/cyber/index.html>
- ISO 31000:2018 Risk management — Guidelines - <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>
- NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments - <https://csrc.nist.gov/pubs/sp/800/30/r1/final>
- https://www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/modello-pco-per-pa_0.pdf

Grazie per l'attenzione

Ing. Gaetano Consalvo
info@gaetanoconsalvo.it

Genova, 16 ottobre 2026