AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2024 | **n. 09/ 2024** | **ottobre 2024**

L'importanza di un sistema integrato di intelligenza artificiale per una struttura sanitaria

Le infrastrutture critiche sono quelle strutture, reti e sistemi che sono essenziali per il funzionamento della società e per la sicurezza pubblica.
Gli ospedali e le strutture sanitarie rientrano in questa categoria perché forniscono servizi sanitari fondamentali, necessari per garantire la salute e il benessere della popolazione: in particolare, svolgono un ruolo fondamentale in caso di emergenze, pandemie, disastri naturali e altre crisi; pertanto, la resilienza delle strutture sanitarie è necessaria per assicurare che possano continuare a operare anche in situazioni critiche, come interruzioni dell'energia, attacchi informatici o un'elevata domanda di cure durante crisi sanitarie.

Negli ultimi anni, l'intelligenza artificiale ha rivoluzionato molti settori, inclusa la sanità. La possibilità di integrare sistemi di IA in una struttura sanitaria rappresenta una delle evoluzioni più promettenti per migliorare la qualità dei servizi, l'efficienza operativa e l'assistenza ai pazienti ed assicurare la resilienza della struttura stessa.
Un **sistema integrato di IA** non si limita a singole funzioni, ma connette varie aree di una struttura sanitaria, facilitando il lavoro del personale medico e migliorando le decisioni cliniche.

Vediamo perché può rivelarsi così importante.

Anzitutto i principali vantaggi sono insiti, ovviamente, nel settore dei trattamenti medici:

- ***Diagnosi più rapide e accurate***

La capacità di analizzare rapidamente grandi quantità di dati clinici, come esami di laboratorio, immagini mediche e storie cliniche dei pazienti, può migliorare enormemente la precisione delle diagnosi, riducendo gli errori umani e accelerando il processo decisionale.
Ad esempio, algoritmi di IA possono essere addestrati ad esaminare immagini diagnostiche (come le radiografie o le risonanze magnetiche) e identificare anomalie che potrebbero sfuggire all'occhio umano. Sistemi di questo tipo sono già utilizzati in ambiti come la diagnosi precoce del cancro o delle malattie cardiovascolari, dove l'accuratezza e la tempestività sono cruciali.

- ***Personalizzazione delle cure***

Un altro beneficio significativo dell'integrazione di sistemi di IA riguarda la personalizzazione dei trattamenti. Analizzando i dati genetici, le informazioni cliniche e gli stili di vita dei pazienti, l'IA può suggerire piani terapeutici su misura, ottimizzando così i risultati clinici. Questo approccio, noto come *medicina di precisione*, tiene conto delle specificità di ogni paziente, riducendo i rischi di complicazioni e migliorando l'efficacia delle terapie.

- ***Supporto decisionale per i medici***

L'IA supporta il lavoro del medico fornendo informazioni aggiornate e suggerimenti basati su dati scientifici. Attraverso l'integrazione con banche dati e letteratura medica, un sistema di IA può fornire

raccomandazioni terapeutiche e diagnosi alternative basate su casi simili. Questo riduce il carico cognitivo dei medici, permettendo loro di concentrarsi maggiormente sull'aspetto umano dell'assistenza sanitaria.

Ma fondamentali ai fini della resilienza di una struttura sanitaria sono anche i seguenti aspetti:

- ***Ottimizzazione della gestione delle risorse***

Le strutture sanitarie sono spesso gravate da problematiche gestionali, come la gestione dei turni, la disponibilità di posti letto o il monitoraggio delle scorte di farmaci. Un sistema integrato di IA può automatizzare molte di queste attività, migliorando la pianificazione e riducendo i costi operativi. Ad esempio, algoritmi di intelligenza artificiale possono prevedere i picchi di affluenza nelle strutture ospedaliere, consentendo una gestione più efficiente del personale e delle risorse.

- ***Manutenzione predittiva delle attrezzature mediche***

Le strutture sanitarie utilizzano una vasta gamma di attrezzature mediche che devono funzionare in modo continuo ed efficiente. L'integrazione dell'IA consente la manutenzione predittiva di queste apparecchiature, monitorando il loro stato e prevedendo possibili guasti prima che si verifichino.
Questo riduce i tempi di inattività e garantisce che le attrezzature critiche (ventilatori, macchine per la dialisi, ecc.) siano sempre operative.

- ***Miglioramento dell'efficienza amministrativa***

La sanità è un settore caratterizzato da una vasta mole di attività amministrative, dalla registrazione dei pazienti alla gestione dei dati clinici e al monitoraggio delle pratiche assicurative. Un sistema integrato di IA può automatizzare molti di questi processi, riducendo i tempi di attesa e migliorando la precisione della gestione dei dati. In un contesto in cui la digitalizzazione è ormai una necessità, l'IA facilita l'integrazione dei dati dei pazienti in un sistema centralizzato, garantendo una visione olistica e un accesso rapido alle informazioni.

- ***Telemedicina e assistenza remota***

L'IA sta rivoluzionando anche l'ambito della telemedicina, consentendo un monitoraggio continuo dei pazienti a distanza. Sensori intelligenti, algoritmi di analisi e chatbot medici consentono di raccogliere dati sullo stato di salute del paziente e di intervenire tempestivamente in caso di anomalie. Questo è particolarmente utile per la gestione delle malattie croniche e per il monitoraggio post-operatorio, riducendo così il numero di ricoveri ospedalieri non necessari.

- ***Sicurezza dei dati e privacy***

Sistemi avanzati di intelligenza artificiale possono monitorare continuamente la sicurezza informatica di una struttura sanitaria, identificando possibili minacce e proteggendo i dati sensibili dei pazienti.

Un sistema integrato di intelligenza artificiale in una struttura sanitaria rappresenta, quindi, una svolta significativa nella gestione e nell'erogazione delle cure. Dalla diagnosi alla personalizzazione dei trattamenti, fino alla gestione efficiente delle risorse, l'IA ha il potenziale per migliorare la qualità dell'assistenza sanitaria, ridurre i costi e aumentare la soddisfazione dei pazienti. La chiave del successo risiede nell'integrazione ottimale tra tecnologia e competenze umane, dove l'IA non sostituisce ma supporta e potenzia le capacità dei professionisti della sanità.

Quelli elencati finora sono i vantaggi di un sistema integrato di intelligenza artificiale in sanità. Alcuni casi di successo sono descritti nel Rapporto "Critical Infrastructure Resilience and Artificial Iintelligence", che è in corso di elaborazione da parte di AIIC (Associazione Italiana Esperti in Infrastrutture Critiche) ad opera di un gruppo di studiosi ed esperti, e che sarà di prossima pubblicazione.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Oltre ai vantaggi sopra elencati è ovvio che esistano anche numerosi rischi. Quali siano questi rischi li vedremo nel prossimo editoriale.

Continuate a leggerci!

Silvano Bari
Docente di "Risk Management" presso l'Università Campus Bio-medico di Roma, è vicepresidente di AIIC

ATTIVITA' DELL'ASSOCIAZIONE

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.

COLLABORAZIONE ALLE ATTIVITA' AIIC

Si invitano tutti i soci a partecipare alle attività sociali (newsletter, webinar, ecc.) inviando articoli, segnalazioni o dando la disponibilità a tenere webinar o seminari o a partecipare alla stesura e redazione della newsletter mensile.
La mail cui scrivere è segreteria@infrastrutturecritiche.it

NEWS E AVVENIMENTI

10 elementi di sicurezza informatica potenziata dall'AI per i CISO - Quali sono i 10 elementi di sicurezza informatica potenziata dall'AI che i CISO dovrebbero considerare? Secondo la MIT Technology Review, il principale vantaggio tangibile dell'IA segnalato finora dai managers aziendali, è il miglioramento della sicurezza e della gestione dei rischi. Attualmente, quasi il 70% delle aziende afferma di non poter rispondere efficacemente alle minacce informatiche senza l'utilizzo di strumenti di sicurezza potenziati dall'Intelligenza Artificiale. Ad evidenziarlo è Check Point, che sottolinea: "Nonostante, però, le opportunità di sicurezza informatica basate sull'IA siano decisamente valide e apprezzabili, il sensazionalismo continua a oscurare il modo con cui questi strumenti possono realmente far progredire le iniziative di sicurezza". *(continua…)*
https://www.snewsonline.com/10-elementi-sicurezza-informatica-potenziata-ai-ciso/
SNEWS - *Redazione - 26 Agosto 2024*

Gestione del rischio idraulico e previsione dell'evoluzione delle onde di esondazione in tempo reale - La descrizione di nuovi strumenti che permettono di descrivere e analizzare gli eventi alluvionali, attraverso lo studio di eventi passati, la modellazione idraulica 2D attuando così misure di mitigazione dei rischi e la corretta gestione delle emergenze.
Rischio idraulico: gli strumenti di analisi degli eventi alluvionali
Tra le più frequenti manifestazioni di fragilità del territorio italiano c'è sicuramente quella legata al rischio idraulico. Negli ultimi anni sono stati sviluppati nuovi strumenti che permettono una descrizione e una analisi più accurata degli eventi alluvionali. Tali strumenti consentono di intervenire in tre diverse fasi distinte:
Nella ricostruzione di eventi passati,
Nella progettazione di misure di mitigazione del rischio idraulico,
Nella gestione delle emergenze.
L'analisi dei dati territoriali per la modellazione idraulica 2D
L'avanzamento negli ultimi vent'anni delle tecniche di rilevamento della superficie terrestre ha permesso di ottenere rilievi di dettaglio in cui sono descritte con accuratezza tutte le forme del

territorio che influiscono nell'evoluzione delle onde di esondazione su una piana alluvionale. (*continua…)*
https://www.ingenio-web.it/articoli/gestione-del-rischio-idraulico-e-previsione-dell-evoluzione-delle-onde-di-esondazione-in-tempo-reale/
INGENIO - *Giovanni Moretti, 19/09/2024*

Il governo conferma: obbligo di polizze catastrofali dal 2025 - Il provvedimento conferma l'obbligo a partire dal prossimo 1° gennaio e l'anticipo immediato del 30% del danno. Confindustria continua a chiedere un rinvio
Indice dei contenuti

1. Illustrati solo i principi del decreto sulle assicurazioni per eventi estremi, manca il testo
2. Obbligo assicurazioni danni da eventi estremi: il quadro normativo
3. I destinatari dell'obbligo di assicurazione per i rischi catastrofali
4. Quali beni riguarda l'obbligo assicurativo contro gli eventi estremi
5. Altri principi dell'obbligo di polizze catastrofali per le imprese
6. L'impatto degli eventi estremi in Italia

Illustrati solo i principi del decreto sulle assicurazioni per eventi estremi, manca il testo
Salta il rinvio di 1 anno per l'obbligo per le imprese di dotarsi di assicurazioni contro i danni da eventi climatici estremi. È stato ritirato l'emendamento al dl Omnibus di Fratelli d'Italia, a prima firma Paola Ambrogio, che prevedeva lo slittamento al 2026. L'ipotesi è rimasta in discussione meno di una settimana, durante la quale si è verificata la nuova alluvione in Emilia-Romagna e il ministero delle Imprese e del Made in Italy (Mimit) ha illustrato alle imprese lo schema di decreto interministeriale che introdurrà l'obbligo di dotarsi di polizze catastrofali. Tuttavia, il Mimit ha presentato soltanto un riassunto sintetico della bozza e non il testo completo.
Vediamo nel dettaglio cosa prevede la bozza del decreto interministeriale, quali sono i nuovi obblighi in materia di assicurazioni contro le catastrofi naturali, quale approccio ha scelto il governo per fronteggiare i danni provocati dalla crisi climatica. *(continua)*
https://www.rinnovabili.it/mercato/politiche-e-normativa/polizze-catastrofali-mimit-decreto/
Rinnovabili - Lorenzo Marinone, 24 Settembre 2024

Difendere le strutture di pronto soccorso - Come migliorare le difese delle strutture di pronto soccorso da possibili attacchi, da parte di pazienti e loro familiari - Sempre più spesso, negli ultimi tempi, le cronache danno notizia di attacchi portati contro il personale del pronto soccorso, da parte di familiari. Vediamo quali possono essere le misure di prevenzione e protezione, che aiutino a mettere sotto controllo questo grave rischio per il personale sanitario.
Le esperienze maturate nell'offrire assistenza a una grande azienda sanitaria dell'Italia settentrionale mi confortano nel mettere a disposizione dei lettori un elenco delle possibili misure di messa sotto controllo del rischio di aggressioni al personale sanitario di pronto soccorso, che negli ultimi tempi ha raggiunto un livello del tutto inaccettabile.
È bene far presente, fin dall'inizio, che una struttura certamente importante, nella protezione delle aree di pronto soccorso, è legata alla presenza delle forze dell'ordine, ad esempio con un ufficio operativo. Purtroppo, questi uffici non sono presenti in tutte le aree di pronto soccorso e spesso non sono presidiati nell'arco delle ventiquattrore. Ecco perché occorre mettere a punto tutta un'altra serie di

misure, di tipo preventivo e repressivo, che possono contribuire in maniera determinante a migliorare il livello di sicurezza del personale presente.*(continua…)*
https://www.puntosicuro.it/criminalita-C-105/difendere-le-strutture-di-pronto-soccorso-AR-24646
Punto Sicuro - *Adalberto Biasiotti, 07/10/2024*

American Water Suffers Network Disruptions After Cyberattack
The largest publicly traded water utility in the US was forced to disconnect some of its online systems, and its website and telecommunications system remained unavailable as of Tuesday morning, Oct. 8.
The website of the largest publicly traded water utility in the US remained offline this morning after a cyberattack Oct. 3 forced the company to shut down some of its connected systems and services.
American Water is a significant supplier of water in the US, serving more than 14 million customers across 14 states and 18 military installations. The company employees about 6,500 people across its facilities. It discovered "unauthorized activity within its computer networks and systems" on Oct. 3 that turned out to be the result of a cybersecurity incident, the company reported in a Form 8-K filing with the US Securities and Exchange Commission.
The company activated incident-response protocols and enlisted third-party cybersecurity experts to help it contain and mitigate the attack, which included disconnecting and deactivating "certain" systems to "protect" systems and data, it reported.
The outages appear to have included the company's online customer-facing sites, as the American Water website as well as its "MyWater" customer portal served up white pages with "Forbidden 403" text today.
An attendant who answered a Dark Reading phone call to American Water's headquarters in Camden, N.J., early on Oct. 8 said she was unable to connect to a member of the media relations team, nor leave a message for anyone because the telecommunications system also "is down." (continua…)
https://www.darkreading.com/cyberattacks-data-breaches/american-water-network-disruptions-cyberattack
***DARKREADING* - Elizabeth Montalbano -October 8, 2024**

European govt air-gapped systems breached using custom malware
An APT hacking group known as GoldenJackal has successfully breached air-gapped government systems in Europe using two custom toolsets to steal sensitive data, like emails, encryption keys, images, archives, and documents.
According to an ESET report, this happened at least two times, one against the embassy of a South Asian country in Belarus in September 2019 and again in July 2021, and another against a European government organization between May 2022 and March 2024.
In May 2023, Kaspersky warned about GoldenJackal's activities, noting that the threat actors focus on government and diplomatic entities for purposes of espionage.
Although their use of custom tools spread over USB pen drives, like the 'JackalWorm,' was known, cases of a successful compromise of air-gapped systems were not previously confirmed.
Air-gapped systems are used in critical operations, which often manage confidential information, and are isolated from open networks as a protection measure.
Entering through the (air)gap
The older attacks seen by ESET begin by infecting internet-connected systems, likely using trojanized software or malicious documents, with a malware called 'GoldenDealer.'
GoldenDealer monitors for the insertion of USB drives on those systems, and when it happens, it automatically copies itself and other malicious components onto it.

Eventually, that same USB drive is inserted into an air-gapped computer, allowing GoldenDealer to install GoldenHowl (a backdoor) and GoldenRobo (a file stealer) onto these isolated systems.
During this phase, GoldenRobo scans the system for documents, images, certificates, encryption keys, archives, OpenVPN configuration files, and other valuable info and stores them in a hidden directory on the USB drive. (continua…)
https://www.bleepingcomputer.com/news/security/european-govt-air-gapped-systems-breached-using-custom-malware/
BleepingComputer *- Bill Toulas -October 8, 2024*

EU Plans Sanctions for Cyberattackers Acting on Behalf of Russia
The European Union's new sanctions framework will target individuals and organizations engaging in pro-Russian activities, such as cyberattacks and information manipulation, to undermine EU support for Ukraine.
Representatives from 27 European Union member states have approved a sanctions mechanism in an effort to thwart adversaries from launching cyberattacks, information manipulation, and interference campaigns on Russia's behalf. This new framework will allow the EU to target individuals, agencies, or organizations that attempt to undermine the values of the member states or their "security, independence and integrity."
The EU said in a statement it had detected an increasing number of these pro-Russian activities. Targets included critical infrastructure as well as "instrumentalisation of migration and other disruption actions." (continua…)
https://www.darkreading.com/cyber-risk/eu-sanctions-sabotage-cyberattacks-russia
DARKREADING *-Jennifer Lawinski -October 10, 2024*

Deepfake e disinformazione: elezioni Usa sotto assedio
Nel 2024, anno di elezioni per 2 miliardi di persone in 76 paesi, cresce il rischio di disinformazione e deepfake, specialmente nelle presidenziali USA. La sinergia tra AI e media manipolati minaccia la stabilità geopolitica, con campagne mirate a influenzare l'opinione pubblica e minare la fiducia nel processo elettorale
Il 2024 è l'anno delle elezioni, definito anche il "più elettorale" di sempre, in cui sono chiamate al voto 2 miliardi di persone in 76 Paesi. Nella maggior parte di questi, come in Regno Unito, India, Russia, Austria, Portogallo, Iran e nell'Unione europea, il processo elettorale è stato già portato a compimento con i conseguenti cambiamenti, o meno, nell'assetto politico e naturalmente geopolitico. Al momento, tra i 76 Paesi, rimane ancora aperto il discorso delle presidenziali degli Stati Uniti, le cui elezioni sono previste per il 5 novembre, in base alla vittoria di Kamala Harris o Donald Trump potrebbe cambiare la postura del Governo di Washington su determinate tematiche di politica ed economia internazionale; ma anche industriali tra cui quelle relative al settore digitale e, in modo particolare, alle policy per la sicurezza cibernetica. (https://www.rainews.it/articoli/2023/12/il-2024-sara-anno-piu-elettorale-di-sempre-oltre-50-elezioni-nel-mondo-alle-urne-76-paesi-92b3804d-2921-43da-8e10-faec53454cae.html) Sebbene in ognuno dei suddetti Paesi siano state registrate campagne di disinformazione e misinformazione, tramite l'utilizzo dell'Intelligenza Artificiale per la creazione di synthetic content e deepfake, nel periodo precedente al voto, con una diffusione e un peso maggiore nei Paesi con istituzioni democratiche, le presidenziali americane sembrano essere il bersaglio principale di attacchi mediatici da parte sia di attori esterni, molto spesso gruppi APT affiliati ad apparati di intelligence di Governi rivali, sia di elementi interni alle stesse correnti politiche.

Innanzitutto, al fine di contestualizzare gli attuali eventi cibernetici nelle presidenziali americane, è utile differenziare i concetti di synthetic content e di deepfake. Secondo il Dipartimento dell'Homeland Security degli Stati Uniti, da un mero punto di vista pratico, il termine synthetic content o synthetic media include al suo interno tutti i media che sono stati creati attraverso strumenti digitali o artificiali o i media che sono stati modificati o manipolati attraverso l'uso della tecnologia, sia analogica che digitale. Di questi sono un esempio gli audio delle cassette a nastro tagliati e riuniti al fine di rimuovere delle parole o frasi intere alterando il contenuto e, quindi, il significato; oppure, ne sono un ulteriore esempio i "cheapfakes", ossia ai contenuti sono applicate tecniche digitali per alterare la percezione di un evento da parte dell'osservatore, come la riduzione della voce e l'accelerazione del video. Restringendo il punto di vista solo sul settore di appartenenza dei synthetic content, questi si possono definire come il risultato del processo creativo di video, voce, immagini e testo generato dall'Intelligenza Artificiale e rientra nel panorama della realtà sintetica, artificiale o virtuale. A prescindere da ciò, il deepfake è una sottocategoria dei synthetic content e il termine deriva dal fatto che le tecnologie coinvolte nella creazione di questo particolare stile di contenuti manipolati, ossia "fake", prevede l'uso di tecniche di deep learning. Questo rappresenta un sottoinsieme delle tecniche di apprendimento automatico, che sono a loro volta un sottoinsieme dell'Intelligenza Artificiale. Durante l'apprendimento automatico, un modello utilizza dati di addestramento per sviluppare un modello per un compito specifico e quanto più robusti e completi sono i dati di addestramento, tanto migliore è il modello. Immagini, video, audio e testo sono tutti tipi di media che potrebbero essere utilizzati per simulare o alterare un individuo specifico o la sua rappresentazione ottenendo come risultato un contenuto deepfake.
(https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf; https://blog.paperspace.com/2020-guide-to-synthetic-media/) (continua…)
https://www.agendadigitale.eu/cultura-digitale/deepfake-e-disinformazione-elezioni-usa-sotto-assedio/
AGENDA DIGITALE *- Luisa Franchina, Corrado Fulgenzi -11 ott 2024*

Reti idriche intelligenti e sostenibili con IA e IoT: strategie e soluzioni innovative
Le reti di distribuzione idrica affrontano sfide di sostenibilità e resilienza. Tecnologie avanzate come l'AI e l'IoT ottimizzano la gestione delle risorse, riducendo perdite e migliorando l'efficienza. Attraverso sensori e algoritmi, si monitorano parametri critici e si prevede la domanda futura, promuovendo un uso più sostenibile dell'acqua
& Data Management – Università di Roma La Sapienza
Le reti di distribuzione condivise dalle utility per la distribuzione di acqua, luce e gas sono ormai dei sistemi molto complessi, spesso poco efficienti e molto vulnerabili, i quali necessitano di monitoraggio e manutenzione continui.
Le attuali infrastrutture, in particolare **i sistemi idrici urbani,** devono affrontare sfide considerevoli in termini di sostenibilità e resilienza. Gli impatti dei cambiamenti climatici e l'aumento della popolazione stanno portando a una riduzione della disponibilità di risorse idriche in varie regioni [1-3]. Inoltre, i sistemi idrici spesso subiscono notevoli perdite di acqua trattata sia in fase di distribuzione che di utilizzo [4,5].
Le tecnologie di ultima generazione hanno abilitato **la gestione intelligente delle reti per migliorarne l'efficienza** nella generazione, nella distribuzione e nell'utilizzo risorse, facilitando così la crescita economica e sostenendo la sostenibilità ambientale. Il progresso delle tecnologie di comunicazione consente alle famiglie e ai servizi idrici di monitorare il consumo di acqua attraverso contatori intelligenti (smart meters) o sistemi di lettura automatica dei contatori (Automated Meter Reading – AMR).

Indice degli argomenti

- **Tecnologie AI e IoT nelle reti idriche intelligenti**
  - I vantaggi l'integrazione degli algoritmi di intelligenza artificiale nelle reti idriche
- **Tecnologie e sistemi di rete idrica intelligente**
  - I dispositivi di misurazione
- **Potenziali benefici delle reti idriche intelligenti**
- **Problemi e soluzioni del sistema idrico urbano**
  - Perdite d'acqua
  - Qualità dell'acqua
  - Disastri
  - Consumo di energia
  - Ostacoli all'implementazione delle reti idriche intelligenti
- **Verso una trasformazione delle metodologie di gestione dell'acqua**
  - L'importanza delle partnership pubblico-private (PPP) per la realizzazione di sistemi di gestione intelligente
- **Bibliografia**

Tecnologie AI e IoT nelle reti idriche intelligenti

Una rete idrica intelligente incorpora sensori, meccanismi di controllo e strumenti analitici per garantire che l'acqua venga fornita in modo efficiente, portandola al momento giusto nel luogo giusto, preservandone al contempo le qualità**. L'elaborazione dei dati provenienti dai dispositivi IoT (Internet of Things)** attraverso algoritmi di **intelligenza artificiale** (AI) ha il potenziale per rivoluzionare il monitoraggio, l'analisi e la gestione delle risorse idriche. (continua…)
https://www.agendadigitale.eu/infrastrutture/reti-idriche-intelligenti-e-sostenibili-con-ia-e-iot-strategie-e-soluzioni-innovative/
AGENDA DIGITALE -*Yas Barzegar, Francesco Bellini - 11 ott 2024*

Direttiva CER: tutto sui nuovi standard di sicurezza per le infrastrutture critiche Ue

La Direttiva Ue sulla Resilienza delle Entità Critiche (CER) amplia la protezione delle infrastrutture critiche oltre energia e trasporti, coprendo undici settori. Promuove la resilienza e l'adattamento alle minacce emergenti. Sfide includono l'omogeneizzazione delle risorse nazionali e la cooperazione transfrontaliera

La **Direttiva CER dell'Unione europe**a**, sulla Resilienza delle Entità Critiche (Critical Entities Resilience Directive)** risponde alla necessità, riconosciuta come prioritaria dall'Unione Europea, di **garantire la sicurezza e la resilienza delle infrastrutture critiche**.

La direttiva, emenata nel 2022, rappresent**a un passo avanti significativo rispetto alla precedente direttiva** sulla **protezione delle infrastrutture critiche** europee (EPCIP) e mira a rafforzare la capacità delle entità critiche di prevenire, resistere, rispondere e riprendersi da perturbazioni significative.

Insieme alla **Direttiva Nis2**, la Direttiva CER fa parte degli sforzi dell'Europa per ottenere un livello più alto di sicurezza informatica e resilienza delle infrastrutture critiche a livello comunitario.

New stronger rules start to apply for the cyber & physical resilience of critical European entities!

Indice degli argomenti

Le infrastrutture critiche: quali sono, perché proteggerle

Le infrastrutture critiche sono quelle risorse, sistemi e reti, fisiche o virtuali, che sono essenziali per il funzionamento del tessuto sociale ed economico. Esse includono, tra le altre, infrastrutture energetiche, di trasporto, sanitarie, delle comunicazioni, bancarie, della gestione delle acque e delle acque reflue, e

della **sicurezza alimentare**. L'interruzione o il danneggiamento di tali infrastrutture può causare gravi danni alla sicurezza nazionale, alla salute pubblica, all'economia e al benessere sociale.

Gli obiettivi della direttiva CER

La Direttiva CER mira a garantire un elevato livello di **resilienza delle entità critiche** che operano all'interno dell'Unione Europea. I suoi obiettivi principali includono:

- **migliorare la resilienza delle entità critiche** compresi piani di continuità operativa e misure di gestione del rischio.
- **migliorare la cooperazione e il coordinamento** tra le entità critiche, gli stati membri e le istituzioni europee, promuovendo lo scambio di informazioni, le migliori pratiche e l'assistenza reciproca.
- **adattare le misure alle nuove minacce** per affrontare le minacce in evoluzione, come attacchi cibernetici, atti terroristici, disastri naturali e pandemie.
- **garantire l'uniformità normativa**: creare un quadro normativo coerente e armonizzato a livello europeo, garantendo che le entità critiche siano soggette a requisiti uniformi in tutti gli stati membri.

Le novità della direttiva CER rispetto alla Direttiva 2008/114/CE

La direttiva CER introduce una serie di novità rispetto alla direttiva precedente del 2008, ampliando il suo ambito di applicazione e migliorando i meccanismi di protezione e resilienza.

Ampliamento del campo di applicazione

Mentre la direttiva del 2008 si concentrava solo sui settori dell'energia e dei trasporti, l**a nuova direttiva copre un totale di ben undici settori:**

- energia;
- trasporti;
- banche;
- infrastrutture dei mercati finanziari;
- sanità;
- acqua potabile;
- acque reflue;
- infrastrutture digitali;
- amministrazione pubblica;
- spazio;
- alimentare.

Questo ampliamento riflette **la crescente complessità e interconnessione delle infrastrutture critiche** e riconosce che molte altre infrastrutture, oltre all'energia e ai trasporti, sono essenziali per la sicurezza, la salute e il benessere pubblico.

Un approccio basato sulla resilienza

La direttiva CER si distingue dalla precedente anche per il suo **approccio basato sulla resilienza**, piuttosto che sulla semplice protezione. Invece di concentrarsi esclusivamente sulla protezione fisica delle infrastrutture, la nuova direttiva enfatizza la capacità delle entità critiche di continuare a funzionare nonostante eventi avversi, di recuperare rapidamente e di adattarsi a circostanze mutevoli. Questo approccio riflette una comprensione più moderna delle minacce complesse e interconnesse che le infrastrutture critiche affrontano oggi.

La Direttiva impone una serie di **obblighi stringenti alle entità designate come critiche** progettati per assicurare che le entità siano preparate a fronteggiare una vasta gamma di minacce e di eventi avversi, mantenendo la continuità operativa dei servizi essenziali. La direttiva rappresenta un

cambiamento di paradigma rispetto alle precedenti normative europee, spostando il focus dalla semplice protezione fisica delle infrastrutture alla resilienza complessiva dell'intero sistema.

Identificazione e designazione delle entità critiche

Uno degli obblighi fondamentali sotto la Direttiva CER riguarda **l'identificazione e la designazione delle entità critiche** da parte degli Stati membri. Questo processo è cruciale perché determina quali organizzazioni e infrastrutture saranno soggette agli obblighi di resilienza stabiliti dalla direttiva.

Criteri di designazione

Gli Stati membri devono tenere conto di **criteri specifici per identificare le entità critiche tra cui:**

- **l'impatto potenziale di una interruzione dei servizi:** il potenziale impatto negativo che un'interruzione dei servizi forniti da un'entità potrebbe avere sulla salute e sicurezza pubblica, sulla sicurezza nazionale, sull'economia e sul benessere della popolazione;
- **la natura essenziale dei servizi forniti:** le entità critiche sono quelle che forniscono servizi essenziali alla società e all'economia. Ciò può includere enti che operano in settori come l'energia, i trasporti, la sanità, le infrastrutture finanziarie, le comunicazioni, l'approvvigionamento alimentare e le risorse idriche. La direttiva amplia il numero di settori rispetto alla direttiva precedente, includendo anche settori emergenti come lo spazio e le infrastrutture digitali;
- **la dipendenza di altri settori:** un altro criterio chiave per la designazione delle entità critiche è la loro interconnessione con altri settori. Alcune entità possono essere considerate critiche perché forniscono servizi o infrastrutture di supporto ad altri settori considerati essenziali;
- **la rilevanza transnazionale:** alcune infrastrutture possono essere designate critiche non solo per il loro impatto all'interno di uno Stato membro, ma anche per il loro ruolo transnazionale.

(continua…)

https://www.agendadigitale.eu/infrastrutture/direttiva-cer-tutto-sui-nuovi-standard-di-sicurezza-per-le-infrastrutture-critiche-ue/

***AGENDA DIGITALE** - Stefano Piroddi - 15 ott 2024*

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link *http://www.infrastrutturecritiche.it/new/per-iscriversi/*

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Per maggiori informazioni sull'Associazione inviare una mail a
segreteria@infrastrutturecritiche.it
o visitate il sito
www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Alberto Traballesi Glauco Bertocchi Silvano Bari Gianluca Cipriani *ai quali potete inviare suggerimenti e quesiti scrivendo a: segreteria@infrastrutturecritiche.it*

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.