AbruzzoWeb
Tutte le notizie d'Abruzzo a portata di click

CYBERSICUREZZA: EVENTO DI FORMAZIONE DELLA REGIONE PER GLI ENTI. MARSILIO, “SERVE IMPEGNO COSTANTE”

24 Marzo 2025



L’AQUILA – “La formazione è uno strumento fondamentale per rafforzare la capacità della pubblica amministrazione di prevenire e affrontare le minacce informatiche. Dopo gli attacchi subiti, a cui abbiamo saputo reagire con prontezza, come riconosciuto anche dall’Agenzia per la cybersicurezza nazionale che ringrazio per la collaborazione, è emersa con forza la necessità di diffondere conoscenze e competenze specifiche”.

Lo ha detto il Presidente della giunta regionale Marco Marsilio, intervenendo oggi all’evento formativo organizzato dalla Regione Abruzzo con l’Agenzia per la Cybersicurezza Nazionale, in collaborazione con il Formez, nella Sala Ipogea del Consiglio regionale.

“Questo evento nasce proprio per rispondere a quella esigenza, offrendo agli operatori pubblici un’occasione concreta di aggiornamento e consapevolezza per difendere sistemi che presentano sempre grandi fragilità”.

Come si spiega in una nota della Regione, la giornata è stata concepita con l’obiettivo di offrire ad amministratori, dirigenti, funzionari pubblici, responsabili IT e operatori della pubblica amministrazione – in particolare del settore sanitario – strumenti operativi per affrontare le principali minacce informatiche, comprenderne le implicazioni pratiche e adottare strategie efficaci di prevenzione e protezione, nel rispetto del quadro normativo vigente. Attraverso un’articolata combinazione di interventi istituzionali, casi studio e momenti di confronto, l’incontro ha rappresentato un’importante occasione di crescita e aggiornamento. L’intento è stato quello di rafforzare la consapevolezza e le competenze degli attori pubblici, promuovendo un approccio proattivo alla cybersecurity e alla tutela dei dati sensibili, e favorendo la diffusione di modelli organizzativi avanzati e best practice in materia di sicurezza digitale.

Sono intervenuti: Nunzia Ciardi, Vicedirettore generale dell'Agenzia per la Cybersicurezza Nazionale, Nicoletta Verì, assessore alle Politiche della Salute, Emanuela Grimaldi, direttore del Dipartimento Sanità, Riccardo Urbani, esperto tecnico del Presidente in materia di Digitalizzazione, innovazione tecnologica e cybersicurezza e capo della task force di recupero dell'Asl 1 L'Aquila, Gianluca Galasso, direttore del Servizio Operazioni/CSIRT Italia dell'Agenzia per la Cybersicurezza Nazionale, Patrizia Consolo, direttore Direzione Capacity Building per i territori Formez PA e Luciano Cococcia, dirigente Servizio Informatico Regione Abruzzo.

«La trasformazione digitale che sta interessando in misura sempre maggiore i servizi pubblici – ha continuato Marsilio – impone un impegno costante sul fronte della sicurezza informatica, soprattutto in ambiti delicati come quello sanitario e nella gestione amministrativa a livello territoriale. La tutela dei dati personali, la protezione delle infrastrutture tecnologiche e la capacità di prevenire e fronteggiare attacchi informatici sono ormai condizioni essenziali per garantire l'efficienza e l'affidabilità dei servizi offerti ai cittadini. Un'attenzione resa ancora più necessaria dagli attacchi informatici che, negli ultimi mesi, hanno preso di mira siti istituzionali a livello nazionale e regionale, coinvolgendo anche il nostro territorio. In un quadro internazionale segnato da tensioni geopolitiche, è fondamentale rafforzare la resilienza digitale della pubblica amministrazione, per evitare che diventi un punto debole del sistema Paese.»

Il consulente informatico della Presidenza Urbani, nel suo intervento, ha ribadito l'urgenza di diffondere competenze e strategie di protezione digitale all'interno del sistema pubblico. "Questa giornata formativa – ha spiegato Riccardo Urbani – nasce proprio con l'obiettivo di informare, sensibilizzare e rafforzare la cultura della sicurezza digitale, che oggi rappresenta una priorità strategica. Le nuove sfide del presente e del futuro non si limitano all'intelligenza artificiale e all'ingegneria, ma comprendono sempre di più la cybersecurity. Dopo l'attacco alla ASL 1, è stato messo in campo un sistema di difesa importante, anche se l'ingegneria clinica rimane oggi uno degli anelli più deboli a livello nazionale. Tuttavia, la Regione Abruzzo ha già fatto un passo avanti: è infatti in partenza un progetto strutturato per la messa in sicurezza dell'intero comparto. L'attacco informatico, con richiesta di riscatto, subito in passato dalla ASL 1, è stato uno dei più gravi che possano colpire una struttura sanitaria. Da qui è possibile comprendere l'importanza di rafforzare la consapevolezza e la preparazione del personale".

È evidente oggi quanto la nostra vita sia completamente digitalizzata, e come i dati digitali rappresentino ormai la sintesi e l'espressione della nostra stessa esistenza. Questo fenomeno ha determinato un significativo aumento degli attacchi informatici contro i sistemi sanitari a livello globale.

"Nel 2024 gli attacchi sono cresciuti del 30% rispetto all'anno precedente e si sono quadruplicati dal 2020 – ha concluso nel suo intervento il vice direttore dell'Agenzia Nunzia Ciardi – Piaccia o meno, che siamo esperti o meno, una quota di responsabilità nella sicurezza informatica appartiene a ciascuno di noi. Tutti dobbiamo acquisire consapevolezza e imparare ad applicare quelle regole, dalle più semplici per i cittadini alle più articolate per gli amministratori, che garantiscano la protezione del sistema che custodisce la nostra vita".

© 2026 Abruzzo Web Enfasi srl - Quotidiano digitale registrato presso il Tribunale dell'Aquila con decreto n°501 del 2 settembre 2003
Iscrizione al ROC n. 26362 - P.IVA 01812420667
Direttore responsabile Berardo Santilli