



Pa digitale, il nodo sicurezza: proteggere i dati per non perdere fiducia

Descrizione

(Adnkronos) Il punto, sottolinea, non è rallentare l'innovazione, ma governarla.

Tecnologia e rischio: un equilibrio da costruire

L'adozione di nuove tecnologie introduce una doppia dimensione di rischio. Da un lato la tecnologia può essere utilizzata in modo improprio, dall'altro può diventare essa stessa uno strumento di attacco, osserva. Un esempio emblematico è l'intelligenza artificiale: offre enormi benefici in termini di efficienza e automazione, ma introduce anche nuove dimensioni di rischio che devono essere gestite con attenzione.

In questo scenario, la cybersecurity assume un ruolo duplice: abilitare un'adozione sicura delle tecnologie e, allo stesso tempo, sfruttarle per rafforzare le difese.

Sicurezza e fiducia: il nodo dei dati

Accanto ai rischi tecnologici, emerge un elemento centrale: la fiducia dei cittadini. La protezione dei dati personali e la sicurezza dei servizi non sono solo categorie di rischio, ma il fondamento della fiducia, sottolinea. Dati anagrafici, sanitari, fiscali e giudiziari rappresentano oggi il vero patrimonio dello Stato e devono essere protetti con lo stesso livello di attenzione riservato alle infrastrutture critiche. Proteggere i dati significa inevitabilmente proteggere anche i servizi digitali che su quei dati si basano, evidenzia.

Dalla singola amministrazione all'ecosistema

Negli ultimi anni, anche grazie al Pnrr, la digitalizzazione della Pa ha accelerato. Ma questa evoluzione ha cambiato il contesto di riferimento. Oggi ogni amministrazione non opera più in modo isolato, ma è parte di un ecosistema digitale interconnesso, osserva.

Questo implica un cambio di paradigma nella gestione della sicurezza. «La valutazione del rischio non riguarda solo l'infrastruttura interna, ma anche l'intero ecosistema di fornitori, piattaforme e servizi condivisi». La sicurezza diventa quindi una responsabilità estesa, che richiede visibilità e controllo lungo tutta la catena del valore digitale.

Security by design e difesa attiva

Per affrontare questa complessità, l'approccio deve cambiare. «È necessario integrare la sicurezza fin dall'inizio dei progetti, secondo un modello di security by design», spiega. A questo si affianca un sistema continuo di verifiche tecniche e un paradigma di difesa attiva, capace di migliorare la rilevazione e la risposta alle minacce. In questa prospettiva, la sicurezza non è un elemento accessorio, ma una componente strutturale del ciclo di vita dei servizi digitali.

Sovranità digitale e governo delle tecnologie

Un altro pilastro è rappresentato dalla sovranità digitale.

«Serve sapere dove risiedono i dati, come vengono utilizzati e chi ne mantiene il controllo», sottolinea. Questo si traduce nella necessità di un sistema di governo e controllo capace di garantire trasparenza e consapevolezza nell'uso delle tecnologie. L'approccio, spiega, è quello di integrare innovazione, sicurezza e governance all'interno di un quadro coerente, che consenta di adottare nuove soluzioni in modo sostenibile.

Prepararsi al futuro: la sfida del quantum

Guardando avanti, nuove tecnologie come il quantum computing pongono ulteriori interrogativi. «Il quantum promette capacità straordinarie, ma apre anche questioni sulla sicurezza crittografica e sulla protezione delle informazioni sensibili».

Prepararsi a uno scenario «quantum-safe» significa iniziare già oggi a ripensare modelli di sicurezza e governance, in grado di resistere alle tecnologie di domani.

La sicurezza come abilitatore

In definitiva, per De Marco il messaggio è chiaro: sicurezza e innovazione non sono in contrapposizione. «La sicurezza non è un freno all'innovazione, ma il suo principale abilitatore», afferma. «Da questa consapevolezza che passa la costruzione di una Pubblica amministrazione più moderna, affidabile e capace di guadagnare la fiducia dei cittadini. «Oggi è già domani: investire in sicurezza, governance e innovazione responsabile significa costruire fin da ora una Pubblica amministrazione solida e credibile», conclude.

«»

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione

Giugno 5, 2026

Autore

redazione

default watermark