

Arriva la digital longevity



**Dalla big picture
all'intelligenza
artificiale:
una nuova
gestione delle
infrastrutture
digitali che usa e si
muove su Cloud**



Le organizzazioni che intraprendono un percorso di digitalizzazione sanno quanto sia importante partire da una visione d'insieme. Il primo passo è normalmente l'assessment, ossia un'analisi volta a chiarire fabbisogni, processi e risorse coinvolte e, laddove necessario, a ridefinire i vari step in maniera lineare ed efficace basandosi sulle best practice.

Partire dalla big picture

Come in qualsiasi progettazione, una volta analizzato il problema, bisogna definire una soluzione, ma per farlo è necessario avere in mente o definire il quadro generale e le prospettive: quali saranno gli sviluppi futuri dell'azienda/ente? Quali servizi o nuove tecnologie si affacceranno sul mercato? Quali sono le principali criticità nei prossimi decenni? Quali "imprevisti" o eventi potrebbero manifestarsi? In quale contesto si colloca la realtà in cui operiamo e quali sono gli stakeholder/territori coinvolti?

Si tratta di guardare in ottica di longevità digitale con un approccio "anticipante". Questa

responsabilità compete al management chiamato ad assumere decisioni strategiche per l'organizzazione. Ogni scelta tecnologica e informatica non riguarda solo i "tecnici", ma incide sulla continuità dei servizi, su rischi, investimenti e capacità di innovazione. Sarà fondamentale allora scegliere un partner digitale in grado di supportare gli sviluppi futuri dell'organizzazione, un soggetto competente, affidabile e solido nel tempo.

I principi guida

Centralità e qualità del dato, interoperabilità, sicurezza, continuità operativa e conformità normativa sono principi guida di ogni progetto di digitalizzazione.

Due aspetti risultano rilevanti: l'integrazione governata dei sistemi e la sicurezza lungo l'intero ciclo di vita. Avere a disposizione software integrati per la gestione dei servizi digitali è quindi fondamentale, anche perché evita la frammentarietà che, non solo richiede il reinserimento di dati nei vari software, ma apre anche le porte ad attacchi informatici.

Oggi anche le realtà che hanno già implemen-

tato gestionali e strumenti digitali si trovano a dover ripensare il loro modo di intendere l'informatizzazione. Il modello attuale non regge più la complessità. Tra gennaio e settembre 2025, nel settore sanitario italiano, CSIRT Italia ha censito 60 eventi cyber, rispetto ai 42 rilevati nello stesso periodo del 2024, con un incremento di circa il 40%. Il dato conferma la forte esposizione del settore sanitario alle minacce informatiche.

La frammentazione dei sistemi è uno degli elementi che apre la porta agli attacchi informatici, oltre ad una scarsa formazione del personale, o ad una cattiva o insufficiente implementazione delle misure di sicurezza più basilari. Per questo motivo è necessario che la progettazione delle infrastrutture informatiche tenga conto non solo delle esigenze operative ma anche di questi fattori, delle attuali tendenze e relativi costi che questa gestione comporta.

Le evoluzioni normative

Il quadro normativo europeo rafforza la necessità di progettare e governare sistemi sicuri, affidabili e verificabili. GDPR, disciplina NIS2 e AI Act introducono obblighi distinti in materia di protezione dei dati, gestione del rischio informatico e utilizzo dell'intelligenza artificiale. In ambito sanitario assumono inoltre particolare rilievo il Regolamento sui dispositivi medici, quando il software persegue una specifica finalità medica e il Regolamento sullo Spazio europeo dei dati sanitari, incentrato su accesso, controllo e scambio sicuro dei dati sanitari elettronici.

Il GDPR si fonda sul principio di responsabilizzazione, che richiede di applicare e poter dimostrare il rispetto delle prescrizioni. Per i soggetti rientranti nel suo ambito di applicazione, la disciplina NIS2 attribuisce agli organi di amministrazione e direttivi specifiche responsabilità nella governance del rischio informatico. L'AI Act introduce invece obblighi differenziati in funzione del ruolo dell'organizzazione e della classificazione del sistema. Questi requisiti devono tradursi in misure architetture, organizzative, contrattuali e documentali verificabili lungo l'intero ciclo di vita.

Ma perché scegliere una infrastruttura basata su Cloud?

Aggiornamenti, sicurezza, backup, monitoraggio continuo: scegliendo servizi software in Cloud è possibile contare su sistemi protetti dove è il provider a dover garantire determinati standard, dal tracciamento degli accessi, agli aggiornamenti. I servizi possono essere monitorati e si possono identificare le difficoltà prima che diventino emergenze.

Un'infrastruttura mantenuta e aggiornata attraverso processi controllati facilita l'adeguamento alle evoluzioni normative e tecnologiche e riduce il debito tecnico che può ostacolare lo sviluppo di nuovi servizi. Ciò vale in particolare per l'integrazione di funzionalità di intelligenza artificiale e telemedicina, per le quali devono essere valutate la sicurezza informatica, la protezione dei dati, l'interoperabilità, la supervisione umana e la conformità normativa.

Quando una funzionalità software persegue una specifica finalità medica, occorre inoltre valutarne la qualificazione come dispositivo medico e applicare, ove pertinente, i requisiti del MDR lungo l'intero ciclo di vita.

Servizi digitali che se gestiti on premise, cioè attraverso server ospitati in casa, presentano dei costi continui di mantenimento e adeguamento, non solo in termini economici, ma anche in termini di tempo e competenze da dedicare, esponendo anche a continui rischi che vanno aggiungersi agli oneri già in essere. Ripensare gli investimenti informatici in una prospettiva futura significa tener conto di tutti questi costi sommersi, tangibili ed intangibili, così come dei costi di eventuali rischi ed emergenze.

Bisogna allora fare il salto di paradigma e pensare in termini di "digital longevity": come posso oggi ripensare alla mia infrastruttura informatica in modo che sia non solo attuale e adeguata oggi, ma anche longeva domani?

Zucchetti Healthcare sta guardando avanti

Oggi, alla luce delle profonde evoluzioni digitali e normative in atto, è sempre più importante affidarsi ad un partner consolidato,

che sia in grado di assumersi le responsabilità della gestione dei servizi digitali e che garantisca continuità ad un settore chiave come quello sociosanitario.

Zucchetti Healthcare mette a disposizione oggi nuovi servizi digitali, progettati per essere longevi nel tempo accompagnando le realtà ad affrontare le sfide del futuro, per ottimizzare la gestione informatica con meno oneri e più tempo da dedicare alla cura. Per questo Zucchetti ha sviluppato Zucchetti Healthcare Infinity hub, un hub di servizi digitali di nuova generazione, in grado di supportare le organizzazioni oggi e in futuro.

(Fonte Agenzia per la cybersicurezza nazionale, "Sanità nel mirino dei cybercriminali: cresce del 40% il numero di attacchi nel 2025", dati relativi al periodo gennaio-settembre 2025)

Zucchetti inventa e mette in pratica soluzioni organizzative "in evoluzione" che guardano al futuro in ottica diversa

