Sede legale: Via Magellano, 1 - 10128 TORINO - Tel. +39 011.508.1111 - www.mauriziano.it - P.I./Cod. Fisc. 09059340019

Piano Triennale per la transizione digitale 2023-2025 DELL'A.O. ORDINE MAURIZIANO
Riferimento al Piano Triennale per l'informatica 2022-2024 pubblicato da AGID

Torino, giugno 2023

Indice generale

PARTE Iª - IL PIANO TRIENNALE

Introduzione

Il Piano Triennale per l'Informatica nella Pubblica amministrazione, realizzato da AgID, è il documento indirizzo strategico ed economico con cui si definisce il modello di riferimento per lo sviluppo dell'informatica pubblica italiana e la strategia operativa di trasformazione digitale del Paese.
Il piano, come prescritto dal suo Statuto e come ribadito dalla Legge di Stabilità per il 2016, definisce:

- le linee operative di sviluppo dell'informatica pubblica;
- il modello strategico di evoluzione del sistema informativo della PA;
- gli investimenti ICT del settore pubblico secondo le linee guida europee e del Governo.

Fin dalla sua prima edizione (2017-2019) il Piano Triennale ha rappresentato il documento di supporto e di orientamento per le Pubbliche amministrazioni italiane nella pianificazione delle attività sul percorso di innovazione tecnologica e nelle edizioni successive ha costituito il riferimento per declinare le strategie che si sono susseguite nel tracciato operativo composto da obiettivi e attività.
Il recente aggiornamento 2022-2024 del Piano Triennale per l'informatica nella Pubblica Amministrazione ("Piano Triennale") conferma l'impostazione generale della precedente edizione 2021-2023 ed il Modello generale a sei componenti (Servizi, Dati, Piattaforme, Infrastrutture, Interoperabilità, Sicurezza) e in modo ancor più evidente, attribuisce uno spazio più rilevante al PNRR, oltre a fornire un quadro organico dei vari ambiti di cui si compone, tramite la collaborazione con i soggetti che esercitano competenze istituzionali e responsabilità sull'implementazione.
La nuova edizione del Piano Triennale si preoccupa di allineare, anche temporalmente, gli obiettivi del Piano Triennale a quelli previsti dal PNRR e comprende

- la revisione del contesto normativo e strategico, in linea con gli ultimi interventi legislativi e le più recenti linee guida adottate;
- l'adeguamento di obiettivi, risultati attesi e linee di azione per gli anni 2022, 2023 e 2024, sulla base degli esiti del monitoraggio 2021, con l'integrazione di riferimenti diretti a target e investimenti previsti dal PNRR;
- il mantenimento delle Linee di azione attribuite alle PA, presenti nelle precedenti edizioni del Piano e ancora attuali, collocate all'interno della sezione "Linee di azione ancora vigenti";
- la riformulazione e ripianificazione delle linee di azione del Piano Triennale 2021-2023 che non hanno raggiunto la naturale conclusione.

In quest'ottica la Commissione UE nella Comunicazione "Progettare il futuro digitale dell'Europa" ha disposto che almeno il venti per cento della spesa complessiva del PNRR sia rivolta a investimenti e riforme nel digitale, con l'obiettivo di migliorare le prestazioni digitali sintetizzate dall'Indice di digitalizzazione dell'economia e della società (DESI).
Il PNRR ha fra i propri assi strategici, condivisi a livello europeo, quello della digitalizzazione e innovazione. Prevede nella componente denominata "Digitalizzazione, innovazione e sicurezza nella PA" investimenti pari a 9,75 Mld, di cui 6,14 Mld destinati alla misura "Digitalizzazione PA". Quest'ultima dovrà essere attuata secondo le linee tracciate dal Piano Triennale, nel pieno rispetto delle disposizioni del CAD e di tutte le altre normative e Linee Guida pubblicate.

In campo normativo il Decreto Semplificazioni "bis" (D.L. 31 maggio 2021 n. 77 come convertito con la legge n. 108 del 29 luglio 2021) ha recentemente introdotto l'art. 18-bis del CAD (Violazione degli obblighi di transizione digitale).

Ruolo del Responsabile per la Transizione al Digitale

Il Responsabile per la transizione al digitale (RTD) è una figura prevista dal Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82) all'interno dell'amministrazione con il ruolo di guidare la PA nella quale opera a rispondere ai cambiamenti richiesti dalla digitalizzazione.
Così come esplicitato dalla circolare nr. 3 del 1 ottobre 2018 del Ministro per la Pubblica Amministrazione, il ruolo del Responsabile della Transizione al Digitale prevede il raccordo e la consultazione delle altre figure coinvolte nel processo di digitalizzazione della Pubblica Amministrazione.
Il Responsabile per la Transizione al Digitale (RTD) è la figura dirigenziale, dotata di alte competenze in ambito tecnologico, manageriale e di informatica giuridica, che, all'interno dell'Amministrazione, ha il compito di attuare e coordinare la trasformazione digitale dell'amministrazione, lo sviluppo dei servizi pubblici digitali, il rispetto degli standard e l'adozione dei nuovi modelli di design, accessibilità, riuso ed open data. L'RTD risponde, con riferimento ai compiti relativi alla transizione alla modalità digitale, direttamente all'organo di vertice politico.
Con Delibera n. 871 del 29 dicembre 2017, in ottemperanza all'art. 17 del CAD (Codice di Amministrazione Digitale) è stato nominato il "Responsabile per la transizione digitale" la figura del Direttore ICT e Sistemi Informativi, allo scopo di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'Amministrazione definite dal Governo.
Fanno capo alla S.C. ICT & Sistemi Informativi gli acquisti di soluzioni e sistemi informatici, al fine di assicurarne la compatibilità con gli obiettivi di attuazione dell'Agenda Digitale ed in particolare, con quelli stabiliti nel Piano Triennale ICT nazionale.

Contesto Strategico

Il presente Piano triennale per la transizione al digitale, redatto in coerenza con quanto prescritto dal Piano Triennale nazionale, ha l'obiettivo di declinare e dare concretezza, attraverso una programmazione definita e integrata con quella finanziaria, alla visione strategica che guiderà la digitalizzazione dei servizi e dei processi dell'A.O. Ordine Mauriziano nel prossimo triennio, in coerenza con quanto finora sviluppato in termini di ricorso alle risorse dell'ICT e di miglioramento continuo dei processi dell'Azienda e con le indicazioni normative a livello regionale e nazionale.
Attraverso il presente Piano l'Azienda intende dare una notevole accelerazione al processo di semplificazione amministrativa e di digitalizzazione, accompagnando la "transizione amministrativa" a quella "digitale", mettendo a sistema le numerose iniziative e progettualità in essere e facendo in modo che sempre più le competenze digitali siano patrimonio di tutti i dipendenti e pazienti/utenti.
Il Piano triennale per l'informatica nella Pubblica Amministrazione declina i seguenti come obiettivi prioritari della strategia nazionale per lo sviluppo digitale della PA:

- Favorire lo sviluppo di una società digitale, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della pubblica amministrazione che costituisce il motore di sviluppo per tutto il Paese.

- Promuovere lo sviluppo sostenibile, etico ed inclusivo, attraverso l'innovazione e la digitalizzazione al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale.
- Contribuire alla diffusione delle nuove tecnologie digitali nel tessuto produttivo italiano, incentivando la standardizzazione, l'innovazione e la sperimentazione nell'ambito dei servizi pubblici.

Partendo da tali obiettivi, attraverso la digitalizzazione dei propri servizi e processi, l'A.O. Ordine Mauriziano intende:

- mantenere alti e ove possibile incrementare i propri livelli prestazionali e qualitativi, rendendo sempre possibile -in assenza di vincoli normativi- anche la fruizione informatica dei servizi e la relazione a distanza con Pazienti, Cittadini e imprese
- semplificare i processi gestionali, eliminando ridondanze e sprechi, in una logica di ottimizzazione delle risorse, trasparenza amministrativa e sostenibilità dell'offerta dei servizi
- innovare sempre più l'offerta dei servizi, rilevando le esigenze dei fruitori ma anche prevenendole grazie all'ascolto e all'analisi dei dati in possesso dell'Azienda

Attraverso questi percorsi l'A.O. Ordine Mauriziano intende sempre più diventare e essere percepito come un ente in grado di offrire servizi di qualità e multicanali, con processi efficaci e efficienti, con una diffusa sensibilità alla semplificazione e alla digitalizzazione delle procedure e che contribuisce alla condivisione e diffusione delle nuove tecnologie digitali.

Con il presente documento, nel rispetto delle indicazioni contenute nel Piano triennale nazionale, l'A.O. Ordine Mauriziano, definisce la propria strategia in materia di trasformazione digitale per il triennio 2023-2025, partendo dal presupposto che l'emergenza COVID 19 ha imposto all'amministrazione nuovi modelli per l'erogazione dei servizi. In primis lo smart working e il potenziamento dei servizi in rete.

Obiettivi e spesa complessiva prevista

Gli obiettivi generali dell'Amministrazione in tema didigitalizzazione per il periodo di riferimento:

- Attuare gli interventi previsti nel progetto M6.C2 – 1.1.1. Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione delle strutture ospedaliere (DEA Dipartimenti di Emergenza e Accettazione di Livello I e II))- Cartella Clinica Elettronica Ospedaliera finalizzato al miglioramento, per la struttura già di livello 4, dello stato di informatizzazione attraverso:
  - l'integrazione del Sistema Informativo Ospedaliero con nuove componenti del Sistema Informativo Sanitario Regionale
  - la realizzazione di nuovi moduli della Cartella Clinica Elettronica (CCE) ospedaliera
  - l'acquisizione di strumenti per il potenziamento della sicurezza aziendale in riferimento alla Cyber Security
  - la sostituzione/dotazione di hardware (postazioni di lavoro, stampanti, scanner, tablet, apparati di rete, server, tablet medicali, Mobile Cart Computer Medical) presso i reparti al fine di migliorare la fruizione dei servizi informatici aziendali utilizzati dagli operatori sanitari dell'Azienda
  - l'archiviazione digitale dei vetrini di Anatomia Patologica
- Migliorare la capacità di generare ed erogare servizi digitali
- Potenziare il Cloud

- Realizzare un'istanza di Disaster Recovery per l'applicativo sanitario "Babele" ospitata presso il Cloud Regionale Nivola
- Adeguamento degli applicativi a FSE 2.0 per tutti i documenti inviati al FSE
- Aggiornamento del sito Web istituzionale

Nella tabella sotto riportata è indicata la previsione della spesa (comprensiva di IVA) con **Risorse dell'**Amministrazione in tema di digitalizzazione per il periodo di riferimento.

Annualità	Spesa Corrente	Investimenti
Anno 2023	€ 2.500.000,00	€ 300.000,00
Anno 2024	€ 2.700.000,00	€ 500.000,00
Anno 2025	€ 2.900.000,00	€ 800.000,00

Nella tabella sotto riportata è indicata la previsione della spesa (comprensiva di IVA) con **Risorse finanziate dal PNRR** in tema di digitalizzazione per il periodo di riferimento.

Dati aggiornati al 20.6.2023	CUP	Importo Totale	Importo già utilizzato	Importo residuo	DG
Misura 1.4.4 - Estensione dell'Utilizzo delle piattaforme d'Identità Digitali - SPID e CIE - PNRR M1C1 Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE" FINANZIATO DALL'UNIONE EUROPEA - NextGenerationEU.	G17H22001810006	€ 14.000,00	€ 8.224,00		185/2023
Misura 1.4.3 ADOZIONE PAGOPA – PNRR M1C1 Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE" FINANZIATO DALL'UNIONE EUROPEA - NextGenerationEU.	G11F22004280006	€ 73.805,00	€ 73.805,00		365/2023
M6.C2 – 1.1.1. Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione delle strutture ospedaliere (DEA Dipartimenti di Emergenza e Accettazione di Livello I e II))- Cartella Clinica Elettronica Ospedaliera	G16G22000070005	€ 4.963.389,10	€ 2.778.416,68		176/2022
PNRR M6 Salute: Interventi digitalizzazione attuazione FSE 2.0.	G17H23000050006	€ 725.501,00	€ 104.973,68		346/2023
Misura 1.4.3 APP IO - ALTRI ENTI - PNRR M1C1 Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE" FINANZIATO DALL'UNIONE EUROPEA - NextGenerationEU.	G17H23000160006	€ 29.520,00	€ 12.200,00		476/2023

PARTE IIa – LE COMPONENTI TECNOLOGICHE

In coerenza con gli obiettivi del Piano Triennale nazionale, il documento è articolato secondo le componenti (Servizi, Dati, Piattaforme, Infrastrutture, Sicurezza ed Interoperabilità) che costituiscono il "Modello Strategico di evoluzione del sistema informativo della Pubblica Amministrazione", integrate dal tema delle progettualità e iniziative che l'Azienda intende mettere in atto a beneficio dei propri utenti/pazienti. In correlazione alle diverse componenti, nel presente documento è evidenziato lo stato dell'arte e le principali progettualità dell'Azienda nell'arco del triennio.
Occorre quindi agire su più livelli e migliorare la capacità delle Pubbliche Amministrazioni di generare ed erogare servizi di qualità attraverso:

- il riuso e la condivisione di *software* e competenze tra le diverse amministrazioni;
- un utilizzo più consistente di soluzioni *Software as a Service* già esistenti;
- l'adozione di modelli e strumenti validati e a disposizione di tutti;
- il costante monitoraggio da parte delle PA dei propri servizi *online*;
- l'incremento del livello di accessibilità dei servizi erogati tramite siti web e app *mobile*
- lo scambio di buone pratiche tra le diverse amministrazioni, da attuarsi attraverso la definizione, la modellazione e l'organizzazione di comunità di pratica.

CAPITOLO 1. Componente Tecnologica 1 - SERVIZI

Il miglioramento della qualità dei servizi pubblici digitali costituisce la premessa indispensabile per l'incremento del loro utilizzo da parte degli utenti (cittadini, imprese o amministrazioni pubbliche). I servizi devono avere un chiaro valore per l'utenza. La qualità finale dipende da un'attenta valutazione organizzativa e dall'adozione di tecnologie abilitanti che consentano di strutturare l'intero processo della prestazione erogata, semplificando i processi interni delle PA e celando la complessità residua

Obiettivi e risultati attesi

OB.1.1 - Migliorare la capacità di generare ed erogare servizi digitali

R.A.1.1a - Diffusione del modello di riuso di software tra le amministrazioni in attuazione delle Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione
Secondo quanto previsto dalle Linee Guida per l'Acquisizione e il Riuso e in rispetto degli artt. 68 e 69 del CAD, il processo di acquisizione del software da parte di una Pubblica Amministrazione prevede la scelta privilegiata nell'ambito di quelli a riuso pubblicati nel catalogo di Developers Italia, ovvero, qualora a riuso sia presente una soluzione in grado di soddisfare le esigenze individuate, il processo di valutazione è concluso e la PA può procedere all'approvvigionamento.
La scelta privilegiata del riuso viene ripresa e rafforzata anche nel Piano Triennale per l'Informatica nella P.A. che identifica proprio nel riuso la condizione necessaria per il miglioramento qualitativo dei servizi pubblici digitali e ne incentiva la diffusione del modello invitando le Amministrazioni Pubbliche a dichiarare all'interno del catalogo di Developers Italia quali software di titolarità di un'altra PA hanno preso in riuso.

Con Deliberazione DG 705 del 4.11.2020, l'Azienda, dopo una valutazione da parte congiunta dei medici ospedalieri e degli informatici, scelse per l'attività di Televisita la piattaforma Trec, sviluppata all'interno del programma TrentinoSalute4.0 da parte della Provincia Autonoma di Trento, della fondazione FBK e di Apss, e rilasciata con licenza open Eupl da parte di Apss in riuso per gli aspetti di tele visita.

L'adozione della soluzione si coniuga principalmente nella disponibilità di un'applicazione di video chat con caratteristiche di flessibilità e sicurezza elevate, che garantiscono un livello ottimale di protezione dei dati e dei contenuti sensibili e individuali; la piattaforma Tre-C Tele visita, integra l'applicativo di video chat completandolo al contempo con altre funzionalità modulari, rendendolo flessibile e adattabile all'introduzione in contesti operativi differenti.

L'applicazione è stata progettata per garantire sicurezza e privacy agli utenti:

- comunicazione basata sullo standard WebRTC
- possibilità di comunicazioni criptate
- le sale virtuali esistono solo per la durata della video visita
- password di protezione della singola video visita
- qualsiasi informazione è gestita all'intero della piattaforma in modalità totalmente aderente alle indicazioni del GDPR e sulla privacy, e viene condivisa solo con altri partecipanti alla riunione. Queste informazioni non vengono inoltre conservate dopo la riunione.

La piattaforma è stata attivata nel I trimestre 2021, a seguito della predisposizione della valutazione di impatto in collaborazione con il DPO aziendale, ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (GDPR).
E' prevista la sostituzione della piattaforma con una soluzione individuata dalla Regione Piemonte nell'ambito del progetto regionale di Telemedicina.

R.A.1.1b - Implementazione Cartella Clinica Mobile
Adozione di soluzioni "mobile" presso i reparti di ricovero, al fine di consentire la fruibilità delle principali funzionalità della CCE anche su dispositivi mobili e quindi in prossimità del letto del paziente. Si prevede il riutilizzo della logica applicativa già disponibile e fruita dall'attuale componente di front-end e l'implementazione di una nuova user-interface, integrandola agli attuali moduli che applicano la logica applicativa.

R.A.1.1c - Diffusione del monitoraggio, da parte delle Amministrazioni, della fruizione dei servizi digitali
I servizi digitali offerti dall'Amministrazione sono rivolti ai dipendenti e ai cittadini.
Nel primo caso il monitoraggio/valutazione dell'utilizzo è effettuato rispetto all'uso degli applicativi software aziendali e all'aggiornamento dei dati: si può dichiarare che sia in ambito amministrativo, sia in ambito sanitario tutti i dati sono trattati con strumenti informatici.
Nel caso di pazienti/cittadini siamo in grado di monitorare:

- il numero di prenotazioni on line
- il numero di accessi per televisita
- il numero di pagamenti attraverso PagoPa
- il numero di accessi tramite SPID
- il numero di accessi al sito aziendale
- il numero di referti ritirati on line

Sul sito esiste una sessione "Servizi in rete" e una breve questionario per bvalutare la "soddisfazione degli utenti"

L'obiettivo è di potenziare questi strumenti per poter "confrontarci" con gli utenti

OB.1.2 - Migliorare l'esperienza d'uso e l'accessibilità dei servizi

R.A.1.2a - Incremento e diffusione dei modelli standard per lo sviluppo di siti
L'Azienda adegua il proprio sito web in aderenza ai principi delle Linee guida di design per i siti internet e i servizi digitali della PA ed è tenuta a:

- Comunicare ad AGID, tramite apposito *form* online, l'uso dei modelli per lo sviluppo web per i propri siti istituzionali
- Effettuare i test di usabilità e comunicare ad AGID, tramite l'applicazione form.agid.gov.it, l'esito dei test di usabilità del proprio sito istituzionale
- Pubblicare, entro il 23 settembre 2023, tramite l'applicazione form.agid.gov.it, una dichiarazione di accessibilità per il proprio sito web
- Reingegnerizzare il Sito Istituzionale e la Intranet tramite il supporto di un fornitore esterno. Il nuovo Sito sarà un CMS conforme alle nuove linee guida AGID rese pubbliche con determina n.224/2022. I punti di attenzione sono rivolti principalmente all'Interfaccia Utente di semplice utilizzo e all'Accessibilità dei contenuti, al fine di cercare di renderli quanto più possibili conformi a quanto richiesto dalle linee guida.
  Una delle soluzione CMS considerate utilizza Drupal aggiornato alla versione 10.0, ed è un Content Management System basato PHP/MySQL e integrato con componenti aggiuntivi, servizi e applicazioni esterne.

R.A.1.2b - Diffusione dei test di usabilità nelle amministrazioni per agevolare il feedback e le valutazioni da parte degli utenti
Il fornitore entrante dovrà occuparsi, prima del rilascio della nuova soluzione, di effettuare nuovi test di usabilità intervistando gli utenti che dovranno utilizzare il Sito Istituzionale ed Intranet.
Verranno effettuate analisi preventive, insieme agli utenti, atte a condividere ed ipotizzare nuove eventuali modifiche. I risultati saranno condivisi mediante canali interni di sondaggio (google forms, google Surveys).

R.A.1.2c - Incremento dell'accessibilità dei servizi digitali della PA, secondo quanto indicato dalle Linee guida sull'accessibilità degli strumenti informatici
La vecchia soluzione ha uno Stato di Conformità parziale, a causa di contenuti (pagine html, pdf, doc, docx, …) non pienamente accessibili per un utilizzo eccessivo di scansioni o di poco rispetto per linee guida di accessibilità. Con la nuova soluzione si mira ad un pieno raggiungimento dei livelli di accessibilità sulle pagine html (poiché prodotte in maniera formale dal CMS) ed un maggior controllo sui file caricati.

R.A.1.2d - Pubblicazione delle statistiche di utilizzo del proprio sito web, aderendo a Web Analytics Italia per migliorare il processo evolutivo dei propri servizi online
L'azienda utilizza il sistema Web Analytics Italia come indicato da AgID. E' prevista l'implementazione di un'integrazione che, attraverso API, permetta la pubblicazione delle statistiche sul sito istituzionale in modo automatico.

R.A.1.2e - Pubblicare gli obiettivi di accessibilità sul proprio sito
Come da comunicato AGID, sono pubblicati, entro il 31 marzo di ogni anno gli obbiettivi di accessibilità del Sito. Vengono riportati alla pagina https://www.mauriziano.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/964
quelli dell'anno in corso e quelli degli anni passati.

Contesto normativo e strategico

Riferimenti normativi italiani:

- Legge 9 gennaio 2004, n. 4 - Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici
- Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD), art. 7, 17, 23, 53, 54, 68, 69 e 71
- Decreto Legge 18 ottobre 2012, n. 179 - Ulteriori misure urgenti per la crescita del Paese, art. 9, comma 7
- Linee Guida AGID per il design dei servizi digitali della Pubblica Amministrazione
- Linee Guida AGID sull'accessibilità degli strumenti informatici
- Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione

Riferimenti normativi europei:

- Regolamento (UE) 2018/1724 del Parlamento Europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) – Single Digital Gateway.
- Direttiva UE 2016/2102 del Parlamento Europeo e del Consiglio del 26 ottobre 2016 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici.
- Circolare AGID n.2/2018, Criteri per la qualificazione dei Cloud Service Provider per la PA
- Circolare AGID n.3/2018, Criteri per la qualificazione di servizi SaaS per il Cloud della PA
- Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici
- Piano Nazionale di Ripresa e Resilienza

Responsabile dell'attuazione della linea d'azione: dr. Sergio Risso – dr. Francesco Petruzza

Fonti di finanziamento: Spesa corrente e finanziamento P.N.R.R.

CAPITOLO 2. Componente tecnologica 2 - PIATTAFORME

Le piattaforme della Pubblica Amministrazione sono piattaforme tecnologiche che offrono funzionalità fondamentali, trasversali, abilitanti e riusabili nella digitalizzazione dei processi e dei servizi della PA. Esse favoriscono la realizzazione di processi distribuiti e la standardizzazione dei flussi di dati tra amministrazioni, nonché la creazione e la fruizione di servizi digitali più semplici e omogenei.
Le principali piattaforme già attive in ambito sanitario sono SPID, pagoPA, AppIO, FSE, ecc,

Negli ultimi anni le iniziative intraprese dai vari attori coinvolti nell'ambito del Piano, hanno favorito una importante accelerazione nella diffusione di alcune delle principali piattaforme abilitanti, in termini di adozione da parte delle PA e di fruizione da parte degli utenti. Tra queste la piattaforma dei pagamenti elettronici pagoPA, le piattaforme di identità digitale

SPID e CIE, nonché la Piattaforma IO che offre un unico punto d'accesso, tramite un'applicazione mobile, ai servizi pubblici locali e nazionali.

Obiettivi e risultati attesi

OB.2.1 - Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa

R.A.2.1a - Incremento del livello di alimentazione e digitalizzazione del Fascicolo Sanitario Elettronico con tutti i documenti sanitari

Dall'anno 2019, l'Azienda sta inviando al FSE tutti i referti di Laboratorio Analisi (LIS), le lettere di dimissione (LDO), i verbali di Pronto Soccorso (VPS), i referti di Anatomia Patologica (AP), i referti di Radiologia (RIS) e relative immagini, i referti ambulatoriali di tutte le altre specialità, i Verbali operatori. E' stata realizzata l'adesione alla piattaforma ROL e l'integrazione dei sistemi PACS. Tutti i referti/lettere di dimissione/verbali sono firmati digitalmente con firma PADES, inviati al Repository e quindi al FSE.

Dal 2023 l'alimentazione del FSE è monitorata mensilmente e confrontata con i dati della piattaforma regionale PADDI: alla data del 31.5.2023 si supera il 95% per i verbali di PS, le lettere di Dimissione, i referti di Radiologia e Anatomia. I referti di specialistica ambulatoriale e di Laboratorio Analisi superano l'80%.

R.A.2.1b - Adeguamento degli Applicativi a FSE 2.0, al fine di indirizzare gli interventi di integrazione degli applicativi con la nuova infrastruttura FSE 2.0.

Il Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 6 Componente 2, promuove il potenziamento del Fascicolo Sanitario Elettronico (FSE) nella sua versione 2.0 al fine di garantirne la diffusione, l'omogeneità e l'accessibilità su tutto il territorio nazionale da parte degli assistiti e operatori sanitari.

Affinché ciò avvenga è necessario che l'infrastruttura tecnologica evolva per:

- rendere FSE omogeneo sul territorio nazionale per dati contenuti, servizi offerti, semplicità di utilizzo/interfaccia e portabilità;
- assicurare che i documenti che alimentano il FSE siano effettivamente prodotti secondo gli standard nazionali;
- rendere più efficace l'interoperabilità tra fascicoli regionali;
- realizzare una effettiva gestione del dato da affiancare a quella del documento;
- garantire che i dati del FSE possano valere anche ai fini secondari (ricerca e governo).

Il FSE 2.0 è una infrastruttura distribuita che comprende elementi regionali e centrali che interoperano tra loro e con altri sistemi secondo modelli di interoperabilità standard. Per consentire una gestione più efficace del dato vengono introdotti due nuovi elementi infrastrutturali: **il Gateway**, che ha il compito di verificare la coerenza nell'applicazione degli standard, sia per dati che per documenti, **l'Ecosistema Dati Sanitari (EDS)** che raccoglie, gestisce e rende fruibile il dato mediante servizi REST. L'EDS, mediante servizi di sottoscrizione e sincronizzazione può alimentare repository regionali con i dati di pertinenza delle regioni nelle modalità indicate dalla norma. L'EDS infine realizza le funzionalità di monitoraggio di alimentazione e di utilizzo del sistema FSE da parte del cittadino e degli operatori sanitari.

Le Linee guida di attuazione del Fascicolo Sanitario elettronico prevedono che nel FSE 2.0 confluiscano: dati in formato HL7 FHIR, direttamente acquisiti dai sistemi produttori delle strutture e archiviati nel Data Repository Centrale (e opzionalmente presso data repository locali) documenti, in formato HL7 CDA2 iniettati in PDF firmati, prodotti a valle della validazione dai sistemi produttori e archiviati nei repository documentali delle strutture

sanitarie stesse (dislocati a livello regionale o aziendale). Stabiliscono inoltre l'elenco dei documenti dei primi 12 mesi, per i quali sono state aggiornate le guide implementative CDA2 e reperibili presso il sito ufficiale di HL7 Italia.
Sono state pubblicate le nuove specifiche tecniche per per l'interoperabilità tra i sistemi regionali di FSE nella versione 2.4. a cui i sistemi FSE regionali e locali dovranno adeguarsi.

OB.2.2 - Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti
R.A.2.2a - Incremento dell'adozione e dell'utilizzo dell'identità digitale (SPID e CIE)
In data 14.6.2022 è stata presentata Domanda di partecipazione all'Avviso Pubblico "Misura 1.4.4 - Estensione dell'Utilizzo delle piattaforme d'Identità Digitali - SPID e CIE - Amministrazioni Pubbliche diverse da Comuni e Istituzioni Scolastiche - maggio 2022" PNRR M1C1 Investimento 1.4 "Servizi e cittadinanza digitale" finanziato dall'Unione Europea – NextGenerationEU

Con Decreto n. 49 - 1 / 2022 - PNRR della *Presidenza del Consiglio dei Ministri Dipartimento per la trasformazione digitale Il Capo Dipartimento,* di approvazione dell'elenco istanze ammesse a valere sull'avviso pubblico "Avviso Misura 1.4.4 "Estensione dell'utilizzo delle piattaforme nazionali di identità digitale - SPID CIE" Amministrazioni Pubbliche diverse da Comuni e Istituzioni Scolastiche Maggio 2022", è stato approvato il finanziamento per l'utilizzo di SPID, con attività da terminare entro il 31.12.2023.

R.A.2.2b - Incremento dei servizi sulla piattaforma PagoPA
A partire dal mese di novembre 2020 l'Azienda si è connessa al polo nazionale e regionale, recuperano e stampano lo IUV sulla cedola di pagamento e trasmettono i dati dei pagamenti al nodo centrale di PagoPA per tutti gli applicativi utilizzati all'interno dell'Ospedale. Dal mese di settembre 2021 è stato avviato l'aggiornamento del software ALPI per la gestione della Libera Professione intramoenia allargata, prevedendo il pagamento PagoPa per tutte le prestazioni effettuati dai medici nelle strutture Convenzionate e l'invio della fattura elettronica al paziente via email.
In data 10.11.2022 è stata presentata Domanda di partecipazione all'Avviso Pubblico "Misura 1.4.3 Adozione Pagopa – Altri Enti (Regioni/Province autonome, Aziende sanitarie locali e ospedaliere, Università, Enti di ricerca e AFAM) - settembre 2022" - PNRR M1C1 Investimento 1.4 "Servizi e cittadinanza digitale" finanziato dall'Unione Europea – NextGenerationEU.
Il Decreto n. 128 - 1 / 2022 - PNRR - 2023 della Presidenza del Consiglio dei Ministri, Dipartimento per la trasformazione digitale *"ELENCO ISTANZE AMMESSE A VALERE SULL'AVVISO PUBBLICO "*Avviso Misura 1.4.3 "Adozione piattaforma pagoPA" - Altri Enti (settembre 2022)", pervenuto il 13.4.2023, contiene la lista delle proposte di finanziamento che hanno superato i controlli di ricevibilità e ammissibilità e per le quali gli enti hanno provveduto alla comunicazione del codice CUP come previsto dall'art. 10 dell'Avviso, e assegna all'amministrazione Azienda Ospedaliera Ordine Mauriziano di Torino un finanziamento di € 73.805,00.

OB.2.3 - Incrementare e razionalizzare il numero di piattaforme al fine di semplificare i servizi ai cittadini
R.A.2.3 - Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)
In data 10.3.2023 è stata presentata Domanda di partecipazione all'Avviso Pubblico "Misura 1.4.3 APP IO - ALTRI ENTI (Regioni /Province autonome, Aziende sanitarie locali e ospedaliere, Università, Enti di ricerca e AFAM) SETTEMBRE 2022" - PNRR M1C1 Investimento 1.4 "SERVIZI E CITTADINANZA DIGITALE" FINANZIATO

DALL'UNIONE EUROPEA – NextGenerationEU *R.A.2.3b – Attivare nuove piattaforme Telemedicina.*
Il Decreto n. 130 - 2 / 2022 - PNRR - 2023 della Presidenza del Consiglio dei Ministri, Dipartimento per la trasformazione digitale "ELENCO ISTANZE AMMESSE A VALERE SULL' AVVISO PUBBLICO MISURA 1.4.3 "ADOZIONE APP IO" ALTRI ENTI (REGIONI/PROVINCE AUTONOME, AZIENDE SANITARIE LOCALI E OSPEDALIERE, UNIVERSITÀ, ENTI DI RICERCA E AFAM) (SETTEMBRE 2022)", pervenuto il 11.5.2023, assegna all'amministrazione Azienda Ospedaliera Ordine Mauriziano di Torino un finanziamento di € 29.520,00.

Contesto normativo e strategico
Generali:

- Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (CAD), artt.5, 6- quater, 50-ter, 62, 62-ter, 64, 64bis, 66
- Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
- Regolamento europeo in materia di protezione dei dati personali n. 679/2016 General Data Protection Regulation (GDPR)
- Piano Nazionale di Ripresa e Resilienza (Sub-Investimento 1.3.1: "Piattaforma nazionale digitale dei dati" - Sub-Investimento 1.4.3: "Servizi digitali e cittadinanza digitale, piattaforme e applicativi" - Sub-Investimento 1.4.4: "Estensione dell'utilizzo delle piattaforme nazionali di Identità Digitale (SPID, CIE) e dell'anagrafe nazionale digitale (ANPR)" - Sub-Investimento 1.4.5: "Piattaforma Notifiche Digitali")

Fascicolo Sanitario Elettronico:

- Legge 11 dicembre 2016, n. 232 - Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019
- Decreto-legge 18 ottobre 2012, n. 179 - Ulteriori misure urgenti per la crescita del Paese
- Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015, n. 178 - Regolamento in materia di fascicolo sanitario elettronico
- Decreto 23 dicembre 2019 "Utilizzo del Fondo per il finanziamento degli investimenti e lo sviluppo infrastrutturale - Fascicolo sanitario elettronico" (GU n.13 del 17-1-2020) (Piano di digitalizzazione dei dati e documenti sanitari)
- Decreto-legge n. 34/2020 - Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché' di politiche sociali connesse all'emergenza epidemiologica da COVID-19
- Decreto-legge n. 137/2020 - Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da Covid-19
- Linee Guida per l'Attuazione del fascicolo Sanitario Elettronico, pubblicate sulla Gazzetta Ufficiale n. 160 del 11.7.2022

SPID

- Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 in materia recante la Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché' dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.

- Regolamento AGID recante le regole tecniche dello SPID
- Regolamento AGID recante le modalità attuative dello SPID
- Schema di convenzione per l'ingresso delle PA nello SPID

PagoPA

- Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (CAD)
- Decreto Legislativo 14 dicembre 2018, n. 135 Art. 8, comma 2 e 3, Piattaforme Digitali -
- Linee Guida per l'Effettuazione dei Pagamenti Elettronici a favore delle Pubbliche Amministrazioni e dei Gestori di Pubblici Servizi (G.U. n. 153 del 03/07/2018)

Responsabile dell'attuazione della linea d'azione: dr. Francesco Petruzza

Fonti di finanziamento: Spesa corrente e Finanziamento P.N.R.R. per l'evoluzione di SPID, Pagopa e nuova piattaforma di Telemedicina

CAPITOLO 3. Componente Tecnologica 3 INFRASTRUTTURE

Lo sviluppo delle infrastrutture digitali è fattore abilitante per l'erogazione di servizi pubblici a cittadini e imprese e di servizi essenziali per il Paese. Tali infrastrutture devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili. L'obiettivo di garantire una maggiore efficienza dei sistemi non può essere disgiunto dall'obiettivo di garantire contestualmente un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati.
A seguito del censimento del Patrimonio ICT della PA, effettuato da Agid, molte infrastrutture della PA risultano prive dei requisiti di sicurezza e di affidabilità necessari e, inoltre, sono carenti sotto il profilo strutturale e organizzativo.
Il nostro data center è stato classificato di gruppo B con l'esigenza di attuare un percorso di razionalizzazione delle infrastrutture per garantire la sicurezza dei servizi oggi erogati , mediante la migrazione degli stessi versi *data center* più sicuri e verso infrastrutture e servizi *cloud* qualificati, ovvero conformi a standard di qualità, sicurezza, performance e scalabilità, portabilità e interoperabilità.
Nel delineare il processo di razionalizzazione delle infrastrutture è necessario considerare che, nel settembre 2021, il Dipartimento per la Trasformazione Digitale e l'Agenzia per la Cybersicurezza Nazionale (ACN) hanno pubblicato il documento di indirizzo strategico sul *cloud* intitolato "Strategia Cloud Italia". Tale documento si sviluppa lungo tre direttrici fondamentali:
i) la creazione del PSN, la cui gestione e controllo di indirizzo siano autonomi da fornitori extra UE, destinato ad ospitare sul territorio nazionale principalmente dati e servizi strategici la cui compromissione può avere un impatto sulla sicurezza nazionale, in linea con quanto previsto in materia di perimetro di sicurezza nazionale cibernetica dal Decreto Legge 21 settembre 2019, n. 105 e dal DPCM 81/2021;
ii) un percorso di qualificazione dei fornitori di cloud pubblico e dei loro servizi per garantire che le caratteristiche e i livelli di servizio dichiarati siano in linea con i requisiti necessari di sicurezza, affidabilità e rispetto delle normative rilevanti

iii) lo sviluppo di una metodologia di classificazione dei dati e dei servizi gestiti dalle Pubbliche Amministrazioni, per permettere una migrazione di questi verso la soluzione cloud più opportuna (PSN o adeguata tipologia di *cloud* qualificato).

Obiettivi e risultati attesi

OB.3.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati migrando gli applicativi *on-premise* (*data center* Gruppo B) verso infrastrutture e servizi *cloud* qualificati

RA.3.1a - Predisposto piano di migrazione dei servizi digitali verso strutture cloud qualificate

Ai sensi della D.G.R. 5-1639 del 9/7/2020 *"Attuazione del Piano Triennale Nazionale per l'informatica nella P.A. 2019-2021. Indirizzi alle aziende sanitarie pubbliche del SSR per l'adozione della Piattaforma di Community Cloud regionale di CSI Piemonte, e interventi per l'evoluzione dell'infrastruttura Regionale Backbone Wi-Pie*", l'Azienda ha predisposto un progetto Progetto di migrazione in Cloud A.O. Mauriziano", trasmesso in Regione Piemonte con nota Prot. 5829 del 13.5.2021, che è in fase di aggiornamento in base alle nuove esigenze ed indicazioni emerse.

Con D.G.R. 15-6172 del 6.12.2022 *"Revoca parziale della D.G.R. n. 5-1639 del 9.7.2020. Indirizzi ad Azienda Zero per il ruolo di coordinamento ai fini dell'aggiornamento e attuazione del Piano Triennale per l'Informatica nelle Aziende Sanitarie Regionali 2021-2023 e s.m.i. e per gli interventi di abilitazione e facilitazione migrazione al cloud per le PA locali",* ha assegnato all'Azienda Sanitaria Zero, nel rispetto degli atti di programmazione e indirizzi regionali, il ruolo di coordinamento ai fini dell'aggiornamento e dell'attuazione del Piano Triennale per l'Informatica nelle ASR 2021-2023 e s.m.i. con particolare riferimento al coordinamento delle azioni aziendali interessate agli interventi di "Abilitazione e facilitazione migrazione al cloud" prevista dal PNRR. Sono in corso valutazioni tecniche ed economiche con l'Azienda Zero

RA.3.1b - Avviata migrazione dei servizi digitali verso struttute cloud qualificate

L'Azienda Ospedaliera Ordine Mauriziano di Torino, in linea con le indicazioni dell'Agenzia per l'Italia Digitale, ed in particolare con quelle del Piano Triennale per l'Informatica nella Pubblica Amministrazione, ha intrapreso da alcuni anni un percorso di migrazione dei servizi applicativi dalla propria infrastruttura verso ambienti cloud che presentano adeguate caratteristiche di sicurezza e affidabilità.

In particolare in fase di acquisizione di nuovi software, o di aggiornamento di quelli esistenti è stato applicato il principio "Cloud First" compatibilmente con le esigenze prestazionali e i limiti di continuità.

Inoltre da alcuni anni l'Azienda A.O. Mauriziano ha intrapreso il processo di esternalizzazione dei software utilizzati presso Data Center di fornitori esterni, conscia che il proprio data Center non fosse così' "adeguato" e che talvolta i costi di nuovi investimenti fossero superiori all'utilizzo di risorse esterne. Spesso la scelta del Data Center è stata strettamente collegata al Fornitore del software che si è assunto anche la gestione dell'infrastruttura esterna. L'Azienda ha in questo caso provveduto a verificare le misure di sicurezza messe in atto dai fornitori sui Data Center ospitanti e a firmare un Accordo di trattamento dei dati con il responsabile ai sensi dell'art. 28 del regolamento UE 2016/679 ("RGPD" o "GDPR") .

Nel 2018, in considerazione che era necessario sostituire l'infrastruttura hardware per la Gestione del Laboratorio Analisi e introdurre il Repository Aziendale, per ottemperare alle

linee guida espresse nel Piano Triennale per l'Informatica nella Pubblica amministrazione 2017–2019, con Deliberazione n. 617 del 27.9.2018, si è aderito alla Convenzione CONSIP lotto 1 " Servizi di cloud computing".
Ad oggi sono ospitate sul cloud Nivola del CSI Piemonte 12 Virtual Machine e ospitate su Cloud/datacenter di fornitori 11 servizi/applicazioni (alcuni offerti in modalità SAAS).
E' attualmente in corso e sarà completato nell'anno il completamento della migrazione di ulteriori 3 VM su Nivola.
Sono inoltre in fase di analisi i progetti di migrazione dei servizi Digital Patology, LIS del Laboratorio Analisi e dell'Anatomia Patologica. L'analisi ha l'obiettivo di stabilire, previo confronto delle condizioni economiche e delle caratteristiche offerte, la migrazione delle suddette soluzioni sul Polo Strategico Nazionale, rispetto alle altre soluzioni di Cloud Qualificato.
L'obbligo per la PA di migrare i propri CED verso ambienti cloud, introdotto dall'ex art. 35 del D.L. 76/2020 di modifica dell'articolo 33-septies (Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese) del DL 179/2012, convertito con modificazioni dalla L. 17 dicembre 2012, n. 221, ha imposto la predisposizione di un "Piano di Migrazione al Cloud", attualmente in fase di ultimazione.

RA.3.1c - Realizzazione di un'istanza di Disaster Recovery ospitata presso il Cloud
E' i fase di analisi la realizzazione di un'istanza di Disaster Recovery ospitata presso un Cloud qualificato per la messa in sicurezza della soluzione applicativa Babele in esercizio presso l'Ospedale, i dettagli sono contenuti nel **Piano di Continuità Operativa**, allegato al presente documento come parte integrale e sostanziale.

OB.3.2 - Migliorare l'offerta di servizi di connettività per le PA
RA.3.2 – Ottimizzare la connettività
Nel 2020 è stata attivata una coppia di fibre spente dalla sede dell'Azienda Ospedaliera al nodo di backbone Wi-Pie di Torino, Corso Unione Sovietica 216, presso il quale viene raccolto ed instradato il traffico generato dal Mauriziano, quale nuovo collegamento principale. Il collegamento layer 3 ad 1 Gbps – ad instradamento differente dal collegamento in fibra spenta – è stato configurato come secondario e in Alta Affidabilità .
La banda end-to-end del collegamento principale è pari a 10 Gbps simmetrici dalla sede dell'Azienda Ospedaliera al nodo del Backbone Wi-Pie di Torino, Corso Unione Sovietica 216.
I due router, principale a 10 Gbps e secondario ad 1 Gbps, sono configurati in HA (High Availability) in maniera da garantire la ridondanza e la continuità del servizio in caso di fault di uno dei collegamenti.
Occorre considerare che le due linee non sono completamente indipendenti condividendo un piccolo tratto di connessione.
Il servizio di manutenzione e di assistenza è erogato dal CSI Piemonte attraverso interventi, atti a garantire il corretto funzionamento delle tratte utilizzate e copre le tratte in fibra ottica da entrambe le terminazioni di attestazione del cavo.

Contesto normativo e strategico

In materia di *data center*, *cloud* e rete esistono una serie di riferimenti sia normativi che strategici a cui le amministrazioni devono attenersi. Di seguito un elenco delle principali fonti.

Riferimenti normativi nazionali:

- Decreto-legge 16 luglio 2020, n. 76, convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120, recante "Misure urgenti per la semplificazione e l'innovazione digitale", articolo 35;
- Decreto legislativo 7 marzo 2005, n.82, recante "Codice dell'amministrazione digitale",articoli. 8-bis e 73;
- Decreto legislativo 18 maggio 2018, n. 65, recante "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione";
- Decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, recante "Ulteriori misure urgenti per la crescita del Paese", articolo 33-septies;
- Decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica".
- Decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile2020, n. 27, recante "Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19", articolo 75;
- Decreto-Legge 31 maggio 2021, n. 77, convertito, con modificazioni dalla legge 29 luglio 2021, n. 108, recante "Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure.";
- Decreto-Legge 31 maggio 2021, n. 82, convertito con modificazioni dalla legge 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza";
- Circolare AGID n. 1/2019, del 14 giugno 2019 - Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali;
- Strategia italiana per la banda ultra-larga;
- Strategia cloud Italia;
- Piano Nazionale di Ripresa e Resilienza (Investimento 1.1: "Infrastrutture digitali" - Investimento 1.2: "Abilitazione e facilitazione migrazione al cloud")

Riferimenti europei:

- Programma europeo CEF Telecom;
- Strategia europea sui dati, Commissione Europea 19.2.2020 COM (2020) 66 final;
- European Commission Cloud Strategy, Cloud as an enabler for the European Commission Digital Strategy, 16 May 2019;
- Data Governance and data policy at the European Commission, July 2020;
- Regulation of the European Parliament and of the Council on European data governance (Data Governance Act).

Responsabile dell'attuazione della linea d'azione: dr. Stefano Geninatti Togli

Fonti di finanziamento: Spesa corrente e Finanziamento P.N.R.R. per i nuovi progetti Cloud

CAPITOLO 4. Componente Tecnologica 4 Interoperabilità

L'interoperabilità permette la collaborazione e l'interazione telematica tra pubbliche amministrazioni, cittadini e imprese, favorendo l'attuazione del principio once only e recependo le indicazioni dell'European Interoperability Framework

Modello di interoperabilità di Regione Piemonte
Le modalità di interazione previste dal modello di interoperabilità di sanità elettronica della Regione Piemonte fra il sistema informativo dell'Azienda Sanitaria e la componente locale, dedicata all'azienda stessa al fine dell'erogazione dei servizi verso il cittadino (Fse e pagamento on line) prevedono un modello con:

- Un nodo centrale comprensivo di un Indice Regionale degli Eventi Clinici (IREC), privo di dati sensibili, nel quale sono mantenute le informazioni dei pazienti che hanno creato il proprio FSE (e relativo consenso alla alimentazione, consultazione e recupero del pregresso) ed i riferimenti alle ASR che possiedono i loro dati/documenti clinici.
- Un nodo locale per ogni ASR, costituito da:
  - Un Indice locale degli Eventi Clinici (ILEC), che in fase transitoria nell'attesa della disponibilità di un RCD aziendale, e limitatamente al LIS, può contenere dati/documenti clinici;
  - I servizi di interoperabilità verso l'IREC;
  - I servizi di integrazione (HL7 o XML) con i sistemi dell'area clinica delle ASR.

L'A.O. Mauriziano, per rendere disponibili dati e documenti al Fascicolo Sanitario Elettronico e al servizio di Ritiro Referti online, dispone di un proprio Repository documentale, comunicante direttamente con la componente locale e con cui mette a disposizione solo i dati strutturati che descrivono e identificano l'evento e il documento .
L'interfacciamento fra sistema informativo dell'Azienda e ILEC può avviene attraverso il protocollo di comunicazione definito dall'IHE.
Le specifiche di implementazione delle transazioni sono descritte nei documenti del Technical
Framework "[1] IHE - IT Infrastructure Technical Framework - Cross-Enterprise Document Sharing (XDS)" mentre, per la valorizzazione dei metadati, il riferimento è il documento "[2] Specifiche tecniche per l'interoperabilità tra i sistemi regionali di FSE (Affinity Domain Italia)".

Inoltre, nell'ambito del nodo locale dedicato per la gestione delle bioimmagini prodotte dai sistemi di diagnostica per immagini, è stato realizzato un connettore basato su protocollo DICOM che consente l'integrazione con il PACS aziendale

Obiettivi e risultati attesi

OB.4.1 - Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
RA.4.1a – Interoperabilità Repository
Il Repository aziendale, è il Sistema che si fa carico della centralizzazione, della raccolta e della consultazione di tutti i principali documenti clinici prodotti all'interno dell'Azienda: referti specialistici, lettera di dimissione, verbali operatori, verbali di pronto soccorso, etc. In questo scenario il Repository Clinico Documentale (RCD) è deputato all'invio in conservazione Sostitutiva e al FSE di tutti i dati e documenti ricevuti.

La soluzione scelta con DG 617/2018 fu di attivare il Repositoty XVALUE in Cloud aderendo alla Convenzione Consip **"** *Servizi di cloud computing" – Lotto 1*
La soluzione applicativa di RCD individuata soddisfa i seguenti requisiti di integrabilità e di interoperabilità e cooperazione applicativa:

- è progetta ed implementa coerentemente con gli standard dell'architettura orientata ai servizi (SOA) per facilitare l'integrazione verso sistemi esterni
- é implementate su architetture software di fascia enterprise
- è indipendente dagli strati di software di base (sistemi operativi, middleware, data base), consentendo l'aggiornamento di questi ultimi (anche per ragioni di sicurezza) in maniera trasparente senza pregiudicarne le funzionalità;
- *utilizza, al fine di perseguire la cooperazione applicativa tra i sistemi informatici, standard in ambito sanitario, quali HL7 e applica i profili previsti dal framework IHE.*

RA.4.1b – Interoperabilità FSE.
Sono state pubblicate le nuove specifiche per l'interoperabilità tra i sistemi regionali di FSE nella versione 2.4, frutto del lavoro congiunto dell'Agenzia per l'Italia Digitale (AgID) e del Consiglio Nazionale delle Ricerche (CNR) in accordo con il Dipartimento per la Trasformazione digitale (DTD) e Sogei e sono redatte in coerenza con il Decreto-Legge del 19 maggio 2020, n. 34 e la successiva normativa in merito al Fascicolo Sanitario Elettronico.
Queste si compongono di due documenti distinti "Framework e dataset dei servizi base" e "Affinity Domain Italia". Il primo documento mira a definire i principi, i processi, i servizi e i dataset dell'interoperabilità dei FSE regionali con l'Infrastruttura Nazionale per l'Interoperabilità (INI), mentre il secondo ne definisce l'Affinity Domain di riferimento.
Sulla base di tali specifiche è in corso l'implementazione della nuova versione del FSE.2.0

RA.4.1c – Immagini
Lo standard DICOM facilita l'interoperabilità delle apparecchiature di *imaging* medico specificando:

- per le comunicazioni di rete, un insieme di protocolli da seguire.
- Sintassi e semantica dei comandi e delle informazioni associate che possono essere scambiate utilizzando questi protocolli;
- per la comunicazione mediatica, un insieme di servizi di archiviazione multimediale che i dispositivi rivendicanti la conformità allo standard devono seguire, così come un formato di file e una struttura di *directory* medica per facilitare l'accesso alle immagini e le relative informazioni memorizzate su media interscambio;
- integra dispositivi di acquisizione immagini, PACS, *workstation*, VNAs e stampanti di diversi produttori.

La gestione in rete delle immagini e dei referti radiologici prodotti rispettivamente dai sistemi software PACS (Picture archiving and communication system) e RIS (Radiology Information System) dell'Azienda è possibile attraverso l'integrazione del PACS:

- con TEMPORE – (TEleconsulto Medico Piemonte Ospedali in REte) per effettuare teleconsulti in regime di emergenza-urgenza
- con Immagini in Rete per condividere immagini DICOM provenienti dai PACS utilizzati dalle radiologie delle strutture sanitarie connesse al sistema e consultare on-line il fascicolo radiologico dei pazienti nel rispetto delle linee guida rilasciate in tema di FSE dal Garante alla Privacy (G.U. n. 178 del 3 agosto 2009) e delle linee guida nazionali emesse dal Ministero della Salute l'11 novembre 2010

RA.4.1d – Digital Pathology

Con Deliberazione n. 355 del 19.4.2023, a seguito di Appalto Specifico, in adesione all'A.Q. Id 2202 "Servizi applicativi sanità digitale – sistemi informativi clinico assistenziali - Lotto 1 "Cartella clinica elettronica ed enterprise imaging - NORD ". CIG: 8765571A03 – mediante Finanziamento del P.N.R.R. da parte dell'Unione europea e all'iniziativa Next Generation EU- (RDO n° 3303489 del 24.11.2022), è stato aggiudicata la fornitura di un sistema di Digital Pathology.
Il modulo di Digital Pathology supporta il servizio di AnatomiaPatologica nell'implementazione di un workflow completamente digitale, ottimizzando le attività di refertazione e diagnosi. Esso consente l'acquisizione, archiviazione, elaborazione e gestione delle immagini generate nel Servizio di Anatomia Patologica da varie tipologie di sorgenti (scanner di vetrini, telecamere montate sui microscopi, sistemi di ripresa delle immagini macroscopiche, sistemi di elaborazione e analisi d'immagine, ecc.) ed è in grado di acquisire e gestire le immagini provenienti dai reparti clinici e diagnostici (immagini laparoscopiche dei siti di prelievo, immagini radiologiche, ecc.).
Il modulo permette la sostituzione della tradizionale osservazione al microscopio del vetrino con l'analisi di un'immagine digitalizzata, immagine che può essere ingrandita e navigata spazialmente dal patologo allo stesso modo della microscopia standard.
Il Sistema dispone di un middleware di integrazione che consente di realizzare facilmente l'interoperabilità con altre applicazioni, sulla base delle linee guida dettate dai profili standard di integrazione IHE Laboratory Technical Framework, "Laboratory Scheduled Workflow" utilizzando messaggi HL7 nelle versioni 2.x e 3.x.
Il Sistema è in grado di predisporre documenti conformi alle specifiche XML 1.0 e successive e secondo lo standard HL7-CDA 2.0
Il middleware di integrazione è caratterizzato da un'elevata flessibilità e configurabilità, tali daconsentire la realizzazione di interfacce di integrazione altamente customizzate e basate su un'ampia varietà di tecnologie per lo scambio dati. In fase di realizzazione del progetto PathoXweb sarà integrato con il sistema gestionale WINSAP3.0, con SPID e con Active Directory o sistema SMAL2.

Contesto normativo e strategico

In materia di interoperabilità esistono una serie di riferimenti sia normativi che strategici a cui le amministrazioni devono attenersi. Di seguito un elenco delle principali fonti.

Riferimenti normativi piemontesi:

- Linee guida per la gestione di un Documento Clinico Elettronico finalizzata alla pubblicazione sui servizi della Piattaforma FSE
- Deliberazione della Giunta Regionale 12 aprile 2019, n. 31-8756 - POR FESR 14-20 Asse II - Ob. specifico II.2c.2 "Digitalizzazione processi amministrativi, diffusione servizi digitali pienamente interoperabili". Azione II.2c.2.2 "Interventi per assicurare l'interoperabilita' delle banche dati pubbliche"
- Deliberazione della Giunta Regionale 29 dicembre 2020, n. 56-2734 - POR FESR 2014-2020 - Asse II "Agenda Digitale" - Ob. specifico II.2c.2 "Digitalizzazione processi amministrativi, diffusione servizi digitali pienamente interoperabili" – Azione II.2c.2.2 "Cloud computing e pubblica amministrazione piemontese", D.G.R. n. 31-8756 del 12/04/2019.
- D.D. 7 gennaio 2021, n. 1 - POR FESR 2014-2020 - Asse II "Agenda Digitale" - Ob. specifico II.2c.2 "Digitalizzazione processi amministrativi, diffusione servizi digitali pienamente interoperabili" – Azione II.2c.2.2 "Cloud computing e pubblica amministrazione piemontese"

Riferimenti normativi italiani:

- Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD), artt. 12, 15, 50, 50-ter, 73, 75
- Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
- Determina AGID 219/2017 - Approvazione e pubblicazione delle "Linee guida per transitare al nuovo modello di interoperabilità"
- Determina AGID 406/2020 - Adozione della Circolare recante le linea di indirizzo sulla interoperabilità tecnica
- Piano Nazionale di Ripresa e Resilienza – Investimento 1.3: "Dati e interoperabilità" Riferimenti normativi europei:
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in breve GDPR)
- Regolamento (UE) 2014/910 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (in breve eIDAS)
- European Interoperability Framework – Implementation Strategy
- Interoperability solutions for public administrations, businesses and citizens

Responsabile dell'attuazione della linea d'azione: dr. Francesco Petruzza e Dr. Sergio Risso

Fonti di finanziamento: spesa corrente e Finanziamento PNRR per il software di Digital Pathology

CAPITOLO 5. Componente Tecnologica 5 Sicurezza informatica

La sicurezza informatica rappresenta un elemento trasversale a tutto il Piano Triennale. Il PNRR ed il decreto attuativo del perimetro di sicurezza nazionale cibernetica pongono la *cybersecurity* a fondamento della digitalizzazione della Pubblica Amministrazione e del Sistema Italia. La nuova Agenzia per la Cybersicurezza nazionale è il soggetto nazionale di riferimento.

Risulta infatti essenziale garantire servizi digitali non solo efficienti e facilmente accessibili, ma anche sicuri e resilienti sotto il profilo informatico, così da accrescerne l'affidabilità e l'utilizzo anche da parte di utenti meno avvezzi all'impiego di tecnologie digitali. La crescente risonanza e copertura mediatica data ad incidenti e ad attacchi cyber, soprattutto in ambiente sanitario, se da un lato contribuisce ad accrescere il livello di consapevolezza sui rischi dello spazio cibernetico, dall'altro può ingenerare un senso di insicurezza nell'impiego dello strumento digitale.

Obiettivi e risultati attesi

OB.5.1 - Aumentare la consapevolezza del rischio cyber (*Cyber Security Awareness*) nell'Azienda

R.A.5.1 - Incremento del livello di Cyber Security Awareness misurato tramite questionari di self-assessment ai dipendenti dell'Azienda

E' prevista:

- la definizione, all'interno dei piani di formazione del personale, di un corso FAD sulle tematiche di Cyber Security (anche valutando l'uso della piattaforma Syllabus).
- incontri periodici con il personale illustranti i rischi e le misure da adottare.
- invio di informative periodiche sul tema.

OB.5.2 - Aumentare il livello di sicurezza informatica

R.A.5.2 - Incremento delle misure di sicurezza

La posta elettronica rimane, comunque uno dei principali vettori, per i malware e per questo motivo l'azienda nel 2022 ha aderito all'accordo quadro "Cybersecurity - prodotti e servizi connessi" e attraverso l' RDO n. 3259089 ha avviato la procedura di rilancio competitivo per l'acquisizione di un sistema di Secure Email Gateway (SEG), aggiudicando in data 28/11/2002 il prodotto LIBRAESVA offerto dalla Telecom. L'installazione e configurazione del SEG è stata completata nel mese di gennaio 2023 prevedendo l'installazione di due appliance virtuali a protezione del traffico email. Grazie a questo sistema è possibile proteggersi in maniera più efficace contro Malware, Phishing, Ransomware, URL e allegati dannosi, compromissione delle e-mail aziendali (BEC) e altre tipologia di attacco.
Sono inoltre previste diverse attività di hardering volte a ridurre la superficie di attacco e limitare i privilegi degli utenti amministrativi.

Oltre alle attività di hardering sopra descritta si citano alcuni progetti specifici, quali:

- Analisi Sostituzione/aggiornamento dei firewall: a seguito della scadenza dei servizi della suite Watchguard Total Security è stato previsto che nel corso del anno venturo saranno esaminati eventuali prodotti alternativi che possano presentare adeguati livelli di sicurezza e che superino alcuni dei limiti di usabilità rilevati sugli attuali strumenti.
- Ricerca di un prodotto XDR (extended detection and response). Nel 2022 sono state valutate alcune soluzioni che non erano conformi ai vincoli di budget (es. Darktrace) o che presentavano una complessità di gestione tale da richiedere personale dedicato allo scopo. Nel 2023 sono proseguiti gli approfondimenti individuando nella soluzione di Bitdefender (sistema EDR previsto in convezione CONSIP, con l'aggiunta dei moduli di analisi del traffico di rete attraverso apposite sonde, di protezione delle identità e di patch management) la soluzione appropriata. Il sistema permette di proteggere tutti gli endpoint (client e server) attraverso luzioni antimalware basati su firma e su euristica, oltre a rilevare le anomalie comportamentali attraverso la correlazioni dei log raccolti sia dagli stessi endpoint che dalle due sonde (rete e di protezione delle identità). Il modulo di patch management inoltre permette di individuare le vulnerabilità derivanti dalla mancata installazione delle patch di sicurezza e ne permette la distribuzione.
- Ricerca di un prodotto PAM (Privilege Access Management). Sono state valutate due soluzioni Wallix e Delinea. E' corso la valutazione di un possibile acquisto tramite l'accordo quadro "Cybersecurity - prodotti e servizi connessi".
- Test trimestrali di Vulnerability effettuati verso gli IP e i servizi esposti pubblicamente
- Introduzione dell'autenticazione a due Livelli per l'accesso via VPN
- Verifica e aggiornamento delle misure minime di sicurezza ICT

OB.5.3 - Aumentare il livello di sicurezza informatica dei portali istituzionali

R.A.5.3 - Incremento del numero dei portali istituzionali che utilizzano il protocollo HTTPS only, misurato tramite tool di analisi specifico

Mantenere costantemente aggiornati i propri portali istituzionali e applicare le correzioni alle vulnerability rilevate dai test trimestrali.

OB.5.4 - Aumentare il livello di sicurezza informatica nei procedimenti di acquisizione di beni e servizi

R.A.5.4 - Far riferimento alle Linee guida sulla sicurezza nel procurement ICT

L'Azienda svolge ogni anno numerose procedure di appalto. La digitalizzazione completa delle procedure promette una significativa riduzione di costi e tempi, facilita la partecipazione di tutti gli operatori economici, anche delle PMI e delle startup che dispongono di una minore capacità finanziaria.
Nel corso del 2022 AGID ha avviato l'elaborazione delle regole tecniche per la digitalizzazione delle procedure, previste dall'art. 44 del Codice dei contratti pubblici. Queste regole tecniche andranno a completare il quadro di regolamentazione tecnica del sistema di e-procurement.
Il nuovo Codice dei contratti pubblici, ha previsto l'aggiornamento delle regole tecniche delle piattaforme di e-procurement delle singole Amministrazioni.
Tutte le amministrazioni aggiudicatrici sono chiamate a mettere a disposizione degli operatori economici servizi di *e-procurement* e ad ampliare quanto più possibile il campo di digitalizzazione delle procedure relative ai propri acquisti.

Contesto normativo e strategico

Di seguito un elenco delle principali fonti.

Riferimenti normativi italiani:

- Decreto-legge 14 giugno 2021 n. 82 – Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la Cybersicurezza Nazionale
- Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n.105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misura volte a garantire elevati livelli di sicurezza
- Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD), art.51
- Decreto Legislativo 18 maggio 2018, n. 65 - Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
- Decreto-legge 21 settembre 2019, n. 105 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
- Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019 - Disposizioni sull'organizzazione e il funzionamento del computer security incident response team - CSIRT italiano
- Piano Nazionale per la Protezione Cibernetica 2017
- Piano Nazionale di Ripresa e Resilienza - Investimento 1.5: "Cybersecurity"

Riferimenti normativi europei:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 in materia di protezione dei dati personali
- Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio – Regolamento eIDAS
- Nuova strategia Cybersicurezza europea

Responsabile dell'attuazione della linea d'azione: dr. Stefano Geninatti Togli

Fonti di finanziamento: Spesa corrente per i servizi, Finanziamento P.N.R.R. per l'acquisto di licenze software e dispositivi hardware

CAPITOLO 6. Le leve per l'innovazione

Il presente capitolo focalizza le leve strategiche su cui investire per accelerare il processo di trasformazione digitale dell'Azienda sottolineando l'importanza di aumentare le competenze digitali dei dipendenti, dei cittadini/pazienti e delle imprese.
Le competenze digitali esercitano un ruolo fondamentale e rappresentano un fattore abilitante, anche in relazione alla efficacia delle altre leve e strumenti proposti e, qui di seguito approfonditi. Di natura trasversale, lo sviluppo di competenze digitali assunto come *asset* strategico, comprende tutto ciò che può essere identificato in termini di bagaglio culturale e conoscenza diffusa per favorire l'innesto, efficace e duraturo, dei processi di innovazione in atto. In questo quadro gli interventi strategici devo riguardare:

1. il potenziamento e lo sviluppo delle competenze digitali della forza lavoro e di e-leadership all'interno dell'Azienda
2. lo sviluppo di competenze specialistiche ICT per fronteggiare le sfide legate alle tecnologie emergenti e al possesso delle competenze chiave per i lavori del futuro, attraverso l'inserimento di nuove figure nell'ambito della funzione ICT
3. la messa in atto di azioni di sensibilizzazione e di formazione che coinvolgano necessariamente i dipendenti dell'Azienda
4. il potenziamento delle competenze digitali necessarie per esercitare i diritti di cittadinanza (inclusa la piena fruizione dei servizi *online*)

Obiettivi e risultati attesi

OB 6.1 - Rafforzare le leve e le competenze digitali per favorire l'innovazione

RA.6.1a - Avviare la Formazione per lo sviluppo delle competenze digitali e sulla sicurezza
Il Ministro per la pubblica amministrazione ha adottato, in data 23 marzo 2023 (registrata con numero Prot. 24/03/2023.0004344.E), la Direttiva *"Pianificazione della formazione e sviluppo delle competenze funzionali alla transizione digitale, ecologica e amministrativa promosse dal Piano Nazionale di Riprese e Resilienza"*, la quale mira a fornire indicazioni metodologiche e operative alle amministrazioni per la pianificazione, la gestione e la valutazione delle attività formative al fine di promuovere lo sviluppo delle conoscenze e delle competenze del proprio personale.
Attraverso la piattaforma "*Syllabus, Nuove competenze per le pubbliche amministrazioni*" del Dipartimento della funzione pubblica, ciascuna amministrazione pianifica la formazione del proprio personale per lo sviluppo delle competenze digitali. L'obiettivo generale del Syllabus è fare in modo che tutti i dipendenti pubblici siano in grado di operare attivamente in modo sicuro, consapevole, collaborativo e orientato al risultato all'interno di una pubblica amministrazione sempre più digitale.
L'Azienda ha aderito all'iniziativa e nel corso del 2023 si prevede la partecipazione di alcuni dipendenti, in collaborazione con l'Area di Formazione Aziendale.
Inoltre è attivo da qualche anno un corso FAD per tutti i dipendenti "*GDPR REGOLAMENTO UE 679/2016 E SICUREZZA INFORMATICA*".

RA.6.1b - Avviare momenti di Informazione per lo sviluppo delle competenza digitali

Nel corso dell'anno sono stati previsti dei questionari relativi alle Misure di Sicurezza e all'uso corretto dei dispositivi al fine di sensibilizzare il personale e individuare le aree di maggior criticità.
Ogni nuova iniziativa "importante" in tema di "Informatica" viene di norma preceduta da una/più comunicazioni via email e da incontri programmati con i dipendenti per poter illustrare obiettivi e modalità

RA.6.1c - Pubblicazione su Intranet di Regolamenti/Procedure Operative/Manuali
Al fine di diffondere "la Cultura informatica" sono stati predisposti e pubblicati su Intranet alcuni Regolamenti/procedure Operative:

- Regolamento uso di Internet e email
- Regolamento Firma Digitale
- Manuale dei processi Documentali per la Conservazione Digitale
- Linee Guida per l'uso della PEC
- Linee Guida per gli Amministratori
- Linee Guida per la Sicurezza Informatica e per il lavoro da remoto
- Linee Guida per il corretto utilizzo degli strumenti (hardware e software) informatici

Sono inoltre pubblicati i manuali d'uso del software utilizzato

Contesto normativo e strategico

Riferimenti normativi italiani:

- Competenze digitali, documento AGID, 13 febbraio 2020
- Strategia Nazionale per le competenze digitali (2020)
- Piano Operativo della Strategia Nazionale per le competenze digitali (2020)
- Guida AGID dei diritti di cittadinanza digitale (2022)

Riferimenti normativi europei:

- Raccomandazione del Consiglio del 22 maggio 2018 relativa alle competenze chiave per l'apprendimento permanente (GU 2018/C 189/01)
- Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM (2020) 67 final del 19 febbraio 2020 - Plasmare il futuro digitale dell'Europa

CAPITOLO 7. Governance

I processi di transizione digitale in cui sono coinvolte le amministrazioni richiedono visione strategica, capacità realizzativa ed efficacia della governance. Con il Piano triennale per l'informatica nella PA, nel corso di questi ultimi anni, visione e metodo sono stati declinati in azioni concrete e condivise, in raccordo con le amministrazioni centrali e locali e attraverso il coinvolgimento dei Responsabili della transizione al digitale che rappresentano l'interfaccia tra AGID e le pubbliche amministrazioni.
I cambiamenti che hanno investito il nostro Paese negli ultimi due anni, anche a causa della crisi pandemica, sono stati accompagnati da una serie di novità normative e da nuove opportunità che hanno l'obiettivo di dare un'ulteriore spinta al processo di trasformazione digitale già iniziata. Il Piano triennale, in questo contesto, si pone come strumento di sintesi tra le differenti linee di trasformazione digitale della Pubblica Amministrazione.
Tra queste va data rilevanza a quella rappresentata dal Piano Nazionale di Ripresa e Resilienza (PNRR), inserita nel programma *Next Generation EU* (NGEU). In particolare, la

Missione 1 del PNRR si pone l'obiettivo di dare un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese affidando alla trasformazione digitale un ruolo centrale. Lo sforzo di digitalizzazione e innovazione è centrale in questa Missione, ma riguarda trasversalmente anche tutte le altre.
In questo mutato contesto obiettivi e azioni del Piano triennale, dunque, non possono che essere definiti e individuati in accordo con le indicazioni del PNRR. Da questo punto di vista, è importante evidenziare che il decreto-legge 31 maggio 2021 n. 77 c.d. "Semplificazioni" (come convertito con la legge n. 108/2021) contiene disposizioni in ordine all'organizzazione della gestione del Piano Nazionale di Ripresa e Resilienza, definendo i ruoli ricoperti dalle diverse amministrazioni coinvolte nonché le modalità di monitoraggio del Piano e del dialogo con le autorità europee.
La prima parte del decreto-legge, in particolare, ha definito, con un'articolazione a più livelli, la *governance* del Piano nazionale di ripresa e resilienza (PNRR).
In base a quanto descritto nella Guida per la redazione format del Piano triennale per le pubbliche amministrazioni, le iniziative di governance, in generale, si focalizzano su diversi ambiti tra cui:

- Monitoraggio, dello stato di attuazione delle iniziative proposte nel PT di riferimento;
- Rafforzamento delle competenze, attraverso iniziative formative di valutazione e di valorizzazione delle competenze digitali dei dipendenti;
- Iniziative verso cittadini e imprese, per rafforzare la cooperazione e i servizi verso e per i cittadini e le imprese attraverso tecnologie digitali.

Gli obiettivi di questa sezione possono essere riferiti a:

- Rafforzare gli strumenti dell'Amministrazione per l'attuazione del Piano, costruendo un sistema condiviso di obiettivi e di indicatori di performance;
- Individuare le azioni e gli strumenti di raccordo con il territorio e di interazione con tutti gli stakeholder;
- Sviluppare il capitale umano, attraverso il rafforzamento delle competenze

Obiettivi e risultati attesi

OB.7.1 Valutazione dei livelli di digitalizzazione tramite il modello di maturità HIMSS-EMRAM

RA.7.1a - "Verification mechanism'
All'interno della Missione 6 Salute del Piano Nazionale di Ripresa e Resilienza (PNRR) l'investimento 1.1.1 della Componente 2 prevede l'ammodernamento del parco tecnologico e digitale ospedaliero (digitalizzazione strutture sede di DEA I e II livello) come intervento "cardine" e di rilevanza strategica per l'evoluzione dei sistemi informativi ospedalieri su scala nazionale. Ai fini dell'attuazione dell'investimento 1.1.1, la Regione ha sottoscritto con il Ministero della Salute il Contratto Istituzionale di Sviluppo (CIS), individuato dalla normativa PNRR quale strumento di programmazione negoziata. A seguito della sottoscrizione dei CIS, è stata avviata la fase di esecuzione degli investimenti,nella quale si è convenuti alla necessità di procedere ad una valutazione del livello di digitalizzazione delle strutture sede di DEA attraverso l'attivazione di idonee procedure/protocolli di verifica validati, nello specifico la Certificazione *Electronic Medical Record Adoption Model (EMRAM) – HIMSS*.

L'Azienda ha già previsto di intraprendere il percorso di certificazione in due fasi: una valutazione iniziale per misurare il grado di digitalizzazione di partenza (AS-IS) ed una

seconda (anno 2025) volta a misurare il grado di digitalizzazione raggiunto a seguito degli interventi di digitalizzazione (TO-BE).

RA.7.1b - Monitoraggio del Piano triennale
Il monitoraggio del Piano triennale si compone delle seguenti attività:

- misurazione dei risultati (R.A.) conseguiti dall'Azienda per ciascuna componente tecnologica e non tecnologica del Piano;
- analisi della spesa e degli investimenti pubblici in ICT

L'attuazione di queste azioni ha la finalità di ottenere una visione delle attività svolte dall'Azienda in relazione alla loro coerenza con il Piano triennale con la possibilità di introdurre azioni correttive necessarie per il raggiungimento degli obiettivi previsti Allo stesso tempo, tali azioni di monitoraggio e verifica hanno l'obiettivo di supportare l'attuazione fisica, finanziaria e procedurale del Piano triennale nel suo complesso.
Le Pubbliche Amministrazioni, secondo la *roadmap* definita dalle Linee d'Azione nel Piano triennale e le modalità operative fornite da AGID, potranno compilare on line il "Format PT" per le PA così da rendere possibile la costruzione e l'alimentazione della base dati informativa.

Contesto normativo e strategico

Di seguito un elenco delle principali fonti, raccomandazioni e norme sugli argomenti trattati a cui le amministrazioni devono attenersi.

Generali:
● Decreto-legge 31 maggio 2021, n. 77 - Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure artt. 1-11 e art. 41

Consolidamento del ruolo del Responsabile per la transizione al digitale:
● Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD) art. 17
● Circolare n.3 del 1° ottobre 2018 del Ministro per la Pubblica Amministrazione sul Responsabile per la transizione al digitale

Il monitoraggio del Piano triennale:
● Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (in breve CAD) art 14-bis, lettera c

APPENDICE 1. Acronimi

Acronimo	Definizione
AGID	Agenzia per l'Italia Digitale
ANPR	Anagrafe nazionale popolazione residente
API	Application Programming Interface
CAD	Codice dell'amministrazione digitale

OBIETTIVI	RISULTATI
OB.1.1 - Migliorare la capacità di generare ed erogare servizi digitali	*R.A.1.1a - Diffusione del modello di riuso di software tra le amministrazioni in attuazione delle Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione*
	R.A.1.1b - Implementazione Cartella Clinica Mobile
	R.A.1.1c - Diffusione del monitoraggio, da parte delle Amministrazioni, della fruizione dei servizi digitali
OB.1.2 - Migliorare l'esperienza d'uso e l'accessibilità dei servizi	*R.A.1.2a - Incremento e diffusione dei modelli standard per lo sviluppo di siti*
	R.A.1.2b - Diffusione dei test di usabilità nelle amministrazioni per agevolare il feedback e le valutazioni da parte degli utenti
	R.A.1.2c - Incremento dell'accessibilità dei servizi digitali della PA, secondo quanto indicato dalle Linee guida sull'accessibilità degli strumenti informatici
	R.A.1.2d - pubblicazione delle statistiche di utilizzo del proprio sito web, aderendo a Web Analytics Italia per migliorare il processo evolutivo dei propri servizi online
	R.A.1.2e - pubblicare gli obiettivi di accessibilità sul proprio sito
OB.2.1 - Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa	*R.A.2.1a - Incremento del livello di alimentazione e digitalizzazione del Fascicolo Sanitario Elettronico con tutti i documenti sanitari*
	R.A.2.1b - Adeguamento degli Applicativi a FSE 2.0, al fine di indirizzare gli interventi di integraione degli applicativi con la nuova infrastruttura. FSE 2.0.
OB.2.2 - Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti	*R.A.2.2a - Incremento dell'adozione e dell'utilizzo dell'identità digitale (SPID e CIE)*
	R.A.2.2b - Incremento dei servizi sulla piattaforma PagoPA
OB.2.3 - Incrementare e razionalizzare il numero di piattaforme al fine di semplificare i servizi ai cittadini	*R.A.2.3 - Incremento dei servizi sulla Piattaforma IO (l'App dei servizi pubblici)*
OB.3.1 - Migliorare la qualità e la sicurezza dei servizi digitali erogati migrando gli applicativi *on-premise* (*data center* Gruppo B) verso infrastrutture e servizi *cloud* qualificati	*R.A.3.1a - Predisposto piano di migrazione dei servizi digitali verso strutture cloud qualificate*
	R.A.3.1b - Avviata migrazione dei servizi digitali verso struttute cloud qualificate
	R.A.3.1c Realizzazione di un'istanza di Disaster Recovery ospitata presso il Cloud
OB.3.2 - Migliorare l'offerta di servizi di	*R.A.3.2 – Ottimizzare la connettività*

connettività per le PA	
OB.4.1 - Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API	*R.A.4.1a – Interoperabilità Repository*
	R.A.4.1b – Interoperabilità FSE.
	R.A.4.1c– Immagini
	R.A.4.1d – Digital Pathology
OB.5.1 - Aumentare la consapevolezza del rischio cyber (*Cyber Security Awareness*) nell'Azienda	*R.A.5.1 - Incremento del livello di Cyber Security Awareness misurato tramite questionari di self-assessment ai dipendenti dell'Azienda*
OB.5.2 - Aumentare il livello di sicurezza informatica	*R.A.5.2 - Incremento delle misure di sicurezza*
OB.5.3 - Aumentare il livello di sicurezza informatica dei portali istituzionali	*R.A.5.3 - Incremento del numero dei portali istituzionali che utilizzano il protocollo HTTPS only, misurato tramite tool di analisi specifico*
OB.5.4 - Aumentare il livello di sicurezza informatica nei procedimenti di acquisizione di beni e servizi	*R.A.5.4 - Far riferimento alle Linee guida sulla sicurezza nel procurement ICT*
OB 6.1 - Rafforzare le leve e le competenze digitali per favorire l'innovazione	*RA.6.1a - Avviare la Formazione per lo sviluppo delle competenze digitali e sulla sicurezza*
	RA.6.1b - Avviare momenti di Informazione per lo sviluppo delle competenza digitali
	RA.6.1c - Pubblicazione su Intranet di Regolamenti/Procedure Operative/Manuali
OB.7.1 Valutazione dei livelli di digitalizzazione tramite il modello di maturità HIMSS-EMRAM	*R.A. 7.1a -"Verification mechanism'*
	R.A.7.1b - Monitoraggio del Piano triennale