Piano Triennale per la Transizione Digitale 2023-2025 dell'Ordine delle Professioni Infermieristiche della provincia di Milano Lodi Monza e Brianza

In riferimento al Piano Triennale per l'informatica

2022-2024 pubblicato da AGID

Rev. 2025

Approvato con delibera del Consiglio dell'Ordine n. 168 / 2025

Sommario

Piano Triennale per la Transizione Digitale 2023-2025 dell'Ordine delle Professioni Infermieristiche della provincia di Milano Lodi 1

Prefazione 5

Struttura 5

L'Ordine delle Professioni Infermieristiche 6

Ruolo del Responsabile per la Transizione al Digitale 7

Contesto Strategico 7

Obiettivi del Piano Triennale per la Transizione Digitale 8

1. Servizi digitali di qualità, accessibili e orientati all'utente 8

2. Innovazione digitale inclusiva, sostenibile ed etica 8

3. Diffusione di tecnologie interoperabili e sicure 8

Principi Guida 9

Servizi 9

Risultati attesi 10

1. Digitalizzazione dei servizi agli iscritti 10

2. Accessibilità e fruibilità dei servizi 10

3. Sicurezza informatica e protezione dei dati 10

4. Comunicazione digitale e trasparenza 10

5. Integrazione e interoperabilità 10

6. Formazione digitale continua 10

Stato di attuazione – Monitoraggio 2025 10

1. **Pagamento della tassa di iscrizione annuale 10**
2. **Procedura di iscrizione all'Albo 11**
3. **Rilascio Certificato di iscrizione 11**
4. **Rilascio dei certificati per soggetti privati 11**

Imposta di bollo 11

Target 2025-2026 – Monitoraggio, risoluzione delle criticità e piena operatività dei servizi digitali 11

Obiettivo 2024 con proseguo 2025 e 2026 12

Obiettivo 2025 e 2026 12

Sicurezza informatica: 12

Azioni previste 12

Indicatori di monitoraggio 12
4. Gestione documentale e interoperabilità 12
5. Trasparenza e accessibilità 13
6. Competenze digitali 13
7. Governance digitale 14
Linee di Intervento 14
Esperienze acquisite 15
Dati 16
Piattaforme e Gestionali Software e infrastrutture 16
Integrazione dei sistemi e condivisione dei dati 18
Contesto normativo e strategico 19
Sicurezza informatica 19
Governare la Transizione Digitale: Ruoli, Responsabilità e Strumenti 21
Riferimenti normativi: 22
Acronimi 23
Normativa di riferimento: 24
Glossario: 25
Once Only 25
Cosa fa un'API? 25
Cloud First nella digitalizzazione della PA 26
Digital & Mobile First 26
Digital Identity Only 26
Servizi inclusivi e accessibili 26
Dati pubblici come bene comune 26
Interoperabilità by Design 26
Sicurezza e Privacy by Design 26
User-Centric, Data-Driven e Agile 26
Transfrontaliero by Design 26
Software Open Source 27
Supply chain digitale 27
Attacchi cyber 27
Architettura Zero Trust 27
Data-driven 27
Disaster Recovery (DR) – Cos'è 28

Crittografia End-to-End (E2EE) – Cos'è 28
Soap e Rest 28
PIANO DI GESTIONE DELLA CYBERSICUREZZA 29
Nota di accompagnamento 29
Capitolo 1 – Governance della Cybersicurezza 29
Capitolo 2 – Piano per la Notifica degli Incidenti 29
Capitolo 3 – Piano di Prevenzione del Rischio Cyber 30
Indicatori di monitoraggio 30
Prossimi sviluppi 30
Allegato 1 – Modulo di Segnalazione Incidente Informatico 31
Allegato 2 – Scheda Evento e Valutazione 32
Allegato 3 – Registro Test Backup e DRP (Disaster Recovery Plan) 33
Allegato 4 – Estratto Politiche di Sicurezza Informatica 34

Prefazione

Nel contesto di un'evoluzione digitale sempre più pervasiva e strategica, l'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza ha scelto di dotarsi di un **Piano Triennale per la Transizione Digitale 2025–2026** che non rappresenti soltanto un adempimento normativo, ma si configuri come uno **strumento operativo, integrato e proattivo**.

La crescente domanda di servizi digitali accessibili, sicuri e interoperabili, proveniente sia dagli iscritti sia dai cittadini, richiede che anche gli Ordini professionali orientino la propria azione verso modelli amministrativi sempre più **efficienti, misurabili e tecnologicamente avanzati**.

Il presente documento nasce dall'analisi delle linee guida contenute nel Piano Triennale per l'informatica nella Pubblica Amministrazione redatto da AGID e ne propone una **traduzione concreta e sostenibile**, adattata alle risorse e alle peculiarità del nostro Ente. L'approccio adottato è stato **pragmatico e orientato ai risultati**, con obiettivi definiti sulla base della fattibilità reale, delle risorse disponibili e dell'impatto atteso sul miglioramento dei servizi e sulla trasparenza dell'azione amministrativa.

Attraverso questo Piano, l'Ordine si impegna a:

- potenziare le infrastrutture digitali esistenti;
- estendere l'adozione delle piattaforme abilitanti (SPID, pagoPA, ANPR);
- migliorare la qualità e la valorizzazione dei dati gestiti;
- garantire la sicurezza informatica come prerequisito imprescindibile;
- sviluppare le competenze digitali del personale;
- rendere il sito istituzionale uno strumento sempre più centrale e fruibile.

La **trasformazione digitale** costituisce per noi una leva essenziale per generare **efficienza, semplificazione e valore pubblico**. Con questo Piano intendiamo affermare il nostro impegno per un'amministrazione sempre più moderna, vicina, consapevole delle sfide attuali e pronta ad affrontare quelle future.

Struttura

Il **Piano Triennale per l'Informatica nella Pubblica Amministrazione** (di seguito "Piano Triennale" o "PT"), elaborato dall'Agenzia per l'Italia Digitale (AgID) e approvato con Decreto del Presidente del Consiglio dei ministri (DPCM), costituisce lo strumento strategico di indirizzo e coordinamento per la trasformazione digitale della Pubblica Amministrazione italiana.
Tale Piano si colloca in un contesto in continua evoluzione, accelerato dall'impulso all'adozione delle tecnologie digitali generato dalla pandemia da Covid-19. In questo scenario, la digitalizzazione assume un ruolo sempre più centrale, richiedendo interventi pianificati, coerenti e capaci di rispondere con efficacia alle dinamiche tecnologiche, normative e finanziarie in atto.

L'innovazione tecnologica, l'adeguamento del quadro normativo e i rilevanti investimenti messi a disposizione a livello europeo e nazionale, in particolare attraverso il **Piano Nazionale di Ripresa e Resilienza (PNRR)**, costituiscono fattori abilitanti fondamentali per sostenere il processo di trasformazione digitale in atto.
Il Piano Triennale rappresenta un riferimento per le amministrazioni pubbliche nel **delineare strategie, obiettivi e attività** coerenti con le politiche di innovazione nazionale.

L'Ordine delle Professioni Infermieristiche

L'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza (di seguito anche "OPI Milano Lodi Monza e Brianza" o "OPI MILOMB) è un ente di diritto pubblico non economico connesso all'esercizio della Professione di Infermiere e Infermiere Pediatrico e finalizzato alla tutela dell'interesse pubblico.

Gli Ordini delle Professioni Infermieristiche, originariamente istituiti come *Collegi* e regolamentati da normative specifiche (Legge n. 1049/1954; Dlcps 233/46 e Dpr 221/50), sono stati successivamente trasformati in *Ordini* e qualificati come enti sussidiari dello Stato con la Legge n. 3/2018.

Agli Ordini sono attribuite, tra le altre, le seguenti finalità:

- **una finalità interna**, volta a promuovere e garantire l'indipendenza, l'autonomia e la responsabilità dei Professionisti, la qualità tecnico-professionale, la valorizzazione della funzione sociale, nonché la salvaguardia dei diritti umani e dei principi etici dell'esercizio professionale, così come sanciti nel Codice Deontologico;
- **una finalità esterna**, orientata alla protezione dei cittadini e alla tutela della salute individuale e collettiva, attraverso l'azione di Professionisti qualificati, in possesso di un titolo abilitante e regolarmente iscritti all'Albo.

L'attività dell'Ordine, dotato di autonomia patrimoniale, è finanziata esclusivamente dalle quote versate dagli iscritti, senza alcun onere per la finanza pubblica. L'ammontare delle quote è determinato anche sulla base delle spese di gestione, dei programmi di attività (formazione, informazione, consulenza, ecc.) e della quota da versare alla Federazione Nazionale.

Gli Organi dell'Ordine sono:

- il Presidente;
- il Consiglio Direttivo;
- la Commissione di Albo, per gli Ordini che comprendono più professioni;
- il Collegio dei Revisori.

L'organo di governo dell'Ordine è il Consiglio Direttivo, eletto ogni quattro anni tramite consultazione di tutti gli iscritti. Al suo interno vengono assegnate le cariche di Presidente, Vicepresidente, Segretario e Tesoriere. Il Presidente rappresenta l'Ordine a livello provinciale ed è membro di diritto del Consiglio nazionale.

L'OPI Milano Lodi Monza e Brianza conta circa 25.800 iscritti (dato aggiornato al 2024) e svolge le proprie attività istituzionali avvalendosi del lavoro di 3 dipendenti a tempo indeterminato e 2 dipendenti interinali.

Al pari delle altre Pubbliche Amministrazioni, anche l'Ordine si colloca, in materia di digitalizzazione, all'interno del quadro normativo e organizzativo delineato dall'Agenzia per l'Italia Digitale (AGID).

In tale contesto, come evidenziato nella parte introduttiva del presente documento, assume particolare rilevanza il Piano Triennale per l'Informatica nella Pubblica Amministrazione, redatto da AGID, che rappresenta uno strumento fondamentale per la promozione della trasformazione digitale del Paese.

Il ruolo di AGID risulta centrale anche nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR), in qualità di soggetto attuatore di numerose misure di digitalizzazione, nonché di supporto tecnico per le amministrazioni coinvolte.

Ruolo del Responsabile per la Transizione al Digitale

L'ufficio è previsto dall'articolo 17 del CAD (Codice dell'Amministrazione Digitale, Dlgs 82/2005) ed è diretto dal **Responsabile per la Transizione al Digitale** (RTD). Il Responsabile per la Transizione al Digitale (RTD) può essere individuato tra i dirigenti preposti a uffici di livello dirigenziale generale. Non essendoci posizioni dirigenziali, come chiarito dalla Circolare n. 3/2018, le funzioni previste dall'art. 17 del Codice dell'Amministrazione Digitale (CAD) possono essere attribuite a un dipendente con funzioni apicali, oppure, in alternativa, a un titolare di posizione organizzativa.

Come indicato nell'Articolo 17 del D.Lgs. 7 marzo 2005, n. 82 («Codice dell'Amministrazione Digitale») - Comma 1-ter: il RTD deve possedere adeguate competenze tecnologiche, di informatica giuridica e

manageriali e risponde, con riferimento ai compiti relativi alla transizione alla modalità digitale, direttamente all'organo di vertice politico (Consiglio Direttivo dell'Ordine delle Professioni Infermieristiche)
Il Responsabile per la Transizione al Digitale (RTD) svolge una funzione strategica all'interno delle pubbliche amministrazioni, finalizzata a garantire l'attuazione delle politiche di digitalizzazione, l'innovazione tecnologica e l'adeguamento al Codice dell'Amministrazione Digitale (D.Lgs. 82/2005).
Con delibera 3 agosto 2021 n. 144/2021 il Consiglio Direttivo ha nominato quale Responsabile per la Transizione al Digitale (RTD) *la dipendente Veronica Banfi*.
Il RTD coordina le attività dell'Ufficio per la Transizione Digitale e coopera con: Responsabile della gestione documentale, Responsabile della protezione dei dati (DPO), e Responsabile della trasparenza e anticorruzione.

Contesto Strategico

Per delineare il contesto strategico di riferimento del presente Piano Triennale per la Transizione Digitale, si evidenzia in via preliminare che l'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza rappresenta una realtà territoriale articolata, con un bacino di circa 25.800 iscritti. L'organico attualmente in servizio è composto da tre dipendenti a tempo indeterminato e due interinali, mentre il Consiglio Direttivo è presieduto dal **Dott. D'Aloia Pasqualino**.
L'Ordine, come previsto per tutti gli OPI provinciali, è parte integrante della Federazione Nazionale degli Ordini delle Professioni Infermieristiche (FNOPI), ente pubblico non economico che riunisce gli ordini provinciali degli infermieri e degli infermieri pediatrici su tutto il territorio della Repubblica Italiana.
In tale quadro, l'Ufficio per la Transizione Digitale dell'Ordine si occupa della definizione annuale e sistematica delle linee di azione in materia di digitalizzazione, attraverso l'approvazione del presente Piano Triennale. Il Piano costituisce lo strumento di programmazione delle attività e delle direttrici di sviluppo, ed è soggetto a successivi aggiornamenti in relazione all'assegnazione degli obiettivi e delle risorse disponibili.
L'attuazione del Piano si fonda su una logica di priorità, individuata in funzione dei fabbisogni espressi dall'utenza interna ed esterna, del grado di obbligatorietà normativa, della necessità di assicurare adeguati livelli di sicurezza, nonché della sostenibilità economico-organizzativa delle singole azioni.
Il coordinamento generale del processo è affidato al Responsabile per la Transizione Digitale, che cura l'elaborazione delle proposte operative, il monitoraggio dell'attuazione e la rendicontazione delle attività svolte.

Obiettivi del Piano Triennale per la Transizione Digitale

Il Piano Triennale per la Transizione Digitale dell'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza si inserisce in un quadro strategico nazionale orientato a promuovere una Pubblica Amministrazione moderna, efficiente e centrata sulle esigenze di cittadini e imprese. Gli assi strategici fondamentali sono:

- **Promuovere la trasformazione digitale** della Pubblica Amministrazione quale leva di sviluppo sistemico per il Paese, garantendo l'erogazione di servizi digitali di qualità, facilmente accessibili e orientati all'utente finale.
- **Favorire uno sviluppo sostenibile, etico e inclusivo**, valorizzando l'innovazione tecnologica al servizio delle persone, delle comunità professionali e del territorio, in coerenza con i principi di sostenibilità ambientale e coesione sociale.
- **Accelerare la diffusione delle tecnologie digitali** nel sistema pubblico e produttivo italiano, sostenendo l'adozione di soluzioni standard, interoperabili e innovative, capaci di abilitare servizi pubblici evoluti, affidabili e sicuri.

1. Servizi digitali di qualità, accessibili e orientati all'utente

- **Digitalizzare completamente i procedimenti amministrativi** relativi a iscrizioni, trasferimenti, cancellazioni e richieste di certificati, con possibilità di presentazione online tramite SPID o CIE.
- **Rendere il sito istituzionale pienamente conforme alle linee guida AGID** in materia di accessibilità, con aggiornamento continuo in base alle evoluzioni normative.
- **Semplificare l'esperienza dell'iscritto**, sviluppando un'area riservata interattiva per la gestione autonoma delle pratiche e della propria posizione ordinistica.
- **Attivare servizi di notifica digitale (PEC, email, SMS)** per comunicazioni tempestive e personalizzate, anche tramite app mobile o portale.

2. Innovazione digitale inclusiva, sostenibile ed etica

- **Promuovere iniziative di alfabetizzazione digitale** rivolte agli iscritti meno esperti, anche attraverso eventi ECM o tutorial dedicati.
- **Diffondere strumenti digitali rispettosi dell'ambiente**, come la firma digitale e l'eliminazione progressiva della documentazione cartacea.
- **Sostenere l'adozione di strumenti inclusivi e interoperabili**, garantendo la protezione dei dati personali e il rispetto del GDPR.

3. Diffusione di tecnologie interoperabili e sicure

- **Implementare sistemi di autenticazione e accesso sicuri**, con l'adozione di SPID professionale;
- **Adottare soluzioni interoperabili basate su API**, per favorire lo scambio dati con enti esterni (es. Co.Ge.A.P.S., Aziende Sanitarie, Università e Opi Provinciali).
- **Rafforzare la sicurezza informatica** con l'introduzione di strumenti avanzati come firewall di nuova generazione, sistemi EDR e piani di risposta agli incidenti (IR).
- **Garantire backup automatizzati e conservazione digitale a norma**, per tutelare la continuità operativa e la protezione del patrimonio informativo.

Nel contesto del Piano Triennale per la Transizione Digitale dell'Ordine, alcuni obiettivi sono già stati tradotti in azioni operative concretamente avviate, mentre altri risultano attualmente in fase di analisi, progettazione o sviluppo. L'attuazione complessiva è prevista in modo progressivo nell'arco del triennio, in coerenza con le priorità strategiche individuate e con le risorse disponibili.

Principi Guida

L'implementazione del Piano è orientata dai seguenti principi operativi, in coerenza con le indicazioni fornite da AGID e dal Dipartimento per la Trasformazione Digitale:

- Digital & Mobile First
- Digital Identity Only
- Cloud First
- Servizi inclusivi e accessibili
- Dati pubblici come bene comune
- Interoperabilità by Design
- Sicurezza e Privacy by Design
- User-Centric, Data-Driven e Agile
- Once Only Principle
- Transfrontaliero by Design
- Software Open Source

Servizi

Il miglioramento della qualità, dell'accessibilità e dell'inclusività dei servizi pubblici digitali rappresenta un presupposto imprescindibile per stimolarne l'adozione da parte degli utenti – siano essi cittadini, professionisti o altre amministrazioni pubbliche.
In questo quadro, l'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza riconosce la necessità di rendere pienamente accessibili e digitalmente fruibili le proprie attività e i servizi rivolti agli iscritti e alla cittadinanza. La digitalizzazione progressiva delle funzioni istituzionali dell'Ente costituisce infatti un'opportunità concreta per ottimizzare i processi, ridurre gli oneri amministrativi e promuovere una maggiore efficienza e inclusività.
Affinché tali obiettivi siano raggiunti, è fondamentale adottare un approccio progettuale multidisciplinare, basato su tecnologie interoperabili e metodologie user-centriche. La qualità complessiva di un servizio, così come la sua sostenibilità economica, dipende dall'analisi e dalla semplificazione dei diversi livelli – tecnologici, organizzativi e procedurali – che ne compongono l'erogazione.
In tale prospettiva, il Regolamento (UE) 2018/1724 (Single Digital Gateway), unitamente al Codice dell'Amministrazione Digitale (CAD) e alle linee guida del presente Piano Triennale, evidenzia la necessità di rivedere i processi amministrativi in chiave digitale, attuare procedure corrette e standardizzate e abilitare la piena interoperabilità, in linea con il principio del "once only", che impone alle amministrazioni di non richiedere agli utenti dati già in loro possesso.
Tra gli obiettivi strategici prioritari vi è quindi quello di garantire un'offerta di servizi interamente digitali, progettati sulla base delle potenzialità offerte dalle piattaforme abilitanti e coerenti con il paradigma ***cloud first***.
Il perseguimento di tale obiettivo dovrà tenere conto del contesto istituzionale in cui opera l'OPI Milano Lodi Monza e Brianza, nonché del necessario allineamento e coordinamento con le azioni promosse a livello nazionale dalla Federazione Nazionale degli Ordini delle Professioni Infermieristiche (FNOPI).

Infine, per favorire un'effettiva transizione verso il digitale, è necessario incentivare l'utenza a privilegiare i canali digitali rispetto a quelli fisici. Questo richiede un deciso e gravoso impegno nella semplificazione dell'esperienza utente, nel miglioramento dell'usabilità dei servizi e nel rispetto pieno dei requisiti in materia di accessibilità e protezione dei dati personali, come previsto dal Regolamento generale sulla protezione dei dati (GDPR) e dalle linee guida AGID.
A complemento di tale linea d'azione, risulta strategico promuovere iniziative volte a incentivare l'utilizzo consapevole delle risorse informatiche, con particolare riferimento alla platea degli iscritti. Tali attività dovranno favorire il rafforzamento dell'alfabetizzazione digitale e incrementare la propensione all'adozione delle tecnologie emergenti, contribuendo così a colmare eventuali divari digitali e a massimizzare l'efficacia delle soluzioni digitali messe a disposizione dall'Ente.

Risultati attesi

L'Ordine delle Professioni Infermieristiche di Milano, Lodi, Monza e Brianza persegue l'obiettivo di ampliare progressivamente l'offerta di servizi digitali, in linea con le esigenze degli iscritti e con i principi di semplificazione amministrativa, accessibilità e digitalizzazione dei processi.

1. Digitalizzazione dei servizi agli iscritti

- Ampliare i servizi disponibili online (es. richieste di certificati, autocertificazioni, aggiornamento dati anagrafici).
- Implementare un'area riservata evoluta per gli iscritti, integrata con SPID/CIE.
- Digitalizzare completamente la procedura di iscrizione, cancellazione e trasferimento.

2. Accessibilità e fruibilità dei servizi

- Adeguare il portale web alle linee guida AgID sull'accessibilità (WCAG 2.1).
- Ottimizzare la navigazione e i contenuti del sito per dispositivi mobili (*mobile first*).
- Introdurre un sistema di chatbot o assistente digitale per supportare le richieste frequenti.

3. Sicurezza informatica e protezione dei dati

- Attivare l'autenticazione a due fattori (MFA) per l'accesso ai servizi digitali.
- Eseguire backup automatizzati e periodici dei dati critici.
- Implementare un sistema EDR per il monitoraggio delle minacce informatiche.

4. Comunicazione digitale e trasparenza

- Automatizzare l'invio di notifiche e comunicazioni tramite e-mail e PEC.
- Potenziare l'uso dei social media per aggiornamenti istituzionali.
- Pubblicare i dati in formato aperto e accessibile nella sezione "Amministrazione Trasparente".

5. Integrazione e interoperabilità

- Consentire alle aziende sanitarie la verifica dell'iscrizione tramite SPID professionale.
- Sviluppare API per la condivisione controllata dei dati con enti terzi (Co.Ge.A.P.S., Regione, Università).
- Implementare il principio "Once Only" per evitare duplicazione nella richiesta di documenti.

6. Formazione digitale continua

- Offrire corsi di alfabetizzazione digitale per gli iscritti meno esperti.
- Formare il personale interno su gestione documentale, PEC, firme digitali e sicurezza.
- Proporre corsi ECM su temi legati alla trasformazione digitale e alla cybersecurity.

Stato di attuazione – Monitoraggio 2025

Alla data attuale, l'Ordine eroga in modalità digitale i seguenti servizi:

1. **Pagamento della tassa di iscrizione annuale** attraverso piattaforma *pagoPA*, sia online che presso punti convenzionati.
2. **Procedura di iscrizione all'Albo**, L'iscrizione all'Albo avviene attualmente mediante una procedura che prevede una prima fase di preiscrizione online, effettuata attraverso la piattaforma dell'Albo Unico Nazionale gestito da FNOPI. Successivamente, l'aspirante iscritto è tenuto a presentarsi presso gli uffici dell'Ordine per consegnare la documentazione prevista. È in corso lo sviluppo di una nuova modalità che consentirà di completare l'intera procedura di iscrizione in modalità digitale, accedendo tramite identità digitale SPID, al fine di garantire maggiore semplificazione, accessibilità e tracciabilità del processo.
3. **Rilascio Certificato di iscrizione** L'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza, in conformità alle disposizioni della Federazione Nazionale degli Ordini delle Professioni Infermieristiche (FNOPI), **non può più rilasciare certificati di iscrizione da utilizzare nei rapporti con la Pubblica Amministrazione** o con i gestori di pubblici servizi. Infatti, ai sensi dell'art. 15, comma 1, della Legge 183/2011 ("Legge sulla decertificazione"), i certificati rilasciati dalle Pubbliche Amministrazioni non possono essere prodotti nei rapporti con altre Pubbliche Amministrazioni o gestori di pubblici servizi, ma esclusivamente nei confronti di soggetti privati. Nei rapporti con le amministrazioni pubbliche o i gestori di pubblici servizi, i certificati di iscrizione devono essere sostituiti da dichiarazioni sostitutive di certificazione ai sensi degli artt. 46 e 47 del DPR 445/2000. L'art. 43, comma 1, del medesimo decreto, modificato dall'art. 15 della Legge 183/2011, stabilisce inoltre che le amministrazioni pubbliche e i gestori di pubblici servizi sono tenuti ad acquisire d'ufficio le informazioni oggetto delle dichiarazioni sostitutive, anche tramite indicazione degli elementi necessari da parte dell'interessato.
4. **Rilascio dei certificati per soggetti privati**. **Gli iscritti all'Ordine possono richiedere il certificato di iscrizione solo se destinato a soggetti privati, inviando apposita richiesta**

esclusivamente tramite la propria casella PEC all'indirizzo opimilomb@cert.ordine-opi.it , allegando:

Imposta di bollo

Con parere del Ministero dell'Economia e delle Finanze (5 settembre 2012), è stato chiarito che:

5. i certificati da presentare a soggetti privati sono soggetti all'imposta di bollo di € 16,00;
6. anche la richiesta del certificato all'Ordine comporta l'applicazione di un'ulteriore marca da bollo da € 16,00, ai sensi dell'art. 3, comma 1, della Tariffa (Parte Prima, Allegato A, DPR 642/1972).

Pertanto, sono necessarie due marche da bollo:

- Una marca da apporre sul modulo di richiesta certificato;
- Una seconda marca da indicare nel modulo di assolvimento con numero identificativo, data e ora di emissione: questa verrà applicata al certificato che sarà trasmesso via PEC dall'Ordine.

Esenzioni dall'imposta di bollo

7. Il certificato può essere rilasciato in esenzione dall'imposta di bollo esclusivamente nei casi previsti dal DPR 642/1972 Tabella Allegato –B o da normative speciali. In tali ipotesi, l'iscritto ha l'obbligo di dichiarare l'uso specifico e citare espressamente la norma che prevede l'esenzione, la quale sarà riportata sul certificato.

Autocertificazione

Per autocertificare la propria iscrizione all'Ordine, è possibile utilizzare un modulo di autocertificazione. Tutte le informazioni sono pubblicate sul sito Istituzionale dell'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza – sezione Certificato di Iscrizione. https://opimilomb.it/richiesta-certificato-di-iscrizione/

Target 2025-2026 – Monitoraggio, risoluzione delle criticità e piena operatività dei servizi digitali

Potenziamento della fruibilità delle informazioni, istruzioni e supporti agli utenti

Obiettivo 2024 con proseguo 2025 e 2026

Promuovere interventi di alfabetizzazione digitale rivolti agli iscritti, mediante azioni mirate quali:

- supporto individuale personalizzato,
- diffusione di guide operative e materiale informativo,
- organizzazione di incontri formativi e sessioni dimostrative

Obiettivo 2025 e 2026

Rafforzamento dell'accessibilità dei servizi digitali secondo le Linee guida AGID tra cui:

Sicurezza informatica:

- Effettuare test di vulnerabilità e analisi del rischio con cadenza periodica sui sistemi informativi dell'Ente (sito istituzionale, server, infrastrutture digitali), al fine di individuare tempestivamente potenziali criticità, prevenire attacchi informatici e garantire la protezione dei dati trattati.

Azioni previste

- Pianificazione annuale di penetration test e vulnerability assessment su server e portali web;
- Coinvolgimento di fornitori qualificati per l'esecuzione dei test in conformità con le best practice di settore;
- Analisi e reportistica degli esiti dei test, con priorità agli interventi correttivi;
- Adozione di contromisure e aggiornamenti delle infrastrutture in base ai risultati emersi;

- Integrazione del ciclo di test nella strategia di sicurezza IT e nei documenti del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Indicatori di monitoraggio

- Numero di test effettuati annualmente
- % vulnerabilità critiche risolte entro 30 giorni
- Stato di aggiornamento dei sistemi e dei CMS impiegati
- Report finale validato da RTD

Scadenza prevista: dicembre 2025 e settembre 2026
Struttura responsabile: Responsabile per la Transizione Digitale

4. Gestione documentale e interoperabilità

- Adozione e aggiornamento del **Manuale di Gestione Documentale** ai sensi del DPCM 148/2021.
- Integrazione con la **PDND (Piattaforma Digitale Nazionale Dati)** per lo scambio dati con altri enti (es. ANPR, INPS).
- Implementazione della **conservazione digitale a norma** dei documenti obbligatori.

Scadenza prevista: settembre 2025
Struttura responsabile: Responsabile per la Transizione Digitale- Responsabile Gestione Documentale in collaborazione con l'Organo Politico dell'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza

5. Trasparenza e accessibilità

- Adeguamento del sito web istituzionale alle **Linee guida AgID su accessibilità** (L. 4/2004).
- Pubblicazione dinamica dei dati nella sezione "**Amministrazione Trasparente**" (es. bilanci, incarichi, delibere).
- Attivazione del **registro degli accessi** e gestione semplificata delle istanze FOIA.
    - **1. Descrizione dell'obiettivo**
    - L'Ordine intende attuare una gestione strutturata, trasparente e semplificata delle istanze di accesso agli atti da parte dei cittadini, in conformità al **Decreto Legislativo 33/2013** e al **FOIA (Freedom of Information Act)** introdotto dal D.Lgs. 97/2016.
    - L'obiettivo è quello di:
    - gestire in maniera efficace le richieste di accesso **documentale**, **civico semplice** e **civico generalizzato**;
    - assicurare la **tracciabilità** e la **risposta nei termini di legge**;
    - **istituire un registro degli accessi** consultabile online (sezione "Amministrazione Trasparente"), come previsto dall'**art. 5, comma 6** del D.Lgs. 33/2013 e dalle Linee guida ANAC.

    2. Azioni previste
    - Predisposizione di un **modulo online standardizzato** per la presentazione delle istanze di accesso.
    - Attivazione di una **procedura digitale interna** (anche via protocollo informatico) per la presa in carico, la valutazione e la risposta.
    - Tenuta di un **registro informatico degli accessi**, contenente:
        1. data della richiesta, oggetto dell'istanza,
        2. tipologia di accesso (documentale, civico semplice, civico generalizzato),
        3. esito e data della risposta.
        4. Pubblicazione periodica del registro nella sezione "Amministrazione Trasparente".

3. Indicatori di monitoraggio

- % di risposte fornite entro 30 giorni
- Numero istanze ricevute per tipologia
- Stato di aggiornamento del registro
- % di rifiuti motivati e contro-dedotti

Scadenza prevista: dicembre 2025 e continuo negli anni
Struttura responsabile: Responsabile per la Transizione Digitale in collaborazione con RTCP

6. Competenze digitali

- Formazione continua per il personale su **CAD, firma digitale, protocollo informatico, conservazione documentale**.
- Definizione di un **piano interno per lo sviluppo delle competenze digitali**, anche tramite piattaforme e-learning PA.

Scadenza prevista: dicembre 2025e settembre 2026
Struttura responsabile: Responsabile per la Transizione Digitale

7. Governance digitale

- Riconferma o nomina del **Responsabile per la Transizione Digitale (RTD)**.
- Istituzione di un **gruppo di lavoro interno** per la transizione digitale e l'attuazione del piano.
- Monitoraggio con indicatori (KPI) su attuazione, impatti e scostamenti rispetto alla pianificazione.
    - Per garantire l'efficacia e la coerenza del Piano di Digitalizzazione, l'Ente attiverà un sistema di monitoraggio basato su **indicatori chiave di prestazione (KPI) ModKPI**, finalizzati a valutare:
        1. lo stato di attuazione delle attività previste dal piano;
        2. l'impatto concreto sui processi interni e sui servizi erogati;
        3. eventuali scostamenti rispetto a tempistiche, costi e obiettivi pianificati.

Area	Indicatore KPI	Valore Obiettivo
Sicurezza informatica	% vulnerabilità risolte entro 30 giorni	≥90%
Servizi digitali	% istanze ricevute tramite moduli online	≥80% entro 12 mesi
Protocollo informatico	% documenti protocollati digitalmente	100% entro fine anno
Formazione personale	Ore medie di formazione digitale per dipendente	≥8 ore/anno
Interoperabilità	Numero di servizi attivi in cooperazione applicativa - servizi digitali dell'Ente sono integrati con altri enti pubblici o sistemi centrali, tramite scambio automatico di dati secondo regole tecniche standardizzate	+2 entro 2026

Scadenza prevista: Gennaio 2026- Dicembre 2026

Struttura responsabile: Responsabile per la Transizione Digitale in collaborazione con RTCP e l'Organo Politico dell'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza.

Linee di Intervento

Potenziare la capacità di generare ed erogare servizi digitali

Ampliamento del ventaglio dei servizi digitali offerti dall'Ordine delle Professioni infermieristiche di Milano Lodi Monza e Brianza.

Attività operative:

- Mappatura dei servizi erogati dall'Ente con analisi tecnica e organizzativa dei relativi processi interni, al fine di individuare le prestazioni potenzialmente digitalizzabili;
- Analisi della normativa vigente e dei regolamenti applicabili a ciascun servizio, per verificarne la piena compatibilità con l'erogazione in modalità digitale;
- Selezione di un fornitore esterno (software house) incaricato dello sviluppo e/o adattamento degli applicativi necessari;
- Fasi di test e collaudo delle soluzioni implementate;
- Inserimento delle nuove funzionalità digitali all'interno dei processi operativi dell'Ordine, con adeguata formazione al personale coinvolto.

Scadenza prevista: dicembre 2025
Struttura responsabile: Responsabile per la Transizione Digitale

Rafforzamento della fruibilità e comprensione dei servizi digitali da parte dell'utenza

Attività operative:

- Erogazione di consulenze personalizzate agli iscritti, finalizzate all'accompagnamento nell'utilizzo delle risorse digitali dell'Ordine (via telefono, incontri online o in presenza);
- Elaborazione e diffusione di documentazione operativa (guide, vademecum, istruzioni) a supporto dell'accesso e della gestione dei servizi online;
- Organizzazione di iniziative formative e informative volte a favorire l'alfabetizzazione digitale degli iscritti.

Scadenza prevista: 30 giugno 2026

Strutture responsabili: Commissione Formazione, Responsabile per la Transizione Digitale, personale amministrativo

Miglioramento dell'accessibilità dei servizi digitali secondo le Linee Guida AGID
Attività operative:

- **Nel gennaio 2025 è stato avviato un restyling del sito istituzionale www.opimilomb.it**, mediante affidamento di incarico a un fornitore qualificato per la revisione strutturale e l'adeguamento della piattaforma digitale dell'Ordine. L'intervento è stato realizzato in conformità alle **Linee Guida AGID** e alla normativa tecnica vigente in materia di **accessibilità digitale**, con particolare riferimento alla **norma UNI CEI EN 301549**, al fine di garantire la piena fruibilità dei contenuti e dei servizi da parte di tutti gli utenti;
- Inserimento sul sito dell'apposita dichiarazione di accessibilità, come previsto dalla normativa vigente.

Scadenza prevista: febbraio 2026
Strutture responsabili: Responsabile per la Transizione Digitale
Fonti di finanziamento: Capitolo di bilancio INFORMATIZZAZIONE COMUNICAZIONE"

Esperienze acquisite

Come già evidenziato, l'Ente eroga attualmente diversi servizi in modalità telematica, tra cui:

- il pagamento online o presso punti convenzionati delle quote annuali di iscrizione;
- l'iscrizione ai corsi di aggiornamento promossi dall'Ordine;
- la richiesta della casella PEC gratuita fornita dall'Ordine;
- l'interazione online con la segreteria;
- la consultazione e modifica dei propri dati anagrafici e professionali.

A partire da aprile 2022, come già indicato in precedenza (Stato di attuazione – Monitoraggio 2025) l'iscrizione all'Albo avviene attualmente mediante una procedura che prevede una prima fase di preiscrizione online, effettuata attraverso la piattaforma dell'Albo Unico Nazionale gestito da FNOPI. Successivamente, l'aspirante iscritto è tenuto a presentarsi presso gli uffici dell'Ordine per consegnare la documentazione prevista.
È in corso lo sviluppo di una nuova modalità che consentirà di completare l'intera procedura di iscrizione in modalità digitale, accedendo tramite identità digitale SPID, al fine di garantire maggiore semplificazione, accessibilità e tracciabilità del processo.

L'esperienza maturata ha messo in luce alcune criticità nell'accesso ai servizi digitali da parte di alcuni iscritti. Per tale motivo l'Ordine ha già avviato attività di supporto e assistenza all'utilizzo degli strumenti informatici, riscontrando un graduale miglioramento nell'autonomia digitale dell'utenza.

Dati

La valorizzazione del patrimonio informatico pubblico rappresenta un obiettivo strategico per la Pubblica Amministrazione, indispensabile per affrontare con efficacia le sfide poste dalla *data economy*, sostenere gli obiettivi delineati dalla Strategia Europea sui dati e favorire la creazione di servizi digitali ad alto valore aggiunto rivolti a cittadini, imprese e a tutti gli stakeholder istituzionali. Essa consente inoltre di fornire ai decisori pubblici strumenti *data-driven*, a supporto dei processi decisionali e operativi. In coerenza con i principi stabiliti dalla normativa vigente e dal Piano Triennale per l'Informatica nella Pubblica Amministrazione, **il presente Piano intende rafforzare l'efficacia dell'attività amministrativa** in tutti i processi che prevedono l'utilizzo, la condivisione e il riutilizzo dei dati. Tale obiettivo si declina sia nella promozione dell'interoperabilità tra pubbliche amministrazioni per finalità istituzionali, sia nell'incentivazione del riutilizzo.
L'analisi dei procedimenti interni dell'Ordine ha tuttavia evidenziato alcune criticità, in particolare legate alla condivisione dei dati tra amministrazioni. Si segnalano, ad esempio, difficoltà nella gestione delle pratiche di trasferimento degli iscritti dovute alla limitata interoperabilità con altri Ordini delle Professioni Infermieristiche. Ulteriori rallentamenti si riscontrano nei procedimenti che dipendono da dati forniti da altri enti, come nel caso delle informazioni anagrafiche provenienti dai Comuni, i cui tempi di risposta non sempre risultano adeguati alle esigenze operative dell'Ente.

Alcuni esempi pratici di approccio *data-driven* applicati all'attività dell'Ordine delle Professioni Infermieristiche di Milano, Lodi, Monza e Brianza:

1. Pianificazione dell'offerta formativa ECM
    - Dati utilizzati: storico dei corsi frequentati, feedback dei partecipanti, numero di iscrizioni per tematica.
    - Utilizzo *data-driven*: analizzando i corsi più richiesti e meglio valutati, l'Ordine può programmare nuovi eventi formativi più rispondenti ai bisogni degli iscritti.

2. Miglioramento dei servizi online
   - Dati utilizzati: statistiche di accesso al sito, errori segnalati dagli utenti, richieste più frequenti alla segreteria.
   - Utilizzo *data-driven*: i dati raccolti possono guidare l'ottimizzazione dell'area riservata, ad esempio semplificando la richiesta di certificati o la procedura di iscrizione all'Albo.
3. Snellimento delle pratiche amministrative
   - Dati utilizzati: tempi medi di gestione delle pratiche (iscrizione, cancellazione, trasferimento), colli di bottiglia rilevati nei flussi.
   - Utilizzo *data-driven*: attraverso questi dati è possibile riprogettare i processi interni (workflow digitali) per ridurre i tempi di risposta e migliorare l'efficienza operativa.
4. Gestione personalizzata della comunicazione
   - Dati utilizzati: età, provenienza geografica, canali di comunicazione preferiti dagli iscritti.
   - Utilizzo *data-driven*: l'Ordine può inviare comunicazioni mirate e differenziate per target, migliorando l'efficacia delle campagne informative (es. reminder per ECM, avvisi scadenze).
5. Monitoraggio della sicurezza informatica
   - Dati utilizzati: log di accesso, tentativi di accesso anomali, segnalazioni di malfunzionamenti.
   - Utilizzo data-driven: l'analisi dei dati può attivare meccanismi di risposta automatica e rafforzare la prevenzione di attacchi informatici, in linea con i principi dello *Zero Trust*.

Piattaforme e Gestionali Software e infrastrutture

l processo di Transizione Digitale promosso dall'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza si fonda, tra i suoi elementi cardine, su un uso sempre più sistemico e integrato delle piattaforme digitali.
Tale approccio comprende:

- **l'adozione delle piattaforme nazionali della Pubblica Amministrazione**, quali SPID (Sistema Pubblico di Identità Digitale) e CIE (Carta di Identità Elettronica), strumenti ormai imprescindibili per l'autenticazione sicura degli utenti;
- **l'integrazione con le piattaforme di settore**, in particolare quelle messe a disposizione dalla Federazione Nazionale degli Ordini delle Professioni Infermieristiche (FNOPI), in coerenza con il contesto normativo e strategico in cui opera l'Ente;
- **l'eventuale sviluppo o personalizzazione di ulteriori applicativi digitali**, volti a supportare esigenze specifiche dell'Ordine e ad assicurare il conseguimento degli obiettivi fissati dalla normativa vigente in materia di digitalizzazione della PA.

Le piattaforme rappresentano infrastrutture abilitanti per l'ottimizzazione dei processi amministrativi, sia di *back-office* che di *front-end*, grazie alla loro capacità di interoperare in modo strutturato e sicuro con altri sistemi. Il loro impiego consente:

- una significativa riduzione degli oneri operativi per l'amministrazione;
- una maggiore uniformità nell'erogazione dei servizi digitali;
- il superamento delle logiche di sviluppo frammentario e duplicazione delle funzionalità applicative;
- un incremento dei livelli di sicurezza informatica, in linea con gli standard nazionali.

Attraverso le piattaforme, la Pubblica Amministrazione può implementare flussi di lavoro più efficienti e processi distribuiti standardizzati, favorendo così la realizzazione di servizi digitali omogenei, accessibili e interoperabili.
Nel quadro del presente Piano, OPI Milano Lodi Monza e Brianza intende pertanto consolidare l'adozione delle piattaforme già previste dalle norme nazionali, promuoverne l'utilizzo tra utenti interni ed esterni, integrare nuove funzionalità e garantire l'aggiornamento continuo delle tecnologie e dei protocolli di sicurezza associati.

Lo sviluppo delle infrastrutture digitali rappresenta una componente strategica fondamentale del processo di modernizzazione della Pubblica Amministrazione. Tali infrastrutture devono essere progettate per garantire affidabilità, sicurezza, efficienza energetica e sostenibilità economica, costituendo il fondamento per l'erogazione di servizi pubblici essenziali.
Tuttavia, l'evoluzione tecnologica introduce nuove vulnerabilità, in particolare sotto il profilo della sicurezza informatica e della protezione dei dati personali. L'incremento dell'efficienza e delle performance dei sistemi non può prescindere da un elevato livello di sicurezza e resilienza delle reti e delle infrastrutture digitali impiegate. Infrastrutture carenti in termini di sicurezza, affidabilità o adeguatezza strutturale-organizzativa possono infatti esporre l'amministrazione a gravi rischi: interruzioni dei servizi, perdita o alterazione dei dati, violazioni dell'integrità dei sistemi o accessi non autorizzati a informazioni sensibili.
Alla luce di tale scenario, emerge la necessità di intraprendere un processo di razionalizzazione delle infrastrutture digitali, finalizzato a garantire continuità operativa, protezione dei dati e conformità ai più aggiornati standard di qualità, sicurezza, performance, scalabilità e interoperabilità. In tal senso, risulta strategico valutare anche la migrazione verso infrastrutture cloud qualificate.
In questo contesto si inserisce la *Strategia Cloud Italia*, definita nel settembre 2021 dal Dipartimento per la Trasformazione Digitale in collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), che si articola su tre direttrici principali:

1.. Qualificazione dei fornitori e dei servizi cloud
La qualificazione cloud rappresenta un passaggio obbligato per garantire che i fornitori di servizi cloud pubblici (Cloud Service Provider – CSP) e le relative soluzioni (Infrastructure as a Service – IaaS, Platform as a Service – PaaS, Software as a Service – SaaS) rispettino criteri stringenti di sicurezza, affidabilità e compliance normativa.
Il sistema di qualificazione, introdotto da AGID e ora sotto la supervisione dell'Agenzia per la Cybersicurezza Nazionale (ACN), prevede:

- La verifica della localizzazione dei dati (preferibilmente in UE);
- La continuità operativa e la resilienza infrastrutturale;
- La protezione da attacchi cibernetici e accessi non autorizzati;
- Il rispetto della normativa europea in materia di protezione dei dati personali (GDPR);
- L'adozione di strumenti di crittografia, backup e disaster recovery.

Le PA, incluse le articolazioni provinciali come gli Ordini, possono avvalersi esclusivamente di fornitori e servizi qualificati, a garanzia della piena tutela del patrimonio informativo pubblico.

L'Ordine delle Professioni Infermieristiche di Milano, Lodi, Monza e Brianza si avvale della suite Microsoft 365 per la gestione della posta elettronica, la collaborazione documentale e l'organizzazione delle attività interne. Tale piattaforma garantisce elevati standard di affidabilità, sicurezza e conformità normativa, grazie a sistemi avanzati di protezione dei dati, crittografia end-to-end, backup automatizzati e strumenti di controllo degli accessi. Microsoft 365 è conforme alle principali certificazioni internazionali in materia di sicurezza informatica e protezione dei dati personali (tra cui ISO/IEC 27001, ISO/IEC 27018 e GDPR), offrendo all'Ente un ambiente cloud sicuro e performante per l'erogazione dei propri servizi.

Integrazione dei sistemi e condivisione dei dati

L'integrazione dei sistemi informativi e la condivisione strutturata dei dati rappresentano un pilastro fondamentale per favorire l'interoperabilità digitale tra le pubbliche amministrazioni, i cittadini e le imprese. Tale processo consente di attuare concretamente il principio del *once only*, secondo cui i dati devono essere forniti una sola volta alla Pubblica Amministrazione, e recepisce le indicazioni contenute nell'European Interoperability Framework.

Il riferimento normativo e tecnico per l'interoperabilità è costituito dal Modello di Interoperabilità (ModI), che, fornisce un quadro sistematico di **standard, regole tecniche e metodologie operative** per favorire:

- lo scambio sicuro di dati tra le PA;
- l'implementazione di servizi digitali interoperabili, attraverso l'uso di API (Application Programming Interface);
- la realizzazione del principio once only, evitando richieste ridondanti di informazioni a cittadini e imprese.

Obiettivo finale

Garantire un **sistema digitale pubblico connesso, sicuro, efficiente** e interoperabile, in cui i dati circolino facilmente e i servizi siano integrati, migliorando l'esperienza d'uso per professionisti infermieri e infermieri pediatrici, cittadini e imprese.

Le *Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni*, adottate con Determinazione AGID n. 547 del 1° ottobre 2021, individuano le tecnologie SOAP e REST come standard di riferimento per la realizzazione delle API. Le modalità di implementazione, i pattern e i profili d'uso sono periodicamente aggiornati al fine di:

- recepire le esigenze operative manifestate dalle amministrazioni;
- allinearsi agli standard europei e internazionali, agevolando la realizzazione di servizi digitali transfrontalieri.

Obiettivi

Tipo di API	Descrizione	Esempio pratico
API interna (o privata)	Utilizzata all'interno dell'organizzazione; consente l'integrazione tra software aziendali.	L'OPI di Milano Lodi Monza e Brianza utilizza Microsoft 365, una suite di applicazioni e servizi cloud di Microsoft che include strumenti come Word, Excel, PowerPoint, Outlook e Teams, pensati per la produttività, la collaborazione e la gestione dei documenti, accessibili da qualsiasi dispositivo. Utilizza inoltra Onedrive, un servizio di archiviazione cloud di Microsoft che consente di salvare, sincronizzare e condividere file in modo sicuro, rendendoli accessibili online da PC, smartphone o tablet.
API esterna (o pubblica/Open API)	l'interoperabilità tra enti.	Consentire le Aziende Ospedaliere l'accesso a una piattaforma dedicata, previa autenticazione tramite **SPID professionale**, per la **verifica in tempo reale dello stato di iscrizione** all'Ordine delle Professioni Infermieristiche dei propri dipendenti, in un'ottica di interoperabilità, trasparenza e

Tipo di API	Descrizione	Esempio pratico
		semplificazione amministrativa. (Settembre 2026)
API partner	Accessibile solo a soggetti esterni autorizzati	Albo Unico Nazionale – FNOPI per la gestione amministrativa degli Iscritti (in atto)

Contesto normativo e strategico

L'interoperabilità tra sistemi informativi delle pubbliche amministrazioni rappresenta un pilastro fondamentale per la trasformazione digitale del settore pubblico. Per garantire un'efficace cooperazione digitale tra Enti, cittadini e imprese, le amministrazioni devono operare in conformità a un quadro normativo e strategico ben definito.

Sicurezza informatica

La sicurezza informatica costituisce un pilastro imprescindibile nel processo di digitalizzazione della Pubblica Amministrazione. A seguito dell'entrata in vigore del Decreto-Legge n. 82/2021, le competenze in materia di cybersicurezza e resilienza cibernetica sono state trasferite all'Agenzia per la Cybersicurezza Nazionale (ACN), che rappresenta oggi il principale punto di riferimento istituzionale per la protezione dello spazio digitale nazionale.

A livello strategico, la Strategia Nazionale di Cybersicurezza 2022–2026 e il relativo Piano di implementazione tracciano le direttrici per il rafforzamento della postura di sicurezza dell'intero ecosistema pubblico e privato. In particolare, le misure n. 6, 10, 11, 14, 19, 20, 55, 58, 59, 70 e 71 del Piano contengono indicazioni operative specifiche per le Pubbliche Amministrazioni, incentrate su prevenzione, monitoraggio, risposta agli incidenti, formazione del personale e gestione della supply chain digitale.

Nel contesto attuale, è essenziale garantire non solo la continuità e l'efficienza dei servizi digitali, ma anche la loro sicurezza e resilienza, al fine di rafforzare la fiducia dei professionisti infermieri e infermieri pediatrici, cittadini e delle imprese, inclusi coloro meno familiari con l'uso delle tecnologie digitali. La crescente esposizione mediatica di incidenti informatici e attacchi cyber ha da un lato aumentato la consapevolezza collettiva sul tema, ma dall'altro ha anche generato un diffuso senso di vulnerabilità.

Per contrastare questi rischi è necessario adottare un approccio sistemico e proattivo alla sicurezza cibernetica, fondato su una gestione dinamica e automatizzata del rischio e sull'implementazione dell'architettura Zero Trust. Questo paradigma di sicurezza prevede la verifica continua dell'identità e dell'autorizzazione degli utenti, dei dispositivi e dei servizi, indipendentemente dalla loro posizione.

Questo modello di sicurezza, fondato sull'approccio *Zero Trust*, implica un controllo continuo delle identità e dei livelli di autorizzazione, senza dare mai per scontata la fiducia tra utenti, dispositivi o applicazioni. In tal modo, si riduce significativamente la superficie di attacco, consentendo un contenimento tempestivo di eventuali violazioni e una maggiore protezione del patrimonio informativo.

La sua attuazione efficace richiede una collaborazione sinergica tra tutti i soggetti coinvolti nel sistema digitale dell'Ente: dai dipendenti, dirigenti e responsabili della transizione digitale, agli iscritti e cittadini che fruiscono dei servizi online, fino ai fornitori di soluzioni informatiche e partner tecnologici.

È quindi essenziale affiancare a tale collaborazione una formazione continua, volta ad aggiornare costantemente le competenze digitali del personale e a promuovere comportamenti consapevoli e sicuri nell'utilizzo delle tecnologie. Al contempo, è necessario adottare strumenti evoluti di monitoraggio, prevenzione e difesa, coerenti con le indicazioni dell'Agenzia per la Cybersicurezza

Nazionale (ACN) e con le più recenti best practice europee in materia di protezione dei sistemi informativi.
Solo attraverso un approccio condiviso, proattivo e strutturato sarà possibile garantire un ecosistema digitale affidabile, resiliente e sicuro, capace di sostenere la trasformazione digitale dell'Ordine e rispondere con prontezza alle nuove sfide del cyberspazio.

Obiettivi:

Area	Obiettivo	Azione RTD	Scadenza	KPI
Formazione e consapevolezza	Formazione periodica obbligatoria del personale e Organo Politico	Organizzare corsi annuali di cybersecurity per tutti i dipendenti	Dicembre 2025	% personale formato ≥ 90%
Formazione e consapevolezza	Eseguire simulazioni di attacco informatico	Pianificare test semestrali di phishing e social engineering	Dicembre 2026 (primo ciclo)	≥ 2 simulazioni/anno
Investimenti tecnologici	Aggiornare antivirus e firewall	Sottoscrivere e monitorare licenze di protezione attiva su tutti i dispositivi	Marzo 2026	100% dispositivi protetti
Investimenti tecnologici	Implementare sistemi EDR su tutti i dispositivi critici dell'ente, al fine di garantire monitoraggio continuo, rilevamento avanzato delle minacce e risposta immediata agli incidenti.	Acquisto e distribuzione di soluzioni EDR su endpoint critici	Dicembre 2026	EDR attivo su 100% endpoint critici
Gestione accessi e dati	Applicare il principio del minimo privilegio	Revisione periodica delle autorizzazioni utente	Settembre 2026	100% utenze verificate ogni 12 mesi
Monitoraggio e risposta incidenti	Redigere piano di risposta agli incidenti	Elaborazione e approvazione del piano IR	Novembre 2025	Piano approvato e testato entro deadline
Monitoraggio e risposta incidenti	Effettuare backup regolari e testati	Automatizzare e verificare i backup con cadenza mensile	In corso (verifica ogni mese)	Backup testato con successo ogni 30 giorni

Governare la Transizione Digitale: Ruoli, Responsabilità e Strumenti

La governance dei processi di transizione digitale dell'Ordine delle Professioni Infermieristiche di Milano, Lodi, Monza e Brianza è affidata prioritariamente al Responsabile per la Transizione Digitale (RTD) Veronica Banfi, figura centrale nella pianificazione, nel coordinamento e nel monitoraggio delle iniziative digitali dell'Ente.
Il RTD opera in sinergia con diversi soggetti che, a vario titolo, concorrono alla realizzazione degli obiettivi di digitalizzazione. Tra questi rientrano:

- **Gate Group Srl**, azienda specializzata nella consulenza IT e gestione infrastrutturale, e si occupa di Sistemi informatici, progettazione e realizzazione di infrastrutture

hardware/software, server, notebook, firewall, NAS, backup e soluzioni di sicurezza - Managed Services (MSP): monitoraggio proattivo remoto, assistenza hardware/software, antivirus e servizi cloud;

- **Tender Srl**, è una Digital Company con sede a Meda e Milano, specializzata nella trasformazione digitale delle aziende. Offre servizi integrati di comunicazione strategica, sviluppo di soluzioni informatiche, siti web e assistenza IT. In particolare, supporta i clienti nella progettazione e realizzazione di piattaforme digitali su misura, prestando attenzione all'user experience (UX), alla sicurezza, e alla compliance normativa;
- **Avv. Valeria Fantigrossi**, in qualità di Responsabile della Protezione dei Dati (DPO);
- **Dott.ssa Chiara Venturini**, Consigliere e Responsabile per la Prevenzione della Corruzione e per la Trasparenza (RPCT).

Le iniziative di governance in materia di transizione digitale si articolano attorno a tre assi principali:

- Monitoraggio costante dello stato di attuazione degli interventi previsti nel Piano Triennale;
- Rafforzamento delle competenze digitali del personale attraverso attività formative, strumenti di autovalutazione e valorizzazione delle skill;
- Azioni di coinvolgimento attivo degli iscritti e dei cittadini, finalizzate a migliorare la qualità dei servizi digitali erogati e a promuovere l'interazione attraverso l'utilizzo di tecnologie abilitanti.

Sono attualmente in fase di valutazione ulteriori azioni mirate a:

- strutturare un sistema di obiettivi e indicatori di performance a supporto dell'attuazione del Piano;
- potenziare il coordinamento con gli stakeholder del territorio;
- consolidare il capitale umano attraverso programmi di aggiornamento continuo e valorizzazione delle competenze digitali.

Riferimenti normativi:

Il presente Piano si fonda su un articolato quadro normativo e regolamentare che disciplina i processi di digitalizzazione della Pubblica Amministrazione. In particolare, si richiamano:

- **Legge 9 gennaio 2004, n. 4** – *"Disposizioni per favorire l'accesso degli utenti, in particolare delle persone con disabilità, agli strumenti informatici"*, nota anche come "Legge Stanca".
- **D.P.R. 11 febbraio 2005, n. 68** – *"Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata (PEC), ai sensi dell'art. 27 della legge 16 gennaio 2003, n. 3"*.
- **D. Lgs. 7 marzo 2005, n. 82** – *"Codice dell'Amministrazione Digitale (CAD)"*, che costituisce il riferimento principale per l'organizzazione e l'erogazione dei servizi digitali da parte della PA.
- **DPCM 2 novembre 2005** – *"Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata"*.
- **D.L. 18 ottobre 2012, n. 179**, convertito con modificazioni dalla **L. 17 dicembre 2012, n. 221** – *"Ulteriori misure urgenti per la crescita del Paese"*.
- **D.L. 14 dicembre 2018, n. 135**, convertito con modificazioni dalla **L. 11 febbraio 2019, n. 12** – *"Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione"*.
- **D.L. 9 giugno 2021, n. 80**, convertito con modificazioni dalla **L. 6 agosto 2021, n. 113** – *"Misure urgenti per il rafforzamento della capacità amministrativa delle PA e per l'attuazione del PNRR"*.
- **D.L. 30 aprile 2022, n. 36**, convertito con modificazioni dalla **L. 29 giugno 2022, n. 79** – *"Ulteriori misure urgenti per l'attuazione del PNRR"*.

  Linee guida e regolamenti AGID

- **Linee guida AGID**:
  - sull'acquisizione e il riuso del software per la PA (2019);

- sull'accessibilità degli strumenti informatici (2020);
- sulla formazione, gestione e conservazione dei documenti informatici (2021);
- di design per i siti web e i servizi digitali della PA (2022).

- **Circolari AGID**:
  - n. 2/2018 – *Criteri per la qualificazione dei Cloud Service Provider per la PA*;
  - n. 3/2018 – *Criteri per la qualificazione dei servizi SaaS per la PA*.
- **Manuale di abilitazione al cloud AGID** (2022).
- **Regolamento AGID 2021** – relativo ai livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA, e alle caratteristiche dei servizi cloud (qualità, performance, scalabilità, portabilità).
- **Determinazioni ACN n. 306/2022 e 307/2022** – di attuazione al Regolamento AGID sopra richiamato.
- **Regole tecniche per i servizi di recapito certificato ai sensi del Regolamento (UE) n. 910/2014 (eIDAS)** – standard ETSI – REMPolicy-IT (2022).
  Piano Nazionale di Ripresa e Resilienza (PNRR)

Riferimenti normativi europei:

- **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*.
- **Regolamento (UE) n. 910/2014** del 23 luglio 2014 – *sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS)*, artt. 43 e 44.
- **Regolamento (UE) 2018/1724** del 2 ottobre 2018 – *che istituisce uno sportello digitale unico (Single Digital Gateway) per l'accesso a informazioni, procedure e servizi di assistenza e risoluzione problemi a livello europeo*.

Acronimi

Acronimo	Definizione
AGID	Agenzia per l'Italia Digitale
ANPR	Anagrafe Nazionale della Popolazione Residente
API	Application Programming Interface
ACN	Agenzia per la Cybersicurezza Nazionale
CAD	Codice dell'Amministrazione Digitale
CIE	Carta di Identità Elettronica
FNOPI	Federazione Nazionale Ordini delle Professioni Infermieristiche
OPI	Ordine delle Professioni Infermieristiche
PNRR	Piano Nazionale di Ripresa e Resilienza
RTD	Responsabile per la Transizione Digitale
SPID	Sistema Pubblico di Identità Digitale
PA	Pubblica Amministrazione
PDND	Piattaforma Digitale Nazionale Dati
PSN	Polo Strategico Nazionale
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
eIDAS	Electronic IDentification, Authentication and trust Services
DGC	Digital Green Certificate (Certificazione verde COVID-19)
UNICA	User Needs Interface & Communication Architecture (linee guida per i servizi digitali)
ModI	Modello di Interoperabilità
REM	Registered Electronic Mail (posta elettronica certificata europea)
PEC	Posta Elettronica Certificata
DPO	Data Protection Officer

Normativa di riferimento:

Categoria	Riferimento	Descrizione
Normativa nazionale	D.Lgs. 7 marzo 2005, n. 82	Codice dell'Amministrazione Digitale (CAD)
Normativa nazionale	Legge 9 gennaio 2004, n. 4	Legge Stanca sull'accessibilità
Normativa nazionale	D.P.R. 11 febbraio 2005, n. 68	Regolamento sull'utilizzo della PEC
Normativa nazionale	DPCM 2 novembre 2005	Regole tecniche per la PEC
Normativa nazionale	Legge 11 febbraio 2005, n. 15 e DPR 12 aprile 2006, n. 184	Trasparenza e accesso ai documenti amministrativi
Normativa nazionale	D.L. 18 ottobre 2012, n. 179	Misure urgenti per la crescita del Paese
Normativa nazionale	Legge 183/2011	Decertificazione – Art. 15
Normativa nazionale	DPR 445/2000	Autocertificazione – Artt. 43, 46, 47
Normativa nazionale	DPR 642/1972	Imposta di bollo e tabelle esenzioni
Normativa nazionale	D.L. 14 dicembre 2018, n. 135	Semplificazioni per PA e imprese
Normativa nazionale	D.L. 9 giugno 2021, n. 80	Capacità amministrativa PA e attuazione PNRR
Normativa nazionale	D.L. 30 aprile 2022, n. 36	Attuazione PNRR
Normativa nazionale	D.L. 21 settembre 2019, n. 105	Perimetro sicurezza nazionale cibernetica
Normativa nazionale	DPCM n. 81/2021	Sicurezza cibernetica e infrastrutture critiche
Normativa nazionale	D.L. 14 giugno 2021, n. 82	Istituzione Agenzia per la Cybersicurezza Nazionale (ACN)
Normativa nazionale	Delibera AGID n. 547 del 1° ottobre 2021	Linee guida sull'interoperabilità tecnica
Normativa europea	Regolamento (UE) 2016/2102	Accessibilità siti web e app PA
Normativa europea	Regolamento (UE) n. 910/2014 (eIDAS)	Identificazione elettronica e servizi fiduciari
Normativa europea	Regolamento (UE) 2018/1724	Single Digital Gateway (SDG)
Normativa europea	European Interoperability Framework (EIF)	Linee guida interoperabilità a livello UE
Normativa europea	Regole tecniche REM (2022)	Servizi di recapito certificato europeo
Strategie e piani nazionali	Piano Triennale per l'Informatica nella PA	Strategia nazionale digitalizzazione PA
Strategie e piani nazionali	Strategia Nazionale di Cybersicurezza 2022–2026	Obiettivi e misure per la sicurezza cibernetica
Strategie e piani nazionali	Piano Nazionale di Ripresa e Resilienza (PNRR)	Finanziamenti per la trasformazione digitale
Strategie e piani nazionali	Strategia Cloud Italia (2021)	Adozione cloud, interoperabilità e PSN
Linee guida AGID	Linee guida 2019	Acquisizione e riuso del software
Linee guida AGID	Linee guida 2020	Accessibilità strumenti informatici
Linee guida AGID	Linee guida 2021	Gestione e conservazione documenti informatici
Linee guida AGID	Linee guida 2022	Design per siti web e servizi PA
Circolari AGID	Circolare n. 2/2018	Qualificazione Cloud Service Provider (CSP)
Circolari AGID	Circolare n. 3/2018	Qualificazione servizi SaaS
Manuale AGID	Manuale abilitazione al cloud (2022)	Guida tecnica per le PA
Regolamento AGID	Regolamento 2021	Sicurezza, capacità, risparmio e affidabilità delle infrastrutture
Regolamenti attuativi ACN	Determinazioni ACN n. 306/2022 e 307/2022	Requisiti tecnici e standard per infrastrutture PA

Glossario:

Once Only

è un concetto chiave della trasformazione digitale della Pubblica Amministrazione, promosso anche a livello europeo (in particolare dalla **Strategia per il Mercato Unico Digitale** e dal **Regolamento UE 2018/1724** sullo sportello digitale unico).
Il principio "Once Only" stabilisce che:
Il cittadino, l'impresa o un'altra amministrazione non debba fornire più volte la stessa informazione alla Pubblica Amministrazione.
Se un'informazione è già stata fornita a una PA (ad esempio il codice fiscale, il domicilio digitale, il titolo di studio o un certificato), questa deve essere **riutilizzata** e **condivisa internamente** fra amministrazioni autorizzate, **senza richiedere nuovamente i dati al soggetto interessato**.
Obiettivi principali

- **Semplificare** i rapporti tra cittadini/imprese e la PA.
- **Ridurre il numero di adempimenti** e le richieste di documenti.
- **Evitare duplicazioni e errori** nelle banche dati pubbliche.
- **Migliorare l'efficienza interna** degli enti pubblici grazie all'interoperabilità.

Come si applica
Per attuare il principio Once Only, è necessaria:

- **Interoperabilità tra banche dati** delle PA (es. ANPR, INPS, Agenzia delle Entrate, Ordini professionali…);
- **Uso di piattaforme digitali** come SPID, CIE, ANPR, PDND (Piattaforma Digitale Nazionale Dati);
- **Adozione di API** (interfacce di programmazione) sicure e standardizzate;
- **Norme chiare su privacy e sicurezza**, secondo il GDPR e le direttive nazionali.

Cosa fa un'API?

Un'API è un insieme di **regole e strumenti** che permette a **due sistemi software diversi** di **comunicare tra loro**. L'interazione avviene in modo **automatico**, senza intervento umano, e consente **lo scambio di dati e comandi** in tempo reale.
Le API sono fondamentali per:

- migliorare l'integrazione tra sistemi,
- ridurre ridondanze nei processi informatici,
- accelerare lo sviluppo di nuovi servizi digitali.

Cloud First nella digitalizzazione della PA

Il principio **Cloud First** significa che ogni nuovo servizio digitale della Pubblica Amministrazione deve essere pensato e realizzato **direttamente in cloud**.
L'obiettivo è rendere i servizi pubblici **più veloci, sicuri, facili da gestire** e **più economici**. Le PA devono quindi **spostare i propri sistemi** su infrastrutture cloud sicure e certificate, come previsto dal **Piano Triennale per l'informatica nella PA** e dal **PNRR**.

Digital & Mobile First

I servizi pubblici devono essere progettati fin dall'inizio in modalità completamente digitale e ottimizzati per l'utilizzo su dispositivi mobili. Questo approccio garantisce un accesso semplice, rapido e moderno ai servizi, in linea con le abitudini digitali dei cittadini.

Digital Identity Only

L'accesso ai servizi digitali deve avvenire esclusivamente tramite strumenti di identità digitale riconosciuti, come **SPID** e **CIE**, assicurando la conformità alla normativa vigente e una maggiore sicurezza nelle interazioni online tra cittadini e PA.

Servizi inclusivi e accessibili

Tutti i servizi digitali devono essere progettati per essere **accessibili a tutti**, comprese le persone con disabilità o con ridotte competenze digitali, promuovendo l'**inclusione digitale** e rispettando le **linee guida sull'accessibilità** (es. WCAG, AgID).

Dati pubblici come bene comune

I dati prodotti e gestiti dalla PA devono essere considerati una **risorsa strategica**. Devono essere pubblicati in **formato aperto e interoperabile**, per favorirne il riutilizzo da parte di cittadini, imprese e altri enti, nel rispetto delle norme sulla protezione dei dati.

Interoperabilità by Design

I servizi devono essere nativamente progettati per **dialogare con altri sistemi pubblici e privati** tramite **API standardizzate**, promuovendo un ecosistema digitale integrato, efficiente e orientato alla collaborazione tra enti.

Sicurezza e Privacy by Design

Fin dalla fase di progettazione, i servizi devono integrare **misure di sicurezza informatica** e garantire la **protezione dei dati personali**, secondo il principio del "**Privacy by Design e by Default**" previsto dal GDPR.

User-Centric, Data-Driven e Agile

Lo sviluppo dei servizi deve essere orientato all'**esperienza dell'utente**, utilizzando un approccio **agile** e iterativo, supportato da **analisi dei dati di utilizzo** per migliorare continuamente prestazioni, accessibilità e qualità dei servizi.

Transfrontaliero by Design

I servizi digitali devono essere concepiti per poter essere **utilizzati anche a livello europeo**, facilitando la **mobilità dei cittadini e delle imprese** all'interno dell'Unione e contribuendo alla **realizzazione del Mercato Unico Digitale**.

Software Open Source

Le PA devono preferire l'adozione o lo sviluppo di **soluzioni open source**, garantendo la **trasparenza**, la **riutilizzabilità del codice** e la **condivisione delle soluzioni** sviluppate, in linea con i principi di economicità e sostenibilità.

Supply chain digitale

La *supply chain digitale* è l'evoluzione tecnologica della catena di approvvigionamento tradizionale, in cui i processi logistici, produttivi e distributivi sono integrati e automatizzati attraverso l'uso di tecnologie digitali come **IoT**, **intelligenza artificiale**, **blockchain**, **cloud** e **big data**. Questa trasformazione consente una **visibilità in tempo reale**, una maggiore **efficienza operativa**, una **collaborazione più stretta** tra attori e una **risposta più rapida** ai cambiamenti della domanda o alle criticità lungo la filiera. Le PA devono preferire l'adozione o lo sviluppo di **soluzioni open source**, garantendo la **trasparenza**, la **riutilizzabilità del codice** e la **condivisione delle soluzioni** sviluppate, in linea con i principi di economicità e sostenibilità.

Attacchi cyber

Gli *attacchi cyber* (o attacchi informatici) sono azioni malevole condotte attraverso strumenti digitali con l'obiettivo di **compromettere, danneggiare, violare o sottrarre dati, sistemi e infrastrutture informatiche**.
Possono essere rivolti a individui, aziende o istituzioni pubbliche, e includono tecniche come **phishing**, **malware**, **ransomware**, **furto di credenziali**, **DDoS** (Distributed Denial of Service) e **violazioni di rete**.
La crescente digitalizzazione rende le organizzazioni sempre più esposte, rendendo fondamentale adottare misure di **cybersicurezza** per prevenire, rilevare e contrastare tali minacce.

Architettura Zero Trust

L'*architettura Zero Trust* è un modello di sicurezza informatica basato sul principio **"mai fidarsi, verificare sempre"**.
A differenza degli approcci tradizionali, che considerano attendibili gli utenti e i dispositivi interni alla rete, Zero Trust **non presume mai la fiducia automatica** e richiede una **verifica continua dell'identità, del contesto e del livello di rischio**, per ogni accesso a risorse e dati, anche all'interno del perimetro aziendale.
Questa architettura si fonda su:
Autenticazione e autorizzazione rigorose (es. autenticazione multifattoriale)
Segmentazione della rete e controllo granulare degli accessi
Monitoraggio costante e analisi dei comportamenti
Minimizzazione del privilegio (principio del minimo privilegio)
L'approccio Zero Trust è oggi considerato essenziale per **proteggere ambienti digitali complessi e distribuiti**, in particolare in contesti cloud, lavoro da remoto e interconnessione tra sistemi pubblici e privati.

Data-driven

significa **basare le scelte su dati concreti**, piuttosto che su intuizioni, consuetudini o valutazioni soggettive. In un'organizzazione pubblica o privata, ciò comporta:

- **Raccogliere e analizzare dati in modo continuo** (es. dati di accesso a un sito, feedback degli utenti, performance operative).
- **Utilizzare i dati per comprendere i bisogni degli utenti**, monitorare le attività e orientare le politiche.
- **Condividere i dati in modo trasparente e interoperabile** tra sistemi e soggetti diversi, nel rispetto della privacy.

Disaster Recovery (DR) – Cos'è

Il Disaster Recovery è l'insieme di misure tecniche, organizzative e procedurali messe in atto da un'organizzazione per ripristinare rapidamente sistemi informatici, dati e servizi digitali in caso di eventi critici o disastrosi.

Questi eventi possono essere:

- Guasti hardware o software gravi
- Attacchi informatici (es. ransomware)
- Blackout elettrici prolungati
- Incendi, alluvioni, terremoti
- Errore umano irreversibile

Crittografia End-to-End (E2EE) – Cos'è

La crittografia end-to-end (E2EE) è una tecnica di protezione dei dati che garantisce che le informazioni siano leggibili solo dal mittente e dal destinatario, impedendo a chiunque altro (inclusi fornitori di servizi, hacker o soggetti terzi) di accedervi durante la trasmissione.
Come funziona
I dati vengono crittografati sul dispositivo del mittente (es. computer, smartphone).
Viaggiano su Internet in forma cifrata (illeggibile).
Vengono decrittati solo sul dispositivo del destinatario, che possiede la chiave corrispondente.

Soap e Rest

SOAP (Simple Object Access Protocol)
SOAP è un protocollo standardizzato per la comunicazione tra applicazioni via Internet, che:

- Usa **XML** per formattare i messaggi
- Funziona tramite protocolli come **HTTP**, **SMTP**, ecc.
- Prevede una struttura **rigida** e **formalizzata**
- Include caratteristiche come **sicurezza avanzata**, **transazioni**, **messaggi firmati**, ecc.

REST (Representational State Transfer)
REST è uno stile architetturale più leggero e flessibile, basato sullo scambio di dati attraverso **HTTP**.
Utilizza:

- Formati di dati come **JSON**, **XML**, **HTML**
- Le classiche operazioni web: **GET**, **POST**, **PUT**, **DELETE**

PIANO DI GESTIONE DELLA CYBERSICUREZZA

Allegato al Piano di Digitalizzazione dell'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza

Nota di accompagnamento

Il presente documento raccoglie le misure adottate dall'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza, in materia di cybersicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione, dal Codice dell'Amministrazione Digitale e dalle linee guida in materia di sicurezza informatica. Contiene una sezione di governance, le procedure operative per la gestione degli incidenti e la prevenzione del rischio, nonché i moduli necessari per l'attuazione delle misure previste. Tutti i contenuti sono soggetti a revisione annuale e aggiornamento continuo da parte del RTD.

Governance della Cybersicurezza

Nel nostro Ente la gestione della cybersicurezza è disciplinata secondo un modello di governance distribuito e coordinato. In caso di evento o incidente informatico:
- Il Responsabile della Transizione Digitale (RTD) Veronica Banfi assume il coordinamento operativo.
- Il Responsabile dei Sistemi Informativi (RSI), Gate Group Srl attiva le misure tecniche di contenimento.
- Il DPO Avv. Valeria Fantigrossi viene informato in caso di potenziale violazione di dati personali.
- Il Presidente Dott. Pasqualino D'Aloia viene aggiornato in caso di eventi critici.

Tutte le attività sono tracciate in registri interni.

Piano per la Notifica degli Incidenti

La procedura per la gestione degli incidenti prevede:
- Segnalazione tramite modulo dedicato.
- Analisi tecnica e redazione della scheda evento.
- Notifica al Garante in caso di data breach.
- Comunicazione interna ai soggetti coinvolti.

Piano di Prevenzione del Rischio Cyber

L'Ordine delle Professioni Infermieristiche di Milano Lodi Monza e Brianza adotta un approccio proattivo basato su:
- Analisi del rischio annuale.
- Verifica mensile degli aggiornamenti.
- Test periodici di backup e DRP.
- Formazione obbligatoria per il personale.
- Politiche di sicurezza documentate e aggiornate.

Indicatori di monitoraggio

- Numero incidenti gestiti
- Tempi medi di risposta
- Partecipazione alla formazione
- Esito test backup/DRP

Prossimi sviluppi

- Adesione a CSIRT Italia
- Introduzione MFA
- Portale interno per segnalazioni

Allegato 1 – Modulo di Segnalazione Incidente Informatico

Da compilare a cura del personale o collaboratore che rileva o sospetta un incidente informatico.

Nome e Cognome del Segnalante:
Ruolo/Ufficio
Data e Ora dell'Evento
Descrizione dell'Evento:
Sistema o Servizio coinvolto
Azione già intraprese:
Altre informazioni utili:

Firma del segnalante: _____

Data: _____

Allegato 2 – Scheda Evento e Valutazione

Da compilare a cura del RTD (Responsabile della Transizione Digitale) e RSI (Responsabile dei Sistemi Informativi)

N. Evento
Data Ricezione segnalazione:
Sintesi tecnica dell'Evento:
Livello di rischio (basso/medio/alto/critico)
Impatto su dati personali (si/no)
Azioni correttive adottate:

Comunicazioni effettuate:
[ ] DPO [ ] Garante Privacy [ ] Presidenza/Direzione [ ] Personale

Firma Responsabile: _____

Data: _____

Allegato 3 – Registro Test Backup e DRP (Disaster Recovery Plan)

Data Test	Tipo di Test (Backup / DRP)	Esito	Note	Firma Responsabile

Legenda:

Data del test: inserire la data in cui è stato effettuato il test.

Tipo di test: indicare se si tratta di test di **ripristino da backup** o test del **piano di disaster recovery**.

Esito del test: valutazione sintetica del risultato (superato, fallito, parzialmente riuscito).

Note: inserire eventuali problemi riscontrati, azioni correttive adottate, anomalie emerse o suggerimenti.

Allegato 4 – Estratto Politiche di Sicurezza Informatica

Le seguenti misure costituiscono il nucleo operativo delle politiche di sicurezza informatica adottate dall'Ente. Esse sono obbligatorie per tutto il personale, dipendenti e collaboratori che utilizzano sistemi digitali o accedono a dati istituzionali.

- Autenticazione obbligatoria con credenziali personali;
- Attivazione MFA per servizi critici;
- Divieto di utilizzo di dispositivi personali per accesso a dati sensibili;
- Obbligo di blocco postazione in assenza;
- Aggiornamenti mensili dei software di sicurezza;
- Segnalazione immediata di anomalie o accessi sospetti.

1. Autenticazione obbligatoria con credenziali personali

Tutti gli utenti devono accedere ai sistemi informativi utilizzando **credenziali individuali (username e password)**, assegnate nominalmente. È vietato l'utilizzo condiviso di account. Le password devono rispettare requisiti minimi di complessità (lunghezza, caratteri speciali, maiuscole/minuscole) e devono essere modificate con cadenza regolare (almeno ogni 6 mesi).

2. Attivazione dell'autenticazione a più fattori (MFA) per i servizi critici

Per tutti i servizi che trattano dati sensibili, personali o strategici (es. PEC, piattaforme di gestione documentale, portali cloud, gestione Albo, anagrafiche), è prevista l'**attivazione obbligatoria del sistema MFA (Multi-Factor Authentication)**. L'accesso a questi sistemi sarà possibile solo previa verifica tramite secondo fattore (es. OTP via app, token o SMS).

3. Divieto di utilizzo di dispositivi personali per accesso a dati sensibili

È fatto **divieto assoluto di utilizzare dispositivi personali** (PC, tablet, smartphone) per accedere o trattare dati istituzionali o sensibili, salvo nei casi espressamente autorizzati e regolati da policy BYOD (Bring Your Own Device). Tutte le attività devono avvenire tramite postazioni ufficiali o dispositivi gestiti e protetti dall'Ente.

4. Obbligo di blocco della postazione in caso di assenza

In caso di assenza anche temporanea dalla postazione di lavoro, l'utente è tenuto a **bloccare immediatamente lo schermo del computer** per evitare accessi non autorizzati. In caso di inadempienza, potranno essere applicate sanzioni disciplinari. I sistemi devono inoltre essere configurati per il blocco automatico dopo 5-10 minuti di inattività.

5. Aggiornamenti mensili dei software di sicurezza

Tutti i dispositivi informatici devono essere **mantenuti aggiornati**. Il Responsabile dei Sistemi Informativi garantisce l'installazione regolare degli aggiornamenti di sicurezza (patch) per sistemi operativi, antivirus, firewall e applicativi principali, almeno **una volta al mese** o in caso di vulnerabilità critiche segnalate da CSIRT Italia o ACN.

6. Segnalazione immediata di anomalie o accessi sospetti

Qualsiasi anomalia tecnica, comportamento inusuale del sistema, accesso sospetto o messaggio anomalo (es. phishing) deve essere **segnalato tempestivamente all'RTD o all'Ufficio Sistemi Informativi** mediante il modulo di segnalazione. La tempestività nella comunicazione è fondamentale per limitare eventuali danni o violazioni.

Nota: Il documento integrale delle *Politiche di Sicurezza Informatica*, comprensivo di misure tecniche e organizzative, livelli di classificazione delle minacce e piano di risposta, è consultabile presso l'**Ufficio del RTD** o, su richiesta, presso la **Presidenza dell'Ordine delle Professioni Infermieristiche di MI Lo Mb**