Comando Generale dell'Arma dei Carabinieri

III Reparto – SM – Ufficio Sviluppo Tecnologico

PIANO TRIENNALE PER L'INFORMATICA

2024 - 2026

ARMA DEI CARABINIERI

INDICE

ACRONIMI E GLOSSARIO

ACRONIMO	DESCRIZIONE
AgID	Agenzia per l'Italia Digitale
ACN	Agenzia per la Cybersicurezza Nazionale
AD	Amministrazione Difesa
AI	Artificial Intelligence
API	Application Programming Interface
AR	Augmented Reality
CAD	Codice dell'Amministrazione Digitale
CERT	Computer Emergency Response Team
CESIT	Centro Sicurezza Telematica
CIE	Carta d'Identità Digitale
DC	Data Center
D.L.	Decreto Legge
DR	Disaster Recovery
F.A.	Forza Armata
F.F.A.A.	Forze Armate
ICT	Information and Communication Technology
IoT	Internet of Things
ISR	Intelligence, Surveillance & Reconnaissance
MR	Mixed Reality
NGEU	Next Generation European Union
NGPA	Next Generation Pubblica Amministrazione
NPL	Natural Processing Language
PA	Pubblica Amministrazione
PP.AA.	Pubbliche Amministrazioni
PNRR	Piano Nazionale di Ripresa e Resilienza
PTI	Piano Triennale per l'Informatica
QR	Quick Response
RRF	Recovery and Resilience Facility
RTD	Responsabile della Transizione Digitale
SGD/DNA	Segretariato Generale della Difesa/Direzione Nazionale Armamenti
SMD	Stato Maggiore della Difesa
SOC	Security Operations Center
SPID	Sistema Pubblico di Identità Digitale
VR	Virtual Reality
XR	Extended Reality
DevSecOps	Development, Security e Operations

1 PREMESSA

Il presente documento ha l'obiettivo principale di delineare il Piano per l'informatica, per il triennio 2024 – 2026 dell'Arma dei Carabinieri, andando a definire le linee di intervento e i progetti già attivi e quelli da attivare.

L'informatica ricopre un ruolo fondamentale all'interno delle organizzazioni e delle Pubbliche Amministrazioni in generale. Una lungimirante strategia di evoluzione dell'informatica consente di innovare le attività e i procedimenti interni, di ripensare e migliorare l'erogazione dei servizi e permette di aprire nuovi canali di comunicazione e spazi di condivisione, sia verso l'interno sia verso l'esterno, oltre che di generare valore. Per questo motivo, le tecnologie **ICT** (*Information* and *Communication Technologies*) vanno considerate come strumenti e fattori abilitanti il cambiamento ed è quindi strategico il modo in cui esse vengono utilizzate e gli investimenti che vengono effettuati per adottarle.

Nei capitoli successivi è descritto in modo dettagliato il contesto in cui si sviluppa il Piano triennale, la cui definizione deve tener conto delle normative, dei regolamenti e delle linee programmatiche, non escludendo la possibilità di approfondire nuovi paradigmi tecnologici organizzativi in cui si evidenziano elementi capaci di condizionare e garantire la progettazione di soluzioni innovative per l'Arma dei Carabinieri, in modo da poter aspirare ad un modello **ICT** efficiente ed efficace per tutti i suoi utenti.

Tale approccio risulta fondamentale per garantire una trasformazione digitale sostanziale, che non miri esclusivamente al miglioramento di quanto già in essere, limitandosi così a recuperare ulteriori margini di efficienza, ma che si ponga l'obiettivo di aggiornare i servizi offerti, allineandoli agli *standard* di riferimento della *customer experience*, in un contesto caratterizzato da un'utenza numerosa, con esigenze molteplici, peculiari e di difficile gestione compartimentale e verticale.

Il Piano triennale per l'informatica, dunque, si prefigge la finalità di abilitare la trasformazione digitale sfruttando l'intera gamma delle opportunità offerte dalle nuove tecnologie [*Cloud*, *cybersecurity*, architetture dati, *blockchain*, IoT (*Internet of Things*), ecc.]. Allo stesso tempo, presuppone un rinnovamento culturale e ordinamentale, in chiave "*digitale*", dell'Arma dei Carabinieri, incentrato sulle persone e basato sulla più ampia condivisione di un modello che, per essere attuato, mantenuto ed evoluto nel tempo, non può prescindere da una coscienza organizzativa consapevole delle potenzialità e delle necessità di un processo di trasformazione così complesso, radicale e sfidante.

Il documento è stato redatto definendo le linee di intervento necessarie a tracciare un percorso che, in linea con gli indirizzi di riferimento delineati da AgID e dal Piano Triennale per l'Informatica nella Pubblica Amministrazione, tenga in considerazione lo stato dell'arte dell'**ICT** dell'Arma dei Carabinieri – in termini di servizi, applicazioni, *governance* e infrastrutture.

2 CONTESTO NORMATIVO

Il presente capitolo si propone di delineare il quadro normativo nazionale di riferimento sulla transizione digitale e le iniziative introdotte per il miglioramento dei processi della PA, elencando le principali disposizioni.
In sintesi, le **P**ubbliche **A**mministrazioni **C**entrali **(PAC)** e le **P**ubbliche **A**mministrazioni **L**ocali **(PAL)**, con il **P**iano **T**riennale per l'**I**nformatica **(PTI)** redatto, con aggiornamenti periodici, dall'**Ag**enzia per l'**I**talia **D**igitale **(AgID)** e con le **Linee Guida** della stessa Agenzia, nonché con gli interventi dell'**A**genzia per la **C**ybersicurezza **N**azionale **(ACN)**, dispongono già di un indirizzo strategico di alto livello, le cui discendenti azioni, sempre nel solco tracciato dalle norme contenute nel **C**odice **A**mministrazione **D**igitale **(CAD)**, potranno concretizzarsi anche grazie alle risorse derivanti dal **P**iano **N**azionale di **R**ipresa e **R**esilienza **(PNRR)**.

Codice dell'Amministrazione Digitale (CAD)

Il **CAD**, emanato con il D.Lgs. 7 marzo 2005, n. 82, è il testo unico delle norme riguardanti l'informatizzazione della PA nei processi interni, nonché nei rapporti con i cittadini e le imprese.
Solo per brevità, si segnala, quale norma significativa, l'art. 17 che, nel prevedere la figura del **R**esponsabile per la **T**ransizione **D**igitale **- RTD** (per l'Arma, con specifico atto di nomina del Ministro della Difesa, è stato individuato il Capo del III Reparto *pro-tempore*), ne stabilisce anche i compiti, relativi, tra l'altro, a:

- indirizzo e coordinamento strategico dello sviluppo dei sistemi informativi e dei servizi forniti dall'Amministrazione, nonché della relativa pianificazione finanziaria, nel rispetto del Piano Triennale e delle Linee guida dell'AgID;
- indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica;
- analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, per ridurre, in particolare, tempi e i costi dell'azione amministrativa;
- promozione delle iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e il punto di accesso telematico.

Le funzioni sopraindicate sono state ulteriormente estese dal Ministro per la Pubblica Amministrazione con la Circ. n. 3 del 1° ottobre 2018, la quale, in ragione della trasversalità della figura, ha suggerito di attribuirle il potere/dovere di:

- costituire tavoli di coordinamento con gli altri dirigenti dell'amministrazione;
- prevedere gruppi tematici per singole attività e/o adempimenti (ad esempio: pagamenti informatici, piena implementazione di SPID, gestione documentale, apertura e pubblicazione dei dati, accessibilità, sicurezza, ecc.);
- proporre l'adozione di circolari e atti di indirizzo sulle materie di propria competenza (ad esempio, in materia di approvvigionamento di beni e servizi ICT);
- predisporre l'adozione dei più opportuni strumenti di raccordo e consultazione del RTD con le altre figure coinvolte nel processo di digitalizzazione della PA (responsabili per la gestione, responsabile per la conservazione documentale, responsabile per la prevenzione della corruzione e della trasparenza, responsabile per la protezione dei dati personali);
- redigere il Piano triennale per l'informatica della singola amministrazione, nelle forme e secondo le modalità definite dall'Agenzia per l'Italia Digitale;

- stilare una relazione annuale sull'attività svolta da trasmettere al vertice politico o amministrativo che lo ha nominato;
- rappresentare la propria organizzazione, quale punto di contatto con la Presidenza del Consiglio dei Ministri per le questioni afferenti alla materia in questione.

È di tutta evidenza, quindi, l'importanza del ruolo ricoperto dal RTD, il quale, proprio in ragione delle responsabilità attribuitegli, è chiamato ad intervenire in ogni processo decisionale della propria amministrazione. In sostanza, la volontà politica sottesa dai provvedimenti normativi di settore ha determinato un cambio di paradigma nella PA: l'informatica, non è più vista come un settore logistico-approvvigionativo, ambito, comunque, importante, ma come componente qualificante della *vision* istituzionale.

Piano Nazionale di Ripresa e Resilienza (PNRR)

Il **P**iano **N**azionale di **R**ipresa e **R**esilienza (**PNRR**) garantirà risorse economiche per 191,5 Mld di euro, da impiegare nel periodo 2021-2026.

Il Piano, che si sviluppa intorno a tre assi strategici ("*digitalizzazione e innovazione*", "*transizione ecologica*" e "*inclusione sociale*"), prevede, tra le molteplici riforme orizzontali, quella della PA ritenuta elemento centrale per il rilancio economico del Paese e volano della sua modernizzazione.

In particolare, nella componente denominata *"eGov"* (*Digitalizzazione e innovazione della PA*), sono previsti fondi per 9,72 Mld di €. Questa misura contribuirà in maniera determinante a supportare la strategia di digitalizzazione in corso, erogando finanziamenti per progetti specifici che dovranno necessariamente essere concepiti in armonia con le disposizioni del CAD e di tutte le altre normative e Linee guida pubblicate dall'AgID. In questa sezione, la quota di investimento più rilevante, è rappresentata da *"Digitalizzazione PA"* alla quale sono destinati 6,14 Mld di € (tale asse prevede, tra l'altro, interventi a *sostegno della migrazione in Cloud dei DC fisici e azioni in tema di Cybersecurity, settore ritenuti di interesse istituzionale e nell'ambito dei quali sono stati destinati all'Arma 50M€, 39 dei quali per il miglioramento della postura di sicurezza cibernetica e 11 per la migrazione verso il Cloud Nazionale – PSN di alcuni servizi ritenuti essenziali – nello specifico il sistema di gestione documentale denominato C-Prot e la piattaforma logistico-amministrativa-contabile C-UNICO*) a testimonianza del sempre più importante impulso che le politiche di investimento stanno convogliando verso il *driver* dell'innovazione tecnologica e digitale.

Piano Triennale per l'Informatica nella Pubblica Amministrazione (PTI)

Il **P**iano **T**riennale per l'**I**nformatica (**PTI**) nella Pubblica Amministrazione 2022-2024, redatto da AgID e pubblicato il 23 gennaio 2023, quale evoluzione delle due precedenti edizioni, è uno strumento essenziale per sostenere la trasformazione digitale del Paese. La strategia contenuta nel documento è pienamente coerente con il Piano di azione europeo sull'*e-Government*. In particolare, sono declinati, in ottica prospettica, gli interventi da porre in essere da parte della PA, gli obiettivi da raggiungere e i risultati attesi. Il modello, ormai consolidato, si poggia su due livelli trasversali – l'interoperabilità e la sicurezza dei sistemi informativi - e su livelli verticali relativi a tematiche quali servizi, dati, piattaforme e infrastrutture:

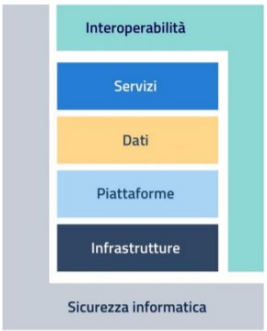

Figura 1: Modello AgID per PTI

Per ciascuno di questi elementi costitutivi, AgID ha previsto una serie di obiettivi e di attività in carico alle singole PA, che sono diventati per l'Arma dei Carabinieri parte integrante della strategia per uno sviluppo sostenibile che porti un miglioramento della produttività e dell'efficienza della propria azione quotidiana a favore dei cittadini.

Nello specifico, il PTI 2022-2024 si pone i seguenti obiettivi e *target*:

- **favorire lo sviluppo di una società digitale**, dove i servizi mettono al centro i cittadini e le imprese, attraverso la digitalizzazione della PA 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.

In tale contesto, AgID ha identificato undici principi guida che le PA dovranno osservare:

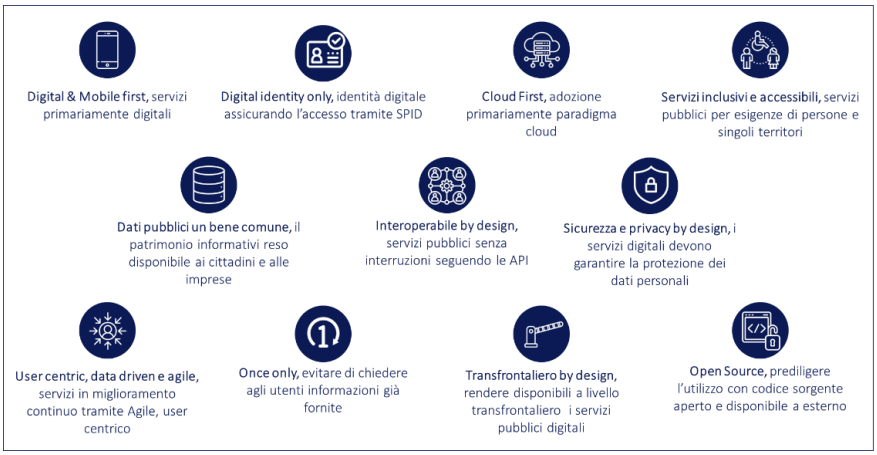

Figura 2: Principi AgID

Oltre ad elaborare gli undici principi a supporto delle PA per guidarle nel processo di trasformazione, AgID ha, tra l'altro, redatto, **con Determinazione n. 628/2021,** un **Regolamento** orientato a disciplinare operativamente le infrastrutture e i servizi Cloud delle PA in relazione alle caratteristiche e ai requisiti minimi richiesti per la migrazione al Cloud. Lungo tale direzione, l'Arma dei Carabinieri, al netto di eventuali vincoli interni e/o di carattere normativo, può valutare l'attivazione del suo **percorso di migrazione al *Cloud*,** in modo sicuro ed efficiente, facendo riferimento al sopracitato atto e in generale alla *Strategia Cloud Italia* **realizzata dal Dipartimento per la Trasformazione Digitale e dall'ACN.**

3 IL PIANO TRIENNALE

3.1 *FRAMEWORK* PER LA COSTRUZIONE DEL PIANO TRIENNALE

L'Ufficio Sviluppo Tecnologico ha definito un *framework* che identifica:

- gli elementi che favoriscono la creazione del Piano, ovvero il quadro normativo e le esigenze organizzative interne, le esigenze IT e i *driver* che guidano nell'innovazione ICT dell'Arma dei Carabinieri:
- i contenuti principali del Piano stesso, ovvero il modello logico infrastrutturale a tendere, gli ambiti di intervento declinati poi in interventi progettuali, da attuarsi secondo una roadmap di implementazione che identifica tempi e risultati, la *Governance* ICT.

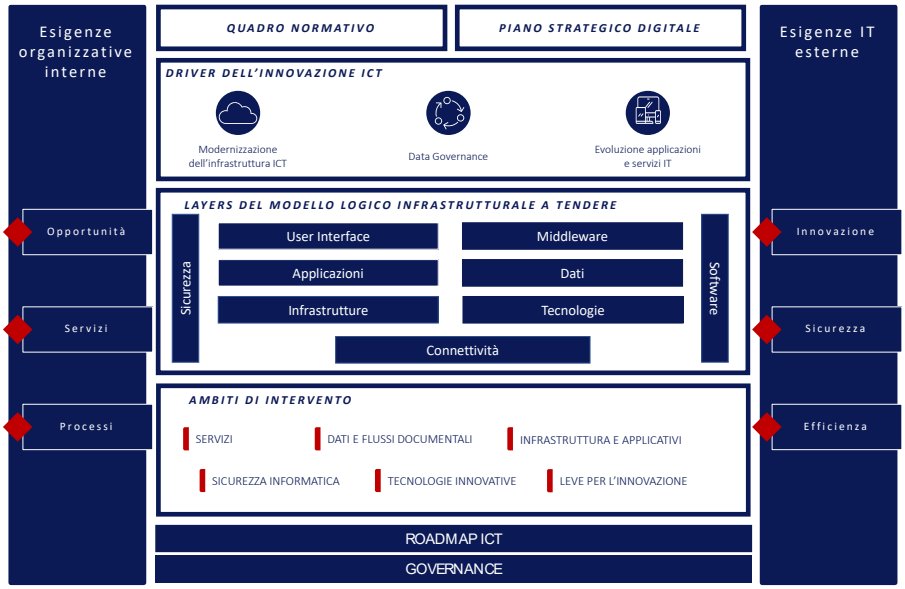

Figura 3: Framework metodologico del Piano Triennale

Il Piano Triennale è costruito a partire dalle evoluzioni in ambito tecnologico e digitale, promosse e suggerite dall'attuale quadro normativo, nonché dai relativi programmi di trasformazione organizzativa, operativa e tecnologica:

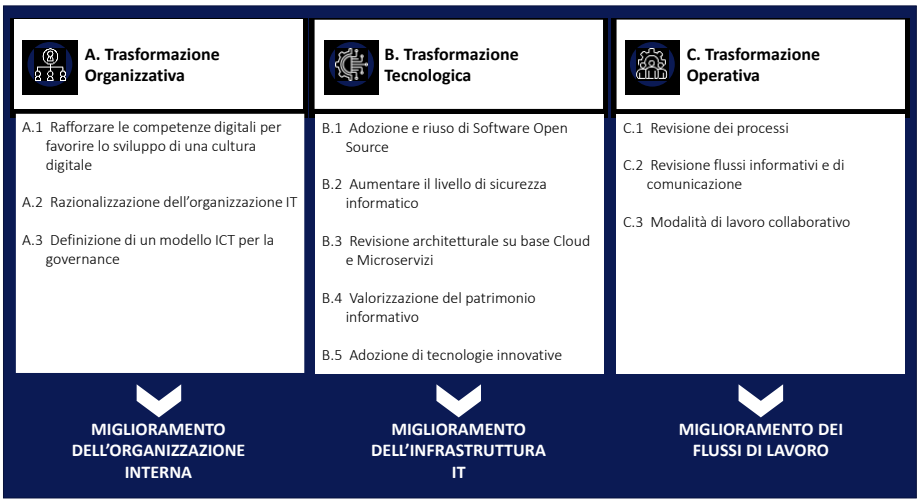

Figura 4: Programmi di intervento dell'Arma dei Carabinieri

Il documento individua obiettivi ben precisi riguardanti la:
- **Trasformazione Organizzativa:** potenziare le competenze e le conoscenze e, al tempo stesso, efficientare i modelli di lavoro, la struttura organizzativa e la governance in ambito ICT;
- **Trasformazione Tecnologica**: progettare nuovi servizi e migliorare quelli esistenti, mediante l'introduzione di nuove tecnologie abilitanti;
- **Trasformazione Operativa:** razionalizzare i processi, i flussi informativi e le modalità di lavoro, al fine di migliorare l'efficienza e la qualità dei servizi digitali che il Comando Generale dell'Arma dei Carabinieri eroga, a vantaggio degli utenti interni ed esterni (cittadini e altre PA).

Il Piano triennale ICT è, altresì, il risultato delle esigenze e richieste di miglioramento, emerse durante l'analisi eseguita sull'organizzazione e sul modello logico infrastrutturale dei sistemi informativi, attualmente utilizzati dall'Arma dei Carabinieri. Tali esigenze possono essere classificate in:

a. **Esigenze organizzative interne**: ovvero esigenze provenienti dall'Arma dei Carabinieri e relative alla definizione di iniziative di sviluppo, a supporto dell'organizzazione interna, che possono nascere da:
   - individuazione di nuove **opportunità** di mercato in ambito tecnologico, che consentono di sviluppare e migliorare l'infrastruttura ICT;
   - necessità di creazione di nuovi **servizi** digitali sia interni che esterni o di evoluzione tecnologica dei servizi esistenti;
   - necessità di miglioramento dei **processi** interni, in termini di efficacia ed efficienza, mediante l'introduzione di strumenti e metodi innovativi.
b. **Esigenze IT esterne**: ovvero esigenze che derivano da fattori esterni all'organizzazione dell'Arma dei Carabinieri e che sono legate a necessità di adeguarsi, ad esempio, a nuovi *standard* in ambito ICT. Tali esigenze possono essere legate ai seguenti elementi:
   - introduzione di nuovi strumenti di **innovazione** da adottare;
   - necessità di raggiungimento di determinati livelli di **sicurezza** ed **efficienza**.

Tra gli elementi che portano alla creazione del Piano vi sono anche i *driver dell'innovazione ICT interne,* individuati nell'ambito del lavoro di analisi delle esigenze e rilevazione delle evidenze emerse:

a. **Modernizzazione delle infrastrutture ICT:** relativa all'evoluzione negli ambiti infrastrutturali, tecnologici e di *facility*, che garantisca maggiori livelli di efficienza, resilienza e scalabilità. Le componenti infrastrutturali da prendere in considerazione sono:
   - **Reti di comunicazione**: trasformare le reti per rendere più veloce l'accesso a Internet e migliorare la qualità dei servizi applicativi, adottando architetture di rete in grado di ottenere, per esempio, una bassa latenza che riduce il ritardo del flusso di dati (architetture *multi-access Edge Computing*);
   - ***Data Center***: garantire la resilienza e l'efficienza dei *Data Center* attraverso l'adozione delle più recenti tecnologie e di *best practice*. In particolare prevedendo un'architettura modulare per facilitare l'espansione e l'aggiornamento ai diversi paradigmi di sviluppo e di produzione, dal *Cloud* all'*Edge Computing*, dalla virtualizzazione alla containerizzazione. Grande attenzione deve essere riservata all'ottimizzazione dei consumi, attraverso il continuo monitoraggio del miglioramento del PUE (*Power Usage Effectiviness*), e all'emissione di CO^2. Il miglioramento continuo della gestione dei carichi di lavoro in ambiente ibrido e *multiCloud* verrà assicurato utilizzando tecniche di bilanciamento e sistemi di orchestrazione finalizzati all'ottimizzazione dell'uso e alla gestione dinamica delle risorse.
   - ***Cloud***: prevedere l'adozione di infrastruttura *Cloud* in un'ottica di salvaguardia del TCO (*Total Cost of Ownership*) dell'intero portafoglio applicativo, attraverso il miglioramento di:
     - adattabilità delle risorse;
     - accesso a tecnologie emergenti (Intelligenza Artificiale, *Machine Learning* e Analisi dei Dati);
     - velocità di sviluppo attraverso l'adozione di metodologie agili come *DevOps* e *Continous Integration/ Continous Deployment*;

- **Sistemi di *disaster recovery* e di *business continuity***: garantire l'evoluzione di tali sistemi per evitare il rischio di perdite dovute a eventuali interruzioni dei sistemi e quindi di *business operations* e processi critici e per rendere la struttura ICT sempre più affidabile, resiliente ed efficiente anche in situazioni avverse;
- **Apparati per il monitoraggio e la sicurezza**: il monitoraggio continuo è essenziale nell'ecosistema della sicurezza informatica di un'organizzazione. Una corretta progettazione, implementazione e monitoraggio continuo forniscono uno specchio reale just-in-time di utenti, dispositivi, reti, dati, attività, carichi di lavoro e stato nell'infrastruttura dell'organizzazione.

b. ***Data Governance***: relativa all'insieme delle attività volte a gestire persone, processi, metodologie e tecnologie dell'informazione al fine di realizzare un costante e corretto trattamento di tutti i dati. Il framework "DAMA[1]" definisce il dominio di conoscenza della gestione dei dati, mettendo la governance di questi ultimi al centro di tali attività. Particolare attenzione viene rivolta a:
   - ***Data Quality***, intesa come l'insieme delle attività volte a misurare e migliorare la qualità dei dati gestiti, aumentandone l'efficacia e l'usabilità in relazione alle aspettative e alle finalità dell'organizzazione;
   - ***Data Security***, che si riferisce alle misure di protezione impiegate per proteggere i dati da accessi non approvati e per preservare la riservatezza, l'integrità e la disponibilità dei dati. Le *best practice* per la sicurezza dei dati includono tecniche di protezione dei dati, come crittografia dei dati, gestione delle chiavi, offuscamento dei dati, sottocategoria dei dati e mascheramento dei dati, nonché controlli di accesso degli utenti privilegiati, auditing e monitoraggio.

c. **Evoluzione applicazioni e servizi IT**: l'IT deve poter reagire più velocemente, intervenendo sui sistemi e sulle metodologie per fare in modo che il *software* sia flessibile e abilitante al processo d'innovazione continua di servizi. A tal riguardo è importante dotarsi di architetture progettate per l'evoluzione, ossia architetture applicative a microservizi facili da aggiornare e rimodellare in base alle necessità. In questo modo, è possibile creare applicazioni facilmente "*smontabili*", i cui componenti possono essere riutilizzati in altri contesti o combinazioni. Sviluppare una serie di microservizi, ciascuno per lo svolgimento di una singola funzione dell'organizzazione (in accordo con il *Single Responsibility Principle*) permette di guadagnare una considerevole flessibilità di sviluppo ed evoluzione delle applicazioni stesse. I servizi, infatti, possono essere sviluppati, aggiornati e testati autonomamente, seguendo lo specifico ciclo di vita delle funzionalità supportate, che sono pensate per operare al meglio nei moderni ambienti IT virtualizzati e di *Cloud*.

IL MODELLO LOGICO ARCHITETTURALE

Il modello logico architetturale è da intendersi come un *format* per descrivere, a livello macro, l'insieme dei sistemi e dell'infrastruttura ICT dell'Arma dei Carabinieri, contenuti all'interno del presente Piano e che si intende raggiungere mediante la realizzazione degli interventi progettuali.

[1] https://dama-italy.org/about-2/

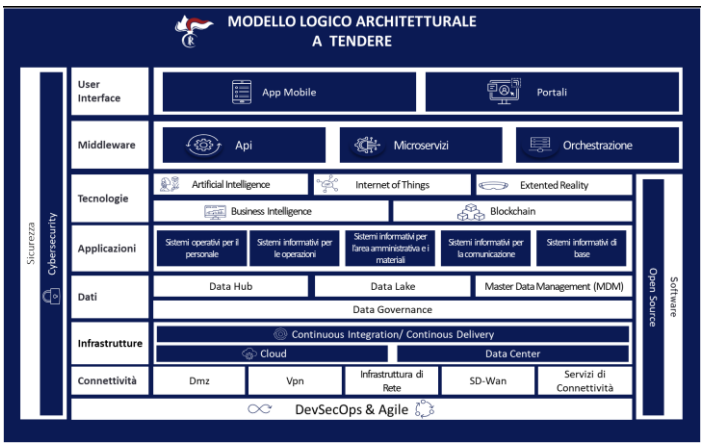

Figura 20: Framework del Modello Logico Architetturale a tendere

Il modello logico architetturale ICT è composto da diversi *layers*: *user interface*, *middleware*, tecnologie, applicazioni, dati, infrastrutture, connettività, sicurezza e *software*.
I *layers* rappresentano comparti omogenei in grado di fornire una visione d'insieme del sistema ICT e di identificare le varie componenti che lo compongono.

a. *User interface e Middleware*

Le *User Interface* sono rappresentate principalmente dalle *web app* e dal portale dell'Arma dei Carabinieri e rappresentano l'insieme dei sistemi dedicati all'interazione con gli utenti, con la finalità di guidare questi ultimi nell'utilizzo dei servizi e nella ricerca delle informazioni. Tali componenti devono essere sviluppate con lo scopo di aumentare la *customer experience* degli utenti, anche attraverso l'utilizzo di assistenti virtuali (*Chatbot*), che utilizzano le tecnologie di intelligenza artificiale e di machine learning. L'erogazione dei servizi tramite *web app* e portale è supportata dallo strato *middleware*, formato dalle API, ovvero l'interfaccia di programmazione delle applicazioni che consentono le interazioni tra i servizi indipendenti di piccole dimensioni (microservizi) con i servizi verso l'esterno. La gestione e il coordinamento tra i microservizi è possibile mediante l'utilizzo di un approccio centralizzato che utilizza due livelli di orchestrazione: a livello di microservizi, tramite un orchestratore (ad esempio il *software open source Kubernetes*[2]) e un *service mesh* (ad esempio il *software open source* Istio[3]) che realizzano un'architettura per facilitare le comunicazioni tra i servizi; a livello di *web services,* tramite un API *Manager* (ad esempio WSO2[4]) e un servizio di *Message Broker* (ad esempio Kafka[5]). L'orchestrazione aiuta a garantire la coerenza e l'affidabilità nelle interazioni tra i microservizi, definendo la sequenza di passaggi che devono essere seguiti.

b. *Tecnologie*

Nel modello logico architetturale sono comprese le tecnologie più rilevanti sulle quali strutturare il sistema ITC dell'Arma dei Carabinieri:

- **Internet of Things** (**IoT**): è un sistema di dispositivi informatici interconnessi, macchine meccaniche e digitali, oggetti, animali o persone dotati di identificatori univoci (UID) con capacità di trasferire dati su una rete senza richiedere l'interazione umana o uomo-computer;
- **Intelligenza Artificiale** (**IA**): è un campo dell'informatica che mira a creare sistemi e programmi che possano eseguire attività con un approccio che simula quanto più possibile il ragionamento umano e le tecniche di apprendimento dell'uomo;

[2] https://kubernetes.io/it/
[3] https://istio.io/
[4] https://wso2.com/
[5] https://kafka.apache.org/

- **Blockchain**: è un registro distribuito condiviso tra i diversi partecipanti di un network (rete peer-to-peer - P2P). Tale tecnologia consente di creare un registro pubblico e immutabile di transazioni, permettendo di condividerne i relativi dati in maniera innovativa, così che tutti gli utenti possano accedere in modo sicuro e affidabile alle stesse informazioni;
- **Extended Reality** (**XR**): l'insieme delle tecnologie immersive che, opportunamente correlate, permettono l'incontro tra il mondo fisico e il mondo virtuale secondo diverse modalità di interazione ["*Virtual Reality*" o "Realtà Virtuale" (VR), "*Augmented Reality*" o "Realtà Aumentata" (AR), "*Mixed Reality*" o "Realtà Mista" (MR)];
- **Business Intelligence** (**BI**): si riferisce a strumenti che consentono di raccogliere e analizzare i dati e le informazioni di un'organizzazione e presentarle in formati intuitivi quali *report*, *dashboard*, grafici e diagrammi. Gli *insight* ottenuti dalla *Business Intelligence* e dall'analisi dei dati permettono di migliorare il processo decisionale basato sui dati.

c. *Applicazioni e Dati*

Il fulcro del modello logico architetturale è costituito dalle Applicazioni, che devono essere realizzate secondo il principio del *Cloud Native Computing* e con una architettura basata sui microservizi per permettere una maggiore flessibilità, una migliore semplicità di gestione dei sistemi complessi e la loro relativa scalabilità. In tale contesto, risulta necessario prevedere interventi di razionalizzazione degli attuali applicativi per semplificare l'infrastruttura IT, riducendo i costi associati alla manutenzione e allo sviluppo nonché evitare ridondanze o l'utilizzo di applicazioni obsolete.

Di fondamentale rilievo risultano i dati che alimentano le applicazioni e, in generale, il patrimonio informativo dell'Arma dei Carabinieri, che necessita di una gestione strutturata per la quale è richiesta l'introduzione di strumenti in grado di ottimizzare il processo di gestione del dato, tra cui si annoverano:

- ***Data hub***: consolida i dati da più fonti per renderli tecnicamente accessibili. **È un'architettura logica o fisica che permette la condivisione dei dati collegando i produttori di dati** (applicazioni, processi e *team*) **con i consumatori** (altre applicazioni, processi e *team*).
- ***Data Lake***: è un ***repository* centralizzato progettato per archiviare, elaborare e proteggere grandi quantità di dati strutturati, semistrutturati e non strutturati**. È un elemento fondamentale per poter passare dalle tecnologie di *Data Analytics* a quelle di Intelligenza Artificiale.
- ***Master data management* (MDM)**: **è uno strumento che permette la centralizzazione e la gestione dei dati master** e consente la definizione di ontologie e di metadatazione dei dati per una migliore fruizione a livello di *insights*. È un sistema che si interfaccia con tutti i processi ed è volto alla costruzione di un repository di qualità, raccogliendo tutti i dati identificati come essenziali. Inoltre, permette di avere dati unificati in termini di definizione e qualità, utilizzabili da tutti i dipartimenti di un'organizzazione.
- **Data governance**: è la disciplina che si occupa di **definire** i **ruoli**, i **processi** e le **tecnologie** necessarie per gestire e proteggere i dati di un'organizzazione.

d. *Infrastrutture e Connettività*

Relativamente all'infrastruttura, il modello target prevede la migrazione in *Cloud* dei dati e dell'infrastruttura IT e/o di determinati servizi. La soluzione più equilibrata potrebbe essere quella del Cloud ibrido (*Hybrid Cloud*) in modalità ***I**nfrastructure **a**s **a** **S**ervice* (**IaaS**), ***P**latform **a**s **a** **S**ervice* (**PaaS**) o ***S**oftware **a**s **a** **S**ervice* (**SaaS**), sfruttando anche tecnologie scalabili (*hyperscaler*).

Il Cloud ibrido prevede un utilizzo contemporaneo di piattaforme pubbliche e private in abbinamento a tecnologie "*on premise*".

Tale soluzione offre la possibilità di incrementare e migliorare la gestione, i requisiti di sicurezza, l'affidabilità, la capacità elaborativa e l'efficienza dell'infrastruttura ICT, che per l'Arma dei Carabinieri evidenzia un certo grado di eterogeneità tecnologica. Inoltre, l'intervento consentirebbe all'Arma di

rafforzare ed estendere le iniziative già in corso e relative all'adozione di una tecnologia a *container* e di un'architettura a microservizi.

L'adozione del Cloud presuppone una diversa gestione della rete di connettività, che deve essere in grado di supportare in modo sicuro le applicazioni Cloud che richiedono maggiore flessibilità, agilità e scalabilità. La rete di sede basata su connessioni private e su reti VPN dedicate e completamente alternative a *Internet* potrebbe assicurare il flusso di dati mission-critical e garantire agli utenti una maggiore qualità del servizio e una migliore customer experience. Per effettuare il passaggio al *Cloud* in modo efficiente bisogna adottare un approccio *Software Defined* (SD). La tecnologia SD-WAN semplifica la configurazione delle reti e permette di instradare il traffico sul percorso più diretto e a bassa latenza verso le applicazioni mission critical. L'approccio SD-WAN è flessibile e può essere automatizzato, permettendo un'orchestrazione che in precedenza era difficile ottenere con il *routing* tradizionale.

e. *Sicurezza*

Al fine di contrastare le minacce alla sicurezza informatica più frequenti, è fondamentale adottare sistemi di controlli di natura tecnologica, organizzativa e procedurale ovvero misure idonee[6] atte a:

- evitare rischi e vulnerabilità che potrebbero condurre a violazioni della sicurezza;
- verificare il rispetto dei requisiti giuridici e legali;
- considerare e prevenire eventuali rischi e criticità legate alla conservazione dei dati;
- valutare le politiche di accesso e condivisione dei dati[7].

La transizione digitale richiede uno sforzo significativo di sviluppo della *cybersecurity*, che protegga dai numerosi data breach (violazione dei dati) o attacchi via posta elettronica relativi al *phishing* e ai *ransomware*. In termini di protezione dei dati personali è fondamentale la collaborazione tra **R**esponsabile della **T**ransizione **D**igitale (RTD) e RPD/DPO per garantire una gestione della *cybersecurity* con caratteristiche di riservatezza, integrità e disponibilità delle informazioni conservate.

f. *Software Open source*

Il modello logico architetturale promuove l'utilizzo di *software* a licenza aperta ("*Open Source*") e il riuso da parte dell'Arma dei Carabinieri di software di proprietà di altre PA, appartenenti all'ecosistema difesa (SMD o altre singole F.F.A.A.) e/o extra dicastero, in conformità con le linee guida[8]definite da AgID, che, adottate in attuazione dagli art. 68 "*Analisi comparativa delle soluzioni*" e 69 "*Riuso delle soluzioni e standard aperti*" del Codice dell'Amministrazione Digitale, prevedono che le PA:

- effettuino una valutazione comparativa tecnico economica sull'acquisto del software, motivando le proprie scelte e privilegiando le soluzioni open source, comprese quelle messe a disposizione dalle altre amministrazioni;
- sviluppino codice sempre con licenza aperta;
- stabiliscano che le soluzioni rese riusabili siano pubblicate con licenza open source in un repository pubblicamente accessibile.

g. *DevSecOps & Agile*

Introduzione di pratiche di ***DevSecOps*** che prevedono un approccio strutturato all'integrazione della sicurezza delle applicazioni e delle infrastrutture IT, sviluppando una responsabilità condivisa tra il team di sviluppo e rilascio applicativo e il team di sicurezza, nei processi di sviluppo ***Agile***. Le pratiche e metodologie *Agile* unite a pratiche di DevSecOps consentono, ai team di sviluppo, di diventare più efficienti nella creazione di applicazioni sicure e nella risposta ai *cambiamenti*.

[6] https://www.agid.gov.it/sites/default/files/repository_files/documentazione/misure_minime_di_sicurezza_v.1.0.pdf
[7] https://docs.italia.it/italia/icdp/icdp-pnd-dmp-docs/it/v1.0-giugno-2022/cose-il-dmp-e-a-che-cosa-serve.html
[8] https://www.agid.gov.it/it/design-servizi/riuso-open-source/linee-guida-acquisizione-riuso-software-pa

4 *AMBITI DI INTERVENTO*

Gli ambiti di intervento, presi in considerazione nel presente Piano corrispondono, in parte e in relazione alle specificità dell'Arma dei Carabinieri, alle componenti tecnologiche definite nel **P**iano Triennale per l'**I**nformatica **(PTI)** dell'AgID, ovvero:

- servizi;
- dati e flussi documentali;
- infrastruttura e applicativi;
- sicurezza informatica;
- leve per l'innovazione;
- tecnologie innovative.

4.1 SERVIZI

4.1.1 DESCRIZIONE

Il miglioramento della qualità e dell'inclusività dei servizi pubblici digitali è un obiettivo importante per la Pubblica Amministrazione. L'Arma dei Carabinieri, nonostante fornisca un ridotto numero di servizi digitali ai cittadini, deve incrementarne la qualità e la facilità di utilizzo, in termini sia di miglioramento dell'esperienza d'uso, sia di incremento del livello di accessibilità, nonché migliorare la capacità di generare ed erogare servizi digitali.

4.1.2 OBIETTIVI E RISULTATI ATTESI

a. 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 (AGID OB.1.1 - R.A. 1.1a)

DESCRIZIONE

Tra i diversi obiettivi indicati nell'ambito del Piano Triennale per l'Informatica nella PA vi è la promozione dell'utilizzo di *software* a licenza aperta ("**Open Source**") e il **riuso di *software*** di proprietà di altre PA[9]. Nelle linee guida dettate da AgID è evidenziata l'importanza dell'uso della licenza aperta in quanto tale soluzione favorisce il riuso delle soluzioni *software* nella Pubblica Amministrazione. In tal modo, un software può essere utilizzato in un contesto diverso da quello per cui è stato originariamente sviluppato, rendendo possibile la condivisione del *software* tra diverse organizzazioni senza incorrere in costi aggiuntivi. Tale obiettivo, inoltre, risponde ad una delle esigenze particolarmente avvertita dall'Arma dei Carabinieri e rappresentata dalla necessità di ridurre la dipendenza dall'utilizzo di licenze di proprietà *Microsoft*. Lungo tale direzione, le linee guida promuovono quindi un vero e proprio cambio culturale verso un più ampio utilizzo del *software* di tipo aperto in modo da permettere che qualsiasi investimento di una PA sia messo a fattor comune delle altre amministrazioni determinando inoltre, una semplificazione delle scelte di acquisto e degli investimenti in termini di servizi digitali. In questo modo, si offre la possibilità di soddisfare esigenze similari senza dover affrontare i costi di progettazione e realizzazione, sostenendo al più le spese di un eventuale adattamento del *software*. In questo modo viene

[9] Un importante progetto di inclusione digitale portato avanti dal Governo e dal Dipartimento per la trasformazione digitale (DTD) ha dato vita a due iniziative, Designers Italia e Developers Italia, per la progettazione e lo sviluppo di servizi digitali della Pubblica Amministrazione per diffondere una cultura della progettazione nella Pubblica Amministrazione e favorire un approccio open source allo sviluppo e al riutilizzo di soluzioni già realizzate (ospitate nel Catalogo del *software* della Pubblica Amministrazione).

migliorato il processo complessivo di digitalizzazione attraverso una diminuzione dei costi e dei tempi necessari al rilascio dell'applicativo stesso.

RISULTATO ATTESO

L'adozione di *software Open Source* consentirà all'Arma dei Carabinieri di ottenere nel medio-lungo periodo diversi benefici, tra cui:

- possibilità di incrementare le prestazioni di un sistema (scalabilità) nel momento in cui vengono fornite nuove risorse (ad esempio cambiando la configurazione a *runtime* con il minor disservizio possibile);
- possibilità di riuso del codice in nuovi software al fine di creare e distribuire nuovi programmi senza costi aggiuntivi (riusabilità);
- compatibilità e conformità con gli applicativi delle altre PA.;
- semplificazione e ottimizzazione degli investimenti e delle scelte di acquisto in termini di servizi digitali;
- aggiornamento tecnologico costante;
- costituzione di un consistente patrimonio (componenti, librerie, *framework*) riutilizzabile per definire nuove idee e progetti;
- riduzione e ottimizzazione dei costi e dei tempi di sviluppo e di gestione.

b. MIGLIORARE L'ESPERIENZA D'USO E L'ACCESSIBILITÀ DEI SERVIZI (AGID OB.1.2)

DESCRIZIONE:

Le Pubbliche Amministrazioni hanno l'obbligo di favorire l'accesso ai servizi *web* migliorandone esperienza d'uso e accessibilità. In relazione all'accessibilità, l'AgID impone la pubblicazione degli obiettivi di accessibilità e degli interventi ad essi associabili suddivisi in sei linee di intervento (postazioni di lavoro, siti tematici, sito istituzionale, *intranet*, formazione e organizzazione del lavoro), e la pubblicazione della dichiarazione di accessibilità per divulgare lo stato di accessibilità di ogni sito *web* e applicazione mobile di cui ciascuna amministrazione è titolare.

RISULTATO ATTESO:

Incremento dell'accessibilità dei servizi digitali della PA, secondo quanto indicato dalle Linee guida sull'accessibilità degli strumenti informatici.

4.1.3 INTERVENTI PROGETTUALI

Ser1 – PUBBLICAZIONE OBIETTIVI DI ACCESSIBILITÀ

 **SCENARIO**	 **COMPLESSITÀ**
Le PA pubblicano entro il 31 Marzo 2024, gli obiettivi di accessibilità sul proprio sito.	Bassa
 **BENEFICI**	 **DEADLINE**
- Miglioramento dei processi che aumentano la soddisfazione dell'utente. - Miglioramento della trasparenza secondo quanto stabilito dalle Linee guida AgID. - Adempimento normativo.	Marzo 2024 (PTI AgID)

Ser2 – PUBBLICAZIONE DICHIARAZIONE DI ACCESSIBILITÀ

SCENARIO

Le PA pubblicano, entro il 23 settembre 2024, tramite l'applicazione form.agid.gov.it, una dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobile.

COMPLESSITÀ

Bassa

BENEFICI

- Miglioramento dei processi che aumentano la soddisfazione dell'utente.
- Miglioramento della trasparenza secondo quanto stabilito dalle Linee guida AgID.
- Adempimento normativo.

DEADLINE

Settembre 2024

(PTI AgID)

Ser3 – ANALISI PRELIMINARE DEGLI APPLICATIVI IN OTTICA DI RIUSO

SCENARIO

Individuare quali applicativi in uso presso altre PA appartenenti all'ecosistema Difesa (SMD o altre singole F.A.) e/o *extra* dicastero (ad esempio l'applicativo "AdHoc" – documentale di MD) possono essere riadattati anche nel contesto dell'Arma dei Carabinieri (principio espresso dall'Art.69 del CAD) per soddisfare proprie specifiche esigenze.

COMPLESSITÀ

Medio-Bassa

BENEFICI

- Riduzione e ottimizzazione dei costi e dei tempi di sviluppo e di gestione degli applicativi.
- Elevata adattabilità all'ecosistema in cui risiede, andando a customizzare l'applicativo in base al modus operandi dell'Arma dei Carabinieri.
- Conformità con le altre PA, anche in relazione alla riduzione del *gap* tecnologico tra Amministrazioni.
- Aggiornamento tecnologico continuo.

DEADLINE

Marzo 2025

Gruppo 1

Ser4 – ADOZIONE DI SOFTWARE "*OPEN SOURCE*"

SCENARIO

Individuare quali tra i software «*open source*» disponibili sul mercato possono essere utilizzati anche all'interno del parco applicativo dell'Arma dei Carabinieri, al fine di sostituire quelli di licenza proprietaria attualmente utilizzati.

COMPLESSITÀ

Medio-Bassa

BENEFICI

- Svincolamento dalla dipendenza dalle licenze che possono pesare notevolmente sul budget dell'Amministrazione.
- Riduzione e ottimizzazione dei costi e dei tempi di sviluppo e di gestione degli applicativi.

DEADLINE

dicembre 2025

Gruppo 1

- Elevata adattabilità all'ecosistema in cui risiede, andando a customizzare l'applicativo in base al modus operandi dell'Arma dei Carabinieri. - Aggiornamento tecnologico continuo. - Riduzione del rischio di obsolescenza degli applicativi utilizzati.	

Ser5 – REINGEGNERIZZAZIONE SITO "CARABINIERI.IT"	
 **SCENARIO**	 **COMPLESSITÀ**
Reingegnerizzare il sito istituzionale www.carabinieri.it anche valutando uso di *Cloud* e pianificando una fase di *update* del CMS (Content Management System) *Sitefinity*.	Medio
 **BENEFICI**	 **DEADLINE**
- Migliore fruibilità del sito ufficiale dell'Arma dei Carabinieri. - Maggiore efficienza di reindirizzamento. - Miglioramento grafica e posizionamento.	Dicembre 2026 (Progetti in corso)

4.2 DATI E FLUSSI DOCUMENTALI

4.2.1 DESCRIZIONE

La valorizzazione del patrimonio informativo, come indicato nel Piano Triennale per l'Informatica di AgID, costituisce obiettivo strategico per la Pubblica Amministrazione per affrontare efficacemente le nuove sfide dell'economia basata sui dati (*Data Economy*). Nell'attuale contesto economico-sociale, sempre maggiormente connotato da innovazione, velocità e conoscenza, risulta necessario adottare un approccio orientato ai dati (*Data Driven*), che consenta cioè di definire l'insieme di processi, ruoli, *policy*, *standard* e metriche finalizzate a garantire un uso efficace ed efficiente delle informazioni. Le informazioni, correttamente gestite, forniscono un supporto strategico all'Arma nel raggiungimento degli obiettivi prefissati per realizzare correttamente la sua mission istituzionale, con particolare riferimento alla:

- **valorizzazione e gestione del patrimonio informativo**, in ottica di favorire il processo di trasformazione verso un modello *data-driven*;
- **revisione dei flussi informativi e di comunicazione**;
- **qualità dei dati e metadati**.

Seguendo tale direttrici, l'Arma dei Carabinieri avrebbe la possibilità di gestire il dato come un vero e proprio *asset*, uno strumento indispensabile per l'estrazione di informazioni di valore utili a supportare decisioni rapide ma consapevoli e per attivare un percorso orientato all'efficientamento dei flussi e degli scambi informativi e comunicazionali interni.

4.2.2 OBIETTIVI E RISULTATI ATTESI

AUMENTARE LA CONSAPEVOLEZZA SULLE POLITICHE DI VALORIZZAZIONE DEL PATRIMONIO INFORMATIVO PUBBLICO E SU UNA MODERNA ECONOMIA DEI DATI (AGID OB.2.3)

DESCRIZIONE:

Nel tempo, il processo di transizione al digitale ha determinato l'incremento sempre più consistente dei flussi dati e, inoltre, la velocità di acquisizione delle informazioni è diventata fondamentale per

attivare in modo consapevole, razionale ed efficiente i diversi processi decisionali. L'identificazione dei dati della PA come "patrimonio informativo" è indicata anche nelle linee guida del Piano Triennale per l'Informatica di AgID, esprimendo l'idea del grande valore che essi possiedono e delle potenzialità derivanti dal loro utilizzo strategico. La valorizzazione di tale patrimonio informativo pubblico rappresenta quindi un obiettivo cruciale per tutte le PA, con la finalità di trasformare i dati in un'importante risorsa che permetta di strutturare soluzioni strategiche al funzionamento efficiente dell'attività amministrativa. Anche per l'Arma dei Carabinieri, quindi, risulta cruciale l'adozione di strumenti orientati alla raccolta, analisi e tutela dei dati per facilitare e ottimizzare la gestione dei flussi provenienti dalle attività di una moltitudine di Unità Operative. In particolare, per il contesto dell'Arma dei Carabinieri, è necessario adottare una strategia specifica di valorizzazione del proprio patrimonio informativo, andando a studiare e analizzare i macro-ambiti su cui strutturare un *framework* di *Data Governance* che meglio riesca a indirizzare le sfide istituzionali e garantire l'accessibilità, la disponibilità e l'affidabilità dei dati stessi.

RISULTATO ATTESO:

La valorizzazione e la corretta gestione del patrimonio informativo consentiranno all'Arma dei Carabinieri di:

- classificare e organizzare i dati per categorie pertinenti in modo che possano essere protetti e utilizzati in modo più efficiente;
- aumentare la sicurezza dei dati: avendo chiara la differente rilevanza degli stessi è possibile definire corretti "coni di visibilità" e concentrare le attività di protezione sui dati critici (ad esempio, in qualità di responsabili del trattamento dei dati, è necessario avere la piena supervisione su dove i dati sono memorizzati, chi li sta aggiornando e chi vi sta accedendo e per quali scopi);
- garantire una maggiore fruibilità e condivisione dei dati nell'ambito delle diverse articolazioni;
- favorire una maggiore trasparenza e verificabilità, efficientando l'utilizzo e riducendo i costi di gestione;
- aumentare il livello di efficienza nello sviluppo e nel monitoraggio dei processi per indirizzare problemi ed opportunità nella gestione del patrimonio informativo, anche tramite l'utilizzo di metriche di calcolo;
- migliorare l'interoperabilità interna grazie ad una maggiore condivisione delle informazioni;
- ottimizzare il processo decisionale.

DIGITALIZZAZIONE DEI FLUSSI INFORMATIVI *END-TO-END*

DESCRIZIONE:

Nel contesto attuale in cui l'Arma dei Carabinieri si trova ad agire, risulta fondamentale non solo acquisire un grande quantitativo di informazioni, ma anche garantire una corretta diffusione delle stesse tra le varie strutture e unità operative interne. In particolare, un'organizzazione con flussi informativi strutturati e digitalizzati pone le basi per l'adozione di un approccio alla gestione del dato in grado di indirizzare aspetti di innovazione sia sul piano organizzativo sia su quello tecnologico e operativo. L'obiettivo "*Revisione dei flussi informativi e di comunicazione*", quindi, ha come presupposto fondamentale quello di analizzare gli attuali flussi di informazione provenienti sia da vari applicativi che da documentazione cartacea, per definire le modalità di dematerializzazione di quelli non digitali e razionalizzazione dei dati ridondanti.

RISULTATO ATTESO:

L'Arma dei Carabinieri, attraverso la revisione e l'ottimizzazione dei flussi informativi end to end mira alla valorizzazione del flusso informativo interno, attraverso:

- una maggiore fluidità ed efficacia tale da favorire una rapida condivisione dei documenti, generando tra l'altro, un incremento della produttività, l'aumento della qualità del lavoro e una generale ottimizzazione dei tempi;
- la possibilità di specificare ruoli e responsabilità per la gestione dei flussi;

- una totale mappatura dei flussi in grado di favorire un maggiore monitoraggio sui dati;
- una maggiore comprensione e consapevolezza del valore informativo dei dati che consente di supportare l'organizzazione nella definizione e comunicazione degli indirizzi strategici.

AUMENTARE LA QUALITÀ DEI DATI E DEI METADATI (AGID OB.2.2)

DESCRIZIONE:

Un elemento fondamentale strettamente collegato alla valorizzazione e gestione del patrimonio informativo è rappresentato dall'aumento della qualità dei dati e dei metadati. La *Data Quality,* è infatti, è una componente fondamentale del processo generale di gestione dei dati ed è legata ai programmi di *Data Governance* che mirano a garantire che i dati siano formattati e utilizzati in modo coerente in tutta l'organizzazione. Quindi, affinché l'Arma dei Carabinieri possa considerare i dati come validi strumenti da cui estrarre informazioni da utilizzare come *driver* nei processi decisionali, è necessario definire una politica e degli *standard* di *Data Quality* orientati a garantire l'accuratezza e l'integrità dei dati acquisiti. In particolare, la qualità dei dati misura il modo in cui un *set* di dati soddisfa i criteri di accuratezza, completezza, validità, coerenza, unicità, tempestività ed è fondamentale per tutte le iniziative di *governance* dei dati all'interno di un'organizzazione. Tali *standard* di qualità permetterebbero all'Arma dei Carabinieri di prendere decisioni basate sui dati per soddisfare i propri obiettivi e svolgere efficacemente la propria mission istituzionale. L'incremento della qualità dei dati raccolti determinerebbe effetti positivi anche in termine di adozione delle nuove tecnologie, come l'Intelligenza Artificiale e gli algoritmi di *Machine Learning*. Tali strumenti, infatti, integrano nei loro flussi di lavoro i dati e quindi disporre di dati di alta qualità è cruciale per una loro efficace adozione.

RISULTATO ATTESO:

In generale, l'incremento della qualità dei dati e dei metadati consentirà all'Arma dei Carabinieri di disporre e gestire un patrimonio informativo costituito da dati integri e di valore tale da favorire:

- processi decisionali più consapevoli, basati su informazioni di valore;
- attività di revisione e pulizia dei dati (favorendo ad esempio l'eliminazione dei dati ridondanti, anomali, mancanti);
- analisi efficaci e report integrati su dati provenienti da una pluralità di fonti;
- utilizzo di metriche orientate al costante monitoraggio del livello di qualità dei dati.

4.2.3 INTERVENTI PROGETTUALI[10]

Nella tabella seguente sono riportati gli interventi progettuali individuati nell'ambito in questione:

D1 – RAZIONALIZZAZIONE E DIGITALIZZAZIONE DEI FLUSSI INFORMATIVI	
SCENARIO	**COMPLESSITÀ**
Analizzare gli attuali flussi di informazione provenienti sia da vari applicativi che da documentazione cartacea per definire le modalità di dematerializzazione dei flussi informativi non digitali e di razionalizzazione dei dati ridondanti.	Medio-Alta
BENEFICI	**DEADLINE**
- Miglioramento dell'interoperabilità interna grazie ad una maggiore condivisione delle informazioni.	Novembre 2024

[10] La modalità di definizione della deadline e del gruppo di riferimento per ciascun intervento progettuale è dettagliata all'interno del capitolo 7 "*Prioritizzazione degli interventi*".

- Flusso di informazioni più fluido ed efficiente tale da favorire una rapida condivisione dei documenti, generando tra l'altro, un incremento della produttività, l'aumento della qualità del lavoro e una generale ottimizzazione dei tempi. - Possibilità di specificare ruoli e responsabilità per la gestione dei flussi. - Totale mappatura dei flussi informativi in grado di favorire un maggiore monitoraggio sui dati. - Maggiore comprensione e consapevolezza del valore informativo dei dati che consente di supportare l'organizzazione nella definizione e comunicazione degli indirizzi strategici.	Gruppo 2

D2 – DEFINIZIONE DATA ACHITECTURE E STRUMENTI A SUPPORTO

SCENARIO

COMPLESSITÀ

Definizione di una strategia di *Data Architecture* che si ponga l'obiettivo di definire la struttura, l'organizzazione e il design degli asset di dati di un'organizzazione e come vengono utilizzati per supportare le operazioni organizzative e l'assunzione delle decisioni. La tematica riguarda vari aspetti, tra cui le fonti di dati, la memorizzazione, l'elaborazione, l'integrazione e i meccanismi di recupero dei dati. Una buona architettura dati è essenziale per garantire la coerenza, l'accuratezza, la sicurezza e l'accessibilità dei dati, e tende a individuare gli strumenti orientati ad ottimizzare il processo di gestione del dato durante tutto il suo ciclo di vita (es. *Data Lineage, Business Glossary, Data Catalog, Data Hub*) e di metriche di «*Data Quality*» utili al monitoraggio e al miglioramento del livello della qualità dei dati, in modo da consentire all'Arma dei Carabinieri di disporre di un patrimonio informativo caratterizzato da dati puliti e consistenti (*Data Cleaning*) e da informazioni affidabili.

La dottrina prevede la definizione di tre principali fasi:

- *Capture* (cattura dei dati): processo di acquisizione e registrazione dei dati prodotti da diverse fonti o dispositivi in formato digitale, in modo che possano essere utilizzate per la loro elaborazione.
- *Curate* (cura del dato): si riferisce al processo di organizzazione, miglioramento, e gestione dei dati al fine di garantirne la qualità, l'accuratezza, l'integrità e l'accessibilità.
- *Consume* (consumo dei dati): si riferisce al processo attraverso il quale gli utenti, le applicazioni o i sistemi accedono, utilizzando o traendo valore dai dati disponibili.

Sottese a queste fasi abbiamo il Data Source (*IoT devices, Customer Application, ERP*, ecc.), Data Ingestion (*API, batch, file transfer, DB connection, event streaming*, ecc), *Storage and Processing* (*Data Lake*), *Data Provisioning* (*API, batch, file transfer*, ecc.), *Data Consuption* (*dashboard/report, application*), ML&AI (*sandbox e data lab*, ecc.), *Data Usage* (*external users, internal users, processes services*, ecc.). A completamento della definizione di una *Data Architecture* è necessario definire una *Data Governance* con ulteriore strato di *Security&Operation* per la gestione della sicurezza del dato.

Medio-Alta

BENEFICI

DEADLINE

- Capacità di mettere a disposizione i dati dell'organizzazione in modo assistito e controllato;
- Maggiore visibilità e accessibilità di tutti i dati da parte delle diverse unità organizzative interne.
- Rappresentazione esplicita del ciclo di vita del dato dalla sua nascita al suo effettivo utilizzo e destinazione.
- Miglioramento strutturale della qualità dei dati, finalizzato alla rimozione definitiva delle cause di anomalia.
- Processo decisionale più consapevole e affidabile.
- Analisi efficaci e *report* integrati su dati provenienti da una pluralità di fonti.
- Attività di revisione e pulizia dei dati (favorendo ad esempio l'eliminazione dei dati ridondanti, anomali, mancanti).

Novembre 2024

Gruppo 2

- Monitoraggio della qualità dei dati attraverso KQI (Key Quality Indicator), *dashboard* e *report* configurabili e declinabili lungo varie dimensioni di analisi (ad es. per applicativo, area informativa, criterio di qualità).

D3 – DEFINIZIONE DATA GOVERNANCE	
SCENARIO	**COMPLESSITÀ**
Definizione di una *Data Governance,* ovvero un insieme di processi, ruoli, *policy*, *standard* e metriche finalizzate a garantire un uso efficace ed efficiente delle informazioni, che permetta a un'organizzazione di raggiungere gli obiettivi prefissati. All'interno di tale processo sarà definito anche il modello operativo di riferimento orientato alla gestione dei dati e che sia ottimale rispetto al contesto specifico dell'Arma dei Carabinieri, delineando i principali ruoli e responsabilità. Tale attività risulta fondamentale per individuare chi può intraprendere determinate azioni, su quali dati, in quali ambiti e utilizzando quali metodi e strumenti.	Medio-Alta
BENEFICI	**DEADLINE**
- Chiara definizione di ruoli e responsabilità in merito all'utilizzo dei dati. - Gestione organica e strutturata del patrimonio informativo. - Definizione delle regole per l'utilizzo dei dati. - Ottimizzazione ed efficientamento dei processi di comunicazione interna in merito all'utilizzo dei dati. - Aumento della sicurezza dei dati: definendo i diversi ruoli e responsabilità, è possibile individuare più facilmente "coni di visibilità" e definire opportune logiche di profilazione/privilegi e concentrare le attività di protezione sui dati critici (ad esempio, in qualità di responsabili del trattamento dei dati, è necessario avere la piena supervisione su dove i dati sono memorizzati, chi li sta aggiornando e chi vi sta accedendo e per quali scopi).	Dicembre 2025 Gruppo 4

4.3 INFRASTRUTTURA E APPLICATIVI

4.3.1 DESCRIZIONE

L'ambito di intervento relativo ad "*infrastruttura e applicativi*" costituisce uno dei principali fattori per garantire l'efficacia del percorso di digitalizzazione intrapreso dall'Arma dei Carabinieri. In particolare, risulta rilevante la presenza di un'infrastruttura digitale che sia in grado di assicurare un elevato livello di efficienza e maggiori standard di sicurezza. Lungo tale direzione, il Piano Triennale per l'Informatica di AgID, con l'intento di guidare le PA nello sviluppo delle proprie Infrastrutture Digitali, ha identificato l'insieme di azioni necessarie per l'ammodernamento dei *Data Center* afferenti alle PA, al fine di soddisfare tutti gli *standard* nazionali ed europei. Di seguito, sono indicati alcuni obiettivi presenti nel Piano Triennale di AgID in linea con le esigenze emerse all'interno del contesto dell'Arma dei Carabinieri, da portare avanti durante il percorso di digitalizzazione intrapreso. In particolare:

- favorire l'adozione e il riuso di ***software Open Source*** e implementare il modello di riuso di software tra le amministrazioni;
- applicare l'approccio "***Cloud First***" a tutti i progetti di digitalizzazione delle piattaforme delle Pubbliche Amministrazioni e attuare un percorso orientato a garantire una revisione architetturale dell'infrastruttura e degli applicativi su base *Cloud* e microservizi;
- favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API e adottare API conformi al Modello di Interoperabilità.

4.3.2 OBIETTIVI E RISULTATI ATTESI

Gli obiettivi relativi a tale ambito di intervento sono ripresi dagli obiettivi che l'AgID ha stilato nell'ambito del Piano Triennale per l'Informatica.

MIGLIORARE LA QUALITÀ E LA SICUREZZA DEI SERVIZI DIGITALI EROGATI DALLE AMMINISTRAZIONI ATTUANDO LA STRATEGIA *CLOUD* ITALIA E MIGRANDO VERSO INFRASTRUTTURE E SERVIZI *CLOUD* QUALIFICATI (INCLUSO PSN) - (AGID OB.4.1)

DESCRIZIONE

Tale ambito di intervento fa riferimento alla strategia *Cloud-First* descritta nel Piano Triennale per l'Informatica di AgID. In particolare, si tratta di una strategia che ha come finalità quella di favorire l'erogazione dei servizi offerti dalle PP.AA. attraverso applicazioni ***Cloud-Native***, cioè quelle applicazioni sviluppate sin dal principio secondo il paradigma *Cloud* e basate sull'utilizzo di **microservizi.** L'obiettivo è in linea con il percorso di ristrutturazione tecnologica intrapreso dall'Arma dei Carabinieri che sta prevedendo il passaggio alla tecnologia a "*Container*" e la possibilità di utilizzo di un'architettura a microservizi in ottica di favorire la gestione, lo sviluppo e il *deploy* degli applicativi.

Con il termine *Cloud* native si intende un approccio nello sviluppo software che utilizza il *Cloud computing* per creare ed eseguire applicazioni scalabili in ambienti moderni e dinamici come *Cloud* pubblici, privati e ibridi[11]. Tecnologie come *container*, microservizi, funzioni *serverless* [12]e "infrastrutture immutabili[13], distribuite tramite API dichiarative" sono elementi comuni di questo stile architetturale e ovviamente devono essere considerate nel contesto dell'adozione di un'architettura *Cloud*. Le tecnologie a supporto "abilitano sistemi debolmente accoppiati (*loosely coupled*) che sono resilienti, gestibili, osservabili" e supportati da una robusta automazione in ottica *Continuous Integration/Continuous Deployment* (CI/CD). Questo consente all'Amministrazione di porsi in un'ottica di sviluppo secondo i canoni della Metodologia "*Agile*" e adottando le *best practices* della metodologia DevSecOps.

Gli elementi caratterizzanti le "*architetture Cloud native"* sono rappresentati da:

- **Tecnologie di container (Containerizzazione)**: i *container* esprimono una tecnologia che consente di isolare una applicazione e tutte le sue dipendenze in un formato, che contiene l'eseguibile che identifica il servizio e le librerie che sono indispensabili al suo funzionamento, costituendo quindi un ambiente autoconsistente ed indipendente dallo specifico environment. Quindi, i container consentono di creare pacchetti e isolare le applicazioni con il loro intero "*Runtime Environment*" e tutti i *file* necessari per l'esecuzione. Inoltre, utilizzando la virtualizzazione a livello di sistema operativo (O.S.), una singola istanza del sistema viene dinamicamente suddivisa tra uno o più container isolati.
- **Microservizi**: approccio architettonico nativo del Cloud che prevede lo sviluppo di componenti autonome di *business* o *data/domain Driven*, in cui il singolo microservizio percorre in maniera completamente autonoma il proprio ciclo di vita ed interagisce con gli altri in modalità flessibile attraverso accoppiamenti non rigidi basati prevalentemente su tecniche *RESTful* e scambio di messaggi JSON. Ogni microservizio può essere implementato, aggiornato, ridimensionato e riavviato indipendentemente da altri servizi, tipicamente come parte di un sistema composito,

[11] Definizione della *Cloud Native Computing Foundation* (CNCF) come da *Design Patterns for Cloud Native Applications – O'Reilly*.
[12] Concettualmente senza accesso e necessità di gestione delle istanze server.
[13] NIST *Special Pubblication*.

consentendo frequenti aggiornamenti delle applicazioni in tempo reale, con un impatto minimo sui servizi complessivi e quindi sull'utenza finale. Inoltre, i microservizi sono progettati in modo da poter essere impiegati anche come parte di un'altra applicazione, vale a dire che possono essere liberamente combinati e copiati per altre applicazioni e riutilizzati secondo necessità. Ciascun microservizio è sviluppato in modo autonomo e, si caratterizza da un ciclo di vita indipendente, consentendo di effettuare aggiornamenti su una piccola area di un'applicazione complessa, con meno rischi di danneggiare l'intero sistema. In tal modo, invece di ridimensionare l'intera applicazione come una singola unità, si ridimensionano solo quei servizi che richiedono per esempio, più potenza di elaborazione o larghezza di banda della rete.

- **DevSecOps**: un insieme di procedure che abbracciano l'intero ciclo di sviluppo del *software*, dalla progettazione iniziale di un'applicazione fino alla consegna e all'operatività di tale applicazione, che mette insieme sviluppo ("*development*"), sicurezza ("*security*") e operazioni IT ("*operations*"), basato sui principi *Agile* e *Lean*. I benefici maggiori sono la riduzione dei tempi di sviluppo ed una continua e automatica messa in produzione, creando una cultura e un ambiente in cui lo sviluppo, il *test* e il rilascio di software sicuro avvengono rapidamente, frequentemente e in modo più coerente rispetto alle esigenze.
- ***Continous Integration / Continous Delivery***: è un processo, spesso visualizzato come una pipeline, che comporta l'aggiunta di un alto grado di automazione e monitoraggio continuo per lo sviluppo di *app Cloud native*, in modo che le modifiche al codice sorgente si traducano automaticamente in un nuovo *container* in fase di costruzione, testato e distribuito in fase di sviluppo e, eventualmente, in produzione.
- ***Robotic Process Automation* (RPA)**: piattaforma in grado di automatizzare, velocizzare e rendere maggiormente *error-free* le normali attività di gestione ed amministrazione delle infrastrutture complesse[14].
- **Orchestrazione**: uno strumento che permette di organizzare, mettere in sequenza e coordinare i microservizi containerizzati e distribuiti su una serie di *Cloud* pubblici e privati. È un processo che consente di accelerare l'erogazione dei servizi e ridurre i costi. Inoltre, permette un minor coinvolgimento del personale così come l'eliminazione di potenziali errori nel *provisioning*, nella scalabilità o in altri processi *Cloud* (ad esempio *Kubernetes*[15]).

Vi è la possibilità di utilizzare piattaforme dove tutte le suddette metodologie e funzionalità sono integrate e predisposte per semplificare l'operatività nelle infrastrutture ICT e lo sviluppo applicativo *Cloud Native* (ad esempio la Piattaforma *Open City Platform* - OCP[16]).

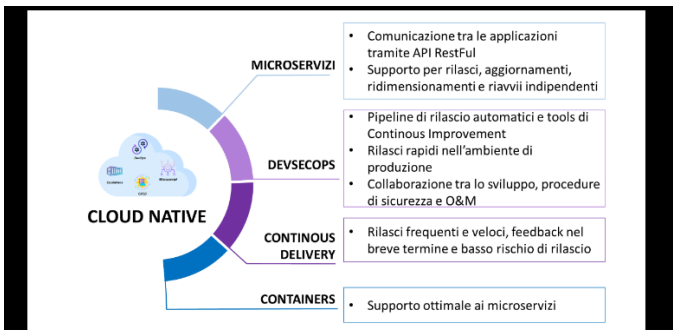

Figura 22: Pilastri dell'approccio Cloud Native

[14] Esistono *software open source* che consentono il *provisioning* e la gestione dell'infrastruttura *Cloud* (ad es. *Ansible* e *Terraform*).
[15] **Sistema di orchestrazione per containers basato su *software open source Kubernetes*.**
[16] www.opencityplatform.eu

PERCORSO DI ADOZIONE DEL *CLOUD*

Di seguito, sono indicati i principali passaggi da seguire per l'adozione di un modello *Cloud* nel contesto dell'Arma dei Carabinieri:

a. definizione di un nuovo **modello di sviluppo delle applicazioni** in ottica *Cloud Native* secondo un approccio strutturato verso un modello pienamente *Service Oriented*, in cui l'infrastruttura stessa viene vista come un elemento di servizio (IaaS, PaaS, SaaS e ulteriori definizioni associate) e caratterizzato dal rispetto dei principi di **modularità**, **riutilizzabilità** e **flessibilità**;
b. declinazione dei **vantaggi specifici per l'Arma dei Carabinieri dei diversi modelli *Cloud*** e dei fattori che influenzano la scelta della soluzione *Cloud* ideale;
c. selezione di uno specifico **modello di adozione *Cloud*** che consenta di decidere, per ogni nuovo servizio, la migliore piattaforma di distribuzione in relazione ai relativi vantaggi;
d. avvio di un'**analisi del codice applicativo** esistente per stabilire le priorità di una eventuale trasformazione verso una abilitazione al *Cloud*;
e. definizione di **modelli di migrazione verso il *Cloud*** del codice applicativo esistente con riferimento specifico al **modello 6R di AgID** (***Docs* Italia, Documenti pubblici, digitali**)[17] e alle "*Linee guida su acquisizione e riuso di software per le Pubbliche Amministrazioni*" [18]. Quanto riportato da tali linee guida si può tradurre in un flusso decisionale che, partendo dal principio ispiratore assunto del *re-architect first*, definisce qual è, tra quelli indicati da AgID e DTD, il *pattern* di migrazione più idoneo per lo specifico *workload* e la modalità della loro implementazione (*Retain, Retire, Re-purchase, Re-host, Re-platform* o *Re-architect*).

RISULTATO ATTESO:

Attivando un percorso orientato alla revisione architetturale su base *Cloud* e microservizi, l'Arma dei Carabinieri sarà in grado di raggiungere un elevato grado di autonomia tecnologica, avere un maggiore controllo sui dati e aumentare la resilienza dei propri servizi digitali. In particolare, in un'ottica futura, attraverso l'adozione di un approccio *Cloud Native* e l'utilizzo dei microservizi l'Arma dei Carabinieri avrà la possibilità di raggiungere diversi vantaggi derivanti dall'adozione del *Cloud computing*:

- **Scalabilità**: possibilità di accedere in modo dinamico a risorse di elaborazione aggiuntive in base alle necessità, riuscendo a gestire eventuali picchi di carico;
- **Flessibilità e agilità**: gestione del ciclo di vita dei servizi applicativi di qualità e in grado di rispondere in tempi rapidi sulle modifiche ai processi che supportano i procedimenti amministrativi;
- **Adattabilità tecnologica**: i microservizi non pongono vincoli e possono essere sviluppati scegliendo i linguaggi e le tecnologie più appropriate per gli scopi da raggiungere;
- **Aggiornamento costante**: le prestazioni delle applicazioni *Cloud native* sono adattate sulla base delle effettive necessità. I singoli microservizi vengono aggiornati indipendentemente e di volta in volta in base alle esigenze. Questi processi di aggiornamento e di autoregolazione vengono spesso eseguiti automaticamente per mezzo di *trigger* (eventi di attivazione) predefiniti;
- **Efficienza**: aumentare l'efficienza sia operativa, in termini di minor spreco di risorse e tempi, sia funzionale, in termini di minor complessità nello sviluppare nuove soluzioni.

[17] https://docs.italia.it/italia/manuale-di-abilitazione-al-Cloud/manuale-di-abilitazione-al-Cloud-docs/it/v1.2/pianificare-la-migrazione/le-strategie-di-migrazione.html?highlight=6R
[18] https://www.agid.gov.it/sites/default/files/repository_files/lg-acquisizione-e-riuso-software-per-pa-docs_pubblicata.pdf

4.3.3 INTERVENTI PROGETTUALI[19]

Nella tabella seguente sono riportati gli interventi progettuali individuati nell'ambito in questione:

I1 – PORTALE DELLA FORMAZIONE

SCENARIO

Il presente intervento è finalizzato allo sviluppo di una piattaforma di nuova generazione, in grado di assicurare la pianificazione e l'erogazione di corsi e di *training* in modalità virtuale, anche da remoto e in mobilità, al fine di soddisfare al meglio le esigenze connesse con la formazione dei Carabinieri. L'azione prevedrebbe lo sviluppo di un vero e proprio Portale dedicato alla formazione per governare tutti i processi e coinvolgere gli attori connessi (Uffici, Istituti di Formazione, Docenti e Frequentatori), nonché per creare un ambiente integrato per l'erogazione di servizi formativi di tipo multimediale (cd. Formazione a distanza – FAD).

COMPLESSITÀ

Media

BENEFICI

- Percorsi di formazione personalizzati e innovativi.
- Maggior coinvolgimento da parte dei discenti.
- Un più alto livello di ritenzione delle informazioni *post-training*.
- Maggiore flessibilità nel percorso di formazione.

DEADLINE

Dicembre 2025

Gruppo 4

I2 – MIGRAZIONE IN *CLOUD* DEL SERVIZIO PEO

SCENARIO

Il presente intervento è finalizzato a:

- estendere il servizio di Posta Elettronica Ordinaria (PEO) a tutto il personale dell'Arma, con l'approvvigionamento iniziale di 80.000 caselle *email* per tutti i militari che ne sono sprovvisti e la successiva migrazione di quelle già esistenti *on premise*;
- prevedere un'interfaccia intuitiva e strutturata come *scrivania digitale* per l'utente, comprensiva di strumenti per la produttività e la collaborazione, che semplificano il lavoro d'ufficio (calendari condivisi, messaggistica istantanea, reminder automatici, *editor* di testo, *videocall*, fogli di calcolo, spazio per la condivisione di dati, anche in mobilità).

COMPLESSITÀ

Media

BENEFICI

- Accesso alle piattaforme da qualunque dispositivo anche non connesso alla rete *intranet*.
- Maggiore scalabilità dei sistemi e modularità dei servizi, al variare delle esigenze istituzionali.
- Rilevanti *standard* di sicurezza informatica e di protezione dei dati, mediante esecuzione di backup e un'efficace difesa dagli attacchi informatici (aggiornamenti in modalità automatica, senza impiego di personale dedicato da parte dell'Amministrazione), nonché maggiore efficienza del *Disaster Recovery*.
- Abbattimento dei costi ulteriori per *Hardware* e *Software* (soggetto a obsolescenza e continua manutenzione), nonché riduzione al minimo dell'impatto ambientale, senza ulteriori sprechi.

DEADLINE

Dicembre 2024

Gruppo 4

(progetto in corso)

[19] La modalità di definizione della deadline e del gruppo di riferimento per ciascun intervento progettuale è dettagliata all'interno del capitolo 7 "Prioritizzazione degli interventi".

I3 – IMPLEMENTAZIONE O EVOLUZIONE DEL SISTEMA DI GESTIONE DOCUMENTALE (C-PROT)

SCENARIO

L'intervento si pone l'obiettivo di evolvere in modo incrementale il sistema documentale attualmente in corso di sviluppo (C-*Prot*) in modo da mantenere elevati *standard* di *performance* e da integrarsi completamente al contesto dell'Arma, supportandola nella digitalizzazione dei processi di lavorazione e della gestione dei flussi di collaborazione tra utenti e uffici.

COMPLESSITA'

Alta

BENEFICI

- Riduzione dei costi grazie ad una sostanziale riduzione del *workflow* documentale interno all'organizzazione.
- Facilità nel reperimento dei documenti di interesse.
- Affidabilità dei documenti, legato alla inalterabilità degli stessi.

DEADLINE

Giugno 2025

Gruppo 2

I4 – DEFINIZIONE DELLA STRATEGIA DI IMPLEMENTAZIONE DELL'APPROCCIO *CLOUD NATIVE*

SCENARIO

L'intervento è orientato a fornire delle linee guida volte all'individuazione delle principali attività da svolgere per rivisitare il parco applicativo in ottica "*Cloud Native*" ed è finalizzato alla revisione architetturale dell'infrastruttura tecnologica presente presso l'Arma dei Carabinieri su base *Cloud* e microservizi.

La strategia di implementazione dell'approccio *Cloud Native* verrà definita in coerenza con quanto previsto dalla Strategia *Cloud* Italia, applicando il principio *Cloud First* e acquisendo servizi *Cloud* solo se qualificati, nonché nel rispetto degli Obiettivi e Linee guida AGID.

COMPLESSITÀ

Alta

BENEFICI

- Innovazione tecnologica degli applicativi.
- Massimizzazione della resilienza grazie a comportamenti prevedibili dei *software* che aderiscono a un *framework* preimpostato.
- Maggiore efficienza operativa data dalla qualità, velocità e stabilità delle applicazioni.
- Automatizzazione del *provisioning* e della configurazione dell'infrastruttura e conseguente efficientamento delle risorse che possono essere ridistribuite in base alle esigenze dell'applicazione.
- Ottimizzazione del ciclo di vita delle applicazioni, migliorando la scalabilità e il ripristino dei guasti.
- La scomposizione delle applicazioni in servizi indipendenti fa sì che gli aggiornamenti siano più frequenti e che questi possano essere ridimensionati e riavviati senza influire sugli altri servizi.

DEADLINE

Gennaio 2025

Gruppo 2

I5 – ADESIONE AL POLO STRATEGICO NAZIONALE (PSN)

SCENARIO

Il Polo Strategico Nazionale (PSN) offre l'opportunità di valutare la migrazione di applicativi su una piattaforma di tipo *Cloud*. L'Arma dei Carabinieri ha determinato di procedere con la migrazione presso quella struttura di due sistemi richiedenti continui incrementi in termini di storage e capacità computazionali, ovvero **C-Prot** (sistema di gestione documentale) e **C-UNICO** (ERP - sistema per la gestione, in un unico ambiente, dei processi finanziari, contabili, amministrativi e logistici). Il relativo sforzo economico è coperto dal Piano Nazionale di Ripresa e Resilienza (PNRR) per reingegnerizzazione, migrazione, l'*hosting*, connettività e primo anno di canone.

COMPLESSITA'

Alta

BENEFICI

La progettualità garantisce capacità di *storage* e computazionali di assoluto valore, utili per alleggerire i *Data Center* fisici dell'Arma dei Carabinieri dalla necessità di continui approvvigionamenti di hardware sempre più performanti e dalle conseguenti ricerche di risorse economiche dedicate.

DEADLINE

Giugno 2025

Gruppo 2

I6 – RAZIONALIZZAZIONE DEL PARCO APPLICATIVO ATTUALE

SCENARIO

L'intervento è finalizzato all'impostazione di un approccio per l'analisi del parco applicativo attualmente in uso presso l'Arma dei Carabinieri, per procedere con un'eventuale revisione e razionalizzazione degli applicativi stessi in un'ottica di efficientamento.

COMPLESSITÀ

Medio-Alta

BENEFICI

- Riduzione dei costi di sviluppo e di gestione degli applicativi.
- Efficientamento delle operazioni e dell'utilizzo dei dati.
- Miglioramento della comunicazione trasversale tra u.o.
- Digitalizzazione di processi analogici e/o ripetitivi.
- Centralità del dato e interfaccia unica utente.
- Accentramento del dato.

DEADLINE

Settembre 2024

Gruppo 2

I7 – LOG AS - SUPPORTO ALL'AVVIO PER L'INTEGRAZIONE DEL PERIMETRO DELLE SORGENTI

SCENARIO

L'intervento è finalizzato, nell'ambito della piattaforma di tracciamento dei *log*, al completamento dell'integrazione delle restanti 40 sorgenti di *log* definiti dall'Arma.

COMPLESSITÀ

Medio-Bassa

BENEFICI	DEADLINE
Maggiore capacità di monitoraggio dei servizi offerti grazie alla possibilità di analisi dei *log* tracciati.	Dicembre 2024 (Progetti in corso)

I8 – INSTALLAZIONE SISTEMA ASC PRESSO RIS

SCENARIO	COMPLESSITÀ
L'intervento è finalizzato a fornire un sistema composito di apparati e soluzioni applicative idoneo ad utilizzare tecnologie innovative per analizzare la scena del crimine.	Medio

BENEFICI	DEADLINE
- Miglioramento tecnologico a supporto delle analisi delle scene del crimine. - Maggiore capacità di analisi delle scene del crimine.	Dicembre 2024 (Progetti in corso)

I9 – REALIZZAZIONE DI ANELLI IN FIBRA

SCENARIO	COMPLESSITÀ
L'intervento è finalizzato alla realizzazione di anelli in fibra per collegare in un'unica struttura di rete i Comandi Compagnia afferenti alle seguenti aree: - Abruzzo-Molise / L'Aquila-Teramo-Pescara-Campobasso- Isernia; - Lazio/Viterbo; - Liguria-Toscana / La Spezia-Massa Carrara; - Lombardia / Lecco-Como; - Lombardia / Mantova-Cremona-Lodi; - Toscana / Livorno; - Trentino-Alto Adige / Bolzano; - Liguria / Imperia- Savona; - Sardegna.	Medio

BENEFICI	DEADLINE
Miglioramento tecnologico dell'infrastruttura fisica di rete.	Dicembre 2026 (Progetti in corso)

I10 – Evoluzione *SPLUNK*

SCENARIO	COMPLESSITÀ
L'intervento è finalizzato a garantire un sistema di tracciamento dei *log* delle attività svolte dagli Amministratori di Sistema.	Medio

BENEFICI	DEADLINE
- Miglioramento nella gestione delle IT *Operation*. - Evoluzione tecnologica nel monitorare ed elaborare dati in tempo reale.	Dicembre 2024 (Progetti in corso)

I11 – Evoluzione C-PERIODICI

SCENARIO	COMPLESSITÀ
L'intervento è finalizzato a garantire un sistema per gestire scadenze e raccolta dati di periodico interesse della linea gerarchica. L'infrastruttura di produzione è già configurata e operativa, oltre che il *software* già *on-line*. Da settembre 2024, si prevede di rilasciare i periodici per i quali sono pervenuti i moduli di definizione, secondo un calendario in via di definizione.	Medio-Bassa

BENEFICI	DEADLINE
Miglioramento della gestione delle scadenze e della raccolta dati.	Dicembre 2024 (Progetti in corso)

I12 – MODULO DI LAVORAZIONE

SCENARIO	COMPLESSITÀ
Miglioramento dei flussi di collaborazione tra utenti e uffici.	Medio

BENEFICI	DEADLINE
L'intervento è finalizzato a garantire il modulo di "*lavorazione*" e gestione dei flussi di collaborazione tra utenti e uffici con lo scopo di realizzare processi di lavorazione con: - l'introduzione strumenti tecnologici evoluti; - lo snellimento processi decisionali; - l'efficientamento attività burocratiche.	Dicembre 2024 (Progetti in corso)

I13 – APP C-MEDIA

SCENARIO	COMPLESSITÀ
L'intervento è finalizzato a dotare Ufficio Stampa di app la gestione centralizzata dei *file* multimediali per la comunicazione istituzionale, con la realizzazione anche di un *Master Data Management* (MDM).	Medio

BENEFICI	DEADLINE
- Introduzione strumenti tecnologici evoluti. - Miglioramento dell'operatività dell'Ufficio stampa.	Dicembre 2025 (Progetti in corso)

I14 – CENTRI RICREATIVI

SCENARIO

L'intervento è finalizzato a reingegnerizzare l'applicativo Centri Ricreativi anche dal punto di vista di processo, con particolare attenzione alla *privacy*. L'applicativo è già stato reingegnerizzato ed è in fase di *test*.

COMPLESSITÀ

Medio-Alta

BENEFICI

- Miglioramento dell'efficienza dell'applicativo Centri Ricreativi.
- Adeguamento dell'applicativo ai cambiamenti operativi e ai processi interni.

DEADLINE

Marzo 2025
(Progetti in corso)

I15 – C-UNICO – *Asset* veterinari

SCENARIO

L'intervento è finalizzato, nell'ambito della piattaforma ERP dell'Arma, denominata C-UNICO, a gestire gli asset veterinari.

COMPLESSITÀ

Medio-Alta

BENEFICI

- Efficientamento delle funzionalità applicative.
- Miglioramento gestione *asset*.

DEADLINE

Dicembre 2024
(Progetti in corso)

I16 – C-UNICO - *Asset* apparati sanitari

SCENARIO

L'intervento è finalizzato, nell'ambito della piattaforma ERP dell'Arma, denominata C-UNICO, a gestire gli asset apparati sanitari.

COMPLESSITÀ

Medio-Alta

BENEFICI

- Efficientamento delle funzionalità applicative.
- Miglioramento gestione *asset*.

DEADLINE

Dicembre 2024
(Progetti in corso)

I17 – C-UNICO - *Asset* infrastrutture

SCENARIO

L'intervento è finalizzato, nell'ambito della piattaforma ERP dell'Arma, denominata C-UNICO, a gestire gli *asset* infrastrutture.

COMPLESSITÀ

Medio-Alta

BENEFICI	DEADLINE
- Efficientamento delle funzionalità applicative. - Miglioramento gestione *asset*.	Dicembre 2024 (Progetti in corso)

I18 – C-UNICO - *Asset* poligoni	
SCENARIO	**COMPLESSITÀ**
L'intervento è finalizzato, nell'ambito della piattaforma ERP dell'Arma, denominata C-UNICO, a gestire gli *asset* poligoni.	Medio-Alta
BENEFICI	**DEADLINE**
- Efficientamento delle funzionalità applicative. - Miglioramento gestione *asset*.	Dicembre 2024 (Progetti in corso)

4.4 SICUREZZA INFORMATICA

4.4.1 DESCRIZIONE

Considerata la missione, l'ambito e il contesto in cui opera il Comando Generale dell'Arma dei Carabinieri e considerato il periodo storico di trasformazione digitale che si sta affrontando, la definizione di una strategia e di una *roadmap* di "*Cyber Resilience*" risulta essere un tassello fondamentale per la garanzia di riservatezza, integrità e disponibilità delle informazioni e dei servizi erogati.

A tal proposito, il *cybersecurity assessment* condotto presso il III Reparto "*Telematica*" ha consentito di evidenziare i principali *gap* di sicurezza e di definire le conseguenti iniziative da implementare nel breve, medio e lungo periodo, con l'obiettivo di incrementare la postura e il livello di maturità *cybersecurity* dell'Istituzione.

Per il raggiungimento di tale scopo, è stato utilizzato il seguente *framework*:

Figura 24: Framework per la definizione della strategia di cybersecurity

Tale *framework* sintetizza le *capability* di sicurezza definite e contestualizzate per il contesto del Comando Generale. Ciascuna *capability* sottende uno o più controlli/quesiti di sicurezza, utilizzati per la fase di raccolta delle informazioni con gli stakeholder individuati del Comando e per la relativa valutazione dei *gap* e definizione del piano delle iniziative.

In particolare, il dettaglio relativo all'*assessment* condotto nel contesto dell'Arma dei Carabinieri circa l'ambito di "*Sicurezza informatica*" e la definizione dello scenario *to-be* con l'indicazione dei diversi interventi progettuali è contenuto nel documento allegato al presente Piano.

Di seguito, invece, si riportano, gli obiettivi, i risultati attesi e gli interventi progettuali indicati dal Piano Triennale AgID.

4.4.2 OBIETTIVI E RISULTATI ATTESI

AUMENTARE LA CONSAPEVOLEZZA DEL RISCHIO *CYBER* (*CYBERSECURITY AWARENESS*) NELLE PA (AGID OB.6.1)

DESCRIZIONE:

I cambiamenti tecnologici dirompenti, oltre a innumerevoli benefici, hanno determinato opportunità anche per la criminalità informatica. Per questa ragione e per poter considerare nuove strategie di difesa efficienti è necessario aumentare la consapevolezza del rischio *cyber* per una comprensione continuativa delle minacce alla sicurezza informatica, promuovere la cultura *cyber* e migliorare la gestione dei rischi.

RISULTATO ATTESO:

Incremento del livello di *Cyber Security Awareness*.

4.4.3 INTERVENTI PROGETTUALI

SI1 – IMPIEGO DELLE MISURE MINIME DI SICUREZZA ICT	
SCENARIO	**COMPLESSITÀ**
Le PA continuano a seguire le Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni.	Medio-Bassa
BENEFICI	**DEADLINE**
- Aumento della protezione contro le minacce informatiche. - Adeguamento normativo.	Luglio 2025 (PTI AgID)

SI2 – INNALZAMENTO LIVELLI DI SICUREZZA	
SCENARIO	**COMPLESSITÀ**
Incrementare le misure di sicurezza per l'accesso ai servizi dell'Arma esposti sulla rete *Internet*, aggiornare l'App CCToken nonché ~~ad~~ implementare il cambio *password* da *Internet*.	Medio

BENEFICI	DEADLINE
- Maggiore livello di sicurezza dei servizi esposti su *internet*. - Facilitazione dell'aggiornamento dei dati di accesso.	Dicembre 2024 (Progetti in corso)

SI3 – CONTROLLO REMOTO DEI NODI AI FINI DI SICUREZZA TELEMATICI

SCENARIO	COMPLESSITÀ
Potenziamento/Fornitura di piattaforma *software* per innalzare il livello di protezione dei server e delle postazioni di lavoro, monitorando, rilevando e bloccando, in tempo reale, le minacce che superano le difese degli antivirus esistenti.	Medio

BENEFICI	DEADLINE
- Innalzamento livello di sicurezza. - Migliore monitoraggio dei nodi e delle minacce alla sicurezza.	Dicembre 2026 (Progetti in corso)

SI4 – SERVIZIO *MANDIANT THREAT INTELLIGENCE VULNERABILITY*

SCENARIO	COMPLESSITÀ
Il seguente intervento, avviato in data 28 settembre 2023, mira al Servizio della *Società Mandiant* per monitoraggio di una vasta gamma di fonti di informazioni finalizzate ad identificare nuove vulnerabilità, analizzare la loro gravità e il rischio associato. Nel servizio sono comprese anche informazioni su *patch* e soluzioni di mitigazione per le vulnerabilità identificate, nonché avvisi immediati per le nuove minacce *cyber*.	Medio

BENEFICI	DEADLINE
- Innalzamento della capacità di rilevare vulnerabilità e minacce cyber. - Maggiore capacità di individuazione delle soluzioni di mitigazione dei rischi e delle minacce.	Settembre 2026 (Progetti in corso)

SI5 – SERVIZIO DI SECURITY AWARENESS IN FAVORE DEL PERSONALE DELL'ARMA

SCENARIO	COMPLESSITÀ
Sviluppo dei servizi formativi (con sessioni teoriche e pratiche) mirati all'incremento della consapevolezza del personale dell'Arma rispetto alle tematiche di sicurezza informatica, all'uso sicuro dei dispositivi digitali e dei *software*.	Bassa

BENEFICI	DEADLINE
Aumento della consapevolezza in ambito della sicurezza informatica per il personale.	Dicembre 2024 (Progetti in corso)

SI6 – *DEEP INSPECTION* DEL TRAFFICO INBOUND VERSO GLI *ASSET* IT DELL'ARMA

SCENARIO	COMPLESSITÀ
Innalzare i livelli di efficienza e di sicurezza dell'infrastruttura telematica tramite l'implementazione di una tecnologia di "*deep inspection*" del traffico verso i servizi IT esposti sulla rete Internet in grado di individuare, monitorare, segnalare e bloccare attività malevole a danno dei singoli servizi ovvero dell'intera infrastruttura telematica dell'Amministrazione. Comprende le attività di fornitura, installazione, gestione e manutenzione (compreso il *patching*) dei sistemi costituenti le piattaforme HW e SW interessate, allo scopo di tenere costantemente aggiornate le capacità di verifica e controllo del traffico in *best-practice*.	Medio

BENEFICI	DEADLINE
Innalzamento dei livelli di efficienza e sicurezza dell'infrastruttura telematica.	Dicembre 2026 (Progetti in corso)

SI7 – ENTERPRISE OF THINGS

SCENARIO	COMPLESSITÀ
Installazione e alla conduzione di un sistema che abbia la capacità di individuare, pressoché in tempo reale, i "dispositivi di qualunque natura" connessi all'infrastruttura telematica dell'Amministrazione, con riguardo particolare verso quelli che si connettono (o tentano di farlo) al *Data Center* e/o alla rete *Internet*, inclusa la possibilità di interrompere e/o dirottare le connessioni, ovvero i tentativi di connessione, e disabilitare i dispositivi ritenuti insicuri, rischiosi, inaffidabili.	Medio-Alta

BENEFICI	DEADLINE
- Maggiore controllo dei dispositivi connessi all'infrastruttura telematica. - Aumentare la capacità di individuare eventuali malfunzionamenti o anomalie dei dispositivi sull'infrastruttura telematica.	Dicembre 2026 (Progetti in corso)

SI8 – CYBER-DEFENCE CONNESSI CON L'ACCORDO ACN-ARMA e finanziati con fondi PNRR	
SCENARIO	**COMPLESSITÀ**
Garantire gli interventi, per i quali saranno elaborati specifici disciplinari tecnici, riguardanti principalmente i seguenti 5 temi ambiti: - Sistema di *Malware Prediction* sui nodi; - *Vulnerability Management e Penetration Testing*; - *User Behaviour Analytics*; - *Cybersecurity Awareness* per il personale Arma; - *Cybersecurity Training* per gli specialisti dell'Arma.	Medio-Alta
BENEFICI	**DEADLINE**
- Innalzamento livello di sicurezza. - Migliore monitoraggio dei nodi e delle minacce alla sicurezza. - Maggiore controllo dei dispositivi connessi all'infrastruttura telematica. - Incremento della capacità di individuare eventuali malfunzionamenti o anomalie dei dispositivi sull'infrastruttura telematica.	Dicembre 2026 (Progetti in corso)

4.5 LE LEVE PER L'INNOVAZIONE

4.5.1 DESCRIZIONE

Il modello organizzativo deve confermare il ruolo strategico della tecnologia e riconoscere all'ICT la capacità di migliorare i servizi informatici e di sostenere i processi finalizzati al governo dell'organizzazione dell'Arma dei Carabinieri.

La trasformazione digitale ha reso i sistemi informatici sempre più centrali per lo svolgimento delle funzioni istituzionali, al punto da richiedere:
- una vera e propria organizzazione orientata all'ICT, da contestualizzare in senso più ampio nei vari processi di gestione;
- il rafforzamento delle competenze digitali e tecnologiche, necessarie all'acquisizione delle conoscenze e abilità da possedere per poter partecipare attivamente alla trasformazione digitale della PA.

4.5.2 OBIETTIVI E RISULTATI ATTESI

Gli obiettivi relativi a tale ambito di intervento sono in parte definiti dalla Strategia Digitale dell'Arma dei Carabinieri in parte ripresi dagli obiettivi che l'AgID ha individuato nell'ambito del Piano Triennale per l'Informatica.

RAFFORZARE LE COMPETENZE DIGITALI PER LA PA E PER IL PAESE E FAVORIRE L'INCLUSIONE DIGITALE (AGID OB.7.2)

DESCRIZIONE:

Un intervento fondamentale per poter gestire e realizzare la transizione al digitale è rappresentato dallo sviluppo di competenze tecnico-specialistiche in ambito ICT, ma anche di competenze

trasversali e complementari rispetto a quelle di natura puramente tecnica, come ad esempio le *digital soft skill (*a titolo esemplificativo e non esaustivo, *Knowledge Networking, Virtual Communication, Digital Awareness, Self Empowerment)*, per favorire lo sviluppo di una cultura digitale all'interno dell'Arma dei Carabinieri.

Relativamente alle competenze tecnico-specialistiche in ambito ICT, la formazione deve riguardare l'***up-skilling***[20] su tematiche specifiche, legate al ruolo ricoperto dal personale dell'Arma dei Carabinieri, nonché il ***re-skilling*** su competenze tecnologiche, ad esempio quelle relative alle tecnologie digitali strategiche per l'Amministrazione, quali *Cloud*, Intelligenza Artificiale, *Blockchain*, *Data Mining*, IoT ed *Extended Reality*.

Le competenze digitali esercitano un ruolo fondamentale e rappresentano un fattore abilitante, in quanto 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. Pertanto, il *re-skilling* e l'*up-skilling,* su tematiche connesse con la trasformazione digitale, rappresentano dei pilastri dell'imponente investimento previsto nell'ambito del PNRR sul capitale umano della pubblica amministrazione italiana e della Strategia "*Ri-formare la PA*".

RISULTATO ATTESO:

Il rafforzamento delle competenze digitali permetterà all'Arma dei Carabinieri di:

- comprendere le esigenze del personale da inserire in organico e le esigenze formative da soddisfare, al fine di creare un modello di competenze flessibile al cambiamento, nel contesto dell'evoluzione digitale e tecnologica;
- diffondere la cultura digitale nella PA, attraverso la promozione dell'accesso dei dipendenti pubblici a percorsi formativi sulle competenze digitali in *e-learning* e per l'attuazione degli obiettivi del Piano Triennale;
- sviluppare le competenze digitali del personale dell'Arma dei Carabinieri, sulla base della definizione dei percorsi di adeguamento e arricchimento delle competenze digitali, coerenti con i fabbisogni rilevati e funzionali alle esigenze istituzionali, in modo da rafforzare la cultura digitale del proprio personale favorendone lo sviluppo.

RAZIONALIZZAZIONE DELL'ORGANIZZAZIONE IT

DESCRIZIONE:

Un contesto dominato dal crescente utilizzo di tecnologie e di servizi digitali richiede un'evoluzione nella cultura organizzativa e, talvolta, rende necessario un adeguamento dei modelli organizzativi verso strutture più flessibili, agili e collaborative. I tempi del cambiamento organizzativo sono, nella maggior parte dei casi, più lenti rispetto a quelli tecnologici; questo è dovuto principalmente a fattori strutturali come, ad esempio, modelli organizzativi verticali, il sottodimensionamento dell'organico e l'anzianità anagrafica e "*di ruolo*" del personale, che frenano il cambiamento e l'innovazione.

È, dunque, importante individuare opportune soluzioni organizzative, che siano in grado di supportare l'innovazione digitale.

RISULTATO ATTESO:

I principali risultati attesi dalla razionalizzazione dell'organizzazione IT riguarderanno l'introduzione di un modello organizzativo efficiente, flessibile e il rafforzamento della qualità ed efficacia delle attività svolte e dei servizi interni ed esterni attraverso:

- l'introduzione di un sistema di gestione per progetti, in relazione alle iniziative previste dal Piano Triennale. Un sistema di questo tipo prevede la definizione di progetti trasversali alle varie funzioni

[20] https://www.syllabus.gov.it/syllabus/

e comporta la creazione di *team* di lavoro interfunzionali (*team* di progetto) per i quali è necessaria l'introduzione di figure di coordinamento;
- la centralizzazione delle funzioni di coordinamento, a garanzia della coerenza complessiva delle iniziative, in termini di pianificazione, monitoraggio dei progetti, validazione delle architetture e acquisizione di beni e servizi IT;
- l'integrazione dei canali di relazione con gli utenti, al fine di garantire maggiore cooperazione tra gruppi che a vario titolo sono coinvolti nell'erogazione dei servizi, accelerando la risoluzione delle necessità degli utenti;
- la valorizzazione del patrimonio informativo dell'Arma dei Carabinieri, al fine di garantire l'uso efficace ed efficiente delle informazioni quale risorsa determinante e fondamentale per supportare i processi operativi, decisionali e strategici;
- la valorizzazione di competenze specifiche all'interno delle strutture di linea, nell'ottica di razionalizzazione degli assetti e di recupero di efficienza.

DEFINIZIONE DI UN MODELLO ICT PER RAFFORZARE *LA GOVERNANCE*

DESCRIZIONE:

Tra gli obiettivi del Piano Triennale, oltre all'evoluzione e all'accrescimento dei fabbisogni tecnologici, è annoverata anche la definizione di un modello di *Governance* ICT, necessaria per garantire un ottimale uso delle risorse, verificare e monitorare l'affidabilità degli strumenti impiegati, nonché indirizzare correttamente azioni volte ad abilitare un approccio proattivo dell'organizzazione nei confronti dell'adozione di nuove tecnologie. Un ruolo importante nell'ambito della *Governance* ICT è quello del RTD, ovvero la figura dirigenziale incaricata di gestire operativamente la trasformazione digitale dell'amministrazione.

La *Governance* ICT per l'Arma dei Carabinieri consiste nella definizione della struttura del *management* e delle regole attraverso le quali monitorare il raggiungimento degli obiettivi di innovazione tecnologica e digitale prefissati. L'adozione di un modello strutturato di *Governance* consente, inoltre, di monitorare e gestire i cambiamenti che impattano l'ICT, valorizzandolo e preservandone il valore percepito.

È, pertanto, uno strumento utile per gestire gli Ambiti di intervento e gli Interventi progettuali delineati all'interno del Piano Triennale.

RISULTATO ATTESO:

L'adozione di un idoneo modello di ICT da parte dell'Arma dei Carabinieri consentirà di:
- migliorare la definizione e il raggiungimento degli obiettivi di digitalizzazione;
- assicurare il costante allineamento tra esigenze dell'organizzazione e innovazione tecnologica;
- governare il fabbisogno tecnologico, costruendo le relazioni logiche ottimali tra la propria missione, la struttura organizzativa, i processi produttivi e le opportunità offerte dal mercato ICT;
- contribuire all'evoluzione tecnologica e digitale.

4.5.3 INTERVENTI PROGETTUALI[21]

Nella seguente tabella sono riportati gli interventi progettuali individuati nell'ambito in questione:

O1 – MAPPATURA COMPETENZE ICT	
SCENARIO	**COMPLESSITÀ**
L'intervento è finalizzato ad effettuare uno *skill assessment* dei ruoli professionali relativi agli ambiti ICT con costruzione di una *gap-analysis* che fornisca elementi oggettivi per la definizione dei bisogni formativi.	Medio-Bassa
BENEFICI	**DEADLINE**
- Chiarezza sul quadro delle competenze detenute e del loro livello. - Aumento della consapevolezza riguardo le competenze delle risorse. - Analisi dei fabbisogni formativi del personale (*gap analysis*) e elaborazione di piani di formazione che tengano conto delle competenze attuali e da sviluppare.	Luglio 2025 Gruppo 3

O2 – COSTRUZIONE DI PERCORSI DI *DIGITAL UPSKILLING* IN AMBITO ICT	
SCENARIO	**COMPLESSITÀ**
L'intervento è finalizzato alla progettazione dei più idonei percorsi di formazione che mirano a migliorare le competenze digitali, sulla base dello *skill assessment* e della *gap analysis* effettuata e in funzione dei profili professionali richiesti in ambito ICT.	Medio-Bassa
BENEFICI	**DEADLINE**
- Efficientamento della formazione e dell'apprendimento. - Massimizzazione dei risultati dell'apprendimento. - Miglioramento della produttività delle risorse. - Favorire lo sviluppo di ulteriori capacità. - Favorire percorsi di crescita all'interno dell'organizzazione.	Gennaio 2025 Gruppo 1

O3 – DEFINIZIONE DI UN SISTEMA DI GESTIONE E MONITORAGGIO DEI PROGETTI	
SCENARIO	**COMPLESSITÀ**
L'intervento è finalizzato all'individuazione di strumenti e procedure più adeguate alla costruzione di un sistema per la gestione e il monitoraggio dei progetti ICT.	Bassa

[21] La modalità di definizione della deadline e del gruppo di riferimento per ciascun intervento progettuale è dettagliata all'interno del capitolo 7 "*Prioritizzazione degli interventi*".

BENEFICI	DEADLINE
- Valutazione costante dell'andamento dei progetti. - Misurazione del raggiungimento degli obiettivi/programmi. - Favorisce l'individuazione di problematiche e consente l'attivazione di azioni correttive. - Creazione di reportistica *ad hoc*.	Dicembre 2025 Gruppo 1

O4 – DEFINIZIONE DI UN MODELLO DI GOVERNANCE ICT

SCENARIO	COMPLESSITÀ
L'intervento è finalizzato alla definizione di una struttura manageriale e di *governance* nonché alla definizione di ruoli e responsabilità nell'ambito della gestione dei progetti ICT.	Medio-Bassa

BENEFICI	DEADLINE
- Governo delle conoscenze applicative e infrastrutturali strategiche per l'organizzazione. - Favorisce la gestione efficiente dei cambiamenti in ambito ICT. - Assicura il raggiungimento degli obiettivi e delle strategie dell'organizzazione. - Assicura che gli investimenti IT generino valore per l'organizzazione. - Garantisce la gestione dei rischi associati all'IT.	Luglio 2025 Gruppo 3

O5 – UTILIZZO DEL PIANO OPERATIVO DELLA STRATEGIA NAZIONALE

SCENARIO	COMPLESSITÀ
Le PA, in funzione delle proprie necessità, utilizzano tra i riferimenti per i propri piani di azione quanto previsto nel Piano operativo della strategia nazionale per le competenze digitali aggiornato 2023.	Medio-Bassa

BENEFICI	DEADLINE
- Miglioramento degli strumenti di monitoraggio delle linee di intervento, come indicate nella Strategia Nazionale Competenze Digitali. - Incremento delle competenze digitali. - Adeguamento normativo.	Da gennaio 2025 (PTI Agid)

4.6 TECNOLOGIE INNOVATIVE

4.6.1 DESCRIZIONE

L'ambito di intervento "*Tecnologie innovative*" fa riferimento all'implementazione delle tecnologie più strategiche per l'Arma, da adottare non solo per essere in linea con le evoluzioni del mercato e

accogliere gli indirizzi derivanti dal contesto normativo, ma soprattutto per garantire una più **efficace** ed **efficiente gestione** dei **processi operativi** e di quelli **strategico decisionali**, nonché per la **corretta** e **sicura gestione** dei **dati** e delle **informazioni**.

L'adozione di nuove tecnologie, inoltre, consente di modificare l'approccio e le modalità con cui si svolgono le attività, innescando meccanismi che permettono di sperimentare nuove modalità di lavoro, offrire nuovi servizi e creare un circolo virtuoso per il miglioramento continuo, che renda l'organizzazione dell'Arma capace di adattarsi facilmente ai cambiamenti.

4.6.2 OBIETTIVI E RISULTATI ATTESI

Gli obiettivi relativi a tale ambito di intervento sono in parte definiti dalla Strategia Digitale dell'Arma dei Carabinieri ed in parte sono ripresi dagli obiettivi che l'AgID ha stilato nell'ambito del Piano Triennale per l'Informatica.

ADOZIONE DI TECNOLOGIE INNOVATIVE

DESCRIZIONE:

L'adozione e l'uso sinergico delle nuove tecnologie IT come l'*Internet of Things* (IoT), l'*Artificial Intelligence* (AI) e il *Machine Learning* (ML) rappresentano una rilevante fonte di innovazione e degli elementi cruciali per rafforzare e ampliare i vantaggi legati al percorso di digitalizzazione.

In particolare, l'IoT consentirebbe al Comando Generale dell'Arma di generare un complessivo efficientamento interno: tale tecnologia, infatti, consentirebbe il soddisfacimento delle esigenze di collegamento dei dispositivi più difficili da collegare e, con l'ausilio del 5G, favorirebbe l'acquisizione, l'elaborazione e la condivisione di dati strategici. Tale tecnologia potrebbe, ad esempio, essere applicata al parco mezzi della F.A., favorendo una gestione più consapevole e razionale dei diversi veicoli utilizzati: la diagnostica predittiva, infatti facilita la gestione del ciclo di vita delle componenti del veicolo e il monitoraggio delle condizioni del sistema, favorendo la pianificazione ottimizzata delle attività di manutenzione in base ai dati di stato del veicolo collegato. In tal modo, si avrebbe una maggiore visibilità e un elevato controllo in tempo reale delle condizioni e dello stato generale degli *asset*, con rilevanti benefici per l'efficienza operativa.

Ulteriori vantaggi, possono derivare dalla combinazione sinergica dell'IoT e delle tecnologie di *Artificial Intelligence* e del *Machine Learning*. L'uso congiunto dell'AI e degli algoritmi di ML consentirebbe di estrapolare il massimo valore dai dati al fine di ottimizzare i processi decisionali. In questo modo, l'uso delle tecniche statistiche dell'apprendimento automatico favorirebbe l'analisi degli eventi/dati storici e attuali e potrebbe fornire valutazioni previsionali.

RISULTATO ATTESO:

I principali risultati attesi derivanti dall'adozione delle nuove tecnologie IT sono rappresentati dal:

- miglioramento delle capacità di monitoraggio in tempo reale degli *asset* (ad esempio monitoraggio intelligente delle scorte e dei consumi) e del personale operativo in attività (es. tracciamento della posizione);
- analisi dei dati e generazione/raccolta di *insights* attraverso gli algoritmi di AI e ML, al fine di migliorare i processi decisionali;
- potenziamento della sicurezza fisica grazie all'implementazione di sensori IoT interconnessi.

4.6.3 INTERVENTI PROGETTUALI[22]

Nella tabella seguente sono riportati gli interventi progettuali individuati nell'ambito in questione:

T1 – PIANO DI AMMODERNAMENTO DEGLI STRUMENTI DI "BUSINESS INTELLIGENCE"	
SCENARIO	**COMPLESSITÀ**
L'intervento è orientato a definire un piano di ammodernamento degli strumenti di BI finalizzato alla migrazione delle piattaforme obsolete su versioni aggiornate.	Medio-Alta
BENEFICI	**DEADLINE**
- Miglioramento delle prestazioni analitiche. - Aumentare la qualità e l'accuratezza dei dati. - Riduzione dei tempi di acquisizione ed elaborazione dei dati grazie all'uso di strumenti di BI più performanti.	Gennaio 2025 Gruppo 2

T2 – ADOZIONE DI SENSORISTICA E DI STRUMENTAZIONE ADEGUATA ALL'IMPLEMENTAZIONE DELL'IOT	
SCENARIO	**COMPLESSITÀ**
L'intervento è orientato ad identificare ed adottare la sensoristica e i principali strumenti necessari ad una graduale implementazione dell'IoT nell'ambito della gestione e controllo del parco mezzi dell'Arma dei Carabinieri, consentendo un monitoraggio continuo ed in tempo reale dei veicoli.	Medio-Alta
BENEFICI	**DEADLINE**
- Utilizzo di dati raccolti dai sensori per il monitoraggio da remoto. - Maggiore capacità di raccolta e analisi dati in tempo reale. - Gestione centralizzata del monitoraggio finalizzato all'assistenza. - Creazione di un sistema di interoperabilità dei dati.	Febbraio 2025 Gruppo 2

4.7 LINEE D'AZIONE TRAGUARDATE

Rispetto agli obiettivi 2022-2024 definiti da AgID per la Pubblica Amministrazione, di seguito vengono riportate le linee d'azione già traguardate dall'Arma dei Carabinieri.

SERVIZI		
Obiettivo PT 2022-2024	**Risultato Atteso**	**Linee d'azione**

[22] La modalità di definizione della deadline e del gruppo di riferimento per ciascun intervento progettuale è dettagliata all'interno del capitolo 7 "*Prioritizzazione degli interventi*".

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	Le PA pubblicano le statistiche di utilizzo dei propri siti *web* e possono, in funzione delle proprie necessità, aderire a *Web Analytics* Italia per migliorare il processo evolutivo dei propri servizi *online* - **CAP1.PA.LA01**
	R.A.1.1d Diffusione del monitoraggio, da parte delle Amministrazioni, della fruizione dei servizi digitali	**Entro ottobre 2022 -** Le PA adeguano le proprie procedure di *procurement* alle Linee Guida di AGID sull'acquisizione del *software* e al CAD (artt. 68 e 69) - **CAP1.PA.LA04**
		Entro dicembre 2022 - Le amministrazioni coinvolte nell'attuazione nazionale del Regolamento sul *Single Digital Gateway* attivano *Web Analytics* Italia per tutte le pagine da loro referenziate sul *link repository* europeo - **CAP1.PA.LA18**
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 disponibili in *Designers* Italia	Le PA effettuano *test* di usabilità e possono comunicare ad AGID, tramite l'applicazione form.agid.gov.it, l'esito dei test di usabilità del proprio sito istituzionale - **CAP1.PA.LA10**
		Le PA devono seguire i principi delle Linee guida di design per i siti *internet* e i servizi digitali della PA - **CAP1.PA.LA26**
		Entro dicembre 2022 - Le Amministrazioni adeguano i propri siti *web* rimuovendo, tra gli altri, gli errori relativi a 2 criteri di successo più frequentemente non soddisfatti, come pubblicato sul sito di AGID - **CAP1.PA.LA21**
	R.A.1.2b Diffusione dei test di usabilità nelle amministrazioni per agevolare il *feedback* e le valutazioni da parte degli utenti	**Entro marzo 2023** - Entro 31 marzo 2023 le PA devono pubblicare gli obiettivi di accessibilità sul proprio sito - **CAP1.PA.LA16**
		Entro settembre 2023 - Le PA pubblicano, entro il 23 settembre 2023, tramite l'applicazione form.agid.gov.it, una dichiarazione di accessibilità per ciascuno dei propri siti *web* e APP mobili - **CAP1.PA.LA28**
		Entro dicembre 2023 - Le PA comunicano ad AGID, tramite l'applicazione form.agid.gov.it, l'esito dei *test* di usabilità del proprio sito istituzionale - **CAP1.PA.LA23**

PIATTAFORME

Obiettivo PT 2022-2024	Risultato Atteso	Linee d'azione

OB.3.2 Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle Pubbliche Amministrazioni	**R.A.3.2a** Incremento dell'adozione e dell'utilizzo di SPID e CIE da parte delle Pubbliche Amministrazioni	Le PA e i gestori di pubblici servizi proseguono il percorso di adesione a SPID e CIE e dismettono le altre modalità di autenticazione associate ai propri servizi online - **CAP3.PA.LA07**

SICUREZZA		
Obiettivo PT 2022-2024	**Risultato Atteso**	**Linee d'azione**
OB.6.1 Aumentare la consapevolezza del rischio *cyber* (*Cybersecurity Awareness*) nelle PA	**R.A.6.1a** Incremento del livello di *Cybersecurity Awareness*.	Le PA nei procedimenti di acquisizione di beni e servizi ICT devono far riferimento alle Linee guida sulla sicurezza nel procurement ICT - **CAP6.PA.LA01**
		Entro dicembre 2022 - Le PA possono definire, in funzione delle proprie necessità, all'interno dei piani di formazione del personale, interventi sulle tematiche di *Cybersecurity Awareness* - **CAP6.PA.LA05**
OB.6.2 Aumentare il livello di sicurezza informatica dei portali istituzionali della PA	**R.A.6.2a** Incremento del numero dei portali istituzionali che utilizzano il protocollo HTTPS only, misurato tramite tool di analisi specifico.	Le PA devono mantenere costantemente aggiornati i propri portali istituzionali e applicare le correzioni alle vulnerabilità - **CAP6.PA.LA08**

LE LEVE PER L'INNOVAZIONE		
Obiettivo PT 2022-2024	**Risultato Atteso**	**Linee d'azione**
OB.7.2 Rafforzare le competenze digitali per la PA e per il Paese e favorire l'inclusione digitale.	**R.A.7.2a** Diffusione delle competenze digitali nella PA, attraverso la promozione dell'accesso da parte dei dipendenti pubblici a percorsi formativi sulle competenze digitali in *e-learning*.	Le PA, in funzione delle proprie necessità, partecipano alle iniziative pilota, alle iniziative di sensibilizzazione e a quelle di formazione di base e specialistica previste dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali - **CAP7.PA.LA12**
		Le PA aderiscono all'iniziativa "*Syllabus per la formazione digitale*" e promuovono la partecipazione alle iniziative formative sulle competenze di base da parte dei dipendenti pubblici, concorrendo al conseguimento dei *target* del PNRR in tema di sviluppo del capitale umano della PA e in linea con il Piano strategico nazionale per le

		competenze digitali - **CAP7.PA.LA19**
		Le PA, in funzione delle proprie necessità, partecipano alle attività di formazione "*Monitoraggio dei contratti ICT*" secondo le indicazioni fornite da AGID - **CAP7.PA.LA13**
	R.A.7.2c Diffusione delle competenze digitali nella PA per l'attuazione degli obiettivi del Piano triennale.	**Da marzo 2023** - Le PA, in funzione delle proprie necessità, utilizzano tra i riferimenti per i propri piani di azione quanto previsto nel Piano operativo della strategia nazionale per le competenze digitali aggiornato 2022 - **CAP7.PA.LA16**

GOVERNANCE		
Obiettivo PT 2022-2024	**Risultato Atteso**	**Linee d'azione**
OB.8.1 Migliorare i processi di trasformazione digitale della PA	**R.A.8.1b** Aumento delle PA con RTD nominato e promozione e diffusione di modalità e modelli di consolidamento del ruolo dei RTD, anche in forma aggregata presso la PAL.	Le PA che hanno nominato il RTD possono aderire alla piattaforma di *community* al fine di partecipare attivamente ai lavori - **CAP8.PA.LA07**
		Le PA, in base alle proprie esigenze, partecipano alle iniziative di formazione per RTD e loro uffici proposte da AGID - **CAP8.PA.LA32**

ACETO PAOLO
ARMA DEI
CARABINIERI
25.09.2024
07:30:55 UTC