Ente di gestione delle aree protette dei Parchi Reali

***Sede legale**: viale C. Emanuele II, 256 – 10078 Venaria Reale (TO) – tel. 011 4993328*
***Sede operativa di Stupinigi**: viale Torino 4, (fraz. Stupinigi) – 10042 Nichelino (TO) – tel. 011 3587575*
partita IVA e codice fiscale 01699930010
http://www.parchireali.it – email: protocollo@parchireali.to.it – parchireali@legalmail.it

Piano di Procurement ICT anno 2025

Sommario

1. INTRODUZIONE E QUADRO NORMATIVO

Il procurement ICT nella Pubblica Amministrazione non si limita alla sola scelta di un fornitore: è un processo complesso, che inizia con la pianificazione strategica e si conclude con il monitoraggio dell'esecuzione contrattuale e la gestione del ciclo di vita delle soluzioni acquisite.

Gli acquisti ICT della Pubblica Amministrazione si riferiscono all'approvvigionamento di beni e servizi informatici e di telecomunicazione, come computer, software e infrastrutture di rete, necessari alle PA per svolgere le proprie attività.

Le infrastrutture di rete sono l'insieme di hardware, software e tecnologie che permettono la connessione e la comunicazione tra dispositivi e sistemi informatici, abilitando il flusso dei dati, l'accesso a Internet e la condivisione di risorse. Componenti chiave includono router, switch, server, cavi, access point e protocolli di rete, che lavorano insieme per instradare le informazioni e garantire la sicurezza e scalabilità delle reti.

Le Linee guida AgID forniscono un insieme di buone pratiche per assicurare che ogni acquisizione ICT sia:

- Sicura (conforme agli standard di sicurezza informatica nazionali ed europei)
- Efficiente (rispettosa dei tempi e dei budget)
- Trasparente (in linea con il principio di pubblicità e imparzialità)
- Sostenibile (favorendo riuso, open source e soluzioni interoperabili)

1.1. Finalità del documento

- Garantire continuità operativa e sicurezza in tutte le fasi del ciclo di vita delle forniture ICT.
- Favorire il riuso e l'adozione di software open source ove possibile.
- Integrare attività di risk assessment, business impact analysis e audit come elementi strutturali del processo.

1.2. Contesto normativo

Il presente piano è redatto sulla base dei seguenti e principali riferimenti normativi:

- D.Lgs. 36/2023 – Codice dei Contratti Pubblici
- Legge 90/2024 – norme sulla cybersicurezza nella PA
- Linee Guida AgID – procurement ICT, riuso software, sviluppo sicuro
- Regolamento Cloud PA – in vigore dal 1 agosto 2024
- Direttiva NIS2 – sicurezza delle reti e sistemi informativi
- Piano della sicurezza informatica dell'EGAP Parchi Reali
- Piano Triennale per la Transizione Digitale dell'EGAP Parchi Reali
- Piano della protezione e modello organizzativo a tutela dei dati personali dell'EGAP Parchi Reali
- Piano integrato di attività e organizzazione dell'EGAP Parchi Reali (PIAO)
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)
- Disciplinare interno per l'utilizzo degli Strumenti Informatici dell'EGAP Parchi Reali

2. PRINCIPI GENERALI

Il presente Piano di Procurement ICT ha lo scopo di definire la strategia, le linee guida e le azioni necessarie affinché l'Ente possa acquisire, gestire e mantenere soluzioni ICT conformi agli standard di sicurezza, efficienza e trasparenza richiesti dalla normativa vigente e dalle best practice di settore.

Il Piano si basa su principi fondamentali volti a garantire la sicurezza, l'affidabilità e la sostenibilità delle forniture ICT, con particolare attenzione ai rischi informatici e alla tutela dei dati personali.

L'Ente si impegna a rispettare i seguenti requisiti di sicurezza nell'ambito del procurement ICT:

- **Confidenzialità:** Assicurare che le informazioni e i dati sensibili gestiti attraverso le soluzioni ICT siano protetti da accessi non autorizzati, garantendo il rispetto della normativa sulla protezione dei dati personali (GDPR e normativa nazionale).
- **Integrità:** Garantire che i dati e i sistemi non vengano alterati in modo non autorizzato durante tutte le fasi del ciclo di vita della fornitura, inclusa la trasmissione, l'elaborazione e l'archiviazione.
- **Disponibilità:** Assicurare la continuità operativa e l'accessibilità delle soluzioni ICT secondo i livelli di servizio concordati, minimizzando i tempi di inattività e prevenendo eventi di interruzione.
- **Tracciabilità:** Mantenere un'adeguata documentazione e registrazione degli accessi e delle attività eseguite sui sistemi ICT, per consentire audit e verifiche di sicurezza.
- **Conformità normativa:** Adeguare le procedure di procurement e gestione delle forniture ICT alle disposizioni legislative, regolamentari e alle linee guida AgID, con particolare attenzione agli obblighi in materia di sicurezza informatica e protezione dei dati.
- **Gestione del rischio:** Eseguire valutazioni di rischio e business impact analysis per identificare, classificare e mitigare le minacce e le vulnerabilità associate ai beni e servizi ICT acquisiti.
- **Sostenibilità e riuso:** Promuovere l'utilizzo di soluzioni a basso impatto ambientale, favorendo il riuso e l'adozione di software open source, in linea con i principi di innovazione e trasparenza.
- **Responsabilità e governance:** Definire chiaramente i ruoli e le responsabilità interne per la gestione del procurement ICT

Oltre ai principi già previsti, l'Ente si impegna a rispettare i seguenti obblighi in materia di protezione dati personali:

- **Sicurezza by Design e by Default (art. 32 GDPR):** Gli strumenti ICT devono essere sicuri, progettati e configurati fin dall'origine per garantire un livello di protezione adeguato al rischio. L'Ente, tenendo conto dello stato dell'arte, dei costi di attuazione e della natura del trattamento, si impegna a richiedere e verificare misure tecniche e organizzative adeguate, quali pseudonimizzazione e cifratura dei dati personali, resilienza dei sistemi, capacità di ripristino e procedure di test periodici delle misure adottate
- **Privacy by Design (art. 25 GDPR):** La tutela dei dati personali deve essere integrata sin dalla fase di progettazione dei servizi, processi o prodotti ICT. Nei casi di esternalizzazione, l'Ente inserirà prescrizioni specifiche e dettagliate in materia di protezione dei dati direttamente nei documenti di gara (bando, capitolato tecnico, schema di contratto), evitando richiami generici alla conformità al GDPR

3. RUOLI E RESPONSABILITÀ NEL PROCUREMENT ICT

Un procurement ICT sicuro ed efficace richiede ruoli ben definiti. Ogni figura ha compiti precisi, competenze specifiche e responsabilità formali, documentate in una matrice di ruoli e responsabilità (AG3).

3.1. Ruoli e responsabilità - matrice RACI (Responsible, Accountable, Consulted, Informed)

Ruolo	Descrizione	Responsabilità principali
Area/Servizio Richiedente	Ufficio o reparto che identifica la necessità di acquisto ICT	Formulare e inviare la richiesta al Servizio Informatico- Collaudare il prodotto o servizio acquisito
Servizio Informatico	Reparto tecnico che supporta e definisce i requisiti tecnici	Analizzare esigenze- Definire requisiti tecnici o specifiche prodotto- Coordinare con Amministratore di Sistema e DPO
Amministratore di Sistema	Esperto tecnico responsabile della sicurezza e gestione ICT	Validare requisiti di sicurezza e conformità- Monitorare sicurezza durante e dopo l'acquisto
DPO (Data Protection Officer)	Responsabile privacy e conformità al GDPR	Verificare conformità privacy dei prodotti e servizi ICT- Fornire consulenza su rischi privacy
Servizio Provveditorato e contratti	Ufficio responsabile dell'acquisto e contrattualizzazione	Preparare e gestire gare o contratti- Effettuare l'acquisto e formalizzare contratti - Assicurare che nei capitolati e negli schemi contrattuali siano inserite clausole dettagliate di protezione dei dati personali (non solo richiami generici al GDPR).
RUP (Responsabile Unico del Procedimento)	Figura che coordina e controlla tutte le fasi del progetto, garantendo tempi, costi, qualità e correttezza delle procedure	Nominato per ogni singolo procedimento di gara o appalto, ha la responsabilità di seguire tutte le fasi del procurement
RSI (Responsabile dei Sistemi Informativi)	Responsabile della gestione, sviluppo e sicurezza dei sistemi informatici dell'Ente	Guida la strategia ICT dell'Ente, coordina le funzioni coinvolte e approva le scelte tecnologiche
Organo politico	Organo di indirizzo e controllo politico-amministrativo	Definire le linee strategiche ICT, approvare il piano annuale e pluriennale di procurement
Fornitore ICT	Soggetto esterno incaricato della fornitura di beni/servizi ICT	Eseguire la fornitura secondo i requisiti contrattuali – Dimostrare l'adeguatezza tecnica e organizzativa (artt. 28 e 32 GDPR) – Garantire sicurezza, tracciabilità e compliance – Collaborare in fase di collaudo, audit e cessazione del rapporto (incl. cancellazione/restizione dati)

3.2. Matrice ruoli-fasi

Fase	Responsabile (R)	Accountable (A)	Consultato (C)	Informato (I)
Richiesta e raccolta esigenze	Area/Servizio Richiedente	Servizio Informatico – RUP	Amministratore di Sistema - DPO	Servizio Provveditorato e contratti – RSI - Fornitore ICT (solo se già in rapporto contrattuale continuativo)

Fase	Responsabile (R)	Accountable (A)	Consultato (C)	Informato (I)
Analisi e definizione requisiti	Servizio Informatico	Servizio Informatico – RUP - RSI	Amministratore di Sistema – DPO - Fornitore ICT (per chiarimenti tecnici, best practice, standard di settore)	Area/Servizio Richiedente
Preparazione gara/contratto	Servizio Provveditorato e contratti	RUP	Servizio Informatico - RSI	Area/Servizio Richiedente - Fornitore ICT (solo in caso di consultazioni preliminari di mercato)
Acquisto e contrattualizzazione	Servizio Provveditorato e contratti - Fornitore ICT (esecuzione contrattuale)	RUP	Amministratore di Sistema - RSI	Area/Servizio Richiedente
Collaudo e verifica finale	Area/Servizio Richiedente - Fornitore ICT (esecuzione test/collaudo assistito)	Servizio Informatico – RUP - RSI	Amministratore di Sistema	Servizio Provveditorato e contratti
Monitoraggio sicurezza	Amministratore di Sistema - Fornitore ICT (implementazione e supporto tecnico per patch/aggiornamenti)	Servizio Informatico	DPO - RSI	RUP
Approvazione strategica finale		Organo politico	RSI – DPO – RUP	Tutti i servizi coinvolti

- **Responsabile (R)**: La persona o il gruppo che svolge effettivamente il lavoro o compie l'attività.
- **Accountable (A)**: Chi ha la responsabilità finale del corretto completamento dell'attività o decisione.
- **Consultato (C)**: Chi viene coinvolto per dare pareri, informazioni o consigli. Sono persone che devono essere consultate prima di prendere decisioni o agire.
- **Informato (I)**: Chi deve essere tenuto aggiornato sugli sviluppi e i risultati.

3.3. Matrice Criticità e Rischi ICT

Area / Rischio	Descrizione	Probabilità	Impatto	Livello Rischio	Contromisure
Sicurezza rete	Attacchi informatici (intrusioni, exploit)	Alta	Alto	Alto	Firewall, IDS/IPS, monitoraggio continuo
Software obsoleto	Vulnerabilità note in software non aggiornato	Media	Alto	Alto	Aggiornamenti regolari, gestione patch
Gestione fornitori	Inadempienze contrattuali o falle di sicurezza esterne	Media	Alto	Alto	Clausole contrattuali, audit fornitori

Area / Rischio	Descrizione	Probabilità	Impatto	Livello Rischio	Contromisure
Backup dati	Perdita o corruzione di dati	Bassa	Alto	Medio	Backup periodici, test di ripristino
Phishing e Social engineering	Furto credenziali e accessi tramite inganni	Alta	Alto	Alto	Formazione personale, filtri email
Malware e ransomware	Cifratura o distruzione dei dati	Alta	Alto	Alto	Antivirus aggiornati, segmentazione rete
Violazione accessi	Accessi non autorizzati a dati o sistemi	Alta	Alto	Alto	MFA, gestione permessi, logging accessi
Interruzione servizio (DoS/DDoS)	Blocco temporaneo dei servizi online	Media	Medio	Medio	CDN, mitigazione DDoS, bilanciamento carichi
Errore umano	Azioni involontarie dannose (cancellazioni, configurazioni errate)	Alta	Medio	Alto	Formazione, procedure operative
Mancata conformità normativa	Violazione GDPR o regolamenti di settore	Media	Alto	Alto	Audit periodici, DPO, DPIA
Dispositivi non protetti	Uso di device personali senza protezioni adeguate	Media	Alto	Alto	Politiche BYOD, cifratura dispositivi
Vulnerabilità nelle API	Exploit tramite interfacce di programmazione	Media	Alto	Alto	API gateway, test di sicurezza
Mancata gestione patch	Ritardi nell'applicazione di aggiornamenti critici	Alta	Alto	Alto	Processo di patch management
Cloud non sicuro	Configurazioni errate o mancata protezione in cloud	Media	Alto	Alto	Audit cloud, crittografia, gestione chiavi
Bias algoritmico / Attacchi adversarial (AI)	Errori o discriminazioni dovuti a dataset non bilanciati o manipolazione dei modelli IA tramite input malevoli	Media	Alto	Alto	Audit algoritmici periodici, revisione dataset, clausole contrattuali su trasparenza AI, supervisione umana delle decisioni, test adversarial specifici

4. STRUTTURA DELLE FASI DEL PROCUREMENT ICT

Il percorso per l'acquisto di beni e servizi ICT nella Pubblica Amministrazione è diviso in tre momenti fondamentali: Programmazione e Progettazione, Affidamento, e Esecuzione con Monitoraggio. Questo serve a garantire che ogni acquisto:

- risponda davvero alle esigenze dell'Ente
- rispetti le leggi in vigore
- sia sicuro in tutte le sue fasi, dalla pianificazione fino all'utilizzo
- possa essere seguito e controllato nel tempo

Le azioni contenute nel presente piano sono suddivise in quattro categorie, in linea con le indicazioni fornite dalle Linee Guida AGID per il procurement ICT nella Pubblica Amministrazione:

- **AG (Azioni Generali):** si riferiscono alle attività da svolgere nella fase di **programmazione e progettazione**, fondamentali per preparare correttamente l'acquisizione dei beni e servizi ICT
- **AP (Azioni Procurement)**: riguardano le operazioni da effettuare nella fase di **affidamento**, cioè la scelta della procedura, la selezione del fornitore e la definizione delle clausole contrattuali
- **AC (Azioni Contratto)**: indicano le attività da eseguire nella fase di **esecuzione e monitoraggio del contratto**, volte a garantire il rispetto degli accordi e la sicurezza continua durante tutto il ciclo di vita della fornitura
- **AI (Azioni Intelligenza Artificiale):** indicano le attività specifiche per **integrare l'intelligenza artificiale nel procurement ICT**, comprendenti la definizione dei requisiti funzionali ed etici, audit algoritmico, clausole contrattuali dedicate, monitoraggio post-implementazione e valutazione dei rischi algoritmici.

Ciclo di vita del Procurement ICT

Questa suddivisione riflette la struttura metodologica suggerita da AGID per assicurare un processo di procurement ICT sicuro, efficiente e conforme alle normative vigenti.

4.1. Fase di Programmazione e Progettazione (Azioni AG)

Durante questa fase, l'Ente:

- Pianifica l'acquisizione partendo dall'analisi dei bisogni
- Mappa e classifica le proprie risorse ICT
- Definisce ruoli, responsabilità e competenze interne
- Prepara le basi per le fasi successive

Secondo le Linee Guida AgID in questa fase è essenziale

- Conoscere lo stato attuale dell'infrastruttura ICT
- Valutare rischi e impatti (Risk Assessment e Business Impact Analysis)
- Definire standard e metodologie di sicurezza
- Organizzare la capacità interna di fare audit e monitoraggio

4.1.1. Azioni AG: linee guida AGID e azioni implementate dall'Ente

Codice Azione	Descrizione Azione	Azioni Implementate dall'Ente
AG1.1 – Competenze	Attivare percorsi di aggiornamento professionale per il personale su procurement management, project management, asset management, change management, risk management e sicurezza informatica.	A tal fine, sono state messe a disposizione piattaforme di formazione sia con operatori privati specializzati, sia tramite piattaforme ministeriali ufficiali, per garantire l'acquisizione delle competenze necessarie e aggiornate in tutti gli ambiti indicati.
AG1.2 – Formazione	Erogare corsi specifici sul procurement ICT e sugli aspetti legali/tecnici della sicurezza.	A tal fine, sono state messe a disposizione piattaforme di formazione sia con operatori privati specializzati, sia tramite piattaforme

Codice Azione	Descrizione Azione	Azioni Implementate dall'Ente
		ministeriali ufficiali, per garantire l'acquisizione delle competenze necessarie e aggiornate in tutti gli ambiti indicati.
AG2 – Analisi Esperienze pregresse	Raccolta di casi di successo e insuccesso da precedenti gare ICT, con focus sulle criticità di sicurezza.	Ogni volta che l'Ente avvia un nuovo processo di procurement ICT, viene attivato un percorso specifico per raccogliere e analizzare le esperienze pregresse relative a casi simili. Il processo include confronto con altri enti pubblici e analisi di documenti e linee guida nazionali. L'obiettivo è creare una base di conoscenza solida per identificare best practice e criticità da integrare nelle fasi successive.
AG3 – Matrice ruoli e responsabilità	Definire e formalizzare la matrice RACI (Responsible, Accountable, Consulted, Informed)	L'Ente ha definito ruoli e responsabilità nelle varie fasi del procurement ICT, assegnando incarichi formali ai profili più idonei all'interno della struttura organizzativa. La matrice RACI è stata formalizzata e riportata in dettaglio nel punto 3.1.
AG4 – Inventario beni ICT	Redigere e mantenere un inventario aggiornato di hardware, software e servizi ICT.	In linea con il Piano della Sicurezza Informatica, l'Amministratore di Sistema redige e mantiene costantemente aggiornato un elenco dettagliato di tutto il patrimonio ICT, strumento fondamentale per la gestione efficace delle risorse e per supportare le attività di sicurezza e monitoraggio nel tempo.
AG5 – Classificazione beni e servizi	Classificare le risorse ICT in base a tecnologia, neutralità tecnologica, GDPR, automazione, impatto e sicurezza.	L'Ente applica questa prassi ogni volta che deve effettuare un nuovo acquisto ICT, classificando le risorse secondo i criteri indicati, valutando tecnologia, privacy, impatto e sicurezza e svolgendo analisi di rischio e business impact come previsto dal Piano della Sicurezza Informatica.
AG6 – Metodologia audit fornitori	Definire processo di audit e controlli di conformità da inserire nei capitolati di gara.	L'Ente ha sviluppato un processo interno di controlli e audit sui fornitori ICT per verificare il rispetto dei requisiti di sicurezza e contrattuali. Sono state definite responsabilità, inserite clausole nei capitolati di gara per verifiche in corso d'opera, e redatte linee guida su modalità, tempi e reportistica degli audit. Ciò permette di monitorare costantemente gli standard di qualità e sicurezza richiesti.

4.1.2. Tabella operativa Azioni AG

Cod. Azione	Descrizione sintetica	Ruolo responsabile	Output richiesto	Riferimento normativo	Esempio pratico
AG1.1	Aggiornamento competenze su procurement	Servizio Provveditorato e contratti	Attestati di formazione	AGID linee guida – AG1.1	Partecipazione a corsi su risk management e

Cod. Azione	Descrizione sintetica	Ruolo responsabile	Output richiesto	Riferimento normativo	Esempio pratico
	ICT sicuro				sicurezza contrattuale
AG2	Raccolta buone prassi e lesson learned	Area/Servizio Richiedente – Servizio Informatico - Fornitore ICT (Consultato su esperienze e procedure)	Report interno di best practice	AGID linee guida – AG2	Analisi di progetto precedente con errori di sicurezza e contromisure
AG4	Inventario beni e servizi ICT	Amministratore di Sistema -Servizio Informatico - Fornitore ICT (Responsible per fornire dati e aggiornamenti su asset forniti)	Registro aggiornato asset ICT	AGID linee guida – AG4	Inventario hardware, software e licenze con data acquisto e criticità
AG5	Classificazione beni e servizi ICT	Amministratore di Sistema - Fornitore ICT (Consultato per fornire dettagli tecnici e criticità)	Documento di classificazione	L. 90/2024 art. 8	Classificazione del sistema anagrafe come “critico”
AG6	Metodologia di audit e controllo	Servizio Provveditorato e contratti - Fornitore ICT (Responsible/Consultato per audit del servizio cloud)	Piano audit	AGID linee guida – AG6	Definizione di audit semestrali sul fornitore cloud

4.1.3. Programmazione delle Esigenze ICT

Il presente capitolo definisce il modello e le procedure per la raccolta, la pianificazione e la programmazione delle esigenze ICT dell’Ente, al fine di garantire coerenza con il Piano della Sicurezza Informatica e con le priorità strategiche approvate dall’organo politico.

4.1.3.1. Raccolta delle Esigenze

Tutte le Aree/Servizi devono comunicare le proprie esigenze ICT secondo il **modello standard di raccolta**. Le informazioni richieste includono:

- **Tipologia di esigenza:** hardware, software, servizi, formazione;
- **Descrizione sintetica:** obiettivo e finalità dell’acquisizione;
- **Priorità:** alta, media, bassa;
- **Tempi di implementazione richiesti:** breve, medio, lungo termine;
- **Stima dei costi:** indicativa o dettagliata;
- **Impatto sulla sicurezza ICT:** eventuali criticità per la continuità operativa e la protezione dei dati.

4.1.3.2. Programmazione Annuale e Pluriennale in coernza con il Piano Triennale dell’Informatica nella PA e al Piano di Trqansizione Digitale dell’Ente

Le esigenze raccolte vengono integrate in un **piano annuale e pluriennale** che consente di:

- Allineare gli acquisti ICT al budget disponibile;

- Garantire l'adozione di soluzioni conformi agli standard di sicurezza e alle normative vigenti;
- Pianificare interventi critici per la continuità dei servizi e la protezione dei dati;
- Supportare la Direzione e l'organo politico nelle decisioni di approvazione delle acquisizioni.

Il piano di procurement ICT è strettamente **allineato alle priorità e agli obiettivi** definiti dal Piano Triennale per l'informatica nella PA e dal Piano di Transizione Digitale dell'Ente (PTD).

In particolare:

- Le **priorità strategiche** (cybersecurity, digitalizzazione dei servizi, cloud e interoperabilità, AI, sostenibilità ambientale) sono già inserite nelle azioni del PTD;
- **Il dettaglio delle azioni operative e delle relative tempistiche** è riportato nel PTD, approvato e aggiornato annualmente;
- Il presente piano di procurement ICT ha lo scopo di **garantire coerenza negli acquisti e negli affidamenti**, a supporto della realizzazione delle iniziative ICT già previste nel PTD.

4.1.3.3. Criteri di Valutazione

Ogni richiesta viene valutata sulla base di:

- Conformità alle linee guida del Piano della Sicurezza Informatica;
- Analisi dei rischi ICT associati;
- Priorità strategica dell'Ente;
- Tracciabilità e documentazione per audit e controllo.

4.1.3.4. Modello Operativo per la Raccolta delle Esigenze ICT

Si allega al presente Piano il **Modello Operativo di Raccolta delle Esigenze ICT (ALL.A)**

4.2. Fase di Affidamento (Azioni AP)

La fase di affidamento è il momento in cui la pianificazione si traduce in una procedura concreta di selezione e contrattualizzazione.

Durante questa fase, l'Ente:

- Definisce requisiti tecnici e funzionali
- Valuta le possibili soluzioni (riuso, open source, proprietarie)
- Sceglie la modalità di utilizzo (cloud o on-premise)
- Redige i documenti di gara e le clausole di sicurezza

In base alle Linee Guida AgID, questa fase deve essere gestita con la massima attenzione alla **qualità tecnica** e alla **conformità normativa**, includendo sempre:

- Clausole per la sicurezza ICT
- Requisiti per la protezione dei dati personali
- Previsioni per audit e controlli periodici
- Obblighi in materia dP qualificazione cloud (se SaaS o servizi cloud)

4.2.1. Azioni AP: linee guida AGID e azioni implementate dall'Ente

Codice Azione	Descrizione	Azioni implementate dall'Ente
AP1 – Documento delle esigenze	Descrivere contesto, flussi operativi, requisiti, obiettivi, budget e tempi.	Per ogni nuova necessità di acquisto ICT, l'Ente effettua l'analisi del contesto e dei flussi operativi, la definizione dei requisiti e degli obiettivi, la stima del budget e dei tempi, la ricognizione di soluzioni esistenti e la formalizzazione del Documento delle esigenze.
AP2 – Classificazione fornitura	Applicare la matrice di criticità definita in AG5.	Per ogni nuova fornitura ICT l'Ente applica la matrice di criticità definita in AG5 (punto 3.3 del Piano) per classificare tipologia e livello di rischio della fornitura.
AP3 – Analisi soluzioni disponibili	Verificare: • Riuso (Developers Italia) • Open source • Proprietarie o sviluppo ex novo - Selezione dei fornitori idonei (art. 28 GDPR)	Per ogni nuova fornitura ICT l'Ente verifica soluzioni riusabili (Developers Italia), open source, proprietarie o sviluppo ex novo, al fine di individuare l'opzione più idonea. Seleziona fornitori idonei: l'Ente si avvarrà esclusivamente di fornitori che offrano garanzie sufficienti di adeguatezza tecnica e organizzativa in materia di protezione dei dati. A tal fine, potranno essere richiesti documenti di supporto (questionari, checklist di conformità, attestazioni), da personalizzare caso per caso
AP4 – Modalità di utilizzo	Definire se in SaaS o on-premise.	Per ogni nuova fornitura ICT l'Ente definisce le modalità di utilizzo, SaaS (il software è usato online tramite abbonamento, senza installarlo nei propri server) o on-premise (il software è installato e gestito direttamente nei server aziendali), in base a requisiti tecnici e organizzativi.
AP5 – Strumento di acquisizione	Scegliere la procedura più adatta (accordo quadro, gara, MEPA, convenzioni Consip), tenendo conto di obblighi di contenimento spesa e norme sul riuso.	Per ogni nuova fornitura ICT l'Ente sceglie la procedura più idonea (accordo quadro, gara, MEPA, convenzioni Consip), rispettando obblighi di contenimento spesa e norme sul riuso.
AP6 – Atti di gara e clausole di sicurezza	Includere: • Clausole L. 90/2024 art. 14 • Requisiti di qualificazione cloud (AgID) • Prescrizioni di sicurezza per soluzioni critiche • Obbligo di compliance a linee guida AgID e GDPR • Formalizzazione degli incarichi (art.28, par.3 GDPR) • Gestione della catena dei sub-responsabili (Sub-processing, art. 28 GDPR) • Cancellazione sicura dei dati alla cessazione del rapporto contrattuale (art. 28.3(g) GDPR)	Per ogni nuova fornitura ICT, l'Ente procede alla **valutazione circa l'osservanza dell'art. 108, co. 4, D.Lgs. n. 36/2023**. Nel caso in cui i beni o servizi informatici rientrino tra quelli individuati dal decreto del Presidente del Consiglio dei Ministri adottato ai sensi dell'art. 14, co. 1, L. n. 90/2024, viene previsto l'inserimento delle relative clausole di cui all'art. 14, co. 2 della stessa legge. Se trattasi di soluzione in cloud, si procede all'inserimento di clausole concernenti il

Codice Azione	Descrizione	Azioni implementate dall'Ente
		possesso della **qualificazione ANC**, come stabilito dal Regolamento per i servizi cloud della PA, efficace dal 1° agosto 2024. Inoltre, vengono sempre incluse le prescrizioni relative alla **sicurezza per soluzioni critiche**, la **compliance alle linee guida AgID** e al **GDPR**. **Formalizzazione degli incarichi**: i rapporti con i fornitori che trattano dati personali per conto dell'Ente saranno regolati da un contratto o altro atto giuridico conforme, contenente tutte le clausole obbligatorie e, ove necessario, istruzioni specifiche per il trattamento ICT **Gestione della catena dei sub-responsabili**: nei moderni servizi digitali, in particolare nel settore cloud, è frequente il ricorso a sub-fornitori. Il Responsabile non può subappaltare alcuna parte del trattamento senza la preventiva autorizzazione scritta del Titolare, che può essere: • *Specifica*: approvazione nominativa di ogni singolo sub-responsabile; • *Generale*: autorizzazione preventiva con obbligo di informativa e diritto di obiezione per ogni nuova nomina o sostituzione. In ogni caso, il Responsabile primario resta pienamente responsabile dell'operato dei sub-responsabili e deve imporre loro contrattualmente i medesimi obblighi di protezione dei dati. L'Ente deve poter identificare in ogni momento tutti i soggetti coinvolti nel trattamento, richiedendo trasparenza sulla loro identità, localizzazione, ruolo e garanzie implementate. Le verifiche e i doveri di controllo si estendono all'intera catena di fornitura, con un livello di scrutinio proporzionale al rischio. **Cancellazione sicura dei dati alla cessazione del rapporto contrattuale:** come indicato nella tabella operativa

Codice Azione	Descrizione	Azioni implementate dall'Ente
		Azione AC11 cap.4.3.2.

4.2.2. Tabella operativa Azioni AP

Cod. Azione	Descrizione sintetica	Ruolo responsabile	Output richiesto	Riferimento normativo	Esempio pratico
AP1	Documento delle esigenze e obiettivi	Area/Servizio Richiedente - Fornitore ICT (Consultato su capacità e limiti tecnici)	Documento di analisi requisiti	AGID linee guida – AP1	Descrizione dei flussi del protocollo informatico e integrazione PEC
AP3	Analisi soluzioni disponibili	Servizio Informatico - Amministratore di sistema - Fornitore ICT (Consultato per fornire dettagli tecnici su software o servizi disponibili)	Report comparativo soluzioni	AGID linee guida – AP3	Verifica software riusabile su Developers Italia
AP4	Definizione modalità di utilizzo	Servizio Informatico - Amministratore di sistema - Fornitore ICT (Responsible per implementazione o configurazione del servizio)	Specifiche tecniche	AGID linee guida – AP4	Scelta SaaS con fornitore qualificato AgID
AP6	Atti di gara con clausole di sicurezza	Servizio Provveditorato e contratti - Fornitore ICT (Consulted per input su requisiti di sicurezza o standard tecnici)	Capitolato tecnico	AGID linee guida – AP6	Clausola per vulnerability assessment semestrali

4.2.3. Richiesta acquisizioni di beni e servizi ICT

Per garantire uniformità e completezza nella trasmissione delle informazioni necessarie all'acquisizione di beni, servizi e soluzioni ICT, l'Ente adotta una modulistica standard per la Fase di Affidamento (Azioni AP).

Tale strumento assicura il rispetto delle Linee Guida AgID, delle prescrizioni in materia di sicurezza ICT e protezione dei dati personali, consentendo al Servizio Provveditorato di disporre di tutti gli elementi tecnici, economici e organizzativi per avviare la procedura di affidamento.

La compilazione del modulo da parte del responsabile richiedente è obbligatoria prima dell'avvio di ogni nuovo affidamento ICT.

4.2.3.1. Modello Operativo di richiesta di affidamento ICT

Si allega al presente Piano il **Modello Operativo di richiesta di affidamento ICT (ALL.B)**

4.3. Fase di Esecuzione e Monitoraggio (Azioni AC)

La fase di esecuzione e monitoraggio non è semplicemente "operativa": è qui che si concretizza la sicurezza e l'efficacia del procurement ICT.

Durante questa fase, l'Ente:

- Controlla accessi e credenziali dei fornitori
- Monitora l'esecuzione tecnica delle forniture
- Esegue verifiche di sicurezza (audit, vulnerability assessment)
- Aggiorna costantemente l'inventario ICT
- Garantisce il deprovisioning a fine progetto

Le Linee Guida AgID sottolineano che in questa fase il **controllo continuo** è determinante per:

- Evitare violazioni di sicurezza
- Assicurare che il fornitore rispetti gli standard dichiarati in gara
- Garantire la tracciabilità delle attività
- Mantenere la documentazione aggiornata

4.3.1. Azioni AC: linee guida AGID e azioni implementate dall'Ente

Codice Azione	Descrizione	Azioni implementate dall'Ente
AC1 – Gestione utenze fornitori	Creare, monitorare e revocare account	L'Ente crea e monitora e revoca gli account dei fornitori per ogni nuova iniziativa ICT.
AC2 – Verifica dispositivi fornitori	Controllo crittografia e conformità dispositivi	L'Ente verifica che i dispositivi dei fornitori siano crittografati e conformi agli standard di sicurezza.
AC3 – Accesso alla rete	Limitare accessi al minimo necessario	L'Ente limita l'accesso alla rete dei fornitori solo alle risorse necessarie.
AC4 – Accesso server/database	Isolare ambienti di sviluppo e produzione	L'Ente isola gli ambienti di sviluppo e produzione per garantire sicurezza e segregazione dei dati.
AC5 – Accordi di riservatezza	Firmare NDA per ogni iniziativa	L'Ente richiede la firma di NDA (Non-Disclosure Agreement – Accordo di riservatezza) a tutti i fornitori per ogni progetto ICT.
AC6 – Controllo sicurezza sviluppo software	Audit periodici su tecnologie e metodologie	L'Ente esegue audit periodici sulle tecnologie e metodologie utilizzate dai fornitori.
AC7 – Monitoraggio ruoli e utenze	Aggiornare costantemente la matrice Progetto–Fornitori–Utenze	L'Ente aggiorna continuamente la matrice Progetto–Fornitori–Utenze per garantire tracciabilità (all.D)
AC8 – Verifica documentazione finale	Ricevere manuali, report di sicurezza e "libretto di manutenzione"	L'Ente riceve e verifica manuali, report di sicurezza e il libretto di manutenzione al termine del progetto.
AC9 – Deprovisioning a fine progetto	Revoca di tutte le credenziali e accessi	L'Ente revoca tutte le credenziali e accessi dei fornitori a fine progetto.
AC10 – Aggiornamento inventario	Inserire hardware/software in inventario e DR	L'Ente aggiorna l'inventario di hardware e software, inclusi i dati per disaster recovery.
AC11 – Wiping dispositivi sostituiti	Cancellazione sicura dei dati alla cessazione del rapporto contrattuale (art. 28.3(g) GDPR)	Alla scadenza o risoluzione del contratto, il Responsabile deve cancellare in modo sicuro o restituire al Titolare tutti i dati personali trattati, distruggendo ogni copia esistente. Le modalità di cancellazione devono essere tecnicamente garantite (es. tecniche di *wiping*) e dettagliate nel contratto. Il fornitore ha inoltre l'obbligo di rilasciare una certificazione di avvenuta

Codice Azione	Descrizione	Azioni implementate dall'Ente
		distruzione dei dati. L'unica eccezione è rappresentata da eventuali obblighi di conservazione derivanti dal diritto dell'Unione o dello Stato membro.
AC12 – Manutenzione e aggiornamenti	Pianificare patch e upgrade	L'Ente pianifica patch e aggiornamenti dei sistemi gestiti dai fornitori.
AC13 – Vulnerability assessment	Almeno annuale o dopo ogni modifica rilevante	L'Ente esegue vulnerability assessment almeno una volta l'anno o dopo modifiche rilevanti ai sistemi.

4.3.2. Tabella operativa Azioni AC

Cod. Azione	Descrizione sintetica	Ruolo responsabile	Output richiesto	Riferimento normativo	Esempio pratico
AC1	Gestione utenze fornitori	Amministratore di Sistema - Fornitore ICT (Consultato per informazioni su utenti da creare)	Account creati, monitorati e revocati	AGID linee guida – AC1	Creazione account per fornitore per progetto ICT
AC2	Verifica dispositivi fornitori	Amministratore di Sistema - Fornitore ICT (Responsible/Consultato per fornire informazioni su dispositivi e aggiornamenti)	Report di conformità dispositivi	AGID linee guida – AC2	Controllo crittografia e aggiornamenti sicurezza
AC3	Accesso alla rete	Amministratore di Sistema - Fornitore ICT (Consultato per configurazione accessi)	Registro accessi	AGID linee guida – AC3	Limitazione accessi alla rete ai soli necessari
AC4	Accesso server/database	Amministratore di Sistema - Fornitore ICT (Responsible per esecuzione configurazioni e accessi autorizzati)	Log accessi	AGID linee guida – AC4	Isolamento ambienti sviluppo e produzione
AC5	Accordi di riservatezza	Servizio Provveditorato e contratti - Fornitore ICT (Responsible per firma NDA)	NDA firmati	AGID linee guida – AC5	NDA firmato da fornitori per progetto ICT
AC6	Controllo sicurezza sviluppo software	Amministratore di Sistema - Fornitore ICT (Responsible per implementare controlli e documentare procedure)	Report audit	AGID linee guida – AC6	Audit periodico su metodologie e tecnologie usate
AC7	Monitoraggio ruoli e utenze	Servizio Informatico - Fornitore ICT (Consultato per aggiornamenti sulle	Matrice aggiornata Progetto–Fornitori–Utenze	AGID linee guida – AC7	Aggiornamento matrice dopo nuove assegnazioni

Cod. Azione	Descrizione sintetica	Ruolo responsabile	Output richiesto	Riferimento normativo	Esempio pratico
		utenze assegnate)			
AC8	Verifica documentazione finale	Servizio Informatico - Fornitore ICT (Responsible/Consultato per fornire manuali e documenti)	Manuali e report di sicurezza ricevuti	AGID linee guida – AC8	Ricezione documentazione tecnica finale e libretto manutenzione
AC9	Deprovisioning a fine progetto	Servizio Informatico / Amministratore di Sistema - Fornitore ICT (Responsible per rimozione account e accessi)	Revoca credenziali e accessi	AGID linee guida – AC9	Cancellazione account fornitori a progetto terminato
AC10	Aggiornamento inventario	Servizio Informatico / Amministratore di Sistema - Fornitore ICT (Consulted per fornire dati sui dispositivi e sui software)	Inventario hardware/software aggiornato	AGID linee guida – AC10	Inserimento nuovi dispositivi e software in inventario e DR
AC11	Wiping dispositivi sostituiti	Amministratore di Sistema - Fornitore ICT (Responsible per eseguire cancellazione sicura)	Certificato cancellazione dati	AGID linee guida – AC11	Cancellazione sicura di dispositivi sostituiti
AC12	Manutenzione e aggiornamenti	Servizio Informatico / Amministratore di Sistema - Fornitore ICT (Responsible per esecuzione patch e upgrade)	Piano patch e upgrade	AGID linee guida – AC12	Programmazione aggiornamenti software e firmware
AC13	Vulnerability assessment	Amministratore di Sistema - Fornitore ICT (Responsible/Consultato per supporto tecnico e test)	Report assessment	AGID linee guida – AC13	Assessment annuale o dopo modifiche critiche

4.3.3. Collaudo e chiusura progetto

Il report di collaudo e chiusura progetto ha l'obiettivo di standardizzare la documentazione relativa al collaudo e alla chiusura di ogni progetto ICT. Esso consente di registrare in modo chiaro e strutturato tutte le fasi di verifica, dall'identificazione degli obiettivi di collaudo fino alla validazione finale del progetto.

Il report permette di:

- Definire i criteri di accettazione e gli obiettivi del collaudo;
- Documentare le attività svolte e i test eseguiti;
- Riportare gli esiti e i riscontri, evidenziando eventuali anomalie o non conformità;
- Registrare le azioni correttive intraprese o necessarie;
- Formalizzare le conclusioni e l'accettazione finale del progetto.

Questo strumento rappresenta un elemento fondamentale per garantire la qualità, la sicurezza e la conformità delle soluzioni ICT implementate, favorendo la tracciabilità e la responsabilizzazione dei soggetti coinvolti.

4.3.3.1. Modello Operativo di collaudo e chiusura progetto ICT

Si allega al presente Piano il **Modello Operativo di Collaudo e chiusura progetto ICT (ALL.C)**

4.3.4. Monitoraggio utenze e accessi dei fornitori

L'Azione AC7 richiede che le aministrazioni pubblichino e mantengano aggiornata una matrice Progetto-Fornitori e Ruoli-Utenze, essenziale per garantire:

- il monitoraggio del personale del fornitore coinvolto in ciascun progetto,
- il controllo della loro qualifica e formazione,
- la corretta rimozione dei permessi (deprovisioning) al termine del loro impiego.

A cosa serve la matrice:

Scopo principale	Descrizione
Tracciabilità delle responsabilità	Associa ciascun fornitore (o membro) al progetto di riferimento.
Controllo degli accessi	Registra ruoli, autorizzazioni e scadenze per un adeguato monitoraggio.
Supporto per il deprovisioning	Facilita la disattivazione puntuale di utenze e accessi al termine delle attività.

4.3.4.1. Modello matrice Progetto-Fornitori-Utenze ICT

Si allega al presente Piano il **Modello matrice Progetto-Fornitori-Utenze ICT (ALL.D)**

4.4. Intelligenza Artificiale e nuovi rischi ICT (Azioni AI)

L'introduzione di soluzioni basate su **Intelligenza Artificiale (AI)** nella Pubblica Amministrazione rappresenta una opportunità per migliorare l'efficienza dei processi, l'erogazione dei servizi e l'analisi dei dati. Tuttavia, l'adozione dell'IA comporta **nuovi rischi ICT** e la necessità di integrare requisiti aggiuntivi nei processi di procurement.

4.4.1. Principi di riferimento

Il procurement di soluzioni AI nell'Ente deve rispettare i seguenti principi:

- **Conformità normativa**: osservanza del **Regolamento Europeo sull'Intelligenza Artificiale (AI Act)**, del **GDPR** e delle **Linee Guida AgID su algoritmi trasparenti e affidabili**.
- **Trasparenza ed explainability**: i sistemi AI utilizzati devono essere comprensibili e spiegabili agli utenti e ai decisori, evitando soluzioni "black box".
- **Supervisione umana**: ogni decisione automatizzata deve essere sottoposta a validazione da parte di personale qualificato.
- **Sicurezza e robustezza**: i sistemi AI devono essere resilienti ad attacchi informatici (es. adversarial attacks) e sottoposti a test di robustezza e penetration test specifici.
- **Etica e non discriminazione**: garantire che gli algoritmi non introducano bias o trattamenti discriminatori.

- **Sostenibilità**: preferenza per soluzioni AI con basso impatto energetico, in coerenza con i principi di Green ICT.

4.4.2. Tabella operativa Azioni AI

Cod. Azione	Descrizione sintetica	Ruolo responsabile	Output richiesto	Riferimento normativo	Esempio pratico
AI1	Documento requisiti IA (funzionali, etici, normativi)	Servizio Informatico – DPO - Fornitore ICT (Consultato per capacità tecniche, limiti e fattibilità dell'algoritmo)	Documento requisiti IA	AI Act – GDPR art. 22 – Linee Guida AgID su algoritmi	Definizione requisiti per chatbot di assistenza utenti
AI 2	Audit algoritmico indipendente (dataset, modelli, risultati)	Amministratore di Sistema – DPO - Fornitore ICT (Consultato/Responsible per fornire dati e log di funzionamento dell'algoritmo)	Report di audit IA	AI Act artt. 9-15 – AgID	Audit su modello di machine learning per analisi ambientali
AI 3	Clausole contrattuali specifiche per IA (trasparenza, explainability, supervisione umana, sostenibilità)	Servizio Provveditorato e contratti – DPO - Fornitore ICT (Consultato per input tecnico su vincoli e capacità IA)	Capitolato tecnico con clausole IA	AI Act art. 13-14 – GDPR	Inserimento clausola per "human-in-the-loop" e tracciabilità decisioni
AI 4	Monitoraggio post-implementazione con KPI su performance e correttezza algoritmi	Servizio Informatico – Amministratore di Sistema - Fornitore ICT (Responsible per raccolta dati operativi e aggiornamento KPI)	Report periodico KPI IA	AI Act – PIAO – Piano sicurezza informatica	KPI su accuratezza del modello e tasso di errore
AI 5	Risk assessment IA integrato nella Matrice Criticità e Rischi ICT	Servizio Informatico – RUP – DPO - Fornitore ICT (Consultato per evidenziare rischi tecnici, bias, vulnerabilità)	Aggiornamento Matrice rischi ICT	AI Act – NIS2 – GDPR	Inserimento voce "Bias algoritmico / Attacchi adversarial" nella matrice

4.4.3. Checklist requisiti etici e di trasparenza per soluzioni AI

Si allega al presente Piano la **Checklist requisiti etici e di trasparenza per soluzioni AI (ALL.E)**

5. SOSTENIBILITÀ E GREEN ICT

La trasformazione digitale deve essere sostenibile e rispettosa dell'ambiente. L'Ente integra criteri di Green Public Procurement (GPP) e dei CAM (Criteri Ambientali Minimi) ICT nelle proprie procedure di affidamento, disciplinati dal Ministero dell'Ambiente e della Sicurezza Energetica (MASE), in attuazione del Codice Appalti.

5.1. Principi di Green ICT

Efficienza energetica: soluzioni ICT con basso consumo e certificazioni ambientali.
Economia circolare: promozione di riuso, ricondizionamento e riciclo.
Cloud sostenibile: preferenza per data center certificati (ISO 50001, EU Code of Conduct).
Dematerializzazione: digitalizzazione processi e riduzione della carta.

6. COLLEGAMENTO TRA PROCUREMENT ICT E PIAO 2025-2027

Il Piano di Procurement ICT 2025 si integra con gli indirizzi strategici e gli obiettivi di performance e trasformazione digitale individuati nel PIAO 2025–2027, garantendo coerenza tra programmazione, acquisti ICT e missione istituzionale dell'Ente.

1. Digitalizzazione dei processi interni

- **PIAO**: Semplificazione e dematerializzazione dei procedimenti amministrativi.
- **Procurement ICT**: Acquisizione di piattaforme documentali e sistemi di workflow management interoperabili.

2. Cybersecurity e compliance

- **PIAO**: Rafforzamento della sicurezza informatica e conformità al GDPR.
- **Procurement ICT**: Gare e contratti con clausole obbligatorie di sicurezza ICT, GDPR e audit periodici; monitoraggio accessi tramite matrice fornitori/utenze.

3. Cloud e interoperabilità

- **PIAO**: Adozione di soluzioni cloud qualificate e integrazione con piattaforme abilitanti nazionali.
- **Procurement ICT**: Predilezione di soluzioni SaaS e cloud, con verifiche di qualificazione AGID e clausole contrattuali specifiche.

4. Sostenibilità ambientale (Green ICT)

- **PIAO**: Riduzione dell'impatto ambientale delle attività amministrative.
- **Procurement ICT**: Inserimento di criteri ambientali minimi (CAM) e clausole ESG nei capitolati di gara ICT.

5. Innovazione e intelligenza artificiale

- **PIAO**: Sperimentazione di strumenti digitali avanzati per migliorare servizi e decisioni.
- **Procurement ICT**: Introduzione di checklist di requisiti etici e di trasparenza per soluzioni AI, con formazione interna sui rischi e benefici dell'IA.

6. Performance organizzativa

- **PIAO**: Monitoraggio dei risultati e della produttività degli uffici.
- **Procurement ICT**: Adozione di un modello operativo di collaudo e chiusura progetto, che certifica la conformità tecnica e amministrativa delle forniture ICT, raccoglie il feedback degli uffici richiedenti e assicura la chiusura regolare del procedimento.

7. REVISIONE E AGGIORNAMENTO DEL PIANO

Il presente Piano di Procurement ICT è un documento dinamico, soggetto a revisione periodica in coerenza con il ciclo di programmazione strategica dell'Ente e in conformità alle Linee Guida AgID.

8. ALLEGATI

All.A Modello operativo di raccolta esigenze ICT
All.B Modello operativo di richiesta di affidamento ICT
All.C Modello operativo di collaudo e chiusura progetto ICT
All.D Modello matrice Progetto-Fornitori-Utenze ICT
All.E Checklist requisiti etici e di trasparenza per soluzioni AI