

Allegato 1											
COMUNE DI VARISELLA - MONITORAGGIO DEGLI ADEMPIMENTI DEL PIANO TRIENNALE PER L'INFORMATICA 2024-2026 - AGGIORNAMENTO 2026 - PIANO PROGRAMMATICO DEL RESPONSABILE DELLA TRANSIZIONE DIGITALE											
AMBITO	CAPITOLO	OBIETTIVI	RISULTATI ATTESI	LINEE DI AZIONE	Codifica AgID	Attuabile	Strategia di procurement	Programmazione della tempistica di intervento	Stato attuazione	Obbligatorietà	
PROCESSI	Capitolo 1 - Organizzazione e gestione del cambiamento	Obiettivo 1.1 - Migliorare i processi di trasformazione digitale della PA	RA1.1.1 - Rafforzare la collaborazione e lo scambio di pratiche e soluzioni tra Amministrazioni	Proporre ad AGID l'attivazione di una comunità digitale tematica/territoriale su rete.digitale.gov.it	CAP1.PA.01	da marzo 2024	Iniziativa strategica di maggior rilievo: Digital Transformation Iniziativa strategica di dettaglio:	Attualmente non programmata	Non completata	No	
				Utilizzo di formati presenti nel kit per proporre nuove comunità digitali ed effettuare monitoraggio semestrali delle attività in esse svolte	CAP1.PA.02	da luglio 2024	2069 - Digital Transformation 2036 - Digital Transformation 2	Attualmente non programmata	Non completata	No	
				In caso di partecipazione alla community su Rete Digitale incentrata sull'AI, condividere pratiche, soluzioni e fabbisogni	CAP1.PA.13	da gennaio 2026		Attualmente non programmata	Non completata	No	
				In caso di partecipazione alle iniziative laboratoriali, fornire contributi e proposte di modifica e integrazione al Vademecum sulla nomina del Responsabile per la transizione al digitale e sulla costituzione dell'Ufficio per la transizione al digitale in forma associata	CAP1.PA.03	da marzo 2024		Attualmente non programmata	Non completata	No	
				In caso di partecipazione alle iniziative laboratoriali e di adozione di modelli organizzativi/operativi per l'Ufficio per la transizione al digitale, condividere le esperienze, gli strumenti sviluppati e i processi implementati	CAP1.PA.04	da marzo 2024		Attualmente non programmata	Non completata	No	
				In caso di partecipazione alle iniziative laboratoriali, sperimentare i modelli proposti e fornire ad AGID il feedback delle esperienze di nomina RTD e UTO in forma associata realizzate	CAP1.PA.05	da luglio 2024		Attualmente non programmata	Non completata	No	
		Obiettivo 1.2 - Diffusione competenze digitali di base nei cittadini e imprese	RA1.2.1 - Diffusione competenze digitali di base nei cittadini e imprese	In funzione alla propria missione istituzionale, realizzare iniziative per lo sviluppo delle competenze digitali dei cittadini previste dal PNRR e in linea con il Piano operativo della Strategia Nazionale per le Competenze Digitali	CAP1.PA.09	Linee di azione vigenti		Attualmente non programmata	Nessuna azione prevista per l'Ente	No	
			RA1.2.2 - Diffusione competenze digitali di base nella PA	Adesione all'iniziativa "Syllabus per la formazione digitale" e promuovere la partecipazione alle iniziative formative sulle competenze di base da parte dei dipendenti pubblici, concorrente 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	CAP1.PA.08	Linee di azione vigenti	Iniziativa strategica di dettaglio: 2069 - Digital Transformation 2036 - Digital Transformation 2	Tempestivamente	In attuazione	Si	
				Partecipazione del RTD e del personale degli UTO alle iniziative di AGID sull'AI/PA, finalizzate al rafforzamento delle competenze e allo scambio di esperienze.	CAP1.PA.14	da ottobre 2025		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgID	Completata	No	
			RA1.2.3 - Diffusione delle competenze specialistiche ICT	In funzione delle proprie necessità, partecipare alle iniziative pilota, alle iniziative di sensibilizzazione e a quelle di formazione di base e specialistica per il proprio personale, come previsto dal Piano triennale e in linea con il Piano strategico nazionale per le competenze digitali	CAP1.PA.07	Linee di azione vigenti		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgID	Completata	No	
			RA1.3.1 - Definizione di un indice di digitalizzazione della PA italiana	In caso di appartenenza al campione, alimentare l'indice di digitalizzazione secondo la metodologia definita dal Gruppo di lavoro	CAP1.PA.10	da febbraio 2026		Entro la scadenza del Piano Triennale per l'Informatica dell'AgID	Non completata	Si - condizionato all'appartenenza all'Ente al campione statistico	
			Obiettivo 1.3 - Monitorare e analizzare lo stato di digitalizzazione del paese	RA1.3.2 - Acquisizione ed elaborazione di informazioni analitiche da Enti locali	Partecipazione alla seconda fase della raccolta dati, garantendo l'accuratezza e la completezza delle informazioni	CAP1.PA.12	da settembre 2025	Iniziativa strategica di maggior rilievo: Digital Transformation Iniziativa strategica di dettaglio: 2069 - Digital Transformation 2036 - Digital Transformation 2	Entro la scadenza del Piano Triennale per l'Informatica dell'AgID	Da attuare	Si - condizionato
	RA1.3.3 - Aumento delle tipologie e delle fonti dati integrate all'interno dell'Osservatorio	Partecipazione alla seconda fase della raccolta dati, garantendo l'accuratezza e la completezza delle informazioni		CAP1.PA.12	da settembre 2025		Entro la scadenza del Piano Triennale per l'Informatica dell'AgID	Da attuare	Si - condizionato		
	Capitolo 2 - Il procurement per la trasformazione digitale	Obiettivo 2.1 - Rafforzare l'ecosistema nazionale di approvvigionamento digitale		RA2.1.1 - Diffusione del processo di certificazione delle piattaforme di approvvigionamento digitale	Dotazione di piattaforme di approvvigionamento, da parte dei soggetti aggregatori, che digitalizzano la fase di esecuzione dell'appalto	CAP2.PA.01	entro giugno 2025		Non di competenza dell'Ente	Non di competenza dell'Ente	Si - condizionato
				Digitalizzazione della fase di esecuzione dell'appalto da parte delle stazioni appaltanti	CAP2.PA.02	entro giugno 2025		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgID	Completata	Si - condizionato	
				I soggetti aggregatori e i gestori pubblici di piattaforme di approvvigionamento mettono a disposizione piattaforme che digitalizzano in modo integrato (nel rispetto del principio once only) tutto il ciclo di vita dell'appalto	CAP2.PA.07	entro giugno 2026		Non di competenza dell'Ente	Non di competenza dell'Ente	Si - condizionato	
		Obiettivo 2.2 - Diffondere l'utilizzo degli appalti innovativi	RA2.2.1 - Incremento della partecipazione di PMI e start up agli appalti di innovazione	Partecipazione alle consultazioni di mercato delle amministrazioni che hanno aderito al programma appalti innovativi;	CAP2.PA.08	da dicembre 2026		Non di competenza dell'Ente	Non di competenza dell'Ente	Si - condizionato	
			RA2.2.2 - Incremento della diffusione degli appalti di innovazione nella PA	Le amministrazioni che hanno avviato appalti di innovazione completano la fase di aggiudicazione e di esecuzione;	CAP2.PA.09	entro giugno 2026		Non di competenza dell'Ente	Non di competenza dell'Ente	Si - condizionato	
		Obiettivo 2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche	RA2.3.1 - Incremento del livello di trasformazione digitale mediante la disponibilità di Gare strategiche allo scopo definito	Nel proprio piano acquisti, programmare i fabbisogni di adesione alle iniziative strategiche disponibili per il perseguimento degli obiettivi del Piano triennale per l'anno 2025 Programma dei fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l'anno 2026 Programma dei fabbisogni di adesione alle iniziative strategiche per il perseguimento degli obiettivi del Piano triennale per l'anno 2027	CAP2.PA.04 CAP2.PA.05 CAP2.PA.06	da settembre 2024 da settembre 2025 da settembre 2026	Nessuna azione prevista per l'Ente Nessuna azione prevista per l'Ente Nessuna azione prevista per l'Ente	Nessuna azione prevista per l'Ente Nessuna azione prevista per l'Ente Nessuna azione prevista per l'Ente	Si - condizionato Si - condizionato Si - condizionato		
	Capitolo 3 - Servizi	Obiettivo 3.1 - Migliorare la capacità di erogare e-service	RA3.1.1 - Incremento del numero di «e-service» registrati sul Catalogo Pubblico POND		Smettere di usare modalità di interoperabilità diverse da POND per le nuove implementazioni	CAP3.PA.01	da gennaio 2024	Iniziativa strategica di maggior rilievo: Servizi applicativi in ottica cloud	Entro la scadenza del Piano Triennale per l'Informatica dell'AgID	In attuazione	Si
					Inizio della migrazione dei servizi erogati in interoperabilità dalle attuali modalità alla POND	CAP3.PA.02	da gennaio 2024	Iniziativa strategica di dettaglio:	Entro la scadenza del Piano Triennale per l'Informatica dell'AgID	In attuazione	Si
				Continuare a popolare il Catalogo delle API della Piattaforma Digitale Nazionale Dati (con le API conformi alle «Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni»)	CAP3.PA.03	da gennaio 2024	2112 - Applicativi Cloud	Entro la scadenza del Piano Triennale per l'Informatica dell'AgID	In attuazione	Si	
				Rispondere ai bandi pubblicati per l'erogazione di API su POND	CAP3.PA.04	da gennaio 2024	2583 - Applicativi Cloud 2	Entro la scadenza del Piano Triennale per l'Informatica dell'AgID	Non completata	Si	
				Le PA centrali (almeno una) per l'erogazione di API su POND	CAP3.PA.05	da gennaio 2024	2634 - Applicativi Cloud 4	Non di competenza dell'Ente	Non di competenza dell'Ente	No	
				Utilizzo delle API presenti sul Catalogo	CAP3.PA.06	da gennaio 2024	2635 - Applicativi Cloud 5	Entro la scadenza del Piano Triennale per l'Informatica dell'AgID	Non completata	Si	
RA3.1.2 - Aumento del numero di Richieste di Fruizione Autorizzate su POND				Effettuare richieste di fruizione di servizi erogati da privati	CAP3.PA.07	da luglio 2025		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgID	Completata	Si	
RA3.1.3 - Ampliamento del numero delle amministrazioni coinvolte nell'evoluzione delle Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni				Evidenziare le esigenze che non trovano riscontro nella «Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni» e partecipare alla definizione di pattern e profili di interoperabilità per l'aggiornamento delle stesse	CAP3.PA.08	da gennaio 2024		Attualmente non programmata	Non completata	Condizionato al fatto che l'Ente estenderà esigenze particolari dentro dalla «Linee guida sull'interoperabilità»	
							Iniziativa strategica di maggior rilievo: Servizi applicativi in ottica cloud Iniziativa strategica di dettaglio: 2112 - Applicativi Cloud 2583 - Applicativi Cloud 2 2634 - Applicativi Cloud 4 2635 - Applicativi Cloud 5 2636 - Applicativi Cloud 6 2637 - Servizi Desktop 1 2638 - Servizi Desktop 2 2639 - Servizi Desktop 3 2640 - Servizi Desktop 4 2641 - Servizi Desktop 5 2642 - Servizi Desktop 6	Nessuna azione prevista per l'Ente	Nessuna azione prevista per l'Ente	No	
				Publicazione, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, della dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili	CAP3.PA.14	entro settembre 2025		Publicata il 23/09/2025	Completata	Si	
				Tutte le Regioni, le Province autonome, le Città metropolitane e i capoluoghi delle Città metropolitane effettuano un test automatico di accessibilità sul proprio sito istituzionale indicato su https://indicapi.gov.it/ipo-portal/, utilizzando la piattaforma MAUVE++	CAP3.PA.23	entro settembre 2025		Non di competenza dell'Ente	Non di competenza dell'Ente	No	
				Publicazione degli obiettivi di accessibilità sul proprio sito web	CAP3.PA.15	entro marzo 2026		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgID	Completata	Si	
				Publicazione, entro il 23 settembre, esclusivamente tramite l'applicazione form.AGID.gov.it, della dichiarazione di accessibilità per ciascuno dei propri siti web e APP mobili	CAP3.PA.16	entro settembre 2026		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgID	Completata	Si	
Obiettivo 3.2 - Migliorare la qualità e l'accesso ai servizi digitali offerti dallo Sportello per l'Italia		RA3.2.1 - 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		Tutte le Regioni, le Province autonome, le Città metropolitane e i capoluoghi delle Città metropolitane effettuano un test automatico di accessibilità sul proprio sito istituzionale indicato su https://indicapi.gov.it/ipo-portal/, utilizzando la piattaforma MAUVE++	CAP3.PA.24	entro settembre 2026		Non di competenza dell'Ente	Non di competenza dell'Ente	No	
							Iniziativa strategica di maggior rilievo: Servizi applicativi in ottica cloud Iniziativa strategica di dettaglio: 2112 - Applicativi Cloud 2583 - Applicativi Cloud 2 2634 - Applicativi Cloud 4 2635 - Applicativi Cloud 5 2636 - Applicativi Cloud 6	Nessuna azione prevista per l'Ente	Nessuna azione prevista per l'Ente	No	
				Verificare che in «Amministrazione trasparente» sia pubblicato il manuale di gestione documentale, la nomina del responsabile della gestione documentale per ciascuna ADO e qualora siano presenti più ADO la nomina del coordinatore della gestione documentale	CAP3.PA.17	entro giugno 2025		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgID	Completata	Si	
				Verificare che in «Amministrazione trasparente» sia pubblicato il manuale di conservazione e la nomina del responsabile della conservazione	CAP3.PA.18	entro giugno 2026		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgID	Completata	Si	
				In caso di adesione agli Accordi, utilizzare gli strumenti dell'Operation Center e svolgere azioni correttive sul funzionamento dei servizi e delle procedure sulla base delle segnalazioni ricevute	CAP3.PA.19	da gennaio 2025	Iniziativa strategica di maggior rilievo: Digital Transformation Iniziativa strategica di dettaglio: 2069 - Digital Transformation 2036 - Digital Transformation 2 2112 - Applicativi Cloud 2583 - Applicativi Cloud 2 2634 - Applicativi Cloud 4 2635 - Applicativi Cloud 5 2636 - Applicativi Cloud 6	Non di competenza dell'Ente	Non di competenza dell'Ente	No	
				RA3.4.2 - Diffusione e pieno utilizzo dello Sportello	In caso di adesione agli Accordi in base alle proprie esigenze, partecipare alle azioni di sensibilizzazione effettuate da AGID	CAP3.PA.20	entro dicembre 2024		Non di competenza dell'Ente	Non di competenza dell'Ente	No
			In caso di adesione agli Accordi in base alle proprie esigenze, partecipare alle azioni di sensibilizzazione effettuate da AGID	CAP3.PA.21	entro dicembre 2025		Non di competenza dell'Ente	Non di competenza dell'Ente	No		

APPLICAZIONI	Capitolo 4 - Piattaforme	Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	RA4.1.1 - Incremento dei servizi sulla piattaforma pa.gov.it	In caso di adesione a pa.gov.it, assicurare l'attivazione di nuovi servizi in linea con i target descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR)	CAPA.PA.01	entro dicembre 2026	Iniziativa strategica di maggior rilievo: Servizi applicativi in etica cloud Iniziativa strategica di dettaglio: 2312 - Applicativi Cloud 2483 - Applicativi Cloud 2 2609 - Applicativi Cloud 4 2626 - Data Management 2666 - Data Management 2 2668 - Data Management 3	L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Completata	Si - condizionato
			RA4.1.2 - Incremento dei servizi sulla Piattaforma ID (l'App dei servizi pubblici)	In caso di adesione ad App IO, assicurare l'attivazione di nuovi servizi in linea con i target descritti e secondo le modalità attuative definite nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR)	CAPA.PA.02	entro dicembre 2026	Iniziativa strategica di maggior rilievo: Servizi applicativi in etica cloud Iniziativa strategica di dettaglio: 2312 - Applicativi Cloud 2483 - Applicativi Cloud 2 2609 - Applicativi Cloud 4 2626 - Data Management 2666 - Data Management 2 2668 - Data Management 3	L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Completata	Si - condizionato
			RA4.1.3 - Incremento degli enti che usano SEND	Integrazione a SEND, in linea con i target descritti e secondo la roadmap di attuazione prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR)	CAPA.PA.03	entro dicembre 2026	Iniziativa strategica di maggior rilievo: Servizi applicativi in etica cloud Iniziativa strategica di dettaglio: 2312 - Applicativi Cloud 2483 - Applicativi Cloud 2 2609 - Applicativi Cloud 4 2626 - Data Management 2666 - Data Management 2 2668 - Data Management 3	L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Completata	Si
			RA4.1.4 - Incremento dell'adozione e dell'utilizzo di SPD o CIE da parte delle Pubbliche Amministrazioni	Proseguire il percorso di adesione a SPD e CIE, dismettendo le altre modalità di autenticazione associate ai propri servizi online e integrando lo SPD uso professionale per i servizi diretti a professionisti e imprese	CAPA.PA.04	Linee di azione vigenti	Iniziativa strategica di maggior rilievo: Servizi applicativi in etica cloud Iniziativa strategica di dettaglio:	Tempestivamente	Non completata	Si
				Cesare il rilascio di credenziali proprietarie a cittadini dotati di SPD e/o CIE	CAPA.PA.05	Linee di azione vigenti	2312 - Applicativi Cloud	L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Già vigente	Si
				Adozione dello SPD e della CIE by default: le nuove applicazioni devono nascere SPD o CIE only a meno che non di siano vincoli normativi o tecnologici, se dedicate a soggetti dotati di SPD o CIE. Gli Enti che intendono adottare lo SPD di livello 2 e 3 devono anche adottare il «Login with eIDAS» per l'accesso transfrontaliero ai propri servizi	CAPA.PA.06	Linee di azione vigenti	2483 - Applicativi Cloud 2	Attualmente non programmato	Non completata	Si
				Adeguamento alle evoluzioni previste dall'ecosistema SPD (tra cui OpenID Connect, uso professionale, Attribute Authorities, servizi per i minori e gestione degli attributi qualificati)	CAPA.PA.07	Linee di azione vigenti	2609 - Applicativi Cloud 4	Tempestivamente	Non completata	Si
			RA4.1.5 - Promuovere l'adesione ai servizi della piattaforma NoIPA per supportare l'azione amministrativa nella gestione del personale	In caso di adesione a NoIPA, esprimere manifestazione di interesse e inviare richiesta	CAPA.PA.08	Linee di azione vigenti	Iniziativa strategica di maggior rilievo: Gare Saas Iniziativa strategica di dettaglio: 2370 - Saas CRM	L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Già vigente	No
		RA4.1.6 - Incremento del livello di alimentazione e digitalizzazione del Fascicolo Sanitario Elettronico	Le Regioni e le Province Autonome rispettano le scadenze delle attività previste nel proprio Piano di adeguamento tecnologico, in coerenza con i decreti attuativi che definiscono i contenuti del FSE e la standardizzazione	Le Regioni e le Province Autonome rispettano le scadenze delle attività previste nel proprio Piano di adeguamento tecnologico, in coerenza con i decreti attuativi che definiscono i contenuti del FSE e la standardizzazione	CAPA.PA.09	entro dicembre 2024	Iniziativa strategica di maggior rilievo: Sanità Digitale Iniziativa strategica di dettaglio:	Non di competenza dell'Ente	Non di competenza dell'Ente	No
					CAPA.PA.10	entro dicembre 2025	2360 - Sanità Digitale 2	Non di competenza dell'Ente	Non di competenza dell'Ente	No
					CAPA.PA.11	entro giugno 2026		Non di competenza dell'Ente	Non di competenza dell'Ente	No
		RA4.1.7 - Semplificazione e creazione di un catalogo di tutte le procedure SUAP e SUE e relativi regimi amministrativi applicati in tutto il territorio nazionale	UnionCamere realizza il Catalogo Unico dei procedimenti del SUAP e gli Enti Interessati (PAC/PAL/Comuni, Regioni, Enti Terzi, Unioncamere) avviano la prima alimentazione del Catalogo		CAPA.PA.12	entro dicembre 2024	Iniziativa strategica di maggior rilievo: Digital Transformation Iniziativa strategica di dettaglio:	Non di competenza dell'Ente	Non di competenza dell'Ente	Si - condizionato
			Regioni, Consorzi, Unioncamere mettono a disposizione soluzioni alternative all'adeguamento alle specifiche tecniche dei propri sistemi informativi SSI, in ambito SUAP, quali, ad esempio: Impresa in un giorno per i comuni e Soluzione Sussidiaria per gli enti terzi		CAPA.PA.15	entro dicembre 2024	2069 - Digital Transformation	Non di competenza dell'Ente	Non di competenza dell'Ente	No
			PAC/PAL/Comuni, Regioni, Enti Terzi e Unioncamere devono adeguare le proprie componenti informatiche interessate nei procedimenti SUAP alle specifiche tecniche di cui al Decreto interministeriale 26/09/2025		CAPA.PA.14	entro agosto 2025	2236 - Digital Transformation 2	Non di competenza dell'Ente	Non di competenza dell'Ente	Si
			Gli Enti Interessati (PAC/PAL/Comuni, Regioni, Enti Terzi, Unioncamere) aggiornano il Catalogo Unico dei procedimenti del SUAP		CAPA.PA.16	entro settembre 2025		Non di competenza dell'Ente	Non di competenza dell'Ente	Si - condizionato
			Gli Enti Interessati (PAC/PAL/Comuni, Regioni, Enti Terzi, Unioncamere) aggiornano costantemente il Catalogo Unico dei procedimenti del SUAP		CAPA.PA.17	entro dicembre 2026		Non di competenza dell'Ente	Non di competenza dell'Ente	Si - condizionato
			133 Enti Locali selezionati tramite avviso di progetto sperimentano il modello operativo relativo al "progetto di digitalizzazione completa dei pagamenti degli Enti locali in SIOPE" e la corretta alimentazione e allineamento della PCC		CAPA.PA.25	entro dicembre 2024		Non di competenza dell'Ente	Non di competenza dell'Ente	No
	Obiettivo 4.2 - Ottenere la piena interoperabilità tra le piattaforme	RA4.1.8 - Miglioramento del processo di digitalizzazione del sistema pubblico dei pagamenti avviato nel 2017 con la realizzazione di SIOPE+	Almeno 10 enti aderenti al progetto SIOPE+ e non inclusi nella prima fase della sperimentazione del "progetto di digitalizzazione completa dei pagamenti degli enti locali in SIOPE" e la corretta alimentazione e allineamento della PCC" effettuano disposizioni di pagamento relative alle spese del personale, attraverso mandati mono beneficiario a favore del singolo dipendente e non attraverso l'uso di liste esterne		CAPA.PA.26	entro dicembre 2025		Non di competenza dell'Ente	Non di competenza dell'Ente	No
			Almeno 20 enti aderenti al progetto SIOPE+ e non inclusi nella prima fase della sperimentazione del "progetto di digitalizzazione completa dei pagamenti degli enti locali in SIOPE" e la corretta alimentazione e allineamento della PCC" effettuano disposizioni di pagamento relative alle spese del personale, attraverso mandati mono beneficiario a favore del singolo dipendente e non attraverso l'uso di liste esterne		CAPA.PA.27	entro giugno 2026		Non di competenza dell'Ente	Non di competenza dell'Ente	No
			Nessuna azione prevista per l'Ente					Nessuna azione prevista per l'Ente	Nessuna azione prevista per l'Ente	No
		RA4.2.1 - Adesione ai nuovi servizi offerti da ANPR	Adesione ai servizi di Stato civile su ANPR		CAPA.PA.18	da febbraio 2024	Iniziativa strategica di maggior rilievo: Servizi applicativi in etica cloud Iniziativa strategica di dettaglio: 2312 - Applicativi Cloud 2483 - Applicativi Cloud 2 2609 - Applicativi Cloud 4 2626 - Data Management 2666 - Data Management 2 2668 - Data Management 3	L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Completata	Si
		RA4.2.2 - Disponibilità dei dati su licizioni e titoli di studio su ANIS	Le Università e gli AFAM statali possono trasmettere i propri dati per l'integrazione su ANIS attraverso servizi resi fruibili dalla POND secondo quanto descritto nell'area tecnica del sito https://www.anis.mur.gov.it/area-tecnica/documentazione		CAPA.PA.19	da gennaio 2024	Iniziativa strategica di maggior rilievo: Data Management Iniziativa strategica di dettaglio:	Non di competenza dell'Ente	Non di competenza dell'Ente	No
			Le Università possono trasmettere i propri dati per l'integrazione su ANIS attraverso l'uso di una web application		CAPA.PA.20	da aprile 2024	2360 - Data Management 2	Non di competenza dell'Ente	Non di competenza dell'Ente	No
		RA4.2.3 - Realizzazione della piattaforma ANIST	Le istituzioni scolastiche possono prendere visione delle informazioni di interesse nell'area tecnica del portale messo a disposizione		CAPA.PA.21	da dicembre 2025	Iniziativa strategica di maggior rilievo: Data Management Iniziativa strategica di dettaglio:	Non di competenza dell'Ente	Non di competenza dell'Ente	No
			Le istituzioni scolastiche accedono alle funzionalità della piattaforma		CAPA.PA.22	da dicembre 2025	2360 - Data Management 2	Non di competenza dell'Ente	Non di competenza dell'Ente	No
	Obiettivo 4.3 - Migliorare la sicurezza, accessibilità e interoperabilità delle basi dati di interesse nazionale	RA4.3.1 - Incremento del numero di basi dati di interesse nazionale conformi alle regole tecniche	Avanzare richiesta di inserimento delle proprie basi di dati nell'elenco di Basi di dati di interesse nazionale gestito da AGID secondo il processo definito		CAPA.PA.23	da gennaio 2026	Iniziativa strategica di maggior rilievo: Data Management Iniziativa strategica di dettaglio:	Non di competenza dell'Ente	Non di competenza dell'Ente	No
			I titolari di basi di dati di interesse nazionale le adeguano all'aggiornamento delle regole tecniche		CAPA.PA.24	da gennaio 2026	2360 - Data Management 2	Non di competenza dell'Ente	Non di competenza dell'Ente	No
Obiettivo 5.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il cittadino e imprese	Obiettivo 5.1 - Favorire la condivisione e il riutilizzo dei dati tra le PA e il cittadino e imprese	RA5.1.1 - Aumento del numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalle linee guida Open Data	Adeguare i metadati, relativi ai dati geografici, all'ultima versione delle specifiche nazionali e documentare i propri dataset nel Catalogo nazionale geodati.gov.it		CAPS.PA.01	Linee di azione vigenti	Iniziativa strategica di maggior rilievo: Data Management Iniziativa strategica di dettaglio:	Tempestivamente	Non completata	Si
			Adeguare i metadati, relativi ai dati non geografici, alle specifiche nazionali e documentare i propri dataset nel Catalogo nazionale geodati.gov.it		CAPS.PA.02	Linee di azione vigenti	2360 - Data Management 2	Tempestivamente	Non completata	Si
		RA5.1.2 - Aumento del numero di dataset resi disponibili attraverso i servizi di rete di cui al framework creato con la Direttiva 2007/2/CE (INSPIRE) e relativi Regolamenti attuativi, con particolare riferimento ai dati di elevato valore di cui al framework creato	Partecipare, in funzione delle proprie necessità, a interventi di formazione e sensibilizzazione sulle politiche open data		CAPS.PA.03	Linee di azione vigenti	2366 - Data Management 2	Attualmente non programmato	Non completata	Condizionato all'effettiva definizione
			Attuare le indicazioni sui dati di elevato valore presenti nel Regolamento di esecuzione (UE) 2023/1318, nelle Linee guida Open Data nonché nella specifica guida operativa		CAPS.PA.04	da giugno 2024	Iniziativa strategica di maggior rilievo: Data Management Iniziativa strategica di dettaglio:	Entro la scadenza del Piano Triennale per l'Informatica dell'AgD	Non completata	Si

Capitolo 5 - Dati e Intelligenza Artificiale

Capitolo 6 - Infrastrutture

TECNOLOGIE

		avere su cui si registrano in esecuzione (UE) 2023/138				<div><div>2302 - Data Management</div><div>2306 - Data Management 2</div></div>			
	RAS 1.3 - Disponibilità delle categorie di dati protetti ai cui all'art. 3 del Regolamento (UE) 2022/868 (DGA) nello sportello unico reso disponibile da AGD	Documentare i dati rientranti nelle categorie di cui all'art. 3 del Regolamento (UE) 2022/868 (DGA) nello sportello unico reso disponibile da AGD	CAPS.PA.26	da gennaio 2026			L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Completata	Si
	RAS 2.1 - Aumento del numero di dataset con metadati di qualità conforme agli standard di riferimento europei e nazionali	Pubblicazione dei metadati relativi ai dati di elevato valore, secondo le indicazioni presenti nel Regolamento di esecuzione (UE) e nelle Linee guida sui dati aperti e rellina guida operativa, nei cataloghi nazionali dati.gov.it e govdati.gov.it	CAPS.PA.05	da giugno 2024	<div>Iniziativa strategica di maggior rilievo: Data Management</div> <div>Iniziativa strategica di dettaglio:</div>		Entro la scadenza del Piano Triennale per l'Informatica dell'AgD	Non completata	Si
	RAS 3.2 - Aumento del numero di dataset di tipo aperto resi disponibili dalle pubbliche amministrazioni e documentati nel portale dati.gov.it	Nessuna azione prevista per l'Ente			<div><div>2302 - Data Management</div><div>2306 - Data Management 2</div></div> <div>Iniziativa strategica di maggior rilievo: Data Management</div> <div>Iniziativa strategica di dettaglio:</div>		Nessuna azione prevista per l'Ente	Nessuna azione prevista per l'Ente	No
	Obiettivo 5.2 - Aumentare la qualità dei dati e dei metadati	Se non ancora presenti nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 3 dataset, qualora si dovesse avere una popolazione tra 10.000 e 100.000 abitanti	CAPS.PA.06	entro dicembre 2024			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Se non ancora presenti nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 5 dataset, qualora si dovesse avere una popolazione tra 100.001 e 250.000 abitanti	CAPS.PA.07	entro dicembre 2024			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Se non ancora presenti nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 10 dataset, qualora si dovesse avere una popolazione > di 250.000 abitanti	CAPS.PA.08	entro dicembre 2024			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Ogni PA centrale (non ancora presente nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 15 dataset	CAPS.PA.09	entro dicembre 2024			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Se non ancora presenti nel 2024 nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 1 dataset, qualora si dovesse avere una popolazione tra 5.000 e 10.000 abitanti	CAPS.PA.10	entro dicembre 2025			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Se non ancora presenti nel 2024 nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 5 dataset, qualora si dovesse avere una popolazione tra 10.001 e 100.000 abitanti	CAPS.PA.11	entro dicembre 2025			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
	RAS 2.3 - Aumento del numero di amministrazioni non ancora presenti nel catalogo dati.gov.it che rendono disponibili dataset di tipo aperto	Se non ancora presenti nel 2024 nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 10 dataset, qualora si dovesse avere una popolazione > di 250.000 abitanti	CAPS.PA.12	entro dicembre 2025	<div>2302 - Data Management</div>		Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Ogni PA centrale (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta al suo interno almeno 15 dataset, qualora si dovesse avere una popolazione > di 250.000 abitanti	CAPS.PA.13	entro dicembre 2025	<div>2306 - Data Management 2</div>		Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Ogni PA centrale (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 30 dataset	CAPS.PA.14	entro dicembre 2025			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Se non ancora presenti nel 2024 nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 3 dataset, qualora si dovesse avere una popolazione tra 5.000 e 10.000 abitanti	CAPS.PA.15	entro dicembre 2026			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Se non ancora presenti nel 2024 nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 10 dataset, qualora si dovesse avere una popolazione tra 10.001 e 100.000 abitanti	CAPS.PA.16	entro dicembre 2026			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Se non ancora presenti nel 2024 nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 15 dataset, qualora si dovesse avere una popolazione tra 100.001 e 250.000 abitanti	CAPS.PA.17	entro dicembre 2026			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Se non ancora presenti nel 2024 nel catalogo dati.gov.it, pubblicare e documentare al suo interno almeno 30 dataset, qualora si dovesse avere una popolazione > di 250.000 abitanti	CAPS.PA.18	entro dicembre 2026			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
		Ogni PA centrale (non ancora presente nel 2024 nel catalogo dati.gov.it) pubblica e documenta nel catalogo almeno 45 dataset	CAPS.PA.19	entro dicembre 2026			Non di competenza dell'Ente	Non di competenza dell'Ente	Si qualora l'Ente non nella fascia di popolazione indicata
	RAS 2.4 - Aumento del numero di dataset documentati sul portale dati.gov.it che rispettano la caratteristica di qualità "attualità" (o "tempestività di aggiornamento") di cui allo Standard ISO/IEC 29512	Nessuna azione prevista per l'Ente			<div><div>2302 - Data Management</div><div>2306 - Data Management 2</div></div> <div>Iniziativa strategica di maggior rilievo: Data Management</div> <div>Iniziativa strategica di dettaglio:</div>		Nessuna azione prevista per l'Ente	Nessuna azione prevista per l'Ente	No
	Obiettivo 5.3 - Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati	RAS 3.1 - Aumento del numero di dataset di tipo aperto documentati nel portale dati.gov.it che adottano le licenze previste dalle Linee guida Open Data	CAPS.PA.20	da gennaio 2024	<div><div>2302 - Data Management</div><div>2306 - Data Management 2</div></div> <div>Iniziativa strategica di maggior rilievo: Data Management</div> <div>Iniziativa strategica di dettaglio:</div>		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Completata	Si
	Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale	RAS 4.1 - Linee guida per promuovere l'adozione dell'IA nella Pubblica Amministrazione	CAPS.PA.21	da dicembre 2025			Entro la scadenza del Piano Triennale per l'Informatica dell'AgD	Da attuare	Si
		RAS 4.2 - Linee guida per i procurement di IA nella Pubblica Amministrazione	CAPS.PA.22	da dicembre 2025			Entro la scadenza del Piano Triennale per l'Informatica dell'AgD	Da attuare	Si
		RAS 4.3 - Linee guida per lo sviluppo di applicazioni di IA per la Pubblica Amministrazione	CAPS.PA.23	da dicembre 2025			Entro la scadenza del Piano Triennale per l'Informatica dell'AgD	Da attuare	Si
		RAS 4.4 - Realizzazione di applicazioni di IA a valenza nazionale	CAPS.PA.24	entro dicembre 2026			Entro Dicembre 2026	Da attuare	Si
	Obiettivo 5.5 - Dati per l'intelligenza artificiale	RAS 5.1 - Basi di dati nazionali strategiche	CAPS.PA.25	entro dicembre 2026			Entro Dicembre 2026	Pianificate	Si
		Se proprietari di data center di gruppo B, richiedere l'autorizzazione ad AGD per le spese in materia di data center nelle modalità stabilite dalla Circolare AGD L/2019 e prevedere in tali contratti, qualora autorizzati, una durata massima coerente con i tempi strettamente necessari a completare il percorso di migrazione previsti nei propri piani di migrazione	CAPL.PA.01		<div>Linee di azione vigenti</div> <div>Iniziativa strategica di maggior rilievo: Servizi applicativi in ottica cloud</div> <div>Iniziativa strategica di dettaglio:</div>		Non di competenza dell'Ente	Non di competenza dell'Ente	Si - condizionato al fatto che l'Ente sia proprietario di data center di gruppo B
		Se proprietari di data center adaffiliati ai requisiti ACN, continuare a gestire e mantenere tali data center in coerenza con quanto previsto dalla Strategia Cloud Italia e dal Regolamento cloud	CAPL.PA.02		<div>Linee di azione vigenti</div> <div>2312 - Applicativi Cloud</div>		Non di competenza dell'Ente	Non di competenza dell'Ente	Si - condizionato al fatto che l'Ente sia proprietario di data center adeguati ai requisiti ACN
	Obiettivo 6.1 - 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)	RA6.1.1 - Numero di amministrazioni migrate	CAPL.PA.03		<div>Linee di azione vigenti</div> <div>2481 - Applicativi Cloud 1</div>		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Già vigente	Si
		Continuare ad applicare il principio cloud first e ad acquisire servizi cloud solo se qualificati	CAPL.PA.04		<div>Linee di azione vigenti</div> <div>2610 - Applicativi Cloud 1</div>		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Già vigente	Si
		Aggiornare l'elenco e la classificazione dei dati e dei servizi digitali in presenza di dati e servizi ulteriori rispetto a quelli già oggetto di conferimento o classificazione come indicato nel Regolamento e di conseguenza aggiornare, ove necessario, anche il piano di migrazione	CAPL.PA.05		<div>Linee di azione vigenti</div> <div>2313 - Public Cloud</div>		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Già vigente	Si
		Trasmissione, ove richiesto dal Dipartimento per la Trasformazione Digitale o da AGD, delle informazioni relative allo stato di avanzamento dell'implementazione dei piani di migrazione	CAPL.PA.06	da settembre 2024	<div>2302 - Cloud Enabling</div>		Entro la scadenza del Piano Triennale per l'Informatica dell'AgD	Non completata	Si - condizionato alla richiesta di informazioni da AGD o DDT
		In caso di realizzazione o/o utilizzo di infrastrutture di prossimità, verificare la conformità di queste ai requisiti del Regolamento di cui al comma 4 dell'articolo 33 septies del Decreto-legge 179/2012 e darne apposita comunicazione ad ACN	CAPL.PA.07	da settembre 2024	<div>2297 - Saas Primo</div> <div>2330 - Saas CBM</div>		Attualmente non programmato	Non completata	Si - condizionato alla realizzazione o/o utilizzo di infrastrutture di prossimità
	Obiettivo 6.2 - Garantire alle amministrazioni la disponibilità della connettività 5G	RA6.2.1 - Rete di connettività	CAPL.PA.10	entro giugno 2026	<div>2010 - Saas B</div> <div>2493 - Saas ITSM</div> <div>2494 - Saas Service 4</div> <div>RA6.2.1 - Rete di connettività</div>		Conclusa il 29/11/2024	Completata	Si
		Sulla base delle proprie esigenze, iniziare la fase di migrazione della propria infrastruttura di rete utilizzando i servizi resi disponibili dalla nuova gara di connettività 5G	CAPL.PA.11	da marzo 2026	<div>5G (Completato)</div>		Attualmente non programmato	Non completata	No
	Obiettivo 7.1 - Adottare una governance della cybersecurity diffusa nella PA	RA7.1.1 - Identificazione di un modello, con ruoli e responsabilità, di gestione della cybersecurity	CAPT.PA.01	da settembre 2024	<div>Iniziativa strategica di maggior rilievo: Sicurezza informatica</div> <div>Iniziativa strategica di dettaglio:</div>		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Completata	Si
		Adottare un modello di governance della cybersecurity	CAPT.PA.02	da dicembre 2024	<div>2296 - Sicurezza da remoto</div>		L'Ente ha realizzato questa linea di azione entro i termini previsti dal Piano Triennale per l'Informatica dell'AgD	Completata	Si
		Nominare i Responsabili della cybersecurity e delle loro strutture organizzative di supporto	CAPT.PA.03	da dicembre 2024	<div>2387 - Sicurezza informatica</div>		Non di competenza dell'Ente	Non di competenza dell'Ente	No
		Formalizzare i processi e le procedure inerenti alla gestione della cybersecurity	CAPT.PA.04	da dicembre 2024	<div><div>2387 - Sicurezza informatica</div><div>2388 - Sicurezza informatica</div><div>2389 - Sicurezza informatica</div><div>2390 - Sicurezza informatica</div><div>2391 - Sicurezza informatica</div><div>2392 - Sicurezza informatica</div><div>2393 - Sicurezza informatica</div><div>2394 - Sicurezza informatica</div><div>2395 - Sicurezza informatica</div><div>2396 - Sicurezza informatica</div><div>2397 - Sicurezza informatica</div><div>2398 - Sicurezza informatica</div><div>2399 - Sicurezza informatica</div><div>2400 - Sicurezza informatica</div><div>2401 - Sicurezza informatica</div><div>2402 - Sicurezza informatica</div><div>2403 - Sicurezza informatica</div><div>2404 - Sicurezza informatica</div><div>2405 - Sicurezza informatica</div><div>2406 - Sicurezza informatica</div><div>2407 - Sicurezza informatica</div><div>2408 - Sicurezza informatica</div><div>2409 - Sicurezza informatica</div><div>2410 - Sicurezza informatica</div><div>2411 - Sicurezza informatica</div><div>2412 - Sicurezza informatica</div><div>2413 - Sicurezza informatica</div><div>2414 - Sicurezza informatica</div><div>2415 - Sicurezza informatica</div><div>2416 - Sicurezza informatica</div><div>2417 - Sicurezza informatica</div><div>2418 - Sicurezza informatica</div><div>2419 - Sicurezza informatica</div><div>2420 - Sicurezza informatica</div><div>2421 - Sicurezza informatica</div><div>2422 - Sicurezza informatica</div><div>2423 - Sicurezza informatica</div><div>2424 - Sicurezza informatica</div><div>2425 - Sicurezza informatica</div><div>2426 - Sicurezza informatica</div><div>2427 - Sicurezza informatica</div><div>2428 - Sicurezza informatica</div><div>2429 - Sicurezza informatica</div><div>2430 - Sicurezza informatica</div><div>2431 - Sicurezza informatica</div><div>2432 - Sicurezza informatica</div><div>2433 - Sicurezza informatica</div><div>2434 - Sicurezza informatica</div><div>2435 - Sicurezza informatica</div><div>2436 - Sicurezza informatica</div><div>2437 - Sicurezza informatica</div><div>2438 - Sicurezza informatica</div><div>2439 - Sicurezza informatica</div><div>2440 - Sicurezza informatica</div><div>2441 - Sicurezza informatica</div><div>2442 - Sicurezza informatica</div><div>2443 - Sicurezza informatica</div><div>2444 - Sicurezza informatica</div><div>2445 - Sicurezza informatica</div><div>2446 - Sicurezza informatica</div><div>2447 - Sicurezza informatica</div><div>2448 - Sicurezza informatica</div><div>2449 - Sicurezza informatica</div><div>2450 - Sicurezza informatica</div><div>2451 - Sicurezza informatica</div><div>2452 - Sicurezza informatica</div><div>2453 - Sicurezza informatica</div><div>2454 - Sicurezza informatica</div><div>2455 - Sicurezza informatica</div><div>2456 - Sicurezza informatica</div><div>2457 - Sicurezza informatica</div><div>2458 - Sicurezza informatica</div><div>2459 - Sicurezza informatica</div><div>2460 - Sicurezza informatica</div><div>2461 - Sicurezza informatica</div><div>2462 - Sicurezza informatica</div><div>2463 - Sicurezza informatica</div><div>2464 - Sicurezza informatica</div><div>2465 - Sicurezza informatica</div><div>2466 - Sicurezza informatica</div><div>2467 - Sicurezza informatica</div><div>2468 - Sicurezza informatica</div><div>2469 - Sicurezza informatica</div><div>2470 - Sicurezza informatica</div><div>2471 - Sicurezza informatica</div><div>2472 - Sicurezza informatica</div><div>2473 - Sicurezza informatica</div><div>2474 - Sicurezza informatica</div><div>2475 - Sicurezza informatica</div><div>2476 - Sicurezza informatica</div><div>2477 - Sicurezza informatica</div><div>2478 - Sicurezza informatica</div><div>2479 - Sicurezza informatica</div><div>2480 - Sicurezza informatica</div><div>2481 - Sicurezza informatica</div><div>2482 - Sicurezza informatica</div><div>2483 - Sicurezza informatica</div><div>2484 - Sicurezza informatica</div><div>2485 - Sicurezza informatica</div><div>2486 - Sicurezza informatica</div><div>2487 - Sicurezza informatica</div><div>2488 - Sicurezza informatica</div><div>2489 - Sicurezza informatica</div><div>2490 - Sicurezza informatica</div><div>2491 - Sicurezza informatica</div><div>2492 - Sicurezza informatica</div><div>2493 - Sicurezza informatica</div><div>2494 - Sicurezza informatica</div><div>2495 - Sicurezza informatica</div><div>2496 - Sicurezza informatica</div><div>2497 - Sicurezza informatica</div><div>2498 - Sicurezza informatica</div><div>2499 - Sicurezza informatica</div><div>2500 - Sicurezza informatica</div><div>2501 - Sicurezza informatica</div><div>2502 - Sicurezza informatica</div><div>2503 - Sicurezza informatica</div><div>2504 - Sicurezza informatica</div><div>2505 - Sicurezza informatica</div><div>2506 - Sicurezza informatica</div><div>2507 - Sicurezza informatica</div><div>2508 - Sicurezza informatica</div><div>2509 - Sicurezza informatica</div><div>2510 - Sicurezza informatica</div><div>2511 - Sicurezza informatica</div><div>2512 - Sicurezza informatica</div><div>2513 - Sicurezza informatica</div><div>2514 - Sicurezza informatica</div><div>2515 - Sicurezza informatica</div><div>2516 - Sicurezza informatica</div><div>2517 - Sicurezza informatica</div><div>2518 - Sicurezza informatica</div><div>2519 - Sicurezza informatica</div><div>2520 - Sicurezza informatica</div><div>2521 - Sicurezza informatica</div><div>2522 - Sicurezza informatica</div><div>2523 - Sicurezza informatica</div><div>2524 - Sicurezza informatica</div><div>2525 - Sicurezza informatica</div><div>2526 - Sicurezza informatica</div><div>2527 - Sicurezza informatica</div><div>2528 - Sicurezza informatica</div><div>2529 - Sicurezza informatica</div><div>2530 - Sicurezza informatica</div><div>2531 - Sicurezza informatica</div><div>2532 - Sicurezza informatica</div><div>2533 - Sicurezza informatica</div><div>2534 - Sicurezza informatica</div><div>2535 - Sicurezza informatica</div><div>2536 - Sicurezza informatica</div><div>2537 - Sicurezza informatica</div><div>2538 - Sicurezza informatica</div><div>2539 - Sicurezza informatica</div><div>2540 - Sicurezza informatica</div><div>2541 - Sicurezza informatica</div><div>2542 - Sicurezza informatica</div><div>2543 - Sicurezza informatica</div><div>2544 - Sicurezza informatica</div><div>2545 - Sicurezza informatica</div><div>2546 - Sicurezza informatica</div><div>2547 - Sicurezza informatica</div><div>2548 - Sicurezza informatica</div><div>2549 - Sicurezza informatica</div><div>2550 - Sicurezza informatica</div><div>2551 - Sicurezza informatica</div><div>2552 - Sicurezza informatica</div><div>2553 - Sicurezza informatica</div><div>2554 - Sicurezza informatica</div><div>2555 - Sicurezza informatica</div><div>2556 - Sicurezza informatica</div><div>2557 - Sicurezza informatica</div><div>2558 - Sicurezza informatica</div><div>2559 - Sicurezza informatica</div><div>2560 - Sicurezza informatica</div><div>2561 - Sicurezza informatica</div><div>2562 - Sicurezza informatica</div><div>2563 - Sicurezza informatica</div><div>2564 - Sicurezza informatica</div><div>2565 - Sicurezza informatica</div><div>2566 - Sicurezza informatica</div><div>2567 - Sicurezza informatica</div><div>2568 - Sicurezza informatica</div><div>2569 - Sicurezza informatica</div><div>2570 - Sicurezza informatica</div><div>2571 - Sicurezza informatica</div><div>2572 - Sicurezza informatica</div><div>2573 - Sicurezza informatica</div><div>2574 - Sicurezza informatica</div><div>2575 - Sicurezza informatica</div><div>2576 - Sicurezza informatica</div><div>2577 - Sicurezza informatica</div><div>2578 - Sicurezza informatica</div><div>2579 - Sicurezza informatica</div><div>2580 - Sicurezza informatica</div><div>2581 - Sicurezza informatica</div><div>2582 - Sicurezza informatica</div><div>2583 - Sicurezza informatica</div><div>2584 - Sicurezza informatica</div><div>2585 - Sicurezza informatica</div><div>2586 - Sicurezza informatica</div><div>2587 - Sicurezza informatica</div><div>2588 - Sicurezza informatica</div><div>2589 - Sicurezza informatica</div><div>2590 - Sicurezza informatica</div><div>2591 - Sicurezza informatica</div><div>2592 - Sicurezza informatica</div><div>2593 - Sicurezza informatica</div><div>2594 - Sicurezza informatica</div><div>2595 - Sicurezza informatica</div><div>2596 - Sicurezza informatica</div><div>2597 - Sicurezza informatica</div><div>2598 - Sicurezza informatica</div><div>2599 - Sicurezza informatica</div><div>2600 - Sicurezza informatica</div><div>2601 - Sicurezza informatica</div><div>2602 - Sicurezza informatica</div><div>2603 - Sicurezza informatica</div><div>2604 - Sicurezza informatica</div><div>2605 - Sicurezza informatica</div><div>2606 - Sicurezza informatica</div><div>2607 - Sicurezza informatica</div><div>2608 - Sicurezza informatica</div><div>2609 - Sicurezza informatica</div><div>2610 - Sicurezza informatica</div><div>2611 - Sicurezza informatica</div><div>2612 - Sicurezza informatica</div><div>2613 - Sicurezza informatica</div><div>2614 - Sicurezza informatica</div><div>2615 - Sicurezza informatica</div><div>2616 - Sicurezza informatica</div><div>2617 - Sicurezza informatica</div><div>2618 - Sicurezza informatica</div><div>2619 - Sicurezza informatica</div><div>2620 - Sicurezza informatica</div><div>2621 - Sicurezza informatica</div><div>2622 - Sicurezza informatica</div><div>2623 - Sicurezza informatica</div><div>2624 - Sicurezza informatica</div><div>2625 - Sicurezza informatica</div><div>2626 - Sicurezza informatica</div><div>2627 - Sicurezza informatica</div><div>2628 - Sicurezza informatica</div><div>2629 - Sicurezza informatica</div><div>2630 - Sicurezza informatica</div><div>2631 - Sicurezza informatica</div><div>2632 - Sicurezza informatica</div><div>2633 - Sicurezza informatica</div><div>2634 - Sicurezza informatica</div><div>2635 - Sicurezza informatica</div><div>2636 - Sicurezza informatica</div><div>2637 - Sicurezza informatica</div><div>2638 - Sicurezza informatica</div><div>2639 - Sicurezza informatica</div><div>2640 - Sicurezza informatica</div><div>2641 - Sicurezza informatica</div><div>2642 - Sicurezza informatica</div><div>2643 - Sicurezza informatica</div><div>2644 - Sicurezza informatica</div><div>2645 - Sicurezza informatica</div><div>2646 - Sicurezza informatica</div><div>2647 - Sicurezza informatica</div><div>2648 - Sicurezza informatica</div><div>2649 - Sicurezza informatica</div><div>2650 - Sicurezza informatica</div><div>2651 - Sicurezza informatica</div><div>2652 - Sicurezza informatica</div><div>2653 - Sicurezza informatica</div><div>2654 - Sicurezza informatica</div><div>2655 - Sicurezza informatica</div><div>2656 - Sicurezza informatica</div><div>2657 - Sicurezza informatica</div><div>2658 - Sicurezza informatica</div><div>2659 - Sicurezza informatica</div><div>2660 - Sicurezza informatica</div><div>2661 - Sicurezza informatica</div><div>2662 - Sicurezza informatica</div><div>2663 - Sicurezza informatica</div><div>2664 - Sicurezza informatica</div><div>2665 - Sicurezza informatica</div><div>2666 - Sicurezza informatica</div><div>2667 - Sicurezza informatica</div><div>2668 - Sicurezza informatica</div><div>2669 - Sicurezza informatica</div><div>2670 - Sicurezza informatica</div><div>2671 - Sicurezza informatica</div><div>2672 - Sicurezza informatica</div><div>2673 - Sicurezza informatica</div><div>2674 - Sicurezza informatica</div><div>2675 - Sicurezza informatica</div><div>2676 - Sicurezza informatica</div><div>2677 - Sicurezza informatica</div><div>2678 - Sicurezza informatica</div><div>2679 - Sicurezza informatica</div><div>2680 - Sicurezza informatica</div><div>2681 - Sicurezza informatica</div><div>2682 - Sicurezza informatica</div><div>2683 - Sicurezza informatica</div><div>2684 - Sicurezza informatica</div><div>2685 - Sicurezza informatica</div><div>2686 - Sicurezza informatica</div><div>2687 - Sicurezza informatica</div><div>2688 - Sicurezza informatica</div><div>2689 - Sicurezza informatica</div><div>2690 - Sicurezza informatica</div><div>2691 - Sicurezza informatica</div><div>2692 - Sicurezza informatica</div><div>2693 - Sicurezza informatica</div><div>2694 - Sicurezza informatica</div><div>2695 - Sicurezza informatica</div><div>2696 - Sicurezza informatica</div><div>2697 - Sicurezza informatica</div><div>2698 - Sicurezza informatica</div><div>2699 - Sicurezza informatica</div><div>2700 - Sicurezza informatica</div><div>2701 - Sicurezza informatica</div><div>2702 - Sicurezza informatica</div><div>2703 - Sicurezza informatica</div><div>2704 - Sicurezza informatica</div><div>2705 - Sicurezza informatica</div><div>2706 - Sicurezza informatica</div><div>2707 - Sicurezza informatica</div><div>2708 - Sicurezza informatica</div><div>2709 - Sicurezza informatica</div><div>2710 - Sicurezza informatica</div><div>2711 - Sicurezza informatica</div><div>2712 - Sicurezza informatica</div><div>2713 - Sicurezza informatica</div><div>2714 - Sicurezza informatica</div><div>2715 - Sicurezza informatica</div><div>2716 - Sicurezza informatica</div><div>2717 - Sicurezza informatica</div><div>2718 - Sicurezza informatica</div><div>2719 - Sicurezza informatica</div><div>2720 - Sicurezza informatica</div><div>2721 - Sicurezza informatica</div><div>2722 - Sicurezza informatica</div><div>2723 - Sicurezza informatica</div><div>2724 - Sicurezza informatica</div><div>2725 - Sicurezza informatica</div><div>2726 - Sicurezza informatica</div><div>2727 - Sicurezza informatica</div><div>2728 - Sicurezza informatica</div><div>2729 - Sicurezza informatica</div><div>2730 - Sicurezza informatica</div><div>2731 - Sicurezza informatica</div><div>2732 - Sicurezza informatica</div><div>2733 - Sicurezza informatica</div><div>2734 - Sicurezza informatica</div><div>2735 - Sicurezza informatica</div><div>2736 - Sicurezza informatica</div><div>2737 - Sicurezza informatica</div><div>2738 - Sicurezza informatica</div><div>2739 - Sicurezza informatica</div><div>2740 - Sicurezza informatica</div><div>2741 - Sicurezza informatica</div><div>2742 - Sicurezza informatica</div><div>2743 - Sicurezza informatica</div><div>2744 - Sicurezza informatica</div><div>2745 - Sicurezza informatica</div><div>2746 - Sicurezza informatica</div><div>2747 - Sicurezza informatica</div><div>2748 - Sicurezza informatica</div><div>2749 - Sicurezza informatica</div><div>2750 - Sicurezza informatica</div><div>2751 - Sicurezza informatica</div><div>2752 - Sicurezza informatica</div><div>2753 - Sicurezza informatica</div><div>2754 - Sicurezza informatica</div><div>2755 - Sicurezza informatica</div><div>2756 - Sicurezza informatica</div><div>2757 - Sicurezza informatica</div><div>2758 - Sicurezza informatica</div><div>2759 - Sicurezza informatica</div><div>2760 - Sicurezza informatica</div><div>2761 - Sicurezza informatica</div><div>2762 - Sicurezza informatica</div><div>2763 - Sicurezza informatica</div><div>2764 - Sicurezza informatica</div><div>2765 - Sicurezza informatica</div><div>2766 - Sicurezza informatica</div><div>2767 - Sicurezza informatica</div><div>2768 - Sicurezza informatica</div><div>2769 - Sicurezza informatica</div><div>2770 - Sicurezza informatica</div><div>2771 - Sicurezza informatica</div><div>2772 - Sicurezza informatica</div><div>2773 - Sicurezza informatica</div><div>2774 - Sicurezza informatica</div><div>2775 - Sicurezza informatica</div><div>2776 - Sicurezza informatica</div><div>2777 - Sicurezza informatica</div><div>2778 - Sicurezza informatica</div><div>2779 - Sicurezza informatica</div><div>2780 - Sicurezza informatica</div><div>2781 - Sicurezza informatica</div><div>2782 - Sicurezza informatica</div><div>2783 - Sicurezza informatica</div><div>2784 - Sicurezza informatica</div><div>2785 - Sicurezza informatica</div><div>2786 - Sicurezza informatica</div><div>2787 - Sicurezza informatica</div><div>2788 - Sicurezza informatica</div><div>2789 - Sicurezza informatica</div><div>2790 - Sicurezza informatica</div><div>2791 - Sicurezza informatica</div><div>2792 - Sicurezza informatica</div><div>2793 - Sicurezza informatica</div><div>2794 - Sicurezza informatica</div><div>2795 - Sicurezza informatica</div><div>2796 - Sicurezza informatica</div><div>2797 - Sicurezza informatica</div><div>2798 - Sicurezza informatica</div><div>2799 - Sicurezza informatica</div><div>2800 - Sicurezza informatica</div><div>2801 - Sicurezza informatica</div><div>2802 - Sicurezza informatica</div><div>2803 - Sicurezza informatica</div><div>2804 - Sicurezza informatica</div><div>2805 - Sicurezza informatica</div><div>2806 - Sicurezza informatica</div><div>2807 - Sicurezza informatica</div><div>2808 - Sicurezza informatica</div><div>2809 - Sicurezza informatica</div><div>2810 - Sicurezza informatica</div><div>2811 - Sicurezza informatica</div><div>2812 - Sicurezza informatica</div><div>2813 - Sicurezza informatica</div><div>2814 - Sicurezza informatica</div><div>2815 - Sicurezza informatica</div><div>2816 - Sicurezza informatica</div><div>2817 - Sicurezza informatica</div><div>2818 - Sicurezza informatica</div><div>2819 - Sicurezza informatica</div><div>2820 - Sicurezza informatica</div><div>2821 - Sicurezza informatica</div><div>2822 - Sicurezza informatica</div><div>2823 - Sicurezza informatica</div><div>2824 - Sicurezza informatica</div><div>2825 - Sicurezza informatica</div><div>2826 - Sicurezza informatica</div><div>2827 - Sicurezza informatica</div><div>2828 - Sicurezza informatica</div><div>2829 - Sicurezza informatica</div><div>2830 - Sicurezza informatica</div><div>2831 - Sicurezza informatica</div><div>2832 - Sicurezza informatica</div><div>2833 - Sicurezza informatica</div><div>2834 - Sicurezza informatica</div><div>2835 - Sicurezza informatica</div><div>2836 - Sicurezza informatica</div><div>2837 - Sicurezza informatica</div><div>2838 - Sicurezza informatica</div><div>2839 - Sicurezza informatica</div><div>2840 - Sicurezza informatica</div><div>2841 - Sicurezza informatica</div><div>2842 - Sicurezza informatica</div><div>2843 - Sicurezza informatica</div><div>2844 - Sicurezza informatica</div><div>2845 - Sicurezza informatica</div><div>2846 - Sicurezza informatica</div><div>2847 - Sicurezza informatica</div><div>2848 - Sicurezza informatica</div><div>2849 - Sicurezza informatica</div><div>2850 - Sicurezza informatica</div><div>2851 - Sicurezza informatica</div><div>2852 - Sicurezza informatica</div><div>2853 - Sicurezza informatica</div><div>2854 - Sicurezza informatica</div><div>2855 - Sicurezza informatica</div><div>2856 - Sicurezza informatica</div><div>2857 - Sicurezza informatica</div><div>2858 - Sicurezza informatica</div><div>2859 - Sicurezza informatica</div><div>2860 - Sicurezza informatica</div><div>2861 - Sicurezza informatica</div><div>2862 - Sicurezza informatica</div><div>2863 - Sicurezza informatica</div><div>2864 - Sicurezza informatica</div><div>2865 - Sicurezza informatica</div><div>2866 - Sicurezza informatica</div><div>2867 - Sicurezza informatica</div><div>2868 - Sicurezza informatica</div><div>2869 - Sicurezza informatica</div><div>2870 - Sicurezza informatica</div><div>2871 - Sicurezza informatica</div><div>2872 - Sicurezza informatica</div><div>2873 - Sicurezza informatica</div><div>2874 - Sicurezza informatica</div><div>2875 - Sicurezza informatica</div><div>2876 - Sicurezza informatica</div><div>2877 - Sicurezza informatica</div><div>2878 - Sicurezza informatica</div><div>2879 - Sicurezza informatica</div><div>2880 - Sicurezza informatica</div><div>2881 - Sicurezza informatica</div><div>2882 - Sicurezza informatica</div><div>2883 - Sicurezza informatica</div><div>2884 - Sicurezza informatica</div><div>2885 - Sicurezza informatica</div><div>2886 - Sicurezza informatica</div><div>2887 - Sicurezza informatica</div><div>2888 - Sicurezza informatica</div><div>2889 - Sicurezza informatica</div><div>2890 - Sicurezza informatica</div><div>2891 - Sicurezza informatica</div><div>2892 - Sicurezza informatica</div><div>2893 - Sicurezza informatica</div><div>2894 - Sicurezza informatica</div><div>2895 - Sicurezza informatica</div><div>2896 - Sicurezza informatica</div><div>2897 - Sicurezza informatica</div><div>2898 - Sicurezza informatica</div><div>2899 - Sicurezza informatica</div><div>2900 - Sicurezza informatica</div><div>2901 - Sicurezza informatica</div><div>2902 - Sicurezza informatica</div><div>2903 - Sicurezza informatica</div><div>2904 - Sicurezza informatica</div><div>2905 - Sicurezza informatica</div><div>2906 - Sicurezza informatica</div><div>2907 - Sicurezza informatica</div><div>2908 - Sicurezza informatica</div><div>2909 - Sicurezza informatica</div><div>2910 - Sicurezza informatica</div><div>2911 - Sicurezza informatica</div><div>2912 - Sicurezza informatica</div><div>2913 - Sicurezza informatica</div><div>2914 - Sicurezza informatica</div><div>2915 - Sicurezza informatica</div></div>				

Capitolo 7 - Sicurezza informatica	Obiettivo 7.3 - Gestione e mitigazione del rischio cyber		Realizzare o acquisire gli strumenti atti alla messa in sicurezza dell'integrità, confidenzialità e disponibilità dei servizi e dei dati, come definito dalle relative procedure	CAPT.PA.10	entro dicembre 2025	2387 - Sicurezza perimetrale	Tempestivamente	Non completata	SI
			Integrare le attività di monitoraggio del rischio cyber, come definito dal relativo Piano, nelle normali attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi informativi	CAPT.PA.11	entro dicembre 2026	2174 - Protezione email, web, dati	Entro Dicembre 2026	Non completata	SI
		RA7.3.2 - Definizione delle modalità di monitoraggio del rischio cyber	Integrare le attività di monitoraggio del rischio cyber, come definito dal relativo Piano, nelle normali attività di progettazione, analisi, conduzione e dismissione di applicativi e sistemi informativi	CAPT.PA.12	da dicembre 2025	Iniziativa strategica di maggior rilievo: Sicurezza informatica Iniziativa strategica di dettaglio: 2296 - Sicurezza da remoto 2387 - Sicurezza perimetrale 2174 - Protezione email, web, dati	Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Non completata	SI
	Obiettivo 7.4 - Potenziare le modalità di prevenzione e gestione degli incidenti informatici	RA7.4.1 - Definizione del framework documentale relativo alla gestione degli incidenti	Definire i presidi per la gestione degli eventi di sicurezza, formalizzandone i processi e le procedure	CAPT.PA.13	da giugno 2024	Iniziativa strategica di maggior rilievo: Sicurezza informatica Iniziativa strategica di dettaglio:	Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Non completata	SI
			Formalizzare ruoli, responsabilità e processi, nonché le capacità tecnologiche a supporto della prevenzione e gestione degli incidenti informatici	CAPT.PA.14	da dicembre 2024	2296 - Sicurezza da remoto 2387 - Sicurezza perimetrale 2174 - Protezione email, web, dati	Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Non completata	SI
		RA7.4.2 - Definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti	Definire le modalità di verifica dei Piani di risposta a seguito di incidenti informatici	CAPT.PA.15	da dicembre 2024	Iniziativa strategica di maggior rilievo: Sicurezza informatica Iniziativa strategica di dettaglio:	Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Non completata	SI
			Definire le modalità di aggiornamento dei Piani di risposta e ripristino a seguito dell'accadimento di incidenti informatici	CAPT.PA.16	da dicembre 2025	2296 - Sicurezza da remoto 2387 - Sicurezza perimetrale 2174 - Protezione email, web, dati	Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Non completata	SI
		Obiettivo 7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale	RA7.5.1 - Definizione dei piani di formazione in ambito cyber	Promuovere l'accesso e l'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersecurity	CAPT.PA.17	da giugno 2024	Iniziativa strategica di maggior rilievo: Sicurezza informatica Iniziativa strategica di dettaglio:	Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Non completata
			Definire piani di formazione inerenti alla cybersecurity, diversificati per ruoli, posizioni organizzative e attività delle risorse dell'organizzazione	CAPT.PA.18	da dicembre 2024	2296 - Sicurezza da remoto 2387 - Sicurezza perimetrale 2174 - Protezione email, web, dati	Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Non completata	SI
	RA7.5.2 - Adozione di strumenti atti alla formazione in ambito cyber		Realizzare iniziative per verificare e migliorare la consapevolezza del proprio personale	CAPT.PA.19	da dicembre 2025		Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Non completata	SI
	Obiettivo 7.6 - Contrastare il rischio cyber attraverso attività di supporto proattivo alla PA	RA7.6.1 - Distribuzione di Indicatori di Compromissione alla PA	Dotarsi degli strumenti idonei all'acquisizione degli IoC ed accreditarsi al CERT-AGID	CAPT.PA.20	da dicembre 2024		Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Pianificata	SI
		RA7.6.2 - Fornitura di strumenti funzionali all'esecuzione dei piani di autovalutazione dei sistemi esposti	Usufruire degli strumenti per la gestione dei rischi cyber messi a disposizione dal CERT-AGID	CAPT.PA.21	da dicembre 2024		Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Pianificata	SI
		RA7.6.3 - Supporto formativo e informativo rivolto alla PA e in particolare agli RTD per l'aumento del livello di consapevolezza delle minacce cyber	Sulla base delle proprie esigenze, partecipare ai corsi di formazione base ed avanzato erogati dal CERT-AGID	CAPT.PA.22	da dicembre 2025		Entro la scadenza del Piano Triennale per l'informatica dell'AgID	Non completata	NO