

Categoria della misura		Misura				Ambito		Rischi	AdeR	Fornitore	
Codice	Nome	Codice	Nome	Descrizione	Tipologia	Ambito di sicurezza	Interscambio dati	Minaccia	Misura da implementare nel software	Misura applicabile nel contesto (SI/NO)	Modalità di applicazione oppure perché la misura non è applicabile
CT65_AS	Trasferimento sicuro dei dati e dei documenti	AS21	Scambio documenti con PEC	Lo scambio con terze parti di documenti riservati in formato elettronico mediante posta elettronica avviene tramite l'utilizzo di PEC	OfficeAutomation	Asset	Generico Interoperabilità Cooperazione applicativa	Divulgazione non autorizzata o accidentale di dati	SI		
CT02_CA	Sistema di autenticazione debole	CA02	Autenticazione, rete interna	Il personale interno si autentica ai servizi intranet dell'organizzazione tramite un'utenza nominale sul dominio Active Directory. Tale requisito si applica anche al personale esterno che per svolgere attività continuativa deve accedere ai servizi dell'organizzazione. Le eventuali deroghe vengono motivate e inviate al responsabile della struttura che si occupa di sicurezza delle informazioni e privacy.	Infrastrutturale	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT04_CA	Gestione sicura delle credenziali di autenticazione	CA03	Autenticazione, form di accesso	Il form di accesso al servizio ICT non fornisce aiuto durante il logon (ad esempio non indica quale delle informazioni inserite è errata) e non fornisce informazioni sul sistema e sulle applicazioni prima che l'accesso dell'utente sia terminato con successo.	ICT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT04_CA	Gestione sicura delle credenziali di autenticazione	CA07	Autenticazione, caratteristiche delle credenziali	I sistemi di controllo accessi implementano i seguenti requisiti per la gestione delle credenziali: - non consentire la creazione di password inferiori a otto caratteri o, solo in caso di impedimenti tecnici, al massimo consentito dal sistema - non consentire la creazione di password contenenti riferimenti riconducibili all'utente (ad es. password uguale al nome utente o che contenga parte del nome utente) - non consentire l'assegnazione ad altri utenti di credenziali già utilizzate in precedenza (credenziali nominali) - modificare la password di accesso al primo utilizzo. Eventuali deroghe per le utenze di servizio vengono motivate e tracciate.	Infrastrutturale	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT04_CA	Gestione sicura delle credenziali di autenticazione	CA08	Autenticazione, blocco delle credenziali	Il sistema di controllo accessi blocca le credenziali a fronte di reiterati tentativi falliti di autenticazione. Eventuali deroghe per le utenze di servizio sono motivate e registrate.	Infrastrutturale	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT04_CA	Gestione sicura delle credenziali di autenticazione	CA09	Autenticazione, memorizzazione e trasmissione credenziali	Il sistema di controllo accessi prevede che le credenziali di autenticazione siano trasmesse in forma cifrata (cifratura delle credenziali e/o del canale) su reti non fidate.	Infrastrutturale	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT04_CA	Gestione sicura delle credenziali di autenticazione	CA10	Autenticazione, disattivazione delle credenziali	Le credenziali di autenticazione non utilizzate da almeno 6 mesi vengono disattivate. Fanno eccezione solamente quelle utilizzate come utenze di servizio. <i>[specificare se il titolare indica tempi diversi]</i>	ICT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT02_CA	Sistema di autenticazione ordinario	CA12	Autenticazione username e password	I dati personali o di media o alta criticità (in termini di Riservatezza e Integrità) sono acceduti direttamente o tramite applicativo, previa autenticazione attraverso username e password con password policy quali: - la password venga comunicata all'utente separatamente rispetto al codice per l'identificazione (user id), sia modificata al primo utilizzo e, successivamente, almeno ogni tre mesi e le ultime tre password non possano essere riutilizzate - la password sia costituita da almeno otto caratteri e contenga caratteri alfanumerici, lettere maiuscole, minuscole e caratteri speciali.	ICT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT03_CA	Sistema di autenticazione forte	CA13	Autenticazione a due fattori	Se il servizio ICT tratta dati sensibili, ipersensibili, giudiziari o critici (in termini di Riservatezza e Integrità), e in caso di rischio particolarmente alto (es. esposizione su reti non fidate), il sistema di controllo accessi prevede l'autenticazione a due fattori <i>[specificare il sistema di autenticazione adottato]</i> .	ICT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT95_CA	Autenticazione forte amministratori e postazioni	CA14	Scambio dati, identificazione postazioni di lavoro	Per le funzionalità che consentono lo scambio di dati tra pubbliche amministrazioni, gli accessi alle banche dati avvengono soltanto tramite postazioni di lavoro censite connesse alla rete IP dell'amministrazione autorizzata oppure dotate di certificato digitale che le identifichi univocamente (anche attraverso reti di accesso sicuro) <i>[specificare la modalità adottata]</i> .	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT04_CA	Gestione sicura delle credenziali di autenticazione	CA15	Scambio dati, distribuzione credenziali	Per le applicazioni che consentono lo scambio di dati tra pubbliche amministrazioni, la distribuzione delle credenziali agli utenti avviene in modo sicuro secondo una procedura prestabilita <i>[specificare, ad es. password comunicata separatamente rispetto allo username o token OTP consegnato de visu]</i> .	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT95_CA	Autenticazione forte amministratori e postazioni	CA16	Scambio dati, autenticazione a due fattori amministratori	Nelle applicazioni che consentono lo scambio di dati tra pubbliche amministrazioni è prevista una procedura di autenticazione a due fattori per: - le classi di utenti con profilo di autorizzazione più alto (in relazione alle funzioni o ai dati accessibili) - tutti i profili di autorizzazione corrispondenti alle funzioni di amministratori locali. <i>[Specificare il sistema di autenticazione adottato]</i>	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT06_CA	Controllo delle sessioni di accesso ai dati	CA18	Scambio dati, numero massimo di utenti	Per le funzionalità che consentono lo scambio di dati tra pubbliche amministrazioni, viene definito e implementato il numero massimo di utenti che possono essere abilitati per ciascuna amministrazione che accede alle banche dati.	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT06_CA	Controllo delle sessioni di accesso ai dati	CA19	Scambio dati, limitazione intervalli temporali di accesso	Per le funzionalità che consentono lo scambio di dati tra pubbliche amministrazioni, l'accesso ai dati è limitato a determinati intervalli temporali o di data <i>[specificare - es. entro gli orari di ufficio. Specificare anche le eventuali deroghe]</i> .	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT08_CA	Verifiche e monitoraggio dei report e degli allarmi	CA20	Scambio dati, controllo status utenti	Le applicazioni che consentono lo scambio dati tra pubbliche amministrazioni implementano funzionalità di visualizzazione dello status di tutte le utenze con i relativi profili abilitativi, comprese quelle cancellate.	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT08_CA	Verifiche e monitoraggio dei report e degli allarmi	CA22	Scambio dati, elenco flussi di trasferimento	Per le applicazioni che consentono lo scambio dati tra pubbliche amministrazioni viene reso disponibile un documento aggiornato che riporta tutti i flussi di trasferimento di dati e tutti gli accessi di tipo interattivo, batch o di altro genere specificando per ognuno: - l'identità dei soggetti legittimati a realizzarlo - la base normativa che ne determina la legittimità - la finalità istituzionale - la natura e la qualità dei dati trasferiti - la frequenza e il volume dei trasferimenti - il numero di soggetti che utilizzano la procedura.	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT05_CA	Gestione dei profili e dei privilegi di autorizzazione	CA23	Scambio dati, inibizione accessi non autorizzati	Per le applicazioni che consentono lo scambio dati tra pubbliche amministrazioni, vengono inibiti gli accessi ai dati da parte delle amministrazioni che non sono autorizzate da norme e non hanno necessità di accesso per finalità istituzionali.	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT06_CA	Controllo delle sessioni di accesso ai dati	CA24	Scambio dati, informazioni su ultimo accesso	Per le applicazioni che consentono lo scambio dati tra pubbliche amministrazioni, nella prima schermata dopo il login vengono visualizzate le informazioni relative alla sessione corrente e all'ultima sessione effettuata (data, ora e indirizzo IP da cui è stato effettuato il precedente accesso).	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT04_CA	Gestione sicura delle credenziali di autenticazione	CA25	Controllo accessi, modifica della password	I sistemi di controllo accessi basati sull'uso di user e password richiedono la modifica della password almeno ogni tre mesi. Eventuali deroghe per le utenze di servizio vengono motivate e tracciate.	Infrastrutturale	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT04_CA	Gestione sicura delle credenziali di autenticazione	CA26	Controllo accessi, utenze di servizio	Le utenze di servizio applicative (ovvero utenze utilizzate dalle applicazioni per connettersi alle basi dati o per richiamare altre applicazioni) non sono utilizzate per effettuare login interattivi allo scopo di accedere direttamente ai dati.	Infrastrutturale	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT06_CA	Controllo delle sessioni di accesso ai dati	CA27	Scambio dati, inibizione accessi contemporanei	Per le applicazioni che consentono lo scambio dati tra pubbliche amministrazioni deve essere esclusa la possibilità di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse [specificare eventuali deroghe].	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT06_CA	Controllo delle sessioni di accesso ai dati	CA28	Controllo accessi, disconnessione della sessione	Il servizio ICT disconnette le sessioni dopo un determinato periodo di inattività (timeout). Eventuali deroghe per le utenze di servizio vengono motivate e tracciate.	ICT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT04_CA	Gestione sicura delle credenziali di autenticazione	CA29	Controllo accessi, verifica identità dell'utente	Il sistema di controllo accessi rispetta i seguenti requisiti: - verifica dell'identità del richiedente in fase di registrazione - distribuzione e recupero delle credenziali subordinati al controllo dell'identità del richiedente.	ICT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT05_CA	Gestione dei profili e dei privilegi di autorizzazione	CA30	Autorizzazione, privilegio minimo	Il sistema di autorizzazione permette di attribuire alle utenze (comprese quelle di servizio) i minimi privilegi necessari per eseguire le attività, in conformità con la normativa, i vincoli contrattuali e di servizio applicabili.	ICT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Divulgazione non autorizzata o accidentale di dati	SI		
CT05_CA	Gestione dei profili e dei privilegi di autorizzazione	CA33	Autorizzazione, separazione delle responsabilità	Il sistema di autorizzazione prevede la separazione delle responsabilità per evitare privilegi in conflitto tra loro individuando le seguenti figure: - <u>Richiedente</u> , che inoltra al proprio Responsabile la domanda di assegnazione di diritti di accesso a specifiche Risorse - <u>Responsabile del Richiedente</u> , che valuta la richiesta e la inoltra al Responsabile della Risorsa - <u>Responsabile della Risorsa</u> , che valuta la richiesta e la inoltra all'Amministratore dei profili - <u>Amministratore dei profili</u> , che verifica la richiesta e implementa i diritti di accesso richiesti, dando opportuno riscontro.	ProcedureIT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT08_CA	Verifiche e monitoraggio dei report e degli allarmi	CA36	Controllo accessi, report per verifica delle utenze	Le strutture dell'organizzazione che si occupano di controllo degli accessi forniscono almeno semestralmente alla struttura che si occupa di sicurezza delle informazioni e privacy una console o un report per eseguire audit e verifica delle utenze di personale interno ed esterno (anche di servizio), con relative autorizzazioni e permessi di accesso.	ProcedureIT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT03_CA	Sistema di autenticazione forte	CA37	Autenticazione per accesso tramite applicativi	Se il servizio ICT tratta dati sensibili, ipersensibili, giudiziari o critici (in termini di Riservatezza e Integrità), e in caso di rischio particolarmente alto (es. esposizione su reti non fidate), le applicazioni che accedono via webservice si autenticano tramite certificato digitale.	ICT	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT95_CA	Autenticazione forte amministratori e postazioni	CA38	Scambio dati, autenticazione delle applicazioni via webservice	L'autenticazione via webservice alle applicazioni che consentono lo scambio di dati tra pubbliche amministrazioni avviene tramite certificato digitale.	ICT	Controllo accessi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT06_CA	Controllo delle sessioni di accesso ai dati	CA39	Controllo accessi, disconnessione della sessione	Sulle postazioni di lavoro e dispositivi portatili e mobili è implementata la disconnessione delle sessioni dopo un determinato periodo di inattività (timeout).	OfficeAutomation	Controllo accessi	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT21_ER	Backup dei sistemi e ripristino del servizio	ER03	Backup, servizio ICT	Per il servizio ICT viene effettuato il backup dei seguenti elementi: - dati - configurazioni dei sistemi - software applicativo - file di log e di alert.	ICT	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Indisponibilità temporanea o prolungata di dati	SI		
CT25_ER	Anonimizzazione dei dati	ER09	Anonimizzazione dei dati	Al fine di ridurre i rischi di trattamento di dati personali, nel servizio ICT devono essere adottate ove applicabili misure di anonimizzazione, tramite la rimozione di qualsiasi elemento riconoscibile che possa permettere a tali informazioni combinate di risalire ad un soggetto specifico identificandolo [specificare i motivi ove non applicabile].	ICT	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Divulgazione non autorizzata o accidentale di dati	SI		
CT09_ER	Pseudonimizzazione dei dati	ER22	Pseudonimizzazione dei dati	Al fine di ridurre i rischi di trattamento di dati personali, nel servizio ICT devono essere adottate ove applicabili misure di pseudonimizzazione, in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative specifiche [specificare i motivi ove non applicabile].	ICT	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Divulgazione non autorizzata o accidentale di dati	SI		

CT12_ER	Cifratura del canale	ER23	Cifratura del canale	Se il servizio ICT consente la trasmissione di dati personali e/o utilizza SPID, i canali di collegamento sono cifrati mediante la versione più aggiornata del protocollo TLS e utilizzano certificati digitali emessi da una Certification Authority ufficiale.	ICT	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT13_ER	Conservazione separata dei dati sensibili	ER24	Conservazione separata	I dati idonei a rivelare lo stato di salute e la vita sessuale trattati da parte di soggetti pubblici sono conservati separatamente da altri dati personali trattati per altre finalità.	ICT	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Divulgazione non autorizzata o accidentale di dati	SI		
CT15_ER	Aggiornamenti periodici dei sistemi informatici tramite patch	ER26	Vulnerabilità tecniche, patching dei sistemi	L'aggiornamento (patching) dei sistemi informatici viene effettuato con cadenza almeno annuale.	Infrastrutturale	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT15_ER	Aggiornamenti periodici dei sistemi informatici tramite patch	ER27	Vulnerabilità tecniche, patching dei sistemi per dati critici	L'aggiornamento (patching) dei sistemi utilizzati per trattare dati sensibili, ipersensibili, giudiziari e per l'erogazione di servizi classificati come critici (in termini di Riservatezza e Integrità) viene effettuato con cadenza almeno semestrale.	Infrastrutturale	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT15_ER	Aggiornamenti periodici dei sistemi informatici tramite patch	ER28	Vulnerabilità tecniche, attività propedeutiche al patching	Prima di installare una patch su un sistema: - si valutano e si documentano i rischi connessi alle vulnerabilità esistenti e agli impatti negativi che si potrebbero avere sulla funzionalità (es. incompatibilità) - si definiscono gli eventuali piani di rientro in caso di incompatibilità - si eseguono e si documentano i relativi test.	Infrastrutturale	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT16_ER	Protezione dei sistemi a livello di rete	ER29	Vulnerabilità tecniche, protezione sistemi in produzione	I sistemi in produzione sono protetti tramite apparati che garantiscono: - la separazione delle reti (reti demilitarizzate) e il controllo del traffico consentito tramite firewall. - la protezione da attacchi informatici condotti mediante i protocolli di rete consentiti (controlli Deep Packet Inspection con sonde IPS, antivirus di rete, anti-botnet, anti ddos)	Infrastrutturale	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT18_ER	Verifica di integrità e non ripudio	ER39	Integrità dei log degli ADS e degli incaricati	I log del servizio ICT e i log di accesso degli Amministratori di sistema e degli incaricati sono protetti da eventuali tentativi di alterazione ed è possibile verificarne l'integrità.	Infrastrutturale	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Modifica non autorizzata o accidentale di dati	SI		
CT19_ER	Gestione della capacità dell'infrastruttura tecnologica	ER41	Capacità dei servizi, monitoraggio	Il servizio ICT è sottoposto a monitoraggio continuo della capacità attraverso l'analisi dei seguenti parametri: - performance della rete (utilizzo della banda) - livelli di carico delle macchine - utilizzo della CPU - occupazione della RAM - occupazione del file system - spazio disco utilizzato e disponibile	Infrastrutturale	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Indisponibilità temporanea o prolungata di dati	SI		

CT18_ER	Verifica di integrità e non ripudio	ER44	Verifica di integrità e non ripudio	Nei casi in cui sia previsto il trattamento di dati non alterabili e/o per norma sottoscritti (es. invio telematico), sono applicate misure tecnologiche che garantiscano la verifica di integrità e, qualora applicabile, il non ripudio <i>[specificare, ad es. firma elettronica]</i> .	ICT OfficeAutomation	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Modifica non autorizzata o accidentale di dati	SI		
CT16_ER	Protezione dei sistemi a livello di rete	ER49	Protezione posta elettronica e internet, filtro sul web	Il traffico web è soggetto a opportuni filtri.	Infrastrutturale	Erogazione del servizio	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT08_CA	Verifiche e monitoraggio dei report e degli allarmi	EV06	Scambio dati, monitoraggio allarmi	Nelle applicazioni che consentono lo scambio di dati tra pubbliche amministrazioni si esegue il monitoraggio statistico delle transazioni di dati eseguite da parte delle altre amministrazioni e, in caso di comportamenti anomali, si attivano specifici allarmi <i>[specificare i comportamenti anomali da monitorare]</i> .	ICT	Gestione eventi	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT75_OR	Conservazione dei dati per un periodo limitato al trattamento	OR10	Conservazione dei dati e cessazione del trattamento	Il Titolare definisce i tempi di conservazione dei dati "nel rispetto del principio di limitazione della conservazione" e le modalità di cessazione del trattamento <i>[specificare: verificati, distrutti, ceduti ad altro titolare, conservati per fini esclusivamente personali o per scopi storici, statistici o scientifici]</i> .	Procedurale	Organizzazione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT77_OR	Consultazione dell'autorità di controllo per il trattamento dei dati	OR22	Autorizzazione, trattamento dati relativi a condanne penali	Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza avviene: - sotto il controllo dell'autorità pubblica oppure - è autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati oppure - è individuato con decreto del ministro della Giustizia da adottarsi sentito il Garante. <i>[specificare]</i> .	Procedurale	Organizzazione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT77_OR	Consultazione dell'autorità di controllo per il trattamento dei dati	OR24	Autorizzazione, trattamento dati sensibili, ipersensibili e biometrici	<p>il trattamento dei dati sensibili, ipersensibili e biometrici può essere effettuato se ricorre una delle seguenti condizioni:</p> <ul style="list-style-type: none"> - l'interessato ha prestato il proprio consenso - il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri - il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; - il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; - il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; 	Procedurale	Organizzazione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT78_OR	Gestione delle richieste da parte dell'interessato	OR28	Procedura per le richieste dell'interessato	<p>E' definita e adottata una procedura per la gestione delle richieste dell'interessato (senza ritardi ingiustificati) di:</p> <ul style="list-style-type: none"> - aggiornamento - rettifica - integrazione - cancellazione - notifica ai destinatari - riscontro all'interessato in formato strutturato, di uso comune e leggibile da dispositivo automatico - trasformazione in forma anonima - blocco dei dati personali trattati - contestazione in caso di profilazione automatica per decisioni giuridiche. 	Procedurale	Organizzazione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT78_OR	Gestione delle richieste da parte dell'interessato	OR31	Diritti dell'interessato	Per ogni trattamento devono essere implementate procedure/funzionalità per la gestione delle richieste da parte dell'interessato di accesso, cancellazione, rettifica dei propri dati, opposizione e limitazione del trattamento.	Procedurale	Organizzazione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT56_EV	Politiche e procedure operative per la gestione degli eventi e degli incidenti di sicurezza	OR46	Data breach, attuazione	Per ogni servizio ICT devono essere implementate le funzionalità che consentono di attuare quanto specificato nella procedura operativa per la gestione del data breach (i.e. notifica al titolare, all'autorità di controllo e all'interessato, secondo i tempi e i contenuti stabiliti)	ProcedureIT	Organizzazione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT66_AS	Gestione delle clausole di sicurezza nei contratti con i fornitori e controlli di conformità	RT24	Contratti con i fornitori per sviluppo software	Nel caso di affidamento all'esterno di sviluppo software, il contratto con i fornitori prevede la garanzia di assenza di codice malevolo nel software consegnato e dell'aderenza del software alle politiche di sicurezza dell'organizzazione.	ProcedureIT	Risorse umane e terze parti	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT84_RT	Informative sul trattamento dei dati e gestione del consenso	RT29	Gestione informative agli utenti e consenso	Per ogni trattamento devono essere implementate procedure/funzionalità a supporto dell'interessato, ove applicabili, quali la comunicazione dell'informativa e la raccolta del consenso.	Procedurale	Risorse Umane e Terze Parti	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT52_ER	Interrogazione sicura delle banche dati	SM03	Scambio dati, indicazione riferimento pratica	Per le funzionalità che consentono lo scambio di dati tra pubbliche amministrazioni è previsto un campo per l'indicazione del numero di riferimento della pratica <i>[specificare. Ad esempio numero del protocollo o del verbale]</i> nell'ambito della quale viene effettuata la consultazione dei dati.	ICT	Sviluppo e Manutenzione	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT52_ER	Interrogazione sicura delle banche dati	SM04	Scambio dati, segmentazione dei dati per limitazione trattamento	Per le funzionalità delle applicazioni che consentono lo scambio di dati tra pubbliche amministrazioni, i dati sono visualizzabili dall'utente secondo i seguenti criteri di segmentazione che ne limitano il trattamento secondo l'effettiva necessità (pertinenza e non eccedenza): - cronologico (es. attuale o storico, per periodi di imposta) - geografico (es. comune, provincia, regione) - tipologia di dati (es. sintesi). <i>[Specificare]</i>	ICT	Sviluppo e Manutenzione	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT65_AS	Trasferimento sicuro dei dati e dei documenti	SM05	Scambio dati, protezione file trasmessi	Per le funzionalità delle applicazioni che consentono lo scambio di dati tra pubbliche amministrazioni tramite file: - il canale di comunicazione utilizzato per lo scambio di file è protetto <i>[specificare. come. Es. cifratura, canale dedicato]</i> - il file messo a disposizione in rete viene rimosso dopo un certo tempo <i>[specificare]</i> dalla richiesta - il file è disponibile solo per gli utenti che lo hanno richiesto - per ogni trasferimento vengono registrati l'utente, la data e l'ora - viene registrato il numero di trasferimenti di un file.	ICT	Sviluppo e Manutenzione	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT52_ER	Interrogazione sicura delle banche dati	SM06	Scambio dati, accesso minimo ai dati	Le funzionalità dei servizi ICT che consentono lo scambio di dati tra pubbliche amministrazioni, offrono un livello minimo di accesso ai dati <i>[specificare se tramite utilizzo di web services di validazione per il controllo sull'esistenza o sulla correttezza di un dato]</i> con risposte limitate a valori di tipo booleano (vero/falso). Le eccezioni vengono autorizzate e documentate <i>[nel caso, specificare]</i> .	ICT	Sviluppo e Manutenzione	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT51_ER	Minimizzazione dei dati	SM07	Minimizzazione dei dati	I dati personali trattati sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità e alla base giuridica per le quali sono trattati	ICT	Sviluppo e Manutenzione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT52_ER	Interrogazione sicura delle banche dati	SM08	Scambio dati, interrogazione puntuale di soggetti	Per le funzionalità che consentono lo scambio di dati tra pubbliche amministrazioni, l'interrogazione diretta delle banche dati o l'invocazione dei web server <i>[specificare la modalità di interrogazione utilizzata]</i> viene effettuata mediante un set minimo di dati in modo che il soggetto cui si riferiscono venga individuato puntualmente. La risposta alla richiesta di dati non contiene mai un elenco dei soggetti a meno di eccezioni documentate in convenzione <i>[nel caso, specificare]</i> .	ICT	Sviluppo e Manutenzione	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT65_AS	Trasferimento sicuro dei dati e dei documenti	SM09	Scambio dati, comunicazione tra applicazioni autorizzate	I web services utilizzati per lo scambio di dati tra pubbliche amministrazioni comunicano esclusivamente con le applicazioni autorizzate sulla base delle convenzioni stipulate dalle amministrazioni.	ICT	Sviluppo e Manutenzione	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT65_AS	Trasferimento sicuro dei dati e dei documenti	SM10	Scambio dati, canali sicuri di comunicazione	Nelle funzionalità che consentono lo scambio di dati tra pubbliche amministrazioni, i dati sono messi a disposizione attraverso i seguenti canali: - il sito istituzionale (accesso via web in un sito appositamente predisposto) - PEC, se la periodicità di acquisizione dei dati è limitata e la quantità di dati è contenuta - FTP sicuro o altra soluzione che garantisca la cifratura del canale. <i>[specificare il canale utilizzato]</i>	ICT	Sviluppo e Manutenzione	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT49_ER	Politiche e procedure operative per lo sviluppo del software	SM13	Change management, procedure operative	Sono definite, pubblicate e attuate le procedure di change management relative al software applicativo che trattino in particolare: - l'approvazione delle richieste di variazione - la gestione del piano di intervento - il tracciamento delle variazioni apportate - la condivisione delle informazioni per finalità relative a test di vulnerabilità tecniche, alla gestione di incidenti di sicurezza o ad audit.	ProcedureIT	Sviluppo e Manutenzione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT54_ER	Sviluppo del software secondo tecniche di programmazione sicura	SM16	Sviluppo sicuro del software	Per lo sviluppo del codice applicativo si adottano linee guida per lo sviluppo sicuro <i>[specificare. Ad esempio metodologia OWASP]</i> .	ProcedureIT	Sviluppo e Manutenzione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT54_ER	Sviluppo del software secondo tecniche di programmazione sicura	SM17	Basi dati di test	Le basi dati di test utilizzate in ambiente di sviluppo/validazione non contengono dati personali riferibili a persone fisiche o dati critici (in termini di Riservatezza e Integrità) (ad esempio mascheramento delle basi dati reali). Le eventuali eccezioni sono documentate <i>[specificare]</i> .	ProcedureIT	Sviluppo e Manutenzione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT54_ER	Sviluppo del software secondo tecniche di programmazione sicura	SM18	Sviluppo software, progettazione	Al termine della progettazione del servizio ICT viene rilasciata la documentazione contenente: - l'architettura logica del servizio - le piattaforme tecnologiche previste - i requisiti di sicurezza applicabili (in relazione alle caratteristiche e alla classificazione del servizio in termini di Riservatezza, Integrità e Disponibilità) e le relative misure di protezione da implementare.	ProcedureIT	Sviluppo e Manutenzione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT54_ER	Sviluppo del software secondo tecniche di programmazione sicura	SM19	Sviluppo software, realizzazione	Al termine della realizzazione del servizio ICT, e prima del rilascio in esercizio, viene rilasciata la documentazione contenente: - l'architettura fisica del servizio - i sistemi installati e configurati La documentazione viene aggiornata in caso di cambiamenti (migrazioni tecnologiche, MEV applicative, ecc).	ProcedureIT	Sviluppo e Manutenzione	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT27_TR	Tracciamento dei servizi ICT	TR02	Tracciamento accessi e operazioni del servizio ICT	Il sistema di tracciamento applicativo del servizio ICT registra le seguenti informazioni per gli accessi da parte di utenti o applicazioni (webservice): - identificativo dell'utente - data e ora dell'operazione richiesta (compresi login, logout e login falliti) - postazione di lavoro dalla quale viene effettuata l'operazione (anche nel caso di utilizzo di dispositivi mobili) - tipo di operazione (es. consultazione, stampa, modifica, ... <i>specificare</i>) - esito dell'operazione (es. completata, fallita, rifiutata, ... <i>specificare</i>) - identificativo delle risorse oggetto dell'operazione (es. archivio, funzionalità, ... <i>specificare</i>) - parametri dell'operazione (es. chiave di ricerca, ... <i>specificare</i>) - dati restituiti all'utente (<i>specificare</i>).	ICT	Tracciamento	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT38_TR	Conservazione dei log per almeno 6 mesi	TR03	Tracciamento, conservazione dei log dei servizi ICT	I log del servizio ICT sono conservati per almeno 6 mesi [<i>specificare il periodo</i>].	ICT	Tracciamento	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT27_TR	Tracciamento dei servizi ICT	TR04	Scambio dati, tracciamento enti esterni	<p>Nelle applicazioni che consentono lo scambio di dati tra pubbliche amministrazioni tramite web services, il sistema di tracciamento registra le seguenti informazioni (log):</p> <ul style="list-style-type: none"> - operazione compiuta in cooperazione applicativa - identificativo dell'utente che accede ai dati e che ha dato origine ad una transazione di accesso ai dati - timestamp - indirizzo IP di provenienza dell'utente o del servizio - indirizzo IP del server interconnesso - dati trattati. 	ICT	Tracciamento	Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT28_TR	Tracciamento del servizio di controllo accessi	TR05	Tracciamento amministratori dei profili CAU	<p>Per gli amministratori dei profili del servizio di controllo accessi, il sistema di tracciamento registra le seguenti informazioni (log):</p> <ul style="list-style-type: none"> - identificativo amministratore - data e ora operazione - tipo operazione (abilitazione, revoca, movimentazione utenti e profili, cambi password) - agenzia dell'amministratore - ufficio dell'amministratore - utente movimentato - ufficio dell'utente movimentato - agenzia dell'utente movimentato - gruppo amministrativo - regola amministrativa - profilo connesso all'utente 	Infrastrutturale	Tracciamento	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT29_TR	Tracciamento degli accessi logici	TR12	Tracciamento ads e incaricati	<p>Per ogni accesso ai sistemi operativi, alla rete, al software di base e ai sistemi complessi in produzione il sistema di tracciamento registra le seguenti informazioni (log):</p> <ul style="list-style-type: none"> - identificativo dell'utenza nominale o non nominale che accede - data e ora di login, logout e login falliti - postazione di lavoro utilizzata per l'accesso (IP client). 	Infrastrutturale	Tracciamento	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT38_TR	Conservazione dei log per almeno 6 mesi	TR13	Tracciamento, conservazione log ads e incaricati	<p>I log relativi agli accessi e alle operazioni effettuate sui sistemi operativi, sulla rete, sul software di base e sui sistemi complessi in produzione sono conservati per un periodo minimo di 6 mesi.</p>	Infrastrutturale	Tracciamento	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		

CT29_TR	Tracciamento degli accessi logici	TR41	Tracciamento degli accessi alle risorse aziendali	<p>Per ogni accesso agli strumenti informatici dell'organizzazione (postazioni di lavoro fisse, rete, servizi interni), il sistema di tracciamento registra le seguenti informazioni (log):</p> <ul style="list-style-type: none"> - identificativo dell'utente che accede - timestamp - indirizzo della postazione utilizzata per l'accesso - operazioni di login, logout e login falliti per codice utente - gestione utenze (creazione, blocco, abilitazione/disabilitazione) - eventi generati dalle soluzioni per la gestione e la verifica della configurazione delle postazioni di lavoro. <p>Fanno eccezione le utenze locali delle postazioni di lavoro.</p>	Infrastrutturale	Tracciamento	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		
CT08_CA	Verifiche e monitoraggio dei report e degli allarmi	TR45	Tracciamento, generazione di report	Il sistema di tracciamento permette la generazione di report e la loro esportazione in formati che consentono di analizzarli (es. excel).	Infrastrutturale	Tracciamento	Generico Interoperabilità Cooperazione applicativa	Accesso non autorizzato e/o trattamento illecito relativo a dati	SI		