DSU TOSCANA

PIANO PER LA SICUREZZA INFORMATICA E LA TUTELA DEI DATI PERSONALI

(Allegato A al "Manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio e all'accesso ai documenti informatici" – Rev. 08)

Sommario

1 PREMESSA

Il "Piano per la sicurezza informatica e la tutela dei dati personali" riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.
Le misure di sicurezza adottate dall'Azienda garantiscono che:

- i documenti e le informazioni trattate dall'Azienda Regionale per il Diritto allo Studio Universitario (di seguito Azienda) siano disponibili, integre e riservate;
- i dati personali di qualsiasi tipologia vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2 FORMAZIONE DEI DOCUMENTI

Le risorse strumentali e le procedure utilizzate dai Servizi aziendali afferenti l'Azienda per la formazione e trasmissione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti Linee Guida dell'Agenzia per l'Italia Digitale[1];
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- la conservazione sostitutiva digitale;
- l'interscambiabilità dei documenti all'interno dell'AOO[2]

I documenti redatti dai servizi aziendali sono prodotti con l'ausilio di applicativi di videoscrittura e possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.
I formati dei documenti prodotti all'interno dell'AOO, nonché gli allegati ad essi, sono principalmente:

- pdf/a
- p7m

fermo restando la possibilità di utilizzare, per determinati contesti, ulteriori tipologie di file avendo cura di seguire le indicazioni contenute nell'Allegato 2 "Formati di file e riversamento" delle Linee Guida sopra citate.
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la

[1] Linee Guida sulla formazione, gestione e conservazione dei documenti informatici entrate in vigore il 10 settembre 2020
[2] AOO=Area Organizzativa Omogenea. L'Azienda Regionale per il Diritto allo Studio Universitario ha definito una AOO unica denominata AOODSUTOSCANA

riservatezza, il documento informatico è sottoscritto con firma digitale.
Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, può essere apposta una marca temporale.

3 GESTIONE, TRASMISSIONE, INTERSCAMBIO E ACCESSO

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente.
Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in maniera tale che:

- gli utenti non possano mai accedere ai documenti al di fuori del sistema di gestione informatica dei documenti;
- avvenga la registrazione delle attività rilevanti ai fini della sicurezza nonché quelle necessarie per la manutenzione svolte sul server di cui sopra dagli utenti abilitati o dai fornitori di servizi di assistenza informatica opportunamente nominati Responsabili esterni del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679[3] in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate;
- venga effettuato periodicamente un backup su risorse esterne (anche in cloud) dei volumi contenenti i documenti presenti nel sistema di gestione documentale e relativi allegati.

Il sistema di gestione informatica dei documenti, intendendo per esso l'applicazione utilizzata per la protocollazione e archiviazione dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti;
- consente la produzione giornaliera del registro di protocollo che viene trasmesso entro la giornata successiva al sistema di conservazione;
- consente la produzione del registro di protocollo annuale;
- assicura la corretta e puntuale registrazione di protocollo dei documenti;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Azienda e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte degli utenti dei Servizi aziendali interessati nonché dagli utenti esterni intendendo per essi:

    - i destinatari delle copie analogiche di documenti informatici ai quali viene apposto il contrassegno elettronico ai sensi dell'art. 23 comma 2 bis del Codice dell'Amministrazione Digitale (D. Lgs 82/2005) i quali accedono tramite credenziali d'accesso univoche ad un server posto in DMZ;
    - i soggetti che abbiano diritto ai sensi della disciplina vigente all'accesso ai documenti soggetti a registrazione di protocollo attraverso il sistema di cui all'art. 40

[3]Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE)

ter del Codice dell'Amministrazione Digitale;

- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

3.1 COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione dei flussi documentali si riferisce principalmente alle attività svolte per l'erogazione delle funzionalità di protocollo informatico, gestione degli atti e della documentazione soggetta a registrazione particolare.
L'Azienda ha individuato nell'ambito della sua organizzazione i servizi aziendali che si occupano di vari aspetti inerenti la sicurezza (figura 2 – situazione al novembre 2020).

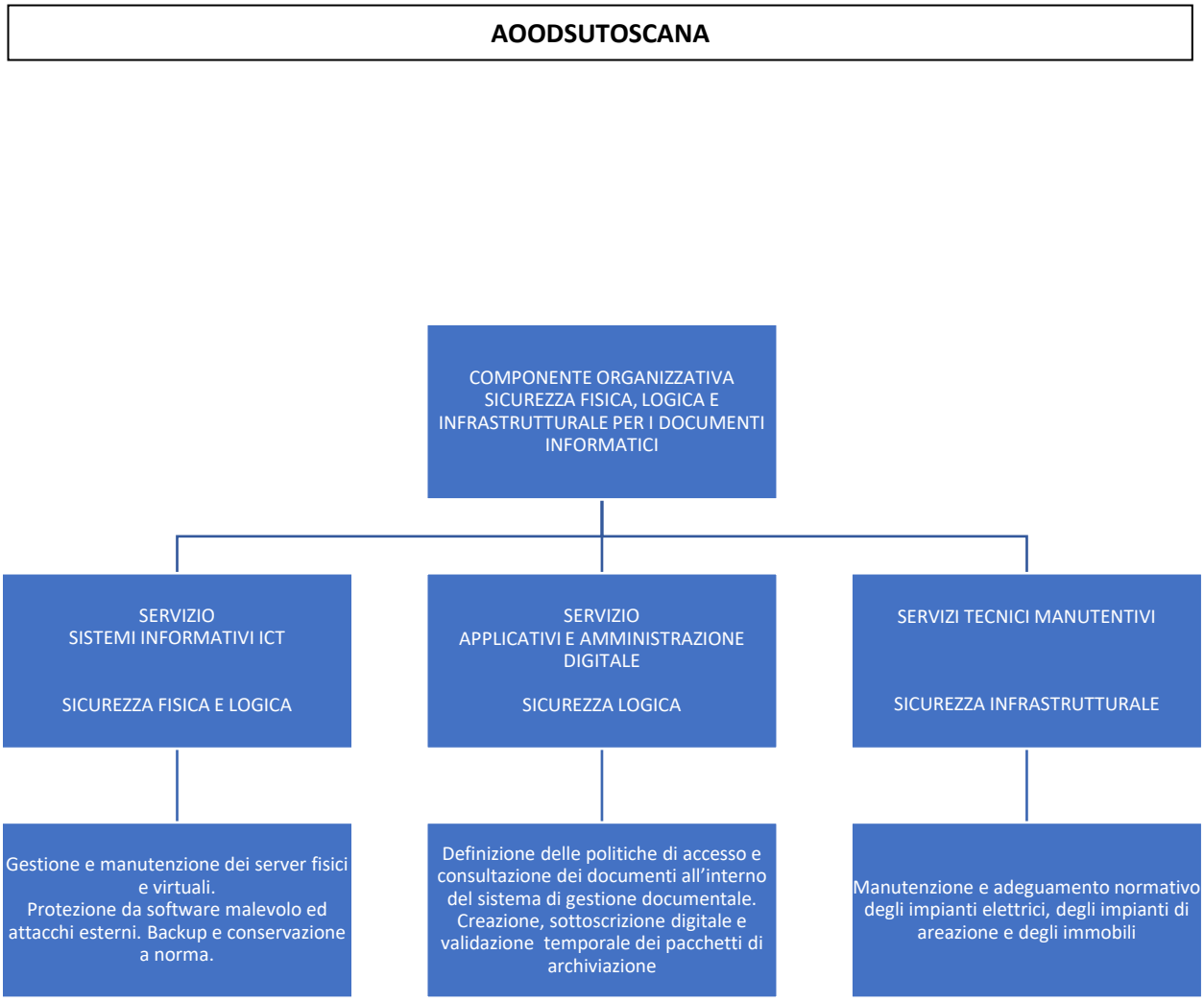

Figura 2 – Servizi aziendali referenti per la componente organizzativa della sicurezza

3.2 COMPONENTE FISICA DELLA SICUREZZA

Il controllo degli accessi fisici alle risorse del sistema informativo dell'Azienda è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale dell'Azienda, nonché a dipendenti di aziende esterne, previa autorizzazione dell'Amministratore di sistema ed esclusivamente per motivi di servizio, manutenzione e controllo;
- l'accesso è altresì consentito al Responsabile della protezione dei dati personali (DPO) esclusivamente per attività di verifica del rispetto dei requisiti di sicurezza (in presenza di personale dell'Azienda autorizzato dall'Amministratore di sistema);
- le chiavi di accesso sono custodite esclusivamente dal personale autorizzato dall'Amministratore di sistema;
- gli accessi fisici alle sedi del sistema informativo dell'Azienda sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;
- il personale in servizio presso ciascuna sede aziendale ha l'obbligo di utilizzare il badge sia in ingresso che in uscita per rilevare la propria presenza.

3.3 COMPONENTE LOGICA DELLA SICUREZZA

3.3.1. CARATTERISTICHE GENERALI DELLA COMPONENTE LOGICA

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.
Tale componente è stata realizzata attraverso:

- la tracciabilità delle operazioni di visualizzazione, smistamento, rimozione dei documenti da parte degli utenti abilitati all'utilizzo dell'applicativo di gestione documentale: tutte le attività elencate sono registrate in forma non modificabile. In particolare, laddove le modifiche di taluni indici siano consentite, viene memorizzato il *versioning* degli stessi in moda da risalire sia all'utente che ha apportato modifiche che ai valori esistenti prima della modifica;
- l'identificazione, autenticazione e autorizzazione degli utenti abilitati all'utilizzo dell'applicativo di gestione documentale;
- la riservatezza dei dati, ottenuta mediante l'attribuzione della visibilità dei documenti esclusivamente ai soggetti e/o ai servizi aziendali competenti;
- l'integrità dei dati, ottenuta mediante l'impossibilità per gli utenti dei servizi aziendali di apportare modifiche ai documenti protocollati;
- la disattivazione delle credenziali di accesso degli utenti non più autorizzati alla consultazione degli archivi (per termine del rapporto di lavoro, trasferimento presso altro Ente, cambio di mansioni, etc...);
- l'installazione su ogni server e su ogni dispositivo in uso agli utenti di un'applicazione di protezione dalle minacce informatiche monitorato a livello centrale dal Servizio Sistemi Informatici (ICT) che comprende i seguenti elementi:

    - antivirus
    - antiransomware
    - prevenzione degli exploit
    - mitigazione degli active adversary
    - lockdown delle applicazioni

- rilevamento antimalware con tecnologie di deep learning
- encryption

Il rilascio delle credenziali di accesso all'applicativo di gestione documentale, la disabilitazione delle utenze cessate, l'attribuzione di eventuali diritti operativi particolari è esclusiva competenza del Responsabile della gestione documentale (o del suo vicario). L'applicazione è accessibile tramite il portale Citrix® utilizzando le credenziali di dominio rilasciate dal Servizio Sistemi Informatici (ICT).[4]
Pertanto l'applicazione non risiede sul client degli utenti.

3.3.2. MISURE MINIME DI SICUREZZA ICT

Con riferimento alle "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni" di cui alla Delibera della Presidenza del Consiglio dei Ministri del 1 agosto 2015 e alla Circolare dell'Agenzia per l'Italia Digitale n. 2/2017 del 18 aprile 2017 si rimanda al "Modulo di implementazione" compilato dall'Amministratore di sistema, agli atti del Servizio Sistemi Informatici (ICT).

3.3.3 COPIE DI SICUREZZA

Situazione al 24/11/2020

Dispositivo	**PERIODICITA' BACKUP**	
	Risorse locali	**Cloud**
VM Database Oracle	giornaliero	giornaliero
VM Documenti e allegati	giornaliero	giornaliero
VM Conservazione Sostitutiva	giornaliera	giornaliero
Supporti ISO Conservazione Sostitutiva	mensile alla creazione dell'iso	mensile, successivo alla copia su NAS

3.4 COMPONENTE INFRASTRUTTURALE DELLA SICUREZZA

La sala server dov'è custodito il complesso principale dell'infrastruttura sistemistica fisica e virtuale è dotata di:

- sistema antincendio;
- rilevazione dell'allagamento;
- luci di emergenza;
- continuità elettrica;
- impianto di condizionamento;
- sistema di antintrusione collegato ad una centrale operativa di vigilanza

[4]Nel corso di vigenza del presente manuale, l'accesso all'applicativo di gestione documentale avverrà esclusivamente tramite interfaccia web.

3.5 TRASMISSIONE DEI DOCUMENTI

La trasmissione dei documenti informatici avviene principalmente tramite posta elettronica certificata. Solo qualora i destinatari non siano in possesso di una casella PEC, il documento viene trasmesso per posta elettronica tradizionale oppure – se necessaria l'attestazione di avvenuta ricezione, attraverso raccomandata con ricevuta di ritorno (previa stampa del documento su supporto cartaceo e apposizione di contrassegno elettronico per consentire al destinatario di poter accedere al documento informatico firmato digitalmente).
La trasmissione dei documenti informatici con destinatari interni all'Azienda avviene principalmente tramite l'applicativo di gestione dei flussi documentali (per coloro che hanno un account attivo) ovvero tramite raccomandata a mano con notifica di consegna (previa stampa del documento su supporto cartaceo e apposizione di contrassegno elettronico per consentire al destinatario di poter accedere al documento informatico firmato digitalmente).

4 ABILITAZIONI PER L'ACCESSO AL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

L'abilitazione per l'accesso al sistema di gestione documentale per gli **utenti interni** all'Azienda, deve essere richiesto dal Direttore o dal Dirigente dell'Area funzionale o dal Responsabile del servizio cui afferisce l'utente, inviando un messaggio di posta elettronica all'indirizzo protocollo@dsu.toscana.it esclusivamente dalla propria casella mail istituzionale, avendo cura di indicare se l'utente:

- dovrà avere accesso alla consultazione dell'eventuale casella PEC assegnata al servizio o all'area funzionale;
- dovrà essere autorizzato all'invio di messaggi di posta elettronica certificata dalla casella PEC eventualmente assegnata al servizio o all'area funzionale;
- dovrà essere autorizzato all'invio di messaggi di posta elettronica tradizionale (dal proprio account istituzionale)

L'abilitazione per l'accesso al sistema di gestione documentale per gli **utenti esterni** all'Azienda, deve essere richiesto dal vertice amministrativo dell'Ente richiedente, inviando apposita richiesta all'indirizzo pec dsutoscana@postacert.toscana.it (esclusivamente dalla casella di posta elettronica certificata dell'Ente). L'abilitazione viene autorizzata dal Responsabile della gestione documentale (o dal suo vicario) sentito il parere del Direttore. In questo caso la scadenza delle credenziali di accesso è fissata in 12 mesi (a meno che non venga richiesto o autorizzato un periodo inferiore ai 12 mesi). Decorso tale periodo è necessario effettuare una nuova richiesta.

5 TUTELA DEI DATI PERSONALI

La gestione dei flussi documentali e il sistema di protocollo informatico dell'Azienda sono ispirati alle norme in materia di tutela dei dati personali di cui al Codice in materia di protezione dei dati personali e al GDPR, soprattutto con particolare riferimento al concetto di *accountability* ed alla capacità di adottare un processo efficace per la protezione degli stessi in grado di ridurre al minimo i rischi di una loro possibile violazione.
I criteri utilizzati per la tutela dei dati personali delle persone fisiche assicurano che tali dati siano protetti in tutto il ciclo di vita del documento (analogico o informatico che sia).
In particolare:

- l'accesso al programma di gestione dei flussi documentali è riservato agli utenti appositamente abilitati dal Responsabile della gestione documentale o dal suo vicario

(vedi par. 4);

- la visualizzazione all'interno del programma di gestione dei flussi documentali, dei documenti contenenti dati personali è sempre limitata agli utenti la cui funzione è strettamente connessa al procedimento collegato alle tipologie documentarie ad essi smistate. La visibilità dei documenti, in generale, è sempre la più limitata possibile;
- tutti gli utenti che accedono al programma di gestione dei flussi documentali sono nominati "autorizzati al trattamento dei dati personali" ai sensi di quanto previsto dal Regolamento UE 2016/679. Ad essi – con particolare riferimento al trattamento dei dati personali nell'ambito della gestione dei flussi documentali, sono impartite le seguenti istruzioni:

    - trattare i dati personali in modo lecito e secondo correttezza;
    - raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
    - verificare che tali dati siano esatti e, se necessario, aggiornarli;
    - comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti;
    - astenersi dal comunicare a terzi, al di fuori dell'ambito lavorativo, qualsivoglia dato personale;
    - informare tempestivamente il Titolare del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
    - informare tempestivamente il Titolare del trattamento qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni riportate nell'atto di nomina, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite;
    - accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
    - accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
    - non fornire telefonicamente, a mezzo fax o attraverso strumenti telematici, dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare;
    - non fornire telefonicamente, a mezzo fax o attraverso strumenti telematici, dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
    - relazionarsi e collaborare con gli altri autorizzati al trattamento dei dati, attenendosi alle indicazioni fornite e provvedendo, a propria volta, a dare indicazioni esaustive in caso di coinvolgimento di altri incaricati nei trattamenti effettuati.

Inoltre, in base alla tipologia di strumento utilizzato per il trattamento sono fornite le seguenti ulteriori prescrizioni.

<u>Trattamenti con strumenti elettronici</u>

- non salvare documenti contenenti dati personali sulle risorse locali (hard disk della postazione pc o del notebook o comunque di qualsiasi dispositivo aziendale) o su

dispositivi di memorizzazione esterni (hard disk esterni, chiavette usb) o ancora su dvd/cd-rom;

- a fine turno di lavoro, cancellare dalle risorse locali (e svuotare il cestino) eventuali file contenenti dati personali (dopo averli salvati – se necessario – come sopra riportato): si faccia attenzione alla cartella "Download" o comunque alla/e cartella/e dove vengono scaricati i file dal browser. Cancellarne il contenuto e svuotare il cestino;
- non dare evidenza delle credenziali di accesso al proprio pc, al portale delle applicazioni Citrix®, alla webmail, agli applicativi (come ad esempio, scrivendo su post-it login+password) o a servizi on line;
- le credenziali di accesso sono strettamente personali e non vanno comunicate ad altri soggetti;
- al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici devono tassativamente essere chiusi a chiave;
- in caso di assenza momentanea dalla propria postazione accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. A tal fine è necessario chiudere la sessione di lavoro sul PC attraverso la disconnessione (logout) oppure, in alternativa, attivare un salvaschermo (screen-saver) protetto dalle credenziali di autenticazione. Relativamente allo screen-saver occorre osservare le seguenti prescrizioni:
  - non deve mai essere disattivato;
  - il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
  - deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito.
- quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare che soggetti non abilitati al trattamento ne prendano visione.

<u>Trattamenti senza strumenti elettronici</u>

- per quanto riguarda l'eventuale documentazione cartacea, gli atti e i documenti contenenti dati personali devono essere conservati, dagli autorizzati al trattamento, per la durata di esso e successivamente riposti in archivi ad accesso controllato, al fine di escludere l'accesso agli stessi da parte di persone non incaricate al trattamento. Ciò vale in generale per tutte le pratiche giornalmente trattate che non devono essere lasciate incustodite al termine del turno di lavoro;
- nel caso di trattamento di dati sensibili o di dati giudiziari, la documentazione deve essere conservata in contenitori muniti di serratura, al fine di escludere l'acquisizione o la presa visione degli stessi, da parte di persone non incaricate al trattamento;
- qualora sia necessario distruggere i documenti contenenti dati personali, è buona norma utilizzare gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili;
- gli autorizzati al trattamento sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto;

- analogamente, per quanto riguarda i flussi di documenti cartacei all'interno degli uffici o fra le sedi territoriali dell'Azienda, devono essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in buste chiuse).

Inoltre, ai sensi di quanto previsto dall'art. 46 del CAD, recante "*Dati particolari contenuti nei documenti trasmessi*", al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del Codice della privacy, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via digitale possono contenere soltanto i dati sensibili e giudiziari consentiti dalla legge o da regolamenti, indispensabili per il perseguimento delle finalità per le quali sono acquisiti.

6 CONSERVAZIONE SOSTITUTIVA DIGITALE

Si rimanda al Manuale della conservazione sostitutiva digitale per le specifiche inerenti il processo di conservazione degli archivi secondo quanto previsto dalle vigenti Linee Guida.