

# **ARTI**

Agenzia regionale per la tecnologia,  
il trasferimento tecnologico  
e l'innovazione

# **PUGLIA**



## **MANUALE DI GESTIONE E CONSERVAZIONE DOCUMENTALE ARTI PUGLIA - ALLEGATO 7**

**Piano della Sicurezza**

Sommario

Premessa..... 3

Protezione Fisica delle Risorse..... 3

Protezione Logica delle Informazioni e Norme per il Personale ..... 4

Formazione dei Documenti..... 4

Gestione dei Documenti ..... 5

Trasmissione e Interscambio dei Documenti Informatici ..... 5

Accesso ai Documenti Informatici..... 6

Conservazione dei Documenti Informatici ..... 7

## Premessa

Il Piano di sicurezza dei documenti informatici 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.

In materia di misure di sicurezza, le linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici, riportano:

*“Nell’attuazione delle presenti Linee Guida, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall’AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della conservazione, di concerto con il responsabile per la transizione digitale, con il responsabile della gestione documentale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell’art. 32 del Regolamento UE 679/201648, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.”*

## Protezione Fisica delle Risorse

L’obiettivo della protezione fisica delle risorse è quello di proteggere le aree e le componenti del sistema informativo.

Generalmente le contromisure di sicurezza fisica possono essere ricondotte a sicurezza dell’area e sicurezza delle apparecchiature.

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi informatici. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all’accesso, alla sicurezza delle sale computer rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

La sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall’altro alla sicurezza degli impianti di alimentazione e di condizionamento. Anche la manutenzione dell’hardware rientra in questa area, come anche la protezione da manomissione o furti.

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

- l'accesso è consentito soltanto al personale dell’Agenzia, 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);
- il personale in servizio presso l’unica sede ha l'obbligo di utilizzare il badge sia in ingresso

che in uscita per rilevare la propria presenza;

- tutti i sistemi informativi sono acquisiti in modalità SaaS (*Software as a Service*) e da fornitori iscritti al Marketplace AgID in grado di garantire la tutela dell'accesso ai sistemi sia fisici che logici e di applicare misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei requisiti di riservatezza, integrità e disponibilità delle informazioni.

## Protezione Logica delle Informazioni e Norme per il Personale

Gli obiettivi della protezione logica delle informazioni sono:

- il controllo degli accessi alle informazioni.
- il mantenimento della loro integrità e riservatezza.
- la sicurezza nella trasmissione e nelle comunicazioni all'interno dell'Amministrazione e con l'esterno (Internet, altre Amministrazioni etc.).
- la sicurezza delle stazioni di lavoro e dei personal computer.
- la tempestiva rilevazione di eventuali incidenti di sicurezza.

Il campo di applicazione della Sicurezza Logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.

## Formazione dei Documenti

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- 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;
- l'interscambiabilità dei documenti all'interno della stessa AOO.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o text editor e possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

Si adottano preferibilmente i formati PDF/a, PDF PAdES, PDF CAdES.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno dell'AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici.

## Gestione dei Documenti

Il sistema di gestione documentale assicura:

- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Il sistema di gestione documentale consente:

- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
- il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il registro giornaliero di protocollo è trasmesso entro le due giornate lavorative successive al sistema di conservazione, garantendone l'immodificabilità del contenuto.

## Trasmissione e Interscambio dei Documenti Informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

SCAMBIO DEI DOCUMENTI ALL'ESTERNO DELL'AMMINISTRAZIONE (INTEROPERABILITÀ DEI SISTEMI DI PROTOCOLLO INFORMATICO)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti.

Ogni messaggio protocollato deve riportare alcune informazioni archivistiche fondamentali, per facilitare il trattamento dei documenti da parte del ricevente. Tali informazioni sono incluse nella segnature informatica di ciascun messaggio protocollato e sono codificate in formato XML.

Con provvedimento dell'Agenzia per l'Italia Digitale, vengono indicati le modalità di trasmissione dei documenti informatici, il tipo ed il formato delle informazioni archivistiche di protocollo minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai messaggi protocollati.

## SCAMBIO DEI DOCUMENTI ALL'INTERNO DELL'AMMINISTRAZIONE

Gli Uffici dell'amministrazione si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica oppure tramite registrazione di protocolli interni.

## Accesso ai Documenti Informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Il sistema documentale adottato dall'amministrazione:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

Ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo ufficio, o agli uffici ad esso subordinati.

Un utente può avere la visibilità completa sul registro di protocollo solo a seguito di abilitazione.

Il RGD, il personale dell'ufficio protocollo generale e dell'ufficio sistemi informatici sono abilitati alla visualizzazione completa sul registro protocollo.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. Nel caso in cui sia effettuata la registrazione di un

documento riservato, la visibilità completa sul documento stesso è possibile solo alla persona destinataria del documento.

Di norma tutti gli utenti che devono protocollare sono abilitati alla consultazione ed inserimento, ma è possibile abilitare un utente anche alla sola consultazione.

Solo il personale dell'UOP è invece abilitato all'annullamento.

## Conservazione dei Documenti Informatici

Ai sensi dell'art. 44 del Codice, la conservazione può essere svolta all'interno della struttura organizzativa del soggetto produttore dei documenti o affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

In attuazione di quanto indicato all'art. 3, commi 1 e 2, e all'art. 11, commi 1, 4 e 5, della Convenzione per l'utilizzo del Servizio di Conservazione, l'amministrazione ha individuato nel Polo di Conservazione Digitale della Regione Puglia, gestito da Innovapuglia S.p.A., il soggetto pubblico accreditato come conservatore presso l'Agenzia per l'Italia digitale, a cui affidare la conservazione digitale dei documenti informatici prodotti. Tale soggetto è in grado di fornire idonee garanzie di sicurezza ed efficacia e dispone della strumentazione tecnica necessaria e di personale adeguato allo scopo.

Per le modalità operative di trasmissione del contenuto del pacchetto di versamento al sistema di conservazione si rimanda al manuale di conservazione.

Il manuale di conservazione inoltre illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.