Camera di Commercio
Terni

Manuale di Conservazione Camera di commercio di Terni

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	23/05/2017	Giuliana Piandoro	Responsabile conservazione della CCIAA di Terni
Verifica			
Approvazione			

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni

Indice

1 Scopo e ambito del documento

Il presente manuale descrive il sistema di conservazione ai sensi dell' art. 44 del CAD e dell'art. 8 delle Regole Tecniche.

In particolare, nel presente documento sono definiti:

- i ruoli e responsabilità nel processo di conservazione;
- l'attivazione del servizio;
- gli oggetti sottoposti alla conservazione;
- il processo di conservazione;
- le misure di sicurezza e di protezione dei dati personali.

La parte del processo di conservazione affidata ad un soggetto esterno è ulteriormente dettagliata nel manuale della conservazione del Soggetto conservatore.

2 Terminologia (glossario e acronimi)

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
AIP	Archival Information Package. Definizione dello standard OAIS e sinonimo di Pacchetto di Archiviazione
CAD	D.lsg 7 marzo 2005 , n. 82 e s.m.i., Codice dell'amministrazione digitale
Circolare AgID	Circolare AgID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
Codice della privacy	Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali
Dublin Core	ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
Manuale SCD_IC	Manuale di conservazione del Soggetto Conservatore (InfoCamere) pubblicato sul sito dell'AgID
OAIS	Open Archival Information System è lo standard IS0:14721:2003 e definisce concetti, modelli e funzionalità inerenti agli archivi digitali e gli aspetti di digital preservation.
Piano della sicurezza	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza.
Ente produttore o Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
Regole Tecniche	DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
Regole CNIPA 2004	Deliberazione CNIPA n. 11/2004 Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali del 19 febbraio 2004. La deliberazione CNIPA n. 11/2004 cessa di avere efficacia nei termini previsti dall' Art. 14 comma 2 e 3 delle Regole Tecniche
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle Regole Tecniche del sistema di conservazione
Sistema CNIPA 2004	Sistema di conservazione che rispetta le regole tecniche definite nella deliberazione CNIPA n. 11/2004 del 19 febbraio 2004
Sistema AgID 2013	Sistema di conservazione che rispetta le regole tecniche definite nel DPCM 3/12/2013 ed i requisiti di qualità e sicurezza previsti per i conservatori accreditati da AgID
Servizi Documentali (SCD_IC)	Applicazione Infocamere per la conservazione dei documenti informatici
UniSincro	UNI 11386:2010 - Supporto all'Interoperabilità nella conservazione e nel Recupero degli oggetti digitali
Utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

3 Normativa e standard di riferimento

3.1 Normativa di riferimento

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 24 dicembre 2007, n. 244 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche per la formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto MEF 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005;
- Decreto MEF 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244;
- Circolare AgID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- Deliberazione Cnipa 21 Maggio 2009, n. 45 – Regole per il riconoscimento e la verifica del documento informatico;

3.2 Standard di riferimento

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO 9001:2008 sistemi di gestione per la qualità – Requisiti
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- ISO/TS 23081-1:2006 Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale.
- ISO 23081-2:2009 - Managing metadata for records – Part 2: Conceptual and implementation issues, Guida pratica per l'implementazione.
- 23081-3:2011 Information and documentation -- Managing metadata for records -- Part 3: Self-assessment method, Guida per un processo di autovalutazione sui metadata.
- ISAD(G) - International Standard Archival description standard adottato dal Comitato per gli standard descrittivi degli archivi
- EAD - Encoded Archival Description, codifica XML dello standard ISAD(G)
- ISAAR - International Standard Archival Authority Records, standard internazionale per I record d’autorità archivistici di enti, persone, famiglie
- EAC - Encoded Archival Context, codifica XML dello standard ISAAR

4 Ruoli e responsabilità

4.1 Produttore / Responsabile della conservazione

Le Regole Tecniche (Glossario, allegato 1) identificano il produttore nel soggetto, titolare dei dati, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.

L'Ente produttore affida la conservazione dei propri documenti informatici e dei fascicoli informatici al responsabile della conservazione. Ai sensi dell'art. 7 delle Regole tecniche, il responsabile della conservazione:

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 delle Regole Tecniche;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
m) predispone il manuale di conservazione di cui all'art. 8 delle Regole Tecniche e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti, in collaborazione con il responsabile della gestione documentale ovvero con il coordinatore della gestione documentale, ove nominato.

Il Responsabile della conservazione viene nominato con atto deliberativo del segretario generale della CCIAA tra i dirigenti e i funzionari con specifica competenza ed esperienza (art. 7, comma 3, Regole Tecniche) e può coincidere con il responsabile della gestione documentale (art, 7, comma 4, Regole Tecniche). Il responsabile della conservazione è stato individuato con determina del Segretario Generale n. 269 del 27/09/2016 nella persona della d.ssa Giuliana Piandoro e il dott. Sergio Fabrini quale vicario per i casi di assenza e impedimento del responsabile.

Attraverso un'apposita convenzione per l'affidamento del servizio di conservazione a norma dei documenti informatici (art. 5, comma 3, Regole Tecniche), il Responsabile della conservazione ha

affidato ad InfoCamere, società consortile delle CCIAA e Soggetto conservatore accreditato presso Agid, le seguenti parti del processo di conservazione:

i. gestire il processo di conservazione, tecniche in conformità con la normativa vigente e a quanto descritto da InfoCamere nel Manuale di conservazione e nelle Specifiche tecniche;
ii. generare il rapporto di versamento secondo le modalità previste nel Manuale di conservazione;
iii. generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale di conservazione;
iv. effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
v. assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
vi. adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adottare analoghe misure con riguardo all'obsolescenza dei formati;
vii. produrre duplicati informatici secondo quanto previsto dal Manuale di conservazione;
viii. adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
ix. assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Il Responsabile della conservazione condivide il Manuale della conservazione con il Soggetto conservatore e con tutti i soggetti coinvolti nel processo di conservazione, a cui comunica tempestivamente ogni eventuale modifica.

4.2 Soggetto conservatore / InfoCamere

InfoCamere, in virtù della convenzione stipulata, opera quale Soggetto conservatore esterno, ai sensi del comma 8 dell'art. 6 delle Regole Tecniche assume il ruolo di responsabile del trattamento dei dati come Previsto dal Codice in materia di protezione dei dati personali.

In base alla normativa vigente, il sistema di conservazione InfoCamere prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso dei dati presso le strutture dedicate allo svolgimento del servizio di conservazione o la sede del produttore.

InfoCamere, come Soggetto conservatore accreditato:

- Rispetta i requisiti organizzativi, di qualità e sicurezza previsti da AgID ed offre idonee garanzie organizzative e tecnologiche per lo svolgimento delle funzioni affidategli.
- Svolge i suoi compiti avvalendosi di persone che per competenza ed esperienza, garantiscono la corretta esecuzione delle operazioni.
- Prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso dei dati presso le strutture dedicate allo svolgimento del servizio di conservazione o la sede del produttore.

4.3 Utente

Le Regole Tecniche (Glossario, allegato 1) identificano l'utente come una persona, ente o sistema, che interagisce con i servizi di un sistema per la conservazione di documenti informatici. L'utente può essere interno o esterno all'Ente produttore.

L'utente richiede al sistema di conservazione l'accesso ai documenti informatici per acquisire le informazioni di interesse nei limiti previsti dalla legge. Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati.

In termini OAIS la comunità degli utenti può essere definita come comunità di riferimento.

4.4 Ruoli

Nella tabella successiva vengono indicati i nominativi delle persone fisiche e/o giuridiche che ricoprono i ruoli indicati nel sistema di conservazione.

Ruoli	Nominativo	periodo nel ruolo	eventuali deleghe
Responsabile della conservazione	Giuliana Piandoro	Dal 27/09/2016	
Vicario	Sergio Fabrini	Dal 27/09/2016	
Soggetto Conservatore	InfoCamere	Dal 19/10/2016	

5 Attivazione del servizio

5.1 Affidamento del servizio

Il Responsabile della conservazione ha affidato il processo di conservazione ad InfoCamere, Soggetto conservatore accreditato presso AgID, attraverso la sottoscrizione della convenzione per l'affidamento del servizio di conservazione a norma dei documenti informatici e delle relative specifiche tecniche, avvenuta in data 19/10/2016 e **con termine 31/12/2018.**

InfoCamere ha un proprio manuale della conservazione i cui contenuti sono conformi all'art. 8 delle Regole Tecniche. La versione aggiornata del Manuale di conservazione di InfoCamere, in quanto Soggetto conservatore accreditato, è pubblicata sul sito dell'Agenzia per l'Italia digitale.

5.2 Accesso al servizio

L'Ente produttore accede al sistema di conservazione attraverso i Servizi documentali InfoCamere che:

- generano i pacchetti di versamento;
- integrano l'applicazione per l'esibizione dei contenuti conservati, in grado di generare i pacchetti di distribuzione.

5.3 Descrizione del servizio

La descrizione del servizio di conservazione, comprensiva di tutte le componenti tecnologiche, fisiche e logiche, è presente nel Manuale di conservazione del Soggetto Conservatore.

5.4 Regole tecniche e Regole CNIPA 2004

In conformità all'art. 14 co. 3 delle Regole Tecniche, L'Ente ha ritenuto opportuno mantenere i documenti già conservati secondo le Regole CNIPA 2004 nel Sistema CNIPA 2004 e di mantenerli invariati fino al termine di scadenza di conservazione dei documenti in esso contenuti.

In conformità all'art. 14 co. 2 delle Regole Tecniche, i Servizi documentali InfoCamere migreranno la procedura di versamento dal Sistema CNIPA 2004 al Sistema AgID 2013 entro aprile 2017. Il piano di migrazione viene definito in concerto con InfoCamere, che comunicherà all'Ente produttore le migrazioni dei Servizi documentali con un anticipo di almeno 10 giorni lavorativi. L'attuazione del piano di migrazione non comporterà interruzioni nell'erogazione del servizio.

6 Oggetti sottoposti a conservazione

Gli oggetti sottoposti a conservazione ricomprendono tutti i documenti informatici prodotti dall'Ente produttore secondo le indicazioni previste nel manuale di gestione dei documenti dell'ente, per legge o dalla prassi archivistica. La lista delle tipologie degli oggetti conservati e dei tempi di conservazione è presente nell'allegato 1 "Tempi di conservazione, classi di contenuto, formati e visualizzatori".

I documenti informatici devono essere statici, in particolare non devono contenere elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione

Il servizio di conservazione permette la conservazione di file PDF e XML firmati digitalmente e marcati temporalmente, supportando i seguenti standard: P7M (CAdES), PAdES (per i file PDF), M7M, TSD. I Servizi documentali InfoCamere garantiscono la validità dei documenti sottoscritti digitalmente e la marcatura temporale, la cui validità pertanto non viene verificata dal sistema di conservazione.

I documenti conservati dall'Ente produttore non vengono cifrati.

6.1 Formati

Le tipologie di formato adottate e gestite dall'Ente produttore ed inviate in conservazione sono dettagliate nell'allegato 1 "Tempi di conservazione, classi di contenuto, formati e visualizzatori".

Il Servizio di conservazione InfoCamere garantisce la conservazione a norma solo dei formati ritenuti idonei alla conservazione, presenti nell'allegato 2 delle Regole Tecniche.

L'Ente produttore ha adottato i formati idonei alla conservazione presenti nell'allegato 2 delle Regole tecniche in quanto questi forniscono le caratteristiche di apertura, sicurezza, portabilità, funzionalità, diffusione, leggibilità nel tempo e supporto allo sviluppo.

In casi eccezionali, l'Ente produttore utilizza formati non presenti in tale lista in virtù di considerazioni sui:

- vincoli tecnici;
- specificità del formato;
- durata della conservazione richiesta dalle tipologia documentale .

Per questi formati, l'Ente produttore fornirà ad InfoCamere il relativo visualizzatore, nel rispetto dei diritti di proprietà intellettuale ed eventuali restrizioni nell'utilizzo del software.

6.2 Classe di contenuto

Vengono approvate le modalità di conservazione dei documenti descritte nel manuale di conservazione InfoCamere secondo la logica archivistica di 'unità documentarie' e 'unità archivistiche'.

Con classe di contenuto si intende l'insiemi di dati (metadati) da associare alla 'unità documentarie' e alla 'unità archivistiche' per identificarle e descriverne il contesto, il contenuto, la struttura. Tali informazioni sono presenti nei pacchetti di versamento, archiviazione e distribuzione del sistema di conservazione.

La lista delle tipologie degli oggetti conservati e dei tempi di conservazione è presente nell'allegato 1 "Tempi di conservazione, classi di contenuto, formati e visualizzatori".

Sono aggiornate in funzione del piano di migrazione dal sistema CNIPA 2004 al sistema AgID 2013 e da eventuali nuove classi di contenuto legate all'utilizzo dei Servizi documentali InfoCamere.

7 Il processo di conservazione

I principali processi del servizio di conservazione sono:

- conservazione;
- esibizione;
- produzione di duplicati e copie informatiche;
- procedura di scarto.

7.1 Conservazione

Il processo di conservazione opera secondo le seguenti fasi:

- Formazione e trasmissione del pacchetto di versamento da parte dell'Ente produttore;
- Presa in carico del pacchetto di versamento da parte del sistema di conservazione;
- Indicizzazione e generazione del pacchetto di archiviazione.

Di seguito, si riportano i dettagli delle suddette fasi.

7.1.1 Formazione e Trasmissione del Pacchetto di Versamento

L'Ente produttore produce i pacchetti di versamento attraverso i Servizi documentali InfoCamere e li invia al sistema di conservazione. I pacchetti di versamento contengono un'unità archivistica o una unità documentaria e rispettano quanto previsto nel Manuale della conservazione di InfoCamere.

7.1.2 Presa in carico del Pacchetto di Versamento da parte del sistema di conservazione

Il sistema di conservazione effettua il controllo del pacchetto di versamento ricevuto. La lista dei controlli automatici effettuati sul pacchetto di versamento è presente nel manuale di conservazione di InfoCamere e nelle specifiche tecniche allegate alla convenzione per l'affidamento del servizio.

Nel caso in cui l'insieme dei controlli abbia avuto esito negativo, il sistema di conservazione comunica al Servizio documentale InfoCamere l'errore riscontrato.

Nel caso in cui l'insieme dei controlli abbia avuto esito positivo, il sistema di conservazione genera un rapporto di versamento verso il Servizio documentale InfoCamere e il pacchetto è preso in carico dal sistema.

7.1.3 Indicizzazione e generazione del pacchetto di archiviazione

L'indicizzazione dei contenuti e la generazione del pacchetto di archiviazione viene descritta nel Manuale della conservazione di InfoCamere.

7.2 Esibizione

L'esibizione dei documenti conservati dal sistema di conservazione avviene tramite l'apposita applicazione web di esibizione dei documenti conservati integrata con i Servizi documentali InfoCamere. L'esibizione di un documento tramite tale funzione è permesso agli operatori dell'Ente produttore abilitati nel Servizio documentale alla gestione/trattamento del documento.

In caso di richiesta di esibizione a norma di documenti conservati, da parte di un utente esterno all'Ente produttore o interno non abilitato alla generazione di pacchetti di distribuzione, è in carico al Responsabile della conservazione:

- valutare la richiesta e generare i pacchetti di distribuzione in base a quanto richiesto, accedendo direttamente al sistema o delegando la generazione dei pacchetti ad utenti dell'Ente produttore abilitati;
- mettere a disposizione il contenuto dei pacchetti di distribuzione al richiedente

7.3 Produzione di duplicati informatici

La produzione di duplicati è realizzata tale l'apposita applicazione web di esibizione dei documenti conservati che forniscono i pacchetti di distribuzione.

7.4 Produzione di copie informatiche

E' in carico all'Ente Produttore:

- valutare i casi in cui sia richiesto produrre copie conformi;
- produrre le copie e richiedere, quando necessario, la presenza di un pubblico ufficiale. L'attestazione di conformità, anche nel caso sia necessario un cambio di formato, rimarrà a carico dell'Ente Produttore.

Il sistema di conservazione prevede appositi metadati per il tracciamento delle operazioni di versamento di copie informatiche che permettono di memorizzare il legame tra le diverse versioni delle unità documentarie.

7.5 Scarto dei pacchetti di archiviazione

Il Responsabile della gestione documentale, d'intesa con il Responsabile della conservazione, esegue la procedura di scarto dei documenti e dei fascicoli contenuti nei pacchetti di archiviazione alla scadenza dei termini di conservazione previsti, secondo quanto indicato nel piano di conservazione del manuale di gestione dell'ente, dalla normativa vigente o dalla prassi archivistica.

Nel rispetto del Decreto 42/2004, è in carico all'Responsabile della gestione documentale fornire all'autorità di vigilanza competente la lista dei contenuti da scartare. Il Responsabile della gestione documentale, una volta ricevuto il nulla-osta provvede ad adeguare, se necessario, l'elenco di scarto e le sue modalità alle decisioni dell'autorità.

Il Responsabile della gestione documentale fornirà al Sistema di conservazione la lista degli identificativi dei contenuti da scartare; potrà allegare alla richiesta di scarto anche il file di autorizzazione allo scarto rilasciata dall'autorità di vigilanza, che in questo modo verrà conservato dal sistema di conservazione.

7.6 Verifiche d'integrità

L'Ente produttore affida al Soggetto Conservatore il compito di verificare periodicamente l'integrità degli archivi. Il Responsabile della conservazione può richiedere via PEC al Soggetto Conservatore l'evidenza dei controlli eseguiti.

7.7 Recesso

Nel caso l'Ente produttore intenda recedere dalla convenzione per l'affidamento del servizio, il Responsabile della conservazione ha il compito di comunicarlo alla PEC del Soggetto Conservatore.

Il Responsabile della conservazione o un suo delegato, ha il compito di scaricare i pacchetti di archiviazione, entro i termini previsti dalla convenzione per l'affidamento del servizio.

8 Piano della sicurezza del sistema di conservazione

In accordo con l'Art 12 delle Regole Tecniche il responsabile della conservazione, di concerto con il responsabile della sicurezza, provvede a predisporre, nell'ambito del piano generale della sicurezza, **il piano della sicurezza del sistema di conservazione**, nel rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del Decreto legislativo 30 giugno 2003, n. 196 e dal disciplinare tecnico di cui all'allegato B del medesimo decreto, nonché in coerenza con quanto previsto dagli articoli 50 - bis e 51 del Codice e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale.

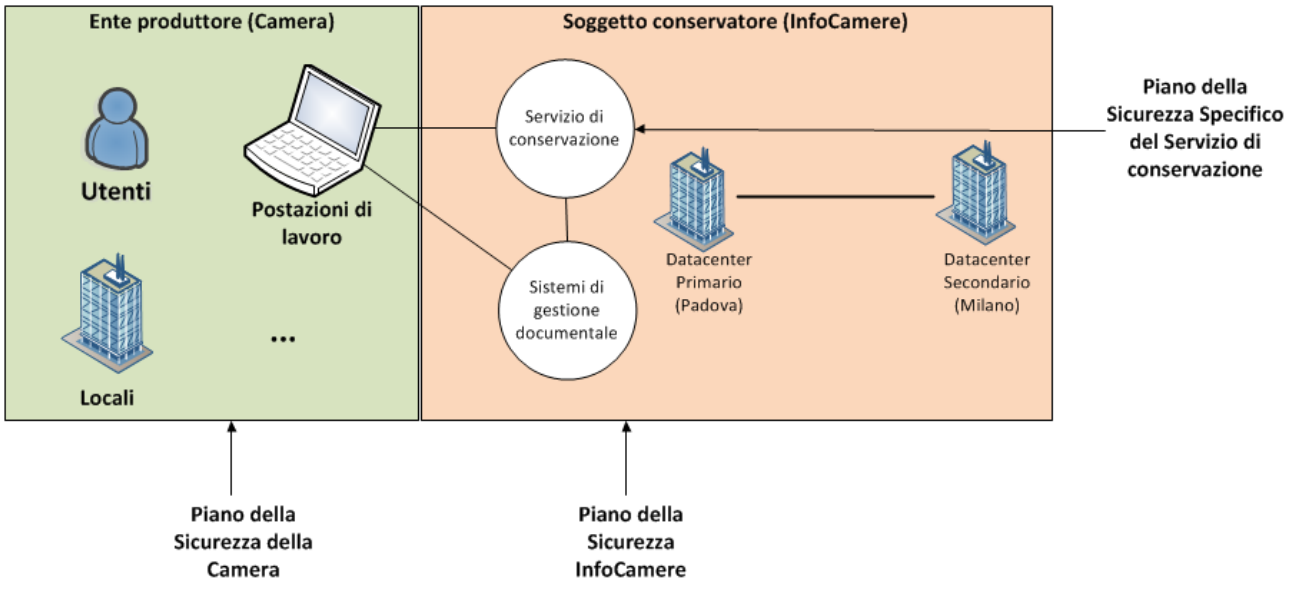
8.1 Finalità

Il piano di sicurezza del sistema di conservazione garantisce che:

- i documenti e le informazioni trattati dal Sistema di Conservazione siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari 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.

8.2 Organizzazione delle responsabilità

La sicurezza complessiva del sistema di conservazione è garantita dall'insieme delle misure di sicurezza adottate dall'Ente produttore e dal Soggetto conservatore, per i propri ambiti di responsabilità, come sintetizzato dallo schema seguente:



Il Soggetto conservatore definisce ed attua idonee misure di sicurezza riguardanti l'erogazione del Servizio di conservazione. L'affidamento del servizio ad InfoCamere, quale Soggetto conservatore accreditato, garantisce inoltre che il Sistema di conservazione:

- rispetti i requisiti previsti dallo standard di Sicurezza delle Informazioni ISO27001:2013, inclusi i controlli applicabili descritti nello standard ISO27002:2013;
- sia conforme alla legislazione vigente applicabile, includendo, in particolare, il D.Lgs. 196/03 e il disciplinare tecnico di cui all'allegato B del medesimo decreto;

- rispetti i Requisiti di Qualità e Sicurezza stabiliti da AgID per i Soggetti conservatori accreditati;
- sia dotato di un Piano di Sicurezza per il sistema di conservazione, periodicamente aggiornato.

Il Soggetto conservatore si impegna a segnalare all'Ente produttore eventuali modifiche significative alle proprie politiche di sicurezza.

L'Ente produttore definisce ed attua idonee misure di sicurezza riguardanti i propri ambiti di responsabilità, in particolare:

- I propri locali e la Continuità Operativa dell'Ente produttore in caso di disastro (vedi 8.1.2 e 8.1.9)
- Le postazioni di lavoro utilizzate dal personale dell'Ente produttore per la gestione dei documenti informatici (vedi 8.1.3-8)
- La formazione e i comportamenti del personale dell'Ente produttore (vedi 8.1.1)

8.3 Misure di sicurezza dell'Ente produttore

L'Ente produttore prevede misure atte a garantire la sicurezza del Sistema di Conservazione nell'ambito della sicurezza generale dei propri processi e flussi di lavoro.

Le misure di sicurezza sono definite nel piano di Sicurezza dei documenti informatici dell'Ente e sono comunicate a tutto il personale dell'Ente e terze parti interessate; tali misure stabiliscono le seguenti regole da rispettare.

8.3.1 Formazione del personale

Con riferimento ai piani di Formazione del personale dell'Ente produttore, per il personale coinvolto nella conservazione, l'Ente garantisce che:

- le iniziative di formazione/aggiornamento sono finalizzate al mantenimento e sviluppo del patrimonio delle conoscenze dell'Ente in un'ottica di formazione continua e in grado di recepire le esigenze formative e le evoluzioni normative, istituzionali e tecnologiche;
- la formazione di ogni persona avvenga sulla base di una pianificazione che considera il percorso formativo seguito, la figura professionale di appartenenza e quindi le attività che la persona svolge o dovrà svolgere, oltreché delle competenze e potenzialità espresse.

8.3.2 Controllo degli accessi fisici

Il controllo degli accessi fisici si applica alle sedi e ai locali dove sono effettuati trattamenti inerenti il Servizio di conservazione; pertanto l'accesso alle sedi e ai locali dell'Ente produttore è regolamentato e controllato.

8.3.3 Sistema antincendio

Tutti gli edifici dell'ente sono protetti da mezzi antincendio mobili azionabili manualmente dal personale camerale operante in ciascuna sede, appositamente incaricato, addetto alla gestione dell'emergenza ed al primo soccorso (ai sensi del D. Lgs. n. 81/2008).

8.3.4 Misure Logiche

Le misure di sicurezza logiche riguardano i criteri che devono essere seguiti dai diversi programmi

software, di sistema o applicativi, per controllare (vale a dire selezionare e/o limitare) l'accesso degli utilizzatori alla rete locale, alle interconnessioni esterne internet, ai server dati ed applicativi e alle funzionalità applicative.

8.3.5 Controllo accesso ai sistemi di elaborazione

L'accesso diretto agli elaboratori e ai server di rete locale è consentito esclusivamente all'Amministratore di sistema o ai suoi incaricati.

L'accesso alle risorse informatiche, locali o di rete, avviene attraverso uno specifico profilo di abilitazione. Tale profilo definisce, per ogni soggetto associato (qualsiasi utente del sistema informatico, interno o esterno), le funzionalità disponibili ed in particolare le seguenti tipologie di abilitazioni di accesso:

- accesso locale alle stazioni di lavoro
- accesso alla rete locale tramite la stazione di lavoro
- accesso ai trattamenti e/o gli archivi presenti sui server della rete locale per cui viene data abilitazione con specifici diritti (sola lettura, modifica, ecc..)
- accesso alle applicazioni presenti sui server dell'intranet per cui viene data abilitazione con le relative funzionalità applicative abilitate
- la possibilità di interconnessione con la rete del sistema dell'ente ovvero con reti esterne, in particolare Internet.

Non è consentito alle singole stazioni di lavoro condividere archivi senza il consenso dell'Amministratore di sistema. Gli aspetti di sicurezza circa l'accessibilità ed integrità degli archivi locali sono a carico del titolare della stazione di lavoro, il quale, per il suo corretto utilizzo, dovrà attenersi alle specifiche direttive predisposte dall'Amministratore di sistema.

Il sistema di controllo accessi delle stazioni di lavoro garantisce:

- l'accesso agli archivi eventualmente presenti sulle stazioni di lavoro esclusivamente ai soggetti identificati dal titolare dell'archivio stesso;
- l'accesso alla rete esclusivamente ai soggetti autorizzati ed attraverso la o le stazioni di lavoro cui lo stesso è abilitato;
- l'accesso agli archivi ed alle applicazioni presenti sui server locali esclusivamente ai soggetti abilitati e per le funzionalità autorizzate;
- L'accesso agli archivi/servizi di InfoCamere e di interconnessione con reti esterne esclusivamente ai soggetti autorizzati.

8.3.6 Identificazione ed Autenticazione degli utenti

Ogni utilizzatore del sistema informatico dell'Ente è identificato mediante un codice personale userid (dato pubblico) e una password (dato privato), assegnati e gestibili dall'Amministratore di sistema, che permettono l'accesso alle stazioni di lavoro ed alla rete locale secondo i diversi profili di abilitazione.

Userid

La userid ha una composizione standardizzata per tutti gli utenti del sistema. Lo stesso codice non può, neppure in tempi diversi, essere assegnato a persone diverse. Ad ogni codice è possibile associare uno o più profili di abilitazione.

Password

Ad ogni userid è associata una password. Al primo utilizzo, l'incaricato del trattamento ha l'obbligo di modificarla tenendo presenti le direttive dell'Amministratore di sistema e le seguenti regole:

- deve essere alfanumerica, di non meno di 8 caratteri di cui almeno 1 numerico
- non deve essere composta utilizzando la userid
- non deve essere ottenuta anagrammando la precedente
- deve essere sostituita almeno ogni 6 mesi (3 mesi nel caso di trattamenti di dati

sensibili) dall'incaricato al trattamento stesso.

Ogni incaricato, in base al proprio profilo di abilitazione, accede alle postazioni di lavoro di riferimento e alle applicazioni di rete, sia internet sia intranet, tramite la sua userid.

8.3.7 Gestione delle credenziali di accesso

Assegnazione, riesame e revoca degli accessi degli utenti

- L'accesso alle informazioni e funzioni di sistemi applicativi deve essere limitato alle effettive necessità lavorative.
- A fronte della cessazione verranno disattivati gli identificativi di accesso del personale non più in servizio e dei soggetti esterni non più operativi.
- Nessun identificativo di accesso dovrà essere cancellato ma dovranno essere eliminate le abilitazioni.
- Gli identificativi utente assegnati una volta non potranno più essere assegnati successivamente a persone diverse.
- A fronte della definizione di nuove credenziali di accesso / modifica delle esistenti, viene inviata una notifica all'interessato; egli accede al sistema informativo aziendale nel quale consulta le credenziali assegnate e registra la propria accettazione.

L'attuazione del processo organizzativo è di responsabilità delle figure designate dall'Ente; le relative richieste sono effettuate a InfoCamere che provvedono, tramite gli opportuni strumenti tecnici, a soddisfarle e a fornire il relativo riscontro ai richiedenti.

8.3.8 Utilizzo delle password

- L'utilizzo e la gestione delle credenziali deve garantire di evitare utilizzi impropri delle password e delle credenziali di autenticazione.
- Le regole relative alla costruzione ed utilizzo delle password si applicano a tutto il personale e terze parti che ne fanno uso per accedere agli asset dell'Ente.
- L'utilizzo delle password ed in genere delle credenziali utente deve essere controllato con un processo di gestione formale, anche automatizzato, fin ove possibile.
- Le credenziali sono personali e non cedibili, devono essere assegnate in base alla necessità di accedere ai dati o ai sistemi dell'Ente e devono essere gestite contemporaneamente alle abilitazioni, sulla base del principio del "minimo privilegio".
- Le password devono essere 'robuste', ovvero costruite in modo da non essere facilmente 'indovinabili' (password guessing) e custodite con cura, nonché variate periodicamente.
- Analoghe regole valgono per i cosiddetti PIN dei dispositivi con a bordo certificati digitali. (smart card etc.).

8.3.9 Responsabilità degli utenti

Le credenziali sono personali e non cedibili.

Ogni utente è responsabile della corretta gestione della propria password, dei dispositivi di riconoscimento, delle informazioni per l'accesso ai sistemi e ai dati.

Le credenziali e i dispositivi di riconoscimento devono essere conservati adeguatamente e non essere mai lasciati incustoditi.

8.4 Politica di gestione delle postazioni di lavoro

L'utilizzo improprio di dispositivi rimovibili può aumentare il rischio di fuga di dati riservati dell'Ente; pertanto il personale:

- non deve consentire ad altro personale il collegamento di dispostivi rimovibili alla propria postazione
- non deve connettere alla propria postazione dispositivi rimovibili e lasciarli incustoditi
- non deve lasciare incustodito il dispositivo all'esterno del perimetro aziendale.

Il personale ha la responsabilità di non modificare le configurazioni standard (sia software che hardware) impostate al momento dell'installazione iniziale nelle postazioni di lavoro, dispositivi mobili o supporti rimovibili affidati in dotazione individuale, senza specifica autorizzazione delle funzioni di sicurezza.

8.4.1 contromisure per la protezione dal malware

- La strumentazione software per la protezione dal malware (c.d. antivirus) è installata su tutte gli apparati con sistema operativo Windows, siano essi server dedicati ad erogare servizi che postazioni di lavoro dalle quali si accede ai servizi; l'antivirus è installato sia sui sistemi fisici (server, personal computer) che virtuali utilizzati dall'Ente.
- Nei sistemi "endpoint" su cui è installato, l'antivirus è sempre attivo e la scansione opera in tempo reale su ogni movimentazione di file, proteggendo così l'apparato dal malware.
- Le componenti sopra descritte sono periodicamente aggiornate per assicurare adeguate misure di protezione.

8.4.2 contromisure per la protezione dallo spamming

I sistemi che gestiscono la posta elettronica utilizzano una strumentazione software per la protezione dallo spamming; le finalità della strumentazione sono:

- controllare le informazioni di provenienza dei messaggi
- a seconda della correttezza di tali informazioni, eliminare, inserire in quarantena o consegnare i messaggi al destinatario
- eliminare dai messaggi ricevuti eventuali programmi eseguibili in essi contenuti
- inviare ai destinatari l'elenco dei messaggi inseriti in quarantena.

Il personale dell'Ente, qualora ritenga che un messaggio ricevuto sia indesiderato, lo può inviare al sistema che aumenta così la base di conoscenza per l'individuazione dello spamming.

Le componenti sopra descritte sono periodicamente aggiornate per assicurare adeguate misure di protezione.

8.5 Scrivania e schermo puliti

Le regole di "scrivania pulita" e "schermo pulito" sono essenziali per proteggere tutti gli apparati di elaborazione delle informazioni sia in utilizzo individuale (postazioni di lavoro) sia condiviso (console di sistemi di controllo, server, cartelle di rete, etc.).

Le regole devono essere rispettate dal personale dell'Ente, dai fornitori e dalle terze parti.

8.5.1 scrivania pulita

Al termine del lavoro o durante lunghe pause, sulle scrivanie non deve essere lasciata alcuna documentazione riservata cartacea o su supporti rimovibili.

8.5.2 schermo pulito

Non lasciare accessibile la postazione di lavoro durante la propria assenza: bloccarla, prevedendo lo sblocco con password e attivare comunque un "savescreen" automatico protetto da password che pulisca la videata entro alcuni minuti in caso di inutilizzo.

Sullo schermo della postazione, anche durante lo svolgimento della propria attività non devono essere facilmente visibili o accessibili informazioni riservate inutili per la corrente sessione di lavoro (ad esempio: lasciare aperto inutilmente un documento contenente informazioni sensibili, che possono essere inopportunamente lette da terzi durante o alla ripresa della sessione).

8.6 Ripristino del servizio e continuità operativa

In attuazione delle disposizioni di cui all'art. 50 bis del CAD, l'Ente produttore assicura, per quanto di sua competenza, la continuità operativa del Sistema di Conservazione, nell'ambito del proprio Piano di Continuità Operativa; analogamente per quanto attiene al Piano di Disaster Recovery.

Allegato 1 – Tempi di conservazione, classi di contenuto, formati e visualizzatori