Originale

Comune di Vigonovo

CITTÀ METROPOLITANA DI VENEZIA

DELIBERAZIONE DELLA GIUNTA COMUNALE N.26

OGGETTO:

Aggiornamento del Manuale della conservazione dei documenti amministrativi informatici - ex art.34 comma 1 bis C.A.D. Approvazione

L'anno duemilaventicinque addì cinque del mese di marzo alle ore dodici e minuti zero nella sala delle adunanze, previa l'osservanza di tutte le formalità prescritte dalla vigente normativa, vennero per oggi convocati i componenti di questa Giunta Comunale, nelle persone dei Signori:

Cognome e Nome	Presente
1. Martello Luca - Sindaco	Sì
2. Sattin Luisa - Vice Sindaco	Sì
3. Danieletto Andrea - Assessore	Sì
4. Dorio Sabrina - Assessore	Sì
5. Cacco Eros - Assessore	Sì
Totale Presenti:	5
Totale Assenti:	0

Con l'intervento e l'opera del Segretario Comunale Signor Piras Guido il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti il Sig. Martello Luca assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

PROPOSTA DI DELIBERA

PREMESSO che:

- Il percorso normativo tracciato dal legislatore nel corso degli ultimi anni in materia di semplificazione e innovazione dei procedimenti amministrativi riconosce alla dematerializzazione documentale un ruolo di primo piano e in tale contesto la conservazione dei documenti nativi digitali e/o digitalizzati diviene fattore imprescindibile per la sostenibilità del processo di materializzazione stesso;
- È fondamentale garantire la conservazione documentale nel lungo periodo così come avviene tradizionalmente per i documenti analogici;
- l'attività volta a proteggere nel tempo gli archivi di documenti informatici e i dati ad essi correlati ha l'obiettivo di impedire la perdita o la distruzione dei documenti e di garantirne autenticità, integrità e accesso controllato ai fini amministrativi e di ricerca;
- sussiste la necessità di definizione di regole, procedure, tecnologie e modelli organizzativi da adottare per la gestione di tali processi, con indicazioni di dettaglio;
- in particolare, le regole tecniche, prendono in considerazione l'intero "ciclo di vita" del documento, dalla formazione alla conservazione nell'ambito di un archivio digitale;
- le regole tecniche per la conservazione dei documenti informatici, adottate con Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, apportando modifiche alla deliberazione CNIPA n. 11/2004, ampliano il concetto di memorizzazione dei documenti informatici introducendo il concetto di "Sistema di conservazione";
- per l'entrata in vigore delle sopracitate regole tecniche, per ogni Pubblica Amministrazione è divenuta obbligatoria l'adozione del Manuale della Conservazione, oggetto del presente documento;

DATO ATTO che il manuale, come previsto dall'art. 7, comma 1, lettera *m* e dall'art. 8 del DPCM 3 dicembre 2013, è uno strumento operativo che descrive e disciplina il modello organizzativo della conservazione adottato e illustra nel dettaglio l'organizzazione del processo di conservazione per l'Ente , definendo i soggetti coinvolti, i ruoli svolti dagli stessi, il modello organizzativo di funzionamento dell'attività di conservazione la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate, ogni altra informazione utile alla gestione ed alla verifica del funzionamento nel tempo del sistema di conservazione;

RICHIAMATO il "Manuale di conservazione" approvato dall'Amministrazione con deliberazione di Giunta Comunale n. 134 del 29.11.2016;

RICHIAMATE le linee guida Agid del 11.9.2020 e suoi allegati *Linee-guida sulla formazione, gestione e conservazione dei documenti informatici*" e in particolare il punto 4.6 che testualmente recita: «*Il manuale di conservazione è un documento informatico che deve illustrare 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. In caso di affidamento del servizio di conservazione ad un conservatore esterno, le Pubbliche Amministrazioni possono descrivere nel proprio manuale anche le*

attività del processo di conservazione affidate al conservatore, in conformità con il contenuto del manuale di conservazione predisposto da quest'ultimo, o rinviare, per le parti di competenza, al manuale del conservatore esterno. Resta fermo l'obbligo in carico alla Pubblica Amministrazione di individuare e pubblicare i tempi di versamento, le tipologie documentali trattate, i metadati, le modalità di trasmissione dei PdV e le tempistiche di selezione e scarto dei propri documenti informatici."

RILEVATO che le Pubbliche Amministrazioni sono tenute a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di conservazione;

RICORDATO che il Comune di Vigonovo è il "soggetto produttore" che intende sottoporre a conservazione digitale fascicoli, serie e aggregazioni documentali, e che il processo di conservazione è stato affidato alla ditta INFOCERT SpA, nel rispetto di quanto previsto dall'art. 34 comma 1 bis del CAD come modificato dal Decreto Semplificazioni D.L. 76/2020, in materia di conservazione dei documenti informatici;

VISTO il D.Lgs. n. 82/2005 e successive modificazioni e integrazioni (Codice dell'amministrazione digitale), che agli art. 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1 disciplina il sistema di conservazione dei documenti informatici;

DATO ATTO che il Responsabile della Conservazione ha predisposto l'aggiornamento del Manuale di conservazione nel testo allegato al presente atto come parte integrante e sostanziale, d'intesa con il Responsabile per la Transizione al Digitale e con il supporto della ditta affidataria del servizio esterno di conservazione;

RITENUTO di procedere alla sua approvazione nel rispetto di quanto previsto dalle Linee Guida AGID;

DATO ATTO che si conferma la modalità di conservazione dei documenti informatici del Comune di Vigonovo a soggetto terzo certificato e già contrattualizzata con la ditta Infocert SpA – nel rispetto di quanto previsto dall'art. 34 comma 1 bis del CAD come modificato dal Decreto Semplificazioni D.L. 76/2020 e della disciplina europea

VISTI:

a) la Legge 241/1990, *Nuove norme sul procedimento amministrativo*;
b) il DPR 445/2000, *Testo unico delle disposizioni legislative e regolamentari in materiadi documentazione amministrativa*;
c) il D.lgs 196/2003 *recante il Codice in materia di protezione dei dati personali*;
d) la Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106, *Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici;*
e) il D.lgs 82/2005 e ss.mm.ii., *Codice dell'amministrazione digitale*;
f) il D.lgs 33/2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*;
g) il DPCM 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, comma 3, lettera b), 35, comma 2, 36,comma 2, e 71;

h) il DPCM 21 marzo 2013, *Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*;
i) il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
j) il DPCM 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione".
k) la Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, *Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui alDPCM 13.12.2013*;
l) il Reg. UE 679/2016 (GDPR), *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*;
m) la Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale*, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni*;
n) la Circolare n. 2 del 9 aprile 2018, *recante i criteri per la qualificazione dei Cloud Service Provider per la PA;*
o) la Circolare n. 3 del 9 aprile 2018, *recante i criteri per la qualificazione di serviziSaaS per il Cloud della PA*;
p) gli artt. 48 e 134 del D.Lgs. 18 Agosto 2000, n. 267;
q) Il Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici, che definisce i nuovi criteri per la fornitura di tali servizi e adottato con Determinazione n. 455/2021, è entrato in vigore il 1° gennaio 2022.

CONSIDERATO che, come precisato dal Consiglio di Stato - nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, n. 2122/2017 del 10.10.2017 - le Linee Guida adottate da AGID, ai sensi dell'art. 71 del CAD, hanno carattere vincolante e assumono valenza *erga omnes*;

DATO ATTO che il presente provvedimento non rileva ai fini contabili;

SI PROPONE

1. La premessa forma parte integrante e sostanziale del presente provvedimento e ne costituisce motivazione ai sensi dell'art. 3, comma 1, della Legge 241/90 e s.m.i.;

2. di approvare, per i motivi esposti in premessa, l'aggiornamento del "Manuale di conservazione documentale" del Comune di Vigonovo allegato al presente provvedimento, del quale costituisce parte integrante e sostanziale;

3. di pubblicare, il Manuale Sul sito web istituzionale dell'Ente, nell'apposita sezione Amministrazione Trasparente prevista dall'art. 9 del d.lgs. 33/2013;

4. di dare mandato alla Responsabile dell'Area Amministrativa, Affari Generali e P.I., di procedere alla comunicazione a tutto il personale dipendente interessato all'applicazione del presente manuale nel rispetto delle normative vigenti in materia e di assegnare ai Responsabile di Posizione Organizzativa il ruolo di coordinatore e garante, per il proprio settore, della corretta applicazione del documento allegato;

5. di dare atto che sul presente provvedimento non sussiste situazione di conflitto di interessi, ai sensi del combinato disposto di cui agli art. 6 bis della L. n. 241/1990 e art. 7 del D.P.R. n. 62/2013 in capo al soggetto che ha istruito il provvedimento e sottoscritto il parere di cui all'art. 49 del T.U.E.L;

6. di dare atto che ai sensi del D. Lgs. 14.03.2013 n. 33 si provvederà alla pubblicazione del presente provvedimento all'Albo Pretorio on-line del Comune di Vigonovo ed al suo inserimento nella sezione "Amministrazione Trasparente – Provvedimenti – Provvedimenti organi di indirizzo politico – Delibere di Giunta Comunale" del sito istituzionale dell'Ente;

7. di dichiarare, con votazione unanime e separatamente resa, per rendere operativo e vigente il presente manuale, la presente deliberazione immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D.Lgs. 18 Agosto 2000, n. 267.

LA GIUNTA COMUNALE

VISTA la suestesa proposta di deliberazione ad oggetto:
Aggiornamento del Manuale della conservazione dei documenti amministrativi informatici - ex art.34 comma 1 bis C.A.D. Approvazione

PRESO ATTO dell'allegato parere favorevole, espresso dal funzionario incaricato ex art. 49, I° comma, D.Lgs. 18/8/2000, n. 267, così come modificato dall'art. 3, comma I, lett. b) del D.L. 10 Ottobre 2012, n. 174, convertito con modificazioni nella Legge 7.12.2012, n. 213:

Parere	Esito	Data	Il Responsabile
PARERE TECNICO	Favorevole	04/03/2025	F.to: BARZON SILVIA

RITENUTA la proposta meritevole di approvazione;

Con voti favorevoli unanimi espressi nei modi e forme di legge;

DELIBERA

Di approvare la suestesa proposta di delibera relativa all'argomento in oggetto.

Quindi, stante l'urgenza di provvedere come motivata nella proposta, con successiva e separata votazione favorevole unanime, di dichiarare il presente atto immediatamente eseguibile ai sensi e per gli effetti di cui all'art. 134, comma 4, del D.Lgs. n. 267/2000.

Letto, confermato e sottoscritto

Il Sindaco	Il Segretario Comunale
Firmato digitalmente	Firmato digitalmente
Martello Luca	Piras Guido

Manuale della Conservazione
Del COMUNE DI VIGONOVO

SOMMARIO

ALLEGATI:

Manuale di Conservazione di Infocert SpA (versione 13/agosto 2024)
Configurazione ambiente di produzione

N° versione	Data emissione	Modifiche apportate
01	Novembre 2016	Prima versione
02	Febbraio 2025	Aggiornamento

© InfoCert S.p.A. – All right reserved

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il manuale della conservazione del Comune di Vigonovo, ai sensi delle **Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici**, ai sensi del **Codice dell'Amministrazione Digitale** (articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1), di cui al decreto legislativo n. 82 del 2005 (pubblicato in GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20) e del Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014.

Il manuale della conservazione 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.

Nel dettaglio, deve riportare:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
c) la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
i) la descrizione delle procedure per la produzione di duplicati o copie;
j) i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate, qualora, nel caso delle Pubbliche

© InfoCert S.p.A. – All right reserved

Amministrazioni, non siano già indicati nel piano di conservazione allegato al manuale di gestione documentale;

k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
l) le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

In caso di ispezione da parte delle autorità di vigilanza preposte, il manuale della conservazione permette un agevole svolgimento di tutte le attività di controllo.

© InfoCert S.p.A. – All right reserved

2. TERMINOLOGIA

TERMINE	DEFINIZIONE
ACCESSO	Operazione che consente di prendere visione dei documenti informatici.
AFFIDABILITÀ	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
ARCHIVIO	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
AUTENTICITÀ	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto, un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
CERTIFICAZIONE	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
CONSERVATORE	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
CONSERVAZIONE	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
DOCUMENTO ELETTRONICO	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
DOCUMENTO INFORMATICO	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
ESIBIZIONE	operazione che consente di visualizzare un documento conservato
FILE	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
FORMATO DEL DOCUMENTO INFORMATICO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
FORMATO "DEPRECATO"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.

© InfoCert S.p.A. – All right reserved

TERMINE	DEFINIZIONE
IDENTIFICATIVO UNIVOCO	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
IMPRONTA CRITTOGRAFICA	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.
INTEGRITÀ	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
INTEROPERABILITÀ	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
LEGGIBILITÀ	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
METADATI	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
PACCHETTO DI ARCHIVIAZIONE	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
PACCHETTO DI DISTRIBUZIONE	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
PACCHETTO DI VERSAMENTO	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
PACCHETTO INFORMATIVO	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
PRESA IN CARICO	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
PROCESSO	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.

© InfoCert S.p.A. – All right reserved

TERMINE	DEFINIZIONE
RAPPORTO DI VERSAMENTO	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLA CONSERVAZIONE	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
RIFERIMENTO TEMPORALE	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
RIVERSAMENTO	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
SCARTO	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
SISTEMA DI CONSERVAZIONE	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
TITOLARE DELL'OGGETTO DI CONSERVAZIONE	Soggetto produttore degli oggetti di conservazione.
UTENTE ABILITATO	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.
VERSAMENTO	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

3. NORMATIVA DI RIFERIMENTO

L'archivio è il complesso dei documenti (analogici e digitali) prodotti o comunque acquisiti da un ente, una persona, una famiglia, durante lo svolgimento della propria attività. I documenti che compongono l'archivio sono pertanto collegati tra loro da un nesso logico e necessario

© InfoCert S.p.A. – All right reserved

detto 'vincolo archivistico' e per la disciplina archivistica l'unitarietà dell'archivio è garantita dalla sua gestione operativa in tre 'fasi di vita':

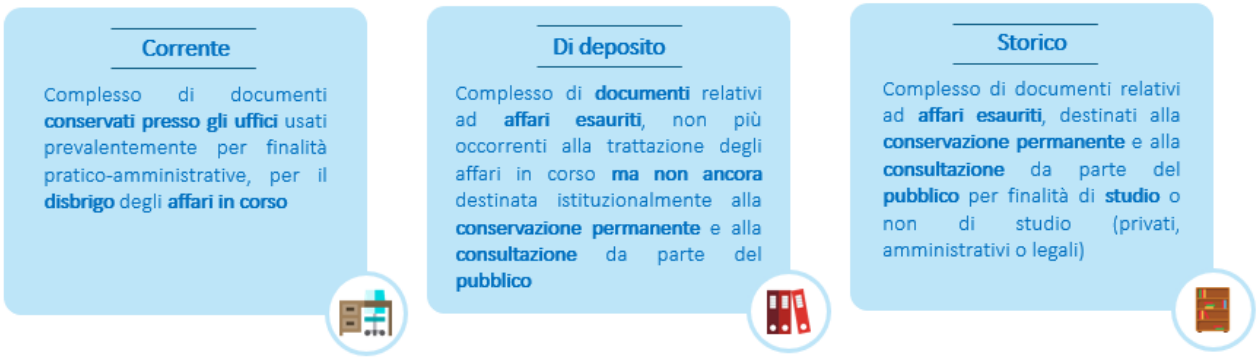

FIGURA 1 FASI D'ARCHIVIO

La **fase corrente** è oggi prevalentemente condotta mediante archiviazione digitale, cioè la memorizzazione di un documento su un Sistema di Gestione Documentale (nel quale possono confluire, ad esempio, le registrazioni effettuate negli applicativi di gestione della contabilità o nel sistema di protocollo informatico, ove presente) principalmente su server/repository o su altri supporti di memorizzazione. È l'archivio che è attualmente in uso ed è in continuo accrescimento. È un processo soggetto a obsolescenza nel tempo.

La **fase di deposito** vede la presenza di documenti ancora utili per finalità amministrative o giuridiche (ad esempio per accertamenti fiscali), ma non più indispensabili per il disbrigo degli affari in corso. Si tratta della fase intermedia del ciclo di vita degli archivi, tra quella dell'archivio corrente e quella dell'archivio storico. È una fase dinamica, di decantazione della documentazione archivistica, dove viene svolta una funzione di intermediazione prima di destinare la documentazione alla conservazione permanente.

Nelle Linee guida AgID viene sottolineato che il processo conservativo può essere avviato sia precocemente a partire dall'archivio corrente, che nella fase di archivio di deposito: in considerazione dei rischi dovuti all'obsolescenza tecnologica, viene previsto che il soggetto produttore dell'archivio possa "sulla base di specifiche esigenze" trasferire al sistema di conservazione anche i documenti relativi a fascicoli e serie ancora aperte, ribadendo quanto previsto dall'art. 44 comma 1 bis del CAD.

Il servizio di conservazione digitale a norma, di cui questo Manuale descrive il processo, risponde prevalentemente all'esigenza di assicurare l'efficacia probatoria dei documenti informatici, soprattutto quelli sottoscritti con firma digitale, in modo da estenderne l'efficacia oltre il periodo di validità tecnologica: è un servizio normato e qualificato, finalizzato al

© InfoCert S.p.A. – All right reserved

mantenimento nel tempo delle caratteristiche di integrità, immodificabilità, leggibilità e autenticità del documento, che può essere oggetto di esibizione a norma per permettere al giudice di valutarne il valore legale in sede di contenzioso.

Secondo il modello delle tre fasi di vita dell'archivio previsto dalla normativa italiana, si distinguono quindi le finalità di una conservazione a norma destinata principalmente a proteggere l'integrità e l'efficacia probatoria dei documenti e le finalità che devono guidare la conservazione illimitata a fini storici e di ricerca (**archivio storico**), dove prevale la dimensione storico-culturale della documentazione sebbene esse possa ancora essere utile a fini pratici.

Di seguito l'elenco dei **principali riferimenti normativi** in materia, ordinati secondo il criterio della gerarchia delle fonti:

- eIDAS (*electronic IDentification Authentication and Signature*) EU Regulation 910/2014 *of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market*, così come modificato dal Regolamento (UE) 2024/1183 del Parlamento Europeo e del Consiglio dell'11 aprile 2024.
- GDPR (*General Data Protection Regulation*) *EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*.
- 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;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss.mm.ii – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) – Codice dell'amministrazione digitale (CAD);

© InfoCert S.p.A. – All right reserved

- DPCM 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;
- DPCM 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 [parzialmente abrogate dalle Linee Guida AgID a partire da gennaio 2022];
- DPCM del 3 aprile 2013 n. 55, linee guida per la gestione dei processi di fatturazione elettronica verso la Pubblica Amministrazione.
- Decreto del Ministero dell'Economia e delle Finanze 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 del 2005;
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici di maggio 2021.
- Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici di dicembre 2021 (MarketPlace), composto di due allegati tecnici, emanato secondo quanto previsto dall'articolo 34, comma 1-bis del decreto legislativo n. 82/2005, come integrato e modificato dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020 e entrato in vigore il 1° gennaio 2022.

Si riportano di seguito gli **standard di riferimento**:

- UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

© InfoCert S.p.A. – All right reserved

4. RUOLI E RESPONSABILITÀ

Il Responsabile della Conservazione, come previsto dalla normativa vigente, definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

In particolare:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera e sottoscrive 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) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;

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) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;

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;

© InfoCert S.p.A. – All right reserved

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 le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate;

m) predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Responsabile della conservazione interno (Nome Cognome)	**Silvia Barzon**
Ruolo	Responsabile dell'Area Amministrativa, Affari Generali e P.I.
Data inizio incarico	2017
Data termine incarico	Fino a revoca/sostituzione/cessazione

Responsabile della conservazione vicario (Nome Cognome)	**Alessandro Rostellato**
Ruolo	Responsabile dell'Area Economico-finanziaria
Data inizio incarico	2019
Data termine incarico	Fino a revoca/sostituzione/cessazione

Referenti di processo interni	**Alessandro Rostellato** **Giuliana Tommasi**

© InfoCert S.p.A. – All right reserved

(Nome Cognome)	**Alessandro Francesco Villa** **Thomas Carraro** **Luca Meneghini** **Silvia Barzon**
Ruolo	**Funzionari responsabili di Area**
Durata incarico	**In vigenza di incarico a funzionario E.Q.**
Ruolo	**Coordinatori e garanti, ciascuno per il proprio settore, della corretta applicazione del documento**

Il Responsabile della Conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a un **Conservatore esterno**, presso cui è individuato un **Responsabile del servizio di conservazione**.

Il Comune di Vigonovo da ottobre 2023 ha rinnovato l'affidamento per lo svolgimento delle attività di conservazione al Conservatore Accreditato AgID:

denominazione sociale	InfoCert S.p.A.
sede legale:	Piazzale Flaminio 1/b, 00196 Roma
sedi operative:	Piazza da Porto, 3, 35131 - Padova Via Fernanda Wittgens, 6, 20123 – Milano Via Gian Domenico Romagnosi 4, 00196 Roma
telefono:	049.7849350
sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
codice fiscale / partita IVA	07945211006
numero REA	RM – 1064345

InfoCert, già Accreditata come Conservatore presso AgID, ha ottenuto dal 2019 la qualifica Cloud Marketplace (CSP Tipo B Infrastruttura e SaaS per il servizio LegalDoc), oggi di ACN, Agenzia per la Cybersicurezza Nazionale e da febbraio 2022 è inoltre iscritta nell'elenco del marketplace AgID dei servizi di conservazione.

© InfoCert S.p.A. – All right reserved

Il dettaglio delle attività delegate al Conservatore è riportato nelle "**Specificità del Contratto – Atto di Affidamento''**.

Il presente documento, quindi, integra e dettaglia il Manuale della Conservazione di InfoCert disponibile nella sezione "*Conservazione>Documentazione*" del sito web **infocert.it** (https://www.infocert.it/) e allegato al presente Manuale, nella versione 13/agosto 2024.

Più concretamente si rimanda al Manuale della Conservazione di InfoCert per i capitoli dedicati a:

- Ruoli di responsabilità del Conservatore
- Dettaglio tecnico del sistema di conservazione, dei controlli di versamento e trattamento dei pacchetti di archiviazione
- Monitoraggio e controlli periodici del Conservatore; verifiche di integrità e leggibilità.

© InfoCert S.p.A. – All right reserved

5. OGGETTI SOTTOPOSTI A CONSERVAZIONE

In generale si definisce '**pacchetto**' un contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.

Il concetto fondamentale è che il documento da conservare sia sempre accompagnato da dati che lo descrivano e ne consentano la gestione nel tempo.

Per "**pacchetto di versamento**" si intende l'insieme di documenti che il Comune di Vigonovo invia al sistema di conservazione in un'unica sessione. Al buon esito del versamento, il sistema di conservazione restituisce una Ricevuta di versamento.

Per "**pacchetto di archiviazione**" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, formato automaticamente dal sistema di conservazione e depositato nei data center InfoCert. Il pacchetto così formato, viene chiuso da un file XLM, detto Indice di Conservazione UNI SInCRO, firmato digitalmente e marcato temporalmente dal Responsabile del servizio di conservazione di InfoCert.

Per "**pacchetto di distribuzione**" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta, cioè dopo una ricerca, che porta all'esibizione del documento conservato.

Il fine ultimo del servizio è rendere i pacchetti di distribuzione sempre ricercabili, leggibili, integri, affidabili, autentici e fruibili dagli utenti della comunità di riferimento, attraverso la mediazione del soggetto produttore, in ottemperanza ai principali standard archivistici nazionali e internazionali.

© InfoCert S.p.A. – All right reserved

5.1 DETTAGLIO DELLE TIPOLOGIE DOCUMENTALI

Per il dettaglio delle tipologie documentali (tipologia, formati, metadati, periodo di conservazione, flussi informatici) si rinvia all'allegato 5 delle Linee Guida AgID, ed al "Manuale della Gestione del Protocollo Informatico, dei documenti e dell'archivio", approvato con deliberazione di G.C. n. 149 del 20.12.2016, e ss.mm.ii..

Dettaglio tipologie documentali conservate

Flusso (Serie, Repertorio, …)	Descrizione / AliasDA	Modalità di versamento in conservazione	Tempo di conservazione
Contratti	accatre_contratti	Automatica	illimitata
Deliberazioni	accatre_deliberazioni	Automatica	illimitata
Registro giornaliero di protocollo	accatre_regprot	Automatica con conferma giornaliera dell'operatore	illimitata
Fattura Ricevuta PA	fatp_pa	Automatica	illimitata
Fascicolo elettorale elettronico	accatre_faelel	Automatica	illimitata
Fattura emessa PA	fata_pa	Automatica	illimitata
Determinazioni	accatre_determinazioni	Automatica	illimitata
Liste elettorali	accatre_listeel	Automatica	illimitata
Atti di liquidazione	accatre_attiliq	Automatica	illimitata
Decreti	accatre_decreti	Automatica	illimitata
Ordinanze	accatre_ordinanze	Automatica	illimitata
Documentazione Interna	accatre_docinterna	Automatica	illimitata
Documenti protocollati	accatre_docprot	Automatica	illimitata
Documenti fiscali	accatre_docfisc	Automatica	illimitata
Doumenti risorse umane	accatre_docrisum	Automatica	illimitata

© InfoCert S.p.A. – All right reserved

6. IL PROCESSO DI CONSERVAZIONE

Il servizio LegalDoc di InfoCert è fruibile con modalità:

- **automatica**, attraverso **integrazione WS** con il **Sistema di interscambio OlimpoCoOutsourcer (Gestione Documentale) acquisito dalla società Siscom SpA**
- **manuale**, attraverso il portale **LegalDoc WEB**.

Il servizio è erogato in modalità **SaaS** (Software as a Service) e permette di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

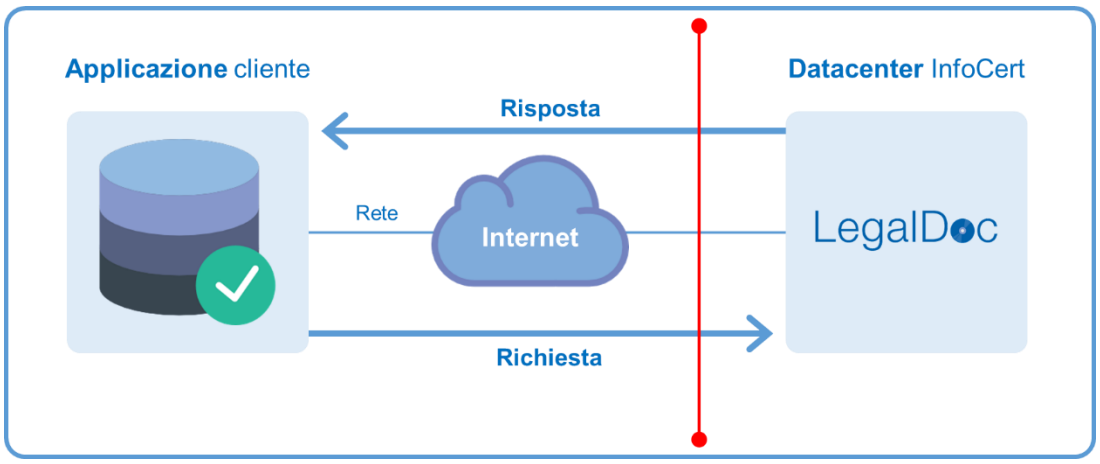

FIGURA 2 RAPPRESENTAZIONE DEL SERVIZIO ATTRAVERSO LA RETE

Principali funzionalità:

- accettazione del pacchetto di versamento;
- conservazione del pacchetto di archiviazione;
- rettifica del pacchetto di archiviazione;
- cancellazione logica del pacchetto di archiviazione;
- scarto del pacchetto di archiviazione;
- ricerca dei documenti conservati;
- esibizione del pacchetto di distribuzione.

Ad ogni documento è associato un **Indice di Conservazione**, nonché un identificativo univoco generato da LegalDoc ("**Token LegalDoc**").

Il documento rappresenta l'unità minima di elaborazione nel senso che viene memorizzato ed

© InfoCert S.p.A. – All right reserved

esibito come un tutt'uno.

Non è possibile estrarre da LegalDoc parti di un documento.

6.1 FIRMA DIGITALE DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, il Responsabile del servizio di conservazione di InfoCert appone la propria firma digitale su ogni pacchetto di archiviazione, mediante un sistema di firma automatica erogato dalla CA - Certification Authority - InfoCert, che si avvale di un dispositivo crittografico ad altre prestazioni HSM.

6.2 MARCA TEMPORALE DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, viene apposta anche una marca temporale su ogni pacchetto di archiviazione. La marca temporale viene richiesta al TSS - Time Stamping Service - InfoCert, che la restituisce firmata con un certificato emesso dalla TSA - Time Stamping Authority - InfoCert. Il TSS è sincronizzato tramite i segnali forniti dai sistemi satellitari GPS, Galileo e GLONASS ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

6.3 ANALISI DEGLI ERRORI

In fase di versamento vengono automaticamente eseguiti dei controlli sui pacchetti:

- Formato dichiarato del documento da conservare (in coerenza con i 'Dati Tecnici di attivazione' e con la configurazione degli ambienti);
- Correttezza della struttura del file di Parametri (contenente le informazioni per la leggibilità nel tempo del documento da conservare);
- Correttezza della struttura del file di Indici (contente i metadati del documento da conservare, alcuni dei quali obbligatori, in coerenza con i 'Dati Tecnici di attivazione');
- Presenza in conservazione sul medesimo path di un documento con lo stesso nome-file del documento da conservare;
- Abilitazione Utenza all'attività di versamento in quel dato ambiente (l'associazione tra utenza -username e password- e singola persona fisica è in capo al Comune di Vigonovo).
- Validità sessione in uso (di default della durata di un'ora tra login e logout);
- Dimensione massima del documento da conservare (di default 256 megabyte, variabile

© InfoCert S.p.A. – All right reserved

su richiesta);

- Validità del certificato qualificato di firma digitale con cui è sottoscritto il documento da conservare (opzionale).

6.4 CONTROLLI DI PROCESSO

I controlli di processo sono i controlli che hanno luogo durante l'elaborazione dei documenti soggetti al processo di conservazione.

LegalDoc è un processo complesso, che movimenta una consistente mole di dati, dei quali è necessario garantire costantemente l'integrità e la coerenza: per questo motivo sono attivati controlli automatici, che richiedono l'intervento del Responsabile del servizio di conservazione solo al verificarsi di eventuali eventi anomali non gestibili in modo automatico. L'apposita procedura, detta ''verificatore'', esegue test di leggibilità binaria mediante il continuo calcolo delle impronte dei documenti conservati, con successivo confronto con l'hash del documento contenuto nel file delle direttive della conservazione versato: se la procedura non registra differenze tra i due hash, il documento è inalterato rispetto a quanto versato.

In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio di conservazione e i suoi Responsabili incaricati sono dotati di apposita Console, con la quale procedono manualmente e periodicamente ad una verifica campionaria di leggibilità sull'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.

Tutti i controlli sono verbalizzati e tutti i verbali sono a loro volta conservati a norma.

© InfoCert S.p.A. – All right reserved

7. IL PROCESSO DI RICERCA ED ESIBIZIONE

Il servizio LegalDoc di ricerca ed esibizione dei documenti conservati è fruibile con modalità:

- **manuale**, attraverso il portale **LegalDoc WEB**.

L'accesso alla ricerca e all'esibizione dei documenti conservati avviene sulla base di credenziali, protette da password e configurate con delle specifiche regole che consentono l'accesso solo ad alcune tipologie documentali, sulla base di quanto richiesto tramite **"Specificità del Contratto – Scheda Dati Tecnici di Attivazione"**.

7.1 RICERCA ED ESIBIZIONE IN LEGALDOC WEB

Il portale LegalDoc WEB permette di ricercare e di estrarre dal sistema un documento di cui sia completata la procedura di conservazione, utilizzando il token o i metadati compilati in fase di versamento e di accedere al così detto 'esibitore a norma', per produrre uno o più pacchetti di distribuzione.

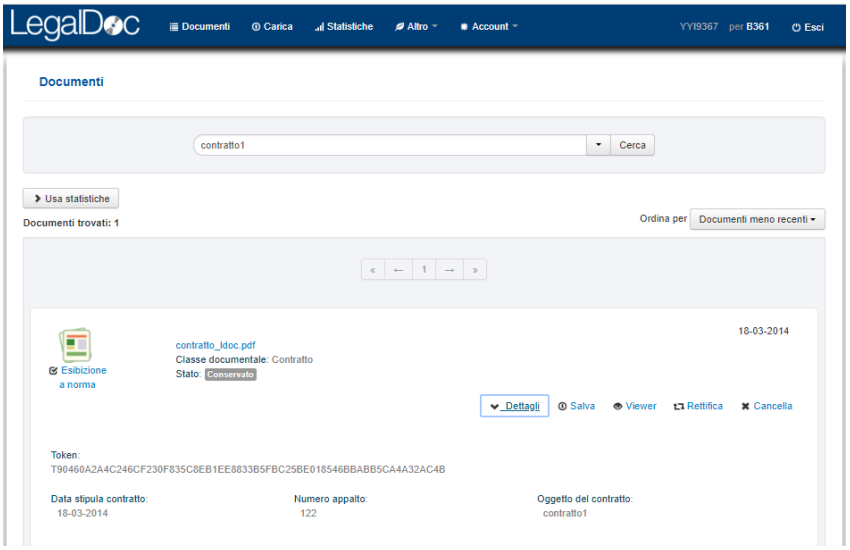

FIGURA 3 INTERFACCIA LEGALDOC WEB

Attraverso l'esibizione diventa possibile:

- estrarre un documento e visualizzarlo a video;

© InfoCert S.p.A. – All right reserved

- produrre copia cartacea o su altro supporto informatico del documento;
- estrarre i visualizzatori memorizzati nel sistema di conservazione, permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione;
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione;
- verificare l'integrità del documento conservato e di tutti i documenti del pacchetto;
- prendere visione dei file a corredo, che qualificano il processo di conservazione attestandone il corretto svolgimento:
    - L'Indice di Conservazione UNI SInCRO, altrimenti detto Indice del Pacchetto di Archiviazione o Indice di Conservazione o Preservation Index (PIndex), firmato e marcato dal Responsabile del servizio di conservazione di InfoCert
    - File di parametri (contante le informazioni per la leggibilità nel tempo)
    - File di indici (contente i metadati del documento conservato)
    - File di dati (documento conservato)
    - Attestazione di corretta conservazione (firmata e marcata dal Responsabile del servizio di conservazione di InfoCert).

L'esibizione del documento ottenuto tramite interrogazione al sistema LegalDoc rappresenta un'esibizione completa e a norma di legge.

© InfoCert S.p.A. – All right reserved

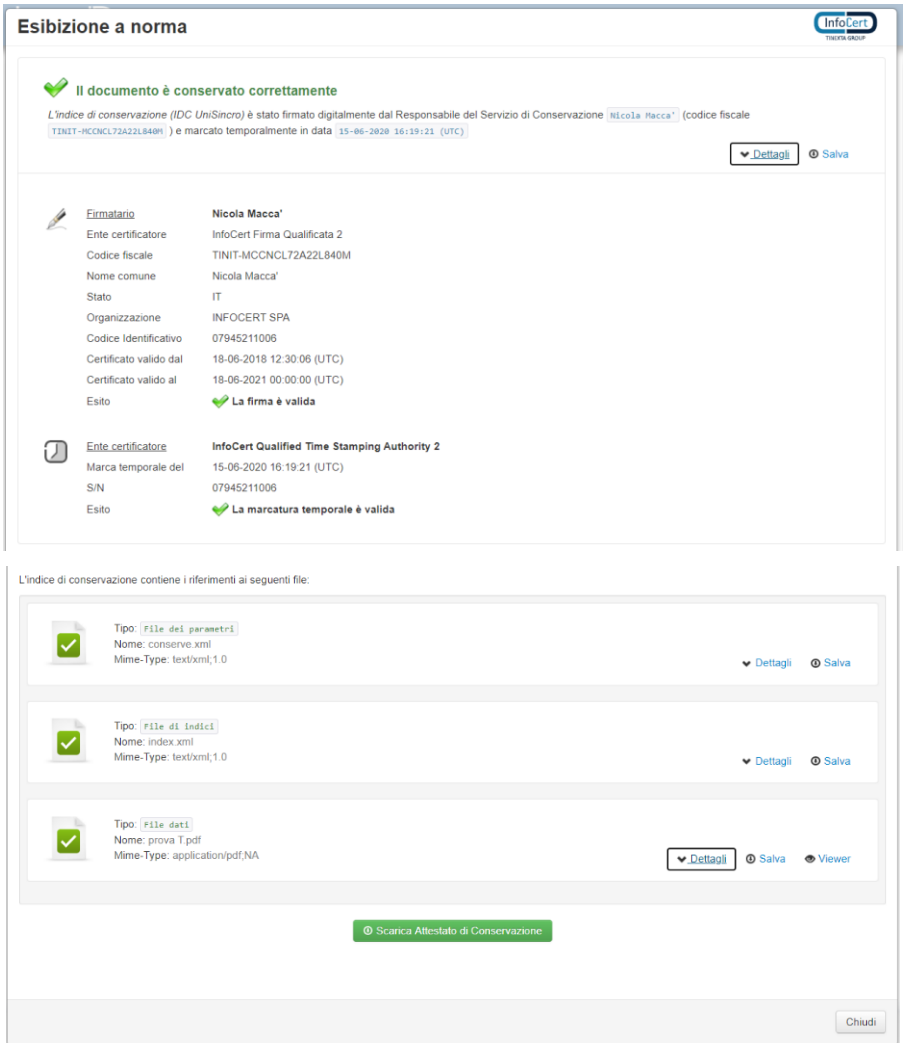

FIGURA 4 ESIBITORE LEGALDOC

© InfoCert S.p.A. – All right reserved

8. SICUREZZA E PROTEZIONE DEI DATI

8.1 POLICY

Il Comune di Vigonovo si è dotato di procedure di sicurezza informatiche interne, per l'utilizzo degli strumenti informatici.

8.2 POLICY INFOCERT

La descrizione tecnica del servizio di conservazione LegalDoc e delle principali misure di sicurezza fisica e logica adottate sono contenute nelle **"Specificità del Contratto – Allegato tecnico".**

8.3 NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Ai sensi del paragrafo 4.10 "Misure di sicurezza" delle Linee guida AgID e del Regolamento UE n. 679/2016, InfoCert in qualità di soggetto esterno a cui il Comune di Vigonovo ha affidato il servizio di conservazione, assume per il proprio ambito di competenza ruolo di responsabile del trattamento dei dati personali.

La nomina è inserita all'interno delle **"Specificità del Contratto – Atto di Affidamento''**.

Il trattamento dei dati è effettuato:

- ai soli fini dell'erogazione del servizio,
- con l'adozione delle misure di sicurezza ex art. 32 del Regolamento,
- nel rispetto degli obblighi posti in carico al Responsabile del trattamento dall'art. 28 del Regolamento.

Inoltre, tutte le richieste di dati formulate dai servizi InfoCert sono configurate per acquisire il set minimo indispensabile per l'erogazione del servizio e nel rispetto della normativa vigente.

Tutte le tempistiche, le tipologie di dati e la loro quantità sono definibili dal Comune di Vigonovo tramite le **"Specificità del Contratto – Scheda Dati Tecnici di Attivazione"**.

InfoCert si è dotata di apposita "Procedura di scarto, *hand-over* e *termination plan"*, tesa a minimizzare il più possibile il trattamento dei dati quantitativamente e qualitativamente.

© InfoCert S.p.A. – All right reserved

9. SPECIFICITÀ DEL CONTRATTO

Il servizio è regolato dai seguenti documenti tecnici e contrattuali, condivisi all'attivazione del servizio.

1. ***Condizioni Generali di Contratto***;
2. ***Scheda dati tecnici per l'attivazione***, che contiene tutte le esigenze in relazione a tipologie documentali, formati, metadati e credenziali di accesso da richiedere;
3. ***File di configurazione***, che descrive la configurazione dell'ambiente di conservazione;
4. ***Atto di affidamento***, che rappresenta la formalizzazione dell'affidamento ad InfoCert del processo di conservazione, la nomina del Responsabile del trattamento dei dati personali ai sensi del Regolamento UE n. 679/2016 GDPR, e stabilisce espressamente quali attività di fatto vengano assunte da InfoCert e quali, al contrario, rimangano a carico dell'affidatario;
5. ***Allegato Tecnico***, che descrive le modalità di fornitura del servizio e l'infrastruttura tecnico-tecnologica utilizzata per la sua erogazione;
6. ***Manuale Utente***, che descrive l'interfaccia web dal punto di vista dell'utente che descrive l'interfaccia web dal punto di vista dell'utente.

© InfoCert S.p.A. – All right reserved

Manuale della Conservazione

di InfoCert S.p.A.

INFOCERT
TINEXTA GROUP

SOMMARIO

InfoCert S.p.A. – all rights reserved

REGISTRO DELLE VERSIONI

N° versione	Data emissione	Modifiche apportate
01	Luglio 2014	Prima versione
02	Novembre 2015	Utilizzo dello schema proposto da AgID
03	Febbraio 2016	Correzioni formali e di layout
04	Marzo 2016	Correzioni formali e di layout
05	Settembre 2017	Glossario, Normativa, Mission, Comunità di riferimento, Riferimenti a policy aziendali interne
05.1	Novembre 2017	Specificità del contratto
06	Luglio 2018	Normativa GDPR, semplificazione glossario e nuovi Responsabili
07	Gennaio 2019	Nuovo logo aziendale
08	Maggio 2019	Nuovo Responsabile sistemi
09	Ottobre 2020	Glossario, nuovi Responsabili, aggiornamento procedure di monitoraggio, semplificazione delle Specificità del contratto
10	Novembre 2020	Ampliamento servizi di storage e introduzione Linee Guida AgID
11	Aprile 2022	Semplificazione nella descrizione dei processi Introduzione del servizio SAFE LTA Aggiornamento procedure di monitoraggio
12	Maggio 2023	Nuovo logo Aggiornamento TSS per la marca temporale
13	Agosto 2024	Semplificazione e aggiornamento Responsabili, Profilo InfoCert (indirizzi e qualificazione ACN), Sistema SAFE LTA e Specificità del contratto

InfoCert S.p.A. – all rights reserved

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il **manuale della conservazione di InfoCert S.p.A.** (del Gruppo Tinexta), ai sensi delle **Linee Guida AgID**, Agenzia per l'Italia Digitale, su formazione, gestione e conservazione dei documenti informatici, richiamate dal **Codice dell'Amministrazione Digitale** - decreto legislativo n. 82 del 2005.

Il manuale della conservazione 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.

In caso di ispezione da parte delle autorità di vigilanza preposte, il manuale della conservazione permette un agevole svolgimento di tutte le attività di controllo.

Ogni soggetto produttore, cliente dei servizi di conservazione di InfoCert e titolare dei documenti conservati, può liberamente far riferimento al presente documento nel proprio manuale della conservazione.

InfoCert S.p.A. – all rights reserved

2. TERMINOLOGIA

TERMINE	DEFINIZIONE
ACCESSO	Operazione che consente di prendere visione dei documenti informatici.
AFFIDABILITÀ	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
AGGREGAZIONE DOCUMENTALE INFORMATICA	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
ARCHIVIO	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
ATTESTAZIONE DI CONFORMITÀ DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITÀ	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
CERTIFICAZIONE	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
CLASSIFICAZIONE	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.

InfoCert S.p.A. – all rights reserved

CONSERVATORE	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
CONSERVAZIONE	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
DESTINATARIO	Soggetto o sistema al quale il documento informatico è indirizzato.
DIGEST	Vedi Impronta crittografica.
DOCUMENTO AMMINISTRATIVO INFORMATICO	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
DOCUMENTO ELETTRONICO	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
DOCUMENTO INFORMATICO	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
DUPLICATO INFORMATICO	Vedi art. 1, comma 1, lett) i quinquies del CAD.
ESEAL	Vedi sigillo elettronico.
ESIBIZIONE	operazione che consente di visualizzare un documento conservato
ESIGNATURE	Vedi firma elettronica.
ESTRAZIONE STATICA DEI DATI	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc..), attraverso metodi automatici o semi-automatici
EVIDENZA INFORMATICA	Sequenza finita di *bit* che può essere elaborata da una procedura informatica.
FASCICOLO INFORMATICO	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
FILE	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
FIRMA ELETTRONICA	Vedi articolo 3 del Regolamento eIDAS.
FIRMA ELETTRONICA AVANZATA	Vedi articoli 3 e 26 del Regolamento eIDAS.

InfoCert S.p.A. – all rights reserved

FIRMA ELETTRONICA QUALIFICATA	Vedi articolo 3 del Regolamento eIDAS.
FLUSSO (BINARIO)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
FORMATO CONTENITORE	Formato di file progettato per consentire l'inclusione ("imbustamento" o *wrapping*), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
FORMATO DEL DOCUMENTO INFORMATICO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
FUNZIONE DI *HASH* CRITTOGRAFICA	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
GESTIONE DOCUMENTALE	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
HASH	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
IDENTIFICATIVO UNIVOCO	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
IMPRONTA CRITTOGRAFICA	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.
INTEGRITÀ	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
INTEROPERABILITÀ	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi

InfoCert S.p.A. – all rights reserved

	informativi per lo scambio di informazioni e l'erogazione di servizi.
LEGGIBILITÀ	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
MANUALE DI CONSERVAZIONE	Documento informatico che descrive il sistema di conservazione e 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.
METADATI	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
OGGETTO DIGITALE	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
PACCHETTO DI ARCHIVIAZIONE	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
PACCHETTO DI DISTRIBUZIONE	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
PACCHETTO DI FILE (*FILE PACKAGE*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
PACCHETTO DI VERSAMENTO	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
PACCHETTO INFORMATIVO	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
PATH	Percorso (*vedi*).
PATHNAME	Concatenazione ordinata del percorso di un file e del suo nome.
PERCORSO	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come

InfoCert S.p.A. – all rights reserved

	concatenazione ordinata del nome dei nodi del percorso.
PIANO DI CONSERVAZIONE	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
PIANO DI ORGANIZZAZIONE DELLE AGGREGAZIONI DOCUMENTALI	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
PIANO GENERALE DELLA SICUREZZA	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
PRESA IN CARICO	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
PROCESSO	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
PRODUTTORE DEI PDV	Persona fisica, 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 il responsabile della gestione documentale.
QSEAL	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
QSIGNATURE	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
RAPPORTO DI VERSAMENTO	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLA CONSERVAZIONE	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne

InfoCert S.p.A. – all rights reserved

	governa la gestione con piena responsabilità ed autonomia.
RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RIFERIMENTO TEMPORALE	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
RIVERSAMENTO	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
SCARTO	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
SIGILLO ELETTRONICO	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
SISTEMA DI CONSERVAZIONE	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
TIMELINE	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
TITOLARE DELL'OGGETTO DI CONSERVAZIONE	Soggetto produttore degli oggetti di conservazione.
TRASFERIMENTO	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
UTENTE ABILITATO	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o

InfoCert S.p.A. – all rights reserved

	di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

InfoCert S.p.A. – all rights reserved

3. NORMATIVA E STANDARD DI RIFERIMENTO

Di seguito l'elenco dei principali riferimenti normativi in materia, ordinati secondo il criterio della gerarchia delle fonti:

- eIDAS (electronic IDentification Authentication and Signature) Reg. 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market, così come modificato dal Reg. (UE) 2024/1183 of the European Parliament and of the Council of April 2024.
- GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- 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 7 agosto 1990, n. 241 e ss.mm.ii. — Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss.mm.ii — Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. — Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. — Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) — Codice dell'amministrazione digitale (CAD) e ss.mm.ii.;
- 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 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 [parzialmente abrogate dalle Linee Guida AgID a partire da gennaio 2022];
- Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 - Modalità di

InfoCert S.p.A. – all rights reserved

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 del 2005;

- 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.
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici pubblicate a settembre 2020, aggiornate nel maggio 2021 e pienamente applicabili dal gennaio 2022.
- Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici di dicembre 2021 (marketplace).

Si riportano di seguito gli standard di riferimento:

- UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- ISO/TR 18492 - Long-term preservation of electronic document-based information;
- ISO 20652 - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard;
- ISO 20104 - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS);
- ISO/CD TR 26102 - Requirements for long-term preservation of electronic records;
- SIARD Software Independent Archiving of Relational Databases 2.0;
- ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert — Communication — Élimination — Restitution - Modification, ver. 2.1, 2018;
- METS - Metadata Encoding and Transmission Standard;

InfoCert S.p.A. – all rights reserved

- PREMIS — PREservation Metadata: Implementation Strategies;
- EAD (3)/ISAD (G);
- EAC (CPF)/ISAAR (CPF)/NIERA (CPF);
- SCONS2/EAG/ISDIAH;
- ISO 16363 - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories;
- ISO/IEC 27001 - Information technology - Security techniques - Information security management systems — Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ETSI TS 101 533-1 V1.2.1 - 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 V1.2.1 - 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.

Inoltre, si segnalano due procedure aziendali interne connesse al servizio:

- **Procedura di handover e scarto**, che descrive le modalità di richiesta ed esecuzione delle attività di versamento da/a un altro Conservatore e delle attività di cancellazione fisica e logica dei documenti, nel rispetto delle Linee Guida AgID e del GDPR.
- **Piano di cessazione**, che descrive le attività di InfoCert in caso di cessazione dei servizi di conservazione, in modo da fornire a utenti e clienti il supporto necessario alla migrazione verso altri Conservatori.

InfoCert S.p.A. – all rights reserved

4. RUOLI E RESPONSABILITÀ

Nel processo di conservazione digitale intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità.

I ruoli individuati dalle Linee Guida AgID sono:

a) **TITOLARE DELL'OGGETTO DELLA CONSERVAZIONE** (soggetto produttore degli oggetti di conservazione);
b) **PRODUTTORE DEI PACCHETTI DI VERSAMENTO** (persona fisica, 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, anche attraverso l'utilizzo di piattaforme o sistemi InfoCert);
c) **UTENTE ABILITATO** (persona, ente o sistema che interagisce con i servizi di conservazione, al fine di fruire delle informazioni di interesse, cioè per le attività di ricerca ed esibizione a norma);
d) **RESPONSABILE DELLA CONSERVAZIONE** (interno al cliente/produttore, che scegliere di affidare il servizio a InfoCert);
e) **CONSERVATORE** (InfoCert).

I primi quattro ruoli sono tipicamente individuati all'interno dell'organigramma di quello che per InfoCert è il cliente/produttore.

Quest'ultimo affida in *full outsourcing* il servizio di conservazione a InfoCert S.p.A., in accordo con quanto previsto dai documenti contrattuali descritti al capitolo 'Specificità del Contratto' e dalle Linee Guida AgID. In particolar modo, nell'Atto di affidamento' sono elencate funzioni e ambiti oggetto della delega.

All'interno dell'organigramma di InfoCert, sono, invece, individuati un **Responsabile del servizio di conservazione**, un **Responsabile della funzione archivistica** (come previsto dal Regolamento AgID) e gli altri ruoli qui di seguito riportati.

PROFILO DI INFOCERT

InfoCert si pone sul mercato europeo come **Trust Service Provider** qualificato ai sensi del Regolamento eIDAS, leader del mercato nei servizi di digitalizzazione e dematerializzazione, nonché una delle principali Certification Authority a livello europeo, fornendo servizi di Posta Elettronica Certificata, Firma Avanzata e Digitale, Conservazione Digitale dei documenti e gestore accreditato AgID dell'identità digitale di cittadini e imprese, in conformità ai requisiti regolamentari e tecnici dello SPID (Sistema Pubblico per la gestione dell'Identità Digitale).
Da sempre la **mission aziendale** è credere nel futuro e nella trasformazione digitale, per questo dedichiamo la nostra esperienza, la nostra capacità di innovazione e la nostra passione per l'eccellenza, a tutti coloro che, in Italia e nel mondo, ricercano sicurezza e affidabilità nelle soluzioni digitali. Investiamo in ricerca e sviluppo per dare vita a nuove idee che supportino i nostri clienti nella costruzione di modelli e processi di business innovativi e

InfoCert S.p.A. – all rights reserved

conformi alle normative, guidandoli verso una efficace trasformazione digitale e un futuro maggiormente sostenibile per le aziende, le persone e la realtà sociale.

La mission aziendale si declina anche nel servizio di Conservazione digitale: innovazione, sicurezza, affidabilità e conformità normativa, con lo scopo di assicurare la corretta gestione, archiviazione e conservazione dei documenti informatici di diversi soggetti produttori, assicurando l'esibizione a norma dei documenti conservati e la consulenza specialistica su progetti di paperless design.

InfoCert dal 2014 è stata tra le prime aziende italiane accreditate dall'Agenzia per l'Italia Digitale (AgID) come Conservatore, requisito normativo necessario per erogare servizi di Conservazione digitale per la Pubblica Amministrazione.

Da febbraio 2022, è iscritta al Marketplace dei servizi di conservazione di AgID come conservatore qualificato - https://conservatoriqualificati.agid.gov.it/

Inoltre, InfoCert è tra i fornitori presenti nel Catalogo delle Infrastrutture digitali e dei Servizi Cloud di ACN (Agenzia per la Cybersicurezza Nazionale), requisito normativo necessario per offrire alla Pubblica Amministrazione, le proprie soluzioni di conservazione digitale a norma: SAFE LTA (SaaS - ID Scheda in ACN: SA-3452) e LegalDoc (SaaS - ID Scheda: SA-779), con la sua Infrastruttura CSP di Tipo B (ID Scheda: IN-335) -

https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud

denominazione sociale	InfoCert S.p.A.
sede legale:	Piazzale Flaminio 1/b, 00196 Roma
sedi operative:	Piazza da Porto, 3, 35131 - Padova Via Fernanda Wittgens, 6, 20123 — Milano Via Gian Domenico Romagnosi 4, 00196 Roma
telefono:	049.7849350
sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
codice fiscale / partita IVA	07945211006
numero REA	RM — 1064345

Oggi il servizio di Conservazione di InfoCert si declina in due prodotti:

- **LegalDoc**, storico servizio, sviluppato sulla base delle Regole Tecniche del 2013, pensato per il mercato italiano e accreditato AgID dal 2014.
- **SAFE LTA** (***Long-Term-Archiving***), sviluppato nel 2021, sulla base delle specifiche *eArchiving building block* del *Connecting Europe Facility* (CEF), in ottica internazionale.

InfoCert S.p.A. – all rights reserved

La **comunità di riferimento** del servizio di Conservazione digitale di InfoCert è un gruppo identificato di clienti e di potenziali utenti in grado di comprendere un determinato set di informazioni: si tratta di un'unica comunità, ben definita, ma con alcune differenziazioni interne (multiple user communities), a seconda del mercato di riferimento (Pubblica Amministrazione centrale e locale, Sanità, Industry, Banking, Pharma, Utilities, Insurance, Ordini e Associazioni, PMI, liberi professionisti) e delle varie geografie internazionali.

Il fine ultimo del servizio di Conservazione digitale è rendere i Pacchetti di Distribuzione ricercabili, esibibili, leggibili, integri, affidabili, autentici e fruibili dagli utenti della comunità di riferimento, attraverso la mediazione del soggetto produttore, in ottemperanza ai principali standard internazionali di *records management* (OAIS ISO14721 e ISO15489).

InfoCert è costantemente impegnata nel monitoraggio della propria comunità designata, al fine di acquisire nuove informazioni o esigenze o standard tecnologici, anche con lo scopo di combattere l'obsolescenza tecnologica.

InfoCert, inoltre, nello svolgimento delle proprie attività, ha conseguito le seguenti certificazioni:

RESPONSABILI INFOCERT

Si riportano di seguito i profili professionali di responsabilità legate al servizio di conservazione e le rispettive attività di competenza.
Tutti i Responsabili sono assunti a tempo indeterminato.

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
Responsabile del servizio di Conservazione	Nicola Maccà	• definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; • definizione delle caratteristiche e dei requisiti	da luglio 2018

InfoCert S.p.A. – all rights reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		del sistema di conservazione in conformità alla normativa vigente; • corretta erogazione del servizio di conservazione all'ente produttore; • gestione delle convenzioni (in collaborazione con Ufficio Legale e Product Marketing Manager), definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	
Responsabile funzione archivistica di conservazione	Marta Gaia Castellan	• definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; • definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; • monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; • collaborazione con l'ente produttore ai fini del trasferimento in	da settembre 2015

InfoCert S.p.A. – all rights reserved

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza; • controlli periodici a campione sulla leggibilità dei documenti conservati.	

Di seguito sono storicizzate le figure professionali che hanno ricoperto ruoli di responsabilità precedentemente:

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile sviluppo e manutenzione del sistema di conservazione	Lucia Bortoletto	da luglio 2018 a gennaio 2022 (data in cui il Regolamento AgID ha ristretto le figure di responsabilità alle due nella precedente tabella)
Responsabile trattamento dati personali	Ilenia Gentilezza	da marzo 2020 a luglio 2023
Responsabile Sicurezza dei sistemi per la conservazione	Giovanni Belluzzo	da luglio 2018 a gennaio 2022
Responsabile sistemi informativi per la conservazione	Stefano Mameli	da maggio 2019 a ottobre 2020
Responsabile trattamento dati personali	Valentina Zoppo	da luglio 2018 a marzo 2020
Responsabile sistemi informativi per la conservazione	Nicolò Poniz	da luglio 2018 a maggio 2019
Responsabile sviluppo e manutenzione del sistema di conservazione	Nicola Maccà	da gennaio 2013 a luglio 2018
Responsabile sistemi informativi per la conservazione	Massimo Biagi	da marzo 2014 a luglio 2018

InfoCert S.p.A. – all rights reserved

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile funzione archivistica di conservazione precedente	Silvia Loffi	da dicembre 2014 ad agosto 2015
Responsabile trattamento dati personali	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile Sicurezza dei sistemi per la conservazione	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile del servizio di Conservazione	Antonio Dal Borgo	da luglio 2008 a luglio 2018
Responsabile del servizio di Conservazione	Pio Barban	da luglio 2007 a luglio 2008

InfoCert S.p.A. – all rights reserved

5. OGGETTI SOTTOPOSTI A CONSERVAZIONE

In generale si definisce '**pacchetto**' un contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche).

I pacchetti sono contrattualizzati con il soggetto produttore e si basano sui documenti che fanno parte delle 'Specificità del Contratto'.

Per "**PACCHETTO DI VERSAMENTO**" si intende l'insieme di documenti che il soggetto produttore invia al sistema di conservazione in un'unica sessione o in una singola chiamata. Le modalità di versamento sono diverse: dal caricamento manuale attraverso portale web, all'utilizzo di chiamate applicative. Il sistema ritorna una Ricevuta di versamento.

Per "**PACCHETTO DI ARCHIVIAZIONE**" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert e associato a un file XML, detto Indice del Pacchetto di Archiviazione (IPdA o indice di conservazione UNI SInCRO) firmato digitalmente e marcato temporalmente dal Responsabile del servizio di InfoCert. In LegalDoc coincide con il Rapporto di versamento.

Questo indice di conservazione, secondo lo standard **UNI 11386 SInCRO 2020**, contiene: una sezione di SelfDescription (con i riferimenti dell'applicativo e del Conservatore), una sezione di PVolume (con lo schema xsd), una sezione MoreInfo per LegalDoc (con token, bucket, policy, operation, target), una sezione FileGroup (con token, hash e SHA dei vari file del pacchetto), una sezione Process (con i riferimenti al manuale, al Responsabile del servizio e al riferimento temporale).

Ogni documento da conservare viene identificato in modo univoco attraverso un token (es. per LegalDoc TB853E72B7552EBB8D0AF3FE9EE1EAB3D97519959346B83DD5E539).

Per "**PACCHETTO DI DISTRIBUZIONE**" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente, in risposta a una sua ricerca e richiesta di esibizione. Il suo contenuto coincide con il "pacchetto di archiviazione".

Eventuali specificità sono concordate con il Soggetto produttore e descritte nelle 'Specificità del Contratto' - Specifiche tecniche per l'integrazione — Allegato Tecnico al Contratto LegalDoc o SAFE LTA.

Un pacchetto di archiviazione in LegalDoc è composto da:

- L'Indice di Conservazione UNI SInCRO, altrimenti detto Indice del Pacchetto di Archiviazione o Indice di Conservazione (firmato e marcato dal Responsabile del servizio di InfoCert)
- File di parametri (contenente le informazioni per la leggibilità nel tempo)
- File di indici (contenente i metadati del documento conservato)
- File di dati (documento conservato)

InfoCert S.p.A. – all rights reserved

Un pacchetto di archiviazione in SAFE LTA è composto da:

- L'Indice di Conservazione UNI SInCRO, altrimenti detto Indice del Pacchetto di Archiviazione o Indice di Conservazione (sigillato e marcato da InfoCert)
- Metadata Descriptive (file XML di metadatazione)
- Metadata Preservation (file XML di metadatazione secondo lo standard PREMIS)
- Schemas (file XSD di metadatazione)
- Representation (documento conservato)

FORMATI

Tipologie documentali e formati sono sempre concordati con il soggetto produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione'.

In LegalDoc i visualizzatori di alcuni formati (definiti in InfoCert come 'standard' perché maggiormente richiesti) sono automaticamente assegnati all'atto dell'attivazione del proprio ambiente di conservazione e sono forniti da InfoCert al soggetto produttore all'atto di attivazione del servizio.

Formato	Estensione	MIME-Type	Standard
PDF o PDF/A	.pdf	application/pdf;NA	ISO 32000-1 (PDF), ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	.tif	image/tiff;NA	ISO 12639(TIFF/IT); ISO 12234 (TIFF/EP)
XML	.xml	text/xml;1.0	
TXT	.txt	text/plain;NA	

Tutti i documenti inviati in conservazione sono associati al visualizzatore configurato per il particolare formato.

Conservare documenti in altri formati (jpeg, Open Document Format, eml, DICOM, ecc..), in conformità con l'**Allegato 2 delle Linee Guida AgID**, è sempre possibile. Qualora un soggetto produttore necessiti di formati aggiuntivi rispetto a quelli standard, può segnalarlo nei 'Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA (compresi nelle 'Specificità del Contratto') o configurarli autonomamente utilizzando l'apposita funzionalità ed eventualmente conservare gli appositi visualizzatori all'interno del sistema. Un'apposita sezione dell'ambiente di conservazione, infatti, è dedicata alla conservazione dei visualizzatori dei formati (*viewer*), che può essere arricchita a seconda delle esigenze.

InfoCert S.p.A. – all rights reserved

Inoltre, il Responsabile del servizio della conservazione mantiene un archivio di tutte le componenti hardware e software obsolete, non più compatibili con i programmi di visualizzazione garantiti e/o depositati dal soggetto produttore, nel caso questi siano i soli strumenti che consentono di rendere leggibili i documenti conservati associati a tale *viewer*.

METADATI

I metadati sono dati associati ai documenti da conservare in fase di formazione, per identificarli, descrivendone il contesto, il contenuto e la struttura, così da permetterne la gestione del tempo. Nei sistemi di conservazione sono anche utilizzati come chiavi di ricerca.

L'**Allegato 5 delle Linee Guida AgID** introduce i metadati minimi per il documento informatico, il documento amministrativo informatico e per le aggregazioni documentali.

Tipologie documentali e metadati sono sempre concordati con il soggetto produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA, che contengono anche delle note operative per una corretta metadatazione, secondo le Linee Guida AgID e nel 'file di configurazione', che descrive nel dettaglio l'ambiente di conservazione (bucket o Company).

Tuttavia, il produttore può in autonomia aggiungere ulteriori metadati ad ogni versamento.

InfoCert S.p.A. – all rights reserved

6. IL PROCESSO DI CONSERVAZIONE

I sistemi di conservazione sono erogati in modalità **SaaS** (Software as a Service) secondo uno schema di Business Process Outsourcing (BPO).

I servizi hanno l'obiettivo di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di tutti i documenti informatici conservati, nel rispetto della normativa vigente.

Il processo può essere così schematizzato:

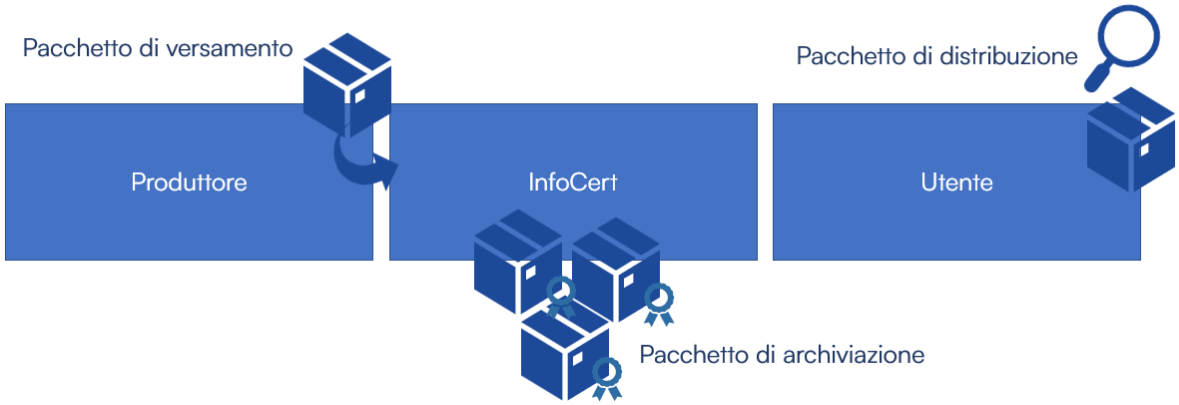

Figura 1 disegno di processo

1. *il produttore invia i documenti in conservazione con un pacchetto di versamento, contenente anche i metadati necessari;*
2. *il pacchetto viene preso in carico dal sistema se rispetta la configurazione concordata (formati, metadati, parametri, policy...) e se l'impronta di hash calcolata coincide con quella contenuta nel pacchetto;*

   in SAFE LTA, il sistema restituisce al produttore il link per potere reperire il rapporto di versamento;

3. *il sistema crea i pacchetti di archiviazione; il Responsabile del servizio firma o sigilla e marca temporalmente l'indice di conservazione UNI SInCRO di ogni singolo pacchetto di archiviazione, a garanzia di integrità, immodificabilità e autenticità;*

   in LegalDoc, il sistema restituisce al produttore l'indice di conservazione come ricevuta (rapporto di versamento);

4. *il database del sistema viene aggiornato, il pacchetto di archiviazione viene indicizzato, memorizzato e ridondato più volte (ogni pacchetto è soggetto a controlli periodici di integrità e leggibilità a distanza di tempo);*

InfoCert S.p.A. – all rights reserved

5. *il documento conservato può essere ricercato attraverso i metadati, su richiesta dell'utente in possesso delle apposite credenziali, in qualsiasi momento, ed esibito mediante un pacchetto di distribuzione, che contiene tutte le evidenze del processo.*

I sistemi consentono, quindi, le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati dal produttore;
- **conservazione del pacchetto di archiviazione**, a norma di legge e per tutta la durata prevista dal contratto;
- **rettifica del pacchetto di archiviazione**, modifica logica, nel pieno rispetto del principio di tracciabilità;
- **ricerca** tra i documenti conservati, utilizzando uno o più metadati popolati in fase di versamento;
- **esibizione del pacchetto di distribuzione**, contente sia il documento conservato che gli altri documenti a corredo della corretta conservazione, che possono essere scaricati in autonomia, in qualsiasi momento;
- **scarto**, su richiesta formale del Responsabile della conservazione del produttore, cioè cancellazione fisica e logica dei pacchetti di archiviazione e di ogni loro duplicato.

I sistemi di conservazione, quindi, integrano il sistema di gestione documentale del soggetto produttore, sia esso un'azienda o un ente, e ne estendono i servizi con funzionalità di archivio di deposito.

Le fasi di formazione e gestione dei documenti sono organizzate liberamente dal cliente/produttore all'interno del proprio sistema di gestione documentale, in quanto i servizi qui descritti intervengono solamente nella fase di conservazione e solamente per i documenti che il soggetto produttore sceglie di conservare.

CONTROLLI DI VERSAMENTO

In fase di versamento vengono automaticamente eseguiti dei controlli sui pacchetti:

- formato dichiarato del documento da conservare (mime type)
- correttezza della struttura dei pacchetti di versamento
- controlli formali di coerenza rispetto alla configurazione
- validazione dei tracciati dei file di indice (metadati)
- abilitazione utenza all'attività di versamento
- validità sessione in uso

secondo regole e policy concordate in fase di attivazione 'Specificità del Contratto — Scheda Dati Tecnici per LegalDoc o *Submission Agreement* per SAFE LTA di attivazione e File di configurazione'.

All'interno delle 'Specificità del Contratto' SPT/NDOCERR — Descrizione dei codici di errore di LegalDoc è presente la griglia riassuntiva dei codici errore che il servizio LegalDoc

InfoCert S.p.A. – all rights reserved

restituisce in seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto. I campi codice e descrizione vengono inseriti nel corpo della risposta HTTP.

La documentazione tecnica per integrare SAFE LTA con altri sistemi via API è disponibile su https://developers.infocert.digital/

Al terzo rifiuto del pacchetto, sarà necessario contattare il servizio di assistenza tecnica di InfoCert per tentare una soluzione del problema.

L'assistenza è contattabile mediante ticket https://help.infocert.it/

PRODUZIONE DI COPIE O DUPLICATI

All'attivazione del servizio vengono concordate con il soggetto produttore le modalità di ricerca ed esibizione dei documenti conservati ('Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA) e vengono create apposite credenziali (user/password).

Gli utenti abilitati possono in qualsiasi momento ricercare e scaricare pacchetti di distribuzione, attraverso interfaccia web o chiamate applicative.

Ogni documento informatico così scaricato in locale è da considerarsi un duplicato, ovvero il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario (CAD art. 1 - i quinquies).

Laddove richiesto dalla natura delle attività, il Responsabile della Conservazione può in autonomia formare copie su diversi supporti dei documenti ottenuti dai pacchetti di distribuzione, anche con l'intervento di un pubblico ufficiale, a garanzia della loro conformità all'originale.

Anche il Responsabile del servizio può valutare il coinvolgimento di un pubblico ufficiale, in relazione all'evolversi dei formati e del contesto tecnologico dei sistemi.

VERIFICHE DI INTEGRITÀ E LEGGIBILITÀ

I sistemi di memorizzazione utilizzati, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architetturale e alle procedure di memorizzazione permanente dei dati, garantiscono l'immodificabilità, l'integrità, la leggibilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione.

I sistemi mantengono traccia di tutte le operazioni effettuate sui documenti in appositi file di log.

InfoCert S.p.A. – all rights reserved

Inoltre, è garantita la tracciatura di tutti i documenti esibiti dal soggetto produttore mediante interrogazione al sistema e conseguentemente esibiti, che rappresenta un'ulteriore prova di leggibilità, effettuata direttamente dal soggetto produttore.

In aggiunta, InfoCert ha attivato sottosistemi di controllo automatico dedicati alla simulazione della navigazione nel sistema e delle operazioni che effettua l'utente, svolgendo controlli di coerenza dei dati e attività di ripristino da situazioni di errore.

In ogni occasione in cui il file viene copiato o spostato di posizione, funzionalità automatiche verificano che le sue dimensioni non siano mutate durante lo spostamento e che non siano intervenute alterazioni, che possano inficiarne la visualizzazione.

I servizi assicurano la **verifica periodica**, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi con procedure automatiche e manuali.

L'apposita procedura, detta **verificatore binario**, esegue il test di integrità mediante il continuo calcolo delle impronte dei documenti conservati, con successivo confronto con l'hash del documento contenuto nel file delle direttive della conservazione inviato dal soggetto produttore. Se la procedura non registra differenze tra i due hash, il documento è inalterato rispetto a quanto trasmesso dal produttore.

Vengono eseguiti i seguenti passi operativi:

- calcolo dell'impronta del documento;
- confronto con quella contenuta all'interno del file IPdA;
- generazione di un report che viene automaticamente sottoposto alla conservazione nell'area dedicata al Responsabile del servizio della conservazione (quindi a sua volta firmato e marcato temporalmente dal Responsabile del servizio della conservazione stesso).

In caso di anomalie, se il documento risulta corrotto in uno dei repository, il sistema tenta il ripristino automatico con il dato presente nel repository integro. Se invece ambedue le copie sono alterate, viene inviato un *alert* al Responsabile del servizio della conservazione, che tenterà il ripristino manuale partendo da un'altra sorgente (per esempio le copie di backup). Se nessuna sorgente è disponibile viene redatto un verbale di incidente, sottoscritto e conservato dal Responsabile del servizio per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.

In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio e i suoi Responsabili incaricati sono dotati di apposita strumentazione (detta CORE, **Console del Responsabile**), con credenziali dedicate, con la quale procedono manualmente e periodicamente ad una verifica campionaria di leggibilità 'umana' dell'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.
Anche in questo caso viene poi redatto automaticamente un verbale con gli identificativi dei

InfoCert S.p.A. – all rights reserved

documenti visualizzati, successivamente sottoscritto e conservato dal Responsabile del servizio.

SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

I servizi di conservazione di InfoCert consentono lo scarto archivistico, cioè la **cancellazione di un pacchetto di archiviazione** e di qualsiasi suo duplicato prodotto durante le attività di conservazione, sia dal punto di vista logico che dal punto di vista fisico, su richiesta formale del Responsabile della conservazione interno al soggetto produttore/titolare del documento.

La procedura può essere attivata per varie ragioni, sia alla chiusura del contratto, sia in continuità di servizio (in itinere), per il venir meno della rilevanza amministrativa, legale o storica dei documenti conservati per il suo produttore, anche in relazione alla *retention period policy* configurata in fase di attivazione del servizio.

Il così detto **scarto in itinere** si può, quindi, richiedere al Customer Care di InfoCert tramite apposito **modulo**, oppure può essere attivato tramite **chiamate applicative**. In entrambi i casi è richiesta una lista di token firmata digitalmente dal Responsabile della Conservazione interno al produttore/titolare.

Per gli enti pubblici e per gli archivi privati dichiarati di notevole interesse storico, le richieste di scarto sono sottoposte a nulla osta delle soprintendenze archivistiche o delle commissioni di sorveglianza di competenza.

La distruzione degli eventuali supporti ottici rimovibili di back-up è effettuata mediante strumentazione adeguata e seguendo le procedure definite per lo smaltimento dei rifiuti prodotti.

Il Responsabile del servizio della conservazione mantiene traccia delle richieste di scarto ricevute e correttamente eseguite, e vengono redatti **Attestati di scarto** firmati digitalmente dal Responsabile del servizio.

Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di handover tra conservatori e scarto'.

HANDOVER E INTEROPERABILITÀ

Gli archivi di conservazione generati dai sistemi InfoCert sono conformi allo standard di interoperabilità **UNI SInCRO**. L'adozione di tale standard permette l'interoperabilità e la trasferibilità dei dati in modo semplificato.

Nel caso il soggetto produttore decida di rescindere, chiudere o interrompere il contratto di affidamento del servizio di conservazione, in qualsiasi momento può effettuare il **download** dei propri **pacchetti di distribuzione** in autonomia, attraverso la procedura di esibizione, o,

InfoCert S.p.A. – all rights reserved

in alternativa, richiedendo il **servizio di restituzione** (su supporto da concordare in base a volume ed esigenze) tramite apposito **modulo**.

Al termine della procedura di handover verso il nuovo Conservatore, i pacchetti verranno cancellati.

Seguendo i dettami dello standard OAIS, il versamento in InfoCert di pacchetti di distribuzione (PdD) provenienti da un altro Conservatore dovrà riguardare sempre **interi pacchetti**, qualsiasi sia il 'modo' con cui vengono formati e le tipologie di metadati o indici che hanno, e non dovrà mai riguardare il singolo documento. È fondamentale in questa procedura di versamento conservare in InfoCert quante più informazioni possibili sul processo di conservazione precedente e sul Conservatore di provenienza.

Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di handover e scarto'.

RICERCA ED ESIBIZIONE DEI DOCUMENTI CONSERVATI

La ricerca e l'esibizione a norma dei documenti conservati può avvenire tramite chiamate applicative o tramite portale WEB.

Le chiavi di ricerca sono i metadati popolati in fase di versamento.

I sistemi restituiscono un pacchetto di distribuzione, contente sia il documento conservato che tutti i report e le evidenze di conservazione.

La guida al portale LegalDoc WEB è disponibile qui:
https://knowledgecenter.infocert.digital/Home/Guida/manuale-utente-legaldoc-web?lang=it

La guida al portale SAFE LTA WEB è disponibile qui:

https://knowledgecenter.infocert.digital/Home/Guida/manuale-utente-safe-lta

InfoCert S.p.A. – all rights reserved

7. I SISTEMI DI CONSERVAZIONE

I sistemi sono organizzati su più siti nel territorio italiano, con applicazioni software in architettura distribuita, molteplici componenti e con una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, firme digitali e sigilli, supporti di conservazione).

I servizi sono accessibili online, tramite portale o chiamate applicative.

Dal punto di vista architetturale **LegalDoc** è realizzato utilizzando la tecnologia dei Web Services, secondo architettura REST su protocollo HTTPS. È protetto da firewall configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile. L'intero sistema viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria.

Dal punto di vista architetturale **SAFE LTA** è erogato in modalità SaaS (Software as a Service): si basa su tecnologie open-source che incorporano le specifiche dei blocchi di costruzione dell'eArchiving (Programma CEF: *Connecting Europe Facility*) e incorporano gli standard comuni per i pacchetti informativi E-ARK (*European Archival Records and Knowledge Preservation*), in coerenza con lo standard ISO 14721 recante il reference model OAIS (*Open Archival Information System*) utilizzato a livello internazionale per la conservazione di risorse digitali.

Si tratta di un'applicazione basata su architettura a microservizi integrata con altri servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, firma digitale, sigillo elettronico qualificato, ecc.).

SAFE LTA è erogato come servizio in *Hybrid-Cloud architecture* attraverso provider Amazon Web Services (AWS) su zona geografica italiana e risiede entro perimetri di virtual private cloud per ragioni di sicurezza. Il servizio è da considerarsi ibrido in quanto fa uso di diversi servizi InfoCert.

I servizi sono:

- Identity Provider InfoCert, in quanto Provider ed erogatore di servizi riferiti alla identità digitale,
- SignAPI InfoCert, in quanto Provider ed erogatore di servizi legati alla Certification Authority.

Sia le applicazioni WEB di interfaccia sia le API REST sono adoperabili solo previa autenticazione:

- l'autenticazione da interfaccia web è governata attraverso flusso di *authorization-code-flow*, così come previsto da standard,
- l'autenticazione da agenti software che integrano le API REST è governata da flusso di *client-credential-flow*, così come previsto da standard.

InfoCert S.p.A. – all rights reserved

SAFE LTA può essere facilmente integrato con altri sistemi attraverso API RESTful. Queste possono essere sfruttate nell'ambito di diverse funzionalità, incluse:

- Provisioning
- Gestione utenti, gruppi e autorizzazioni
- Invio in conservazione dei pacchetti di versamento e trasformazione in pacchetti di archiviazione E-ARK
- Attività di ricerca avanzata
- Recupero di documenti e metadati
- Download di pacchetti di distribuzione.

SAFE LTA non solo effettua la validazione di pacchetti di versamento, ma si occupa anche di effettuare una verifica formale dei formati.
L'autenticità dei dati inviati in conservazione è garantita dalla registrazione dei metadati PREMIS ogni qualvolta un'azione viene effettuata su un oggetto digitale.
Tutte le interazioni tra gli utenti e l'archivio sono registrate in appositi log per ragioni di sicurezza e trasparenza.
Ogni *endpoint* è protetto tramite autenticazione con Kong e Keycloak.

La configurazione degli ambienti di conservazione di SAFE LTA prevede le seguenti definizioni:

- **Company Group**: identifica un contenitore logico dal quale possono dipendere una o più Company, cioè aree di conservazione. Ogni Company Group è ad uso esclusivo di un solo cliente/titolare.
- **Company**: area di conservazione dei documenti, che può essere usata, ad esempio, per raggruppare i documenti delle diverse società/aziende di un gruppo (Company Group), denominando ogni Company con il nome della singola azienda facente parte del Gruppo.
- **Country**: identifica gli standard normativi adottati dal sistema per la conservazione rispetto alle varie geografie, ed è configurabile a livello di Company.
- **Document Class**: identifica una tipologia documentale con i suoi metadati. Ad esempio: fatture attive, contratti, libri e registri contabili, ecc.

La documentazione tecnica di dettaglio è disponibile su https://developers.infocert.digital/

FIRMA/SIGILLO DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, il Responsabile del servizio della conservazione di InfoCert appone una firma digitale (per LegalDoc) o un sigillo qualificato (per SAFE LTA) su ogni pacchetto di archiviazione. Il servizio utilizza un sistema automatico erogato dalla CA - Certification Authority — InfoCert.

MARCA TEMPORALE DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, viene apposta anche una marca temporale su

InfoCert S.p.A. – all rights reserved

ogni pacchetto di archiviazione. La marca temporale viene richiesta al TSS - *Time Stamping Service* - InfoCert, che la restituisce firmata con un certificato emesso dalla TSA - *Time Stamping Authority* - InfoCert. Il TSS è sincronizzato tramite i segnali forniti dai sistemi satellitari GPS, Galileo e GLONASS ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

STORAGE

L'intero sistema di conservazione viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria per la sicurezza.

Il sistema di conservazione di InfoCert e dei suoi partner tecnologici supporta la memorizzazione dei file sia su storage magnetici ad alte performance che su sistema Object Storage S3. Tali storage, scelti tra i primari fornitori di tecnologie presenti sul mercato, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato e rispondono all'esigenza di memorizzazione a lungo termine dei *fixed content*, ossia dei file che devono essere conservati con garanzia nel tempo di integrità e disponibilità del contenuto.

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni che prevedano la cifratura dei documenti che contengono dati sensibili ed eventualmente anche degli altri.

I sistemi di storage sono stati valutati da InfoCert e dai suoi partner tecnologici sotto molteplici profili e, in virtù delle loro caratteristiche fisiche e architetturali, sono ritenuti idonei ad essere utilizzati nel sistema di conservazione.

Per il sistema di *Object Storage S3* InfoCert si avvale dei servizi cloud computing Amazon Web Services (AWS) che garantisce la ridondanza e il rispetto delle misure di sicurezza.

SAFE LTA è interamente erogato su cloud AWS.

Per entrambi i servizi cloud è stata scelto AWS Europe (*Region Milan*), quindi, tutti i dati risiedono in **territorio italiano**.

SICUREZZA E PROTEZIONE DEI DATI

InfoCert si impegna a mantenere i più alti livelli di qualità e sicurezza, assegna un'importanza strategica alla gestione sicura delle informazioni e riconosce la necessità di sviluppare, mantenere, controllare e migliorare costantemente un **sistema di gestione della sicurezza delle informazioni (ISMS)** in conformità alla **norma UNI CEI EN ISO/IEC 27001: 2017**. Nella policy di sicurezza di InfoCert per ciascun capitolo della norma ISO vengono fornite le indicazioni da seguire nello svolgimento di tutte le attività. In particolar modo:

- *Management direction for information security,*
- *Organization of information security,*

InfoCert S.p.A. – all rights reserved

- *Human resource security,*
- *Asset management,*
- *Access control, Cryptography,*
- *Physical and environmental security,*
- *Operations security,*
- *Communications security,*
- *System acquisition, development, and maintenance,*
- *Supplier relationships,*
- *Information security incident management,*
- *Information security aspects of business continuity management,*
- *Compliance with legal and contractual requirements.*

InfoCert ha anche ottenuto il **Report SOC 2 Tipo II**, su sicurezza, disponibilità, integrità del trattamento, riservatezza e privacy dei servizi, in conformità all'International **Standard on Assurance Engagements (ISAE) 3000**.

I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio. L'azienda ha mappato tutti i flussi di dati interni e di quelli da e per l'esterno. Sono implementati controlli automatici per evitare l'interconnessione con server esterni non autorizzati. L'accesso alla rete e ai sistemi è consentito esclusivamente agli utenti autorizzati, seguendo quanto prescritto dalla policy aziendale relativa agli Amministratori di Sistema e alla gestione degli accessi logici. Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione. Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione. Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity e al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti.

A supporto di tali censimenti è stato implementato un CMDB (*Configuration Management Data Base*).

Viene effettuata una valutazione di impatto sulla protezione dei dati personali. Il ciclo di vita dei dati è definito e documentato.

Tutti gli accessi (fisici e logici) sono regolati da policy apposite. I diritti di accesso sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.

L'integrità di rete è protetta. Le reti di comunicazione e controllo sono protette.

I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili.

Sono attivi ed amministrati piani di *Incident Response* e di *Business Continuity, Incident Recovery, Disaster Recovery e Vulnerability Management.*

InfoCert S.p.A. – all rights reserved

I sistemi informativi, il personale e gli asset sono costantemente monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione. Sono implementati meccanismi che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse.

È attiva una policy di gestione dei log, inclusiva della conservazione dei log di sicurezza dei sistemi.

L'organizzazione ha implementato un processo formalizzato di *Incident Management* che include i criteri per documentare l'incidente ai fini del *problem management*, delle comunicazioni istituzionali e delle comunicazioni verso gli stakeholder.

Tutti gli utenti sono informati e addestrati.

Ai sensi del Regolamento UE n. 679/2016 GDPR, InfoCert assume il ruolo di Responsabile del trattamento dei dati personali. La nomina è inserita all'interno delle ''Specificità del Contratto — Atto di Affidamento''.

Il trattamento dei dati è effettuato:

- ai soli fini dell'erogazione del servizio,
- con l'adozione delle misure di sicurezza ex art. 32 del Regolamento
- nel rispetto degli obblighi posti in carico al Responsabile del trattamento dall'art. 28 del Regolamento.

PROCEDURE DI GESTIONE E MONITORAGGIO

I sistemi di conservazione di InfoCert e i processi da questi implementati rispondono interamente alle norme di legge che regolano la materia. La loro progettazione e il loro continuo miglioramento sono il frutto di una intensa opera di confronto tra le professionalità e le competenze delle diverse funzioni aziendali, al fine di giungere all'erogazione di servizi architetturalmente stabili, affidabili, e che garantiscano elevati livelli di servizio all'utente, in condizioni di assoluta sicurezza, certezza degli accessi e tracciabilità delle operazioni.

Punto fondante del processo di progettazione è l'attenta disamina delle norme e degli standard, al fine di definire puntualmente i requisiti di *compliance*. Oltre a questi sono definiti ulteriori requisiti funzionali, di architettura e di connettività e interoperabilità, anche in relazione con le evoluzioni tecnologiche, sfruttando le economie di scala e di conoscenza. I Responsabili InfoCert, infatti, sono costantemente impegnati nell'attività di *technology watch* attraverso la partecipazione a gruppi di lavoro nazionali e internazionali, forum e associazioni di settore, con lo scopo di monitorare e prevenire l'obsolescenza tecnologica sia logica che fisica.

Inoltre, InfoCert ha deciso di adottare un sistema di gestione dei servizi IT (SMS) conforme a **ISO IEC 20000** (standard internazionale di gestione dei servizi IT) al fine di mantenere e migliorare la qualità dei servizi aziendali che fornisce. Questi hanno un'attenzione particolare

InfoCert S.p.A. – all rights reserved

alle esigenze dei clienti, sostenuti da un ciclo continuo di monitoraggio, reporting e revisione degli SLA concordati.

Inoltre, InfoCert ha adottato un sistema di gestione dei servizi IT (SMS) certificato per la norma **ISO/IEC 20000-1:2018** (standard internazionale di gestione dei servizi IT) al fine di mantenere e migliorare la qualità dei servizi aziendali che fornisce. Questi hanno un'attenzione particolare alle esigenze dei clienti, sostenuti da un ciclo continuo di monitoraggio, reporting e revisione degli **SLA concordati**.

Tale modello di *Service Management System* ha permesso di:

- mappare ed integrare i Livelli di Servizio (SLA) garantiti ai clienti in relazione ai Livelli di servizio operativi garantiti internamente e quelli contrattuali garantiti dai fornitori;
- strutturare e governare la catena di composizione del valore dei servizi;
- ottimizzare la gestione dei processi aziendali integrando processi produttivi con processi di business fornendo un modello per la gestione sui servizi erogati;
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti;
- garantire un controllo dei fornitori che concorrono alla erogazione dei nostri servizi;
- migliorare la qualità dei servizi di business erogati.

Le attività di istituzione, attuazione, monitoraggio e sviluppo del Service Management System-SMS seguono il modello ciclico PDCA che si sviluppa nelle seguenti fasi:

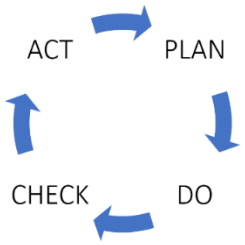

Figura 3 Rappresentazione del modello PDCA SMS

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche e i requisiti per la gestione dei servizi inerenti il campo di applicazione; si stabiliscono gli obiettivi di gestione del servizio a tutti i livelli pertinenti;
- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement continuo dei servizi sulla base di quanto definito nel service management plan, con particolare attenzione al controllo delle modifiche al SMS valutando e limitando I rischi;
- azioni di monitoraggio e revisione del sistema-SMS (Check);
- attuazione di misure a miglioramento del sistema-SMS (Act) ove sono pianificate e attuate idonee azioni correttive sulla base dei risultati della fase precedente.

InfoCert S.p.A. – all rights reserved

Il processo di gestione dei Livelli di Servizio [Service Level Management] è considerato un processo cardine del Service Management System in quanto ha effetto sui tre obiettivi principali quali:

- allineare i servizi di business con i bisogni correnti e futuri del cliente
- coordinare i requisiti del mercato sui servizi offerti con gli obbiettivi aziendali
- migliorare la qualità dei servizi di business erogati
- fornire attraverso gli SLA una base per la determinazione del valore del servizio.

Nello specifico InfoCert ha definito degli SLA baseline di riferimento in relazione ai seguenti KPI (*Key Performance Indicator*):

- orario di servizio
- disponibilità di servizio.

Inoltre, InfoCert si è dotata di una soluzione di monitoraggio denominata **NEW RELIC**, un Software as a Service che permette la completa gestione dei dati ai team DEVOPS.
Questa è una piattaforma di osservabilità di secondo livello, in grado di identificare e prevedere problemi di tipo infrastrutturale e applicativo.
Utilizzando un evoluto sistema di gestione e raccolta dati effettua un monitoring full-stack, fornisce gli strumenti per la prevenzione e l'ottimizzazione dei servizi, oltre ad un'efficiente gestione di segnalazione degli incident. Inoltre, è stata sviluppata l'integrazione con la piattaforma di controllo ***Cloudwatch***, tool nativo di AWS, che consente di avere il pieno controllo e la gestione delle metriche di tutte le componenti presenti in cloud.

Il tool è composto da tre elementi fondamentali:

- AGENT: risiedono sui server e collezionano le metriche inviando (con connessione unidirezionale) i dati alla piattaforma centrale posta in cloud attraverso protocollo TLS. Gli agent effettuano un controllo sia di tipo infrastrutturale che di performance, consentendo anche la costruzione di schemi architetturali tra i servizi;

- NEWRELIC ANALYTICS PLATFORM: è il cuore dello strumento, dove vengono raccolte ed elaborate le metriche e che consente di gestire, aggregare ed elaborare i dati, definendo la modalità di visualizzazione e gestione degli alert;

- LOCATIONS: server nei quali risiedono gli script che simulano la user experience, possono essere privati o pubblici e grazie a questa diversa collocazione è possibile verificare il corretto funzionamento di un servizio sia della rete interna che da rete pubblica.

Con le metriche raccolte si popola una base di dati in ottica di *business intelligence*, che risulta di fondamentale importanza per la redazione della reportistica riguardante gli SLA dei vari servizi ma anche, e soprattutto, per supportare i processi di decisione aziendale.
La soluzione di monitoraggio fin qui descritta risulta indispensabile per individuare e prevenire

InfoCert S.p.A. – all rights reserved

tempestivamente anomalie sui servizi erogati da InfoCert, segnalando in modo puntuale le componenti impattate.
Il monitoring della disponibilità del servizio viene svolta coerentemente con le procedure generali di InfoCert. In particolare, tutte le componenti costituenti il sistema di conservazione, ovvero i servizi applicativi, i processi di elaborazione batch e le interfacce per l'utente finale, sono monitorate con i tool definiti nella piattaforma NEW RELIC precedentemente descritta. A fronte di anomalie rilevate, lo strumento, grazie all'integrazione nativa, invia delle segnalazioni ad OPSGENIE, tool di gestione delle notifiche in conformità ai processi di Incident Management aziendali. Tali processi sono descritti nelle procedure che definiscono il Sistema di gestione integrato InfoCert.

CONTROLLI PERIODICI E AUDIT

In InfoCert è attiva una struttura appositamente preposta alla supervisione e controllo della gestione dei problemi e del rispetto dei livelli del sistema per tutte le applicazioni. La struttura si avvale di un gruppo di lavoro trasversale, ed effettua la raccolta dei dati relativi al funzionamento dei servizi. Il gruppo si riunisce periodicamente, al fine di individuare le cause dei malfunzionamenti registrati nel periodo, analizzare le soluzioni contingenti adottate per il superamento del problema e sviluppare eventuali proposte per rimedi strutturali.

Ad ogni semestre il Responsabile del servizio della conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento. Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).

Inoltre, il programma di audit aziendale è attuato secondo le procedure del Sistema Integrato di Gestione, con il fine di determinare se i processi aziendali sono:

- in accordo con quanto previsto nei documenti di riferimento
- *compliant* alla normativa di riferimento
- *compliant* agli standard adottati dai sistemi di conservazione
- attuati efficacemente
- idonei al conseguimento degli obiettivi della Qualità e miglioramento servizi.

L'audit è un processo fondamentale per lo screening dei sistemi, in quanto consente l'individuazione delle aree critiche d'intervento e la pianificazione dei necessari interventi, ragion per cui è svolto periodicamente.

In ogni processo aziendale, le modalità di audit sono improntate alle indicazioni dello standard UNI EN ISO 19011 ed hanno per oggetto:

- strutture organizzative

InfoCert S.p.A. – all rights reserved

- risorse utilizzate
- procedure
- processi
- prodotti e i risultati dell'attività
- documentazione
- addestramento
- segnalazioni dei clienti e terze parti.

Le attività di audit sono in capo all'area *Management System*, che le esegue direttamente o le delega a personale esterno qualificato.

A fronte di non conformità rilevate in sede di verifica ispettiva, il Responsabile del servizio valutata definisce un piano di attuazione delle azioni correttive o migliorative richieste.

InfoCert S.p.A. – all rights reserved

8. SPECIFICITÀ DEL CONTRATTO

Le ***Condizioni Generali di Contratto*** o ***Accordo Quadro*** regolano la vendita in generale di tutti i servizi InfoCert.

A questi tipicamente si aggiungono i seguenti allegati:

Allegato A — Offerta Commerciale,

Allegato B — DPA - *Data Processing Agreement*,

Allegato C — Allegato Tecnico,

Allegato D — Misure di Sicurezza,

Allegato E — Manuale Operativo.

Nell'**Allegato C — Allegato Tecnico** sono descritte le condizioni particolari di LegalDoc e SAFE LTA ed è inserito l'***Atto di Affidamento***, che rappresenta la formalizzazione della delega ad InfoCert del servizio di conservazione e stabilisce espressamente quali attività di fatto vengano assunte da InfoCert e quali, al contrario, rimangano a carico dell'affidatario, soggetto produttore, come stabilito dalle Linee Guida AgID.

Qui è maggiormente dettagliata anche l'infrastruttura tecnica e l'architettura di ciascun servizio.

Sono richiamati anche la ***Scheda dati tecnici d'attivazione*** per LegalDoc e il ***Submission Agreement*** per SAFE LTA, con cui il soggetto produttore/cliente/titolare fornisce tutte le informazioni necessarie su tipologie documentali, metadati, formati e utenze di accesso, per la configurazione degli ambienti di conservazione.

InfoCert S.p.A. – all rights reserved

Padova, 13/11/2023

CONFIGURAZIONE LEGALDOC

AMBIENTE DI PRODUZIONE

1. Dati di configurazione del servizio

Ragione sociale:	Comune di Vigonovo
Id bucket:	B48597
Codice account:	HE4141
Casella posta certificata:	protocollo.comune.vigonovo.ve@pecveneto.it
Data attivazione:	06/09/2016

2. User associate

2.1. HE414102

Accesso: Abilitato
Tipo di accesso: WebServices + Interfaccia
Viewer: Sola lettura
Impronta: Lettura e creazione

Tipologie documentali:

Tipologia documentale	Download	Conserva	Rettifica	Elimina	Ricerca
accatre_attiliq	SI	SI	SI	SI	SI
accatre_contratti	SI	SI	SI	SI	SI
accatre_decreti	SI	SI	SI	SI	SI
accatre_deliberazioni	SI	SI	SI	SI	SI
accatre_determinazioni	SI	SI	SI	SI	SI
accatre_docfisc	SI	SI	SI	SI	SI
accatre_docinterna	SI	SI	SI	SI	SI
accatre_docprot	SI	SI	SI	SI	SI
accatre_docrisum	SI	SI	SI	SI	SI
accatre_faelel	SI	SI	SI	SI	SI
accatre_listeel	SI	SI	SI	SI	SI
accatre_ordinanze	SI	SI	SI	SI	SI
accatre_regprot	SI	SI	SI	SI	SI
fata_pa	SI	SI	SI	SI	SI
fatp_pa	SI	SI	SI	SI	SI

2.2. HE414101

Accesso: Abilitato
Tipo di accesso: WebServices + Interfaccia
Viewer: Sola lettura
Impronta: Lettura e creazione

Tipologie documentali:

Tipologia documentale	Download	Conserva	Rettifica	Elimina	Ricerca
accatre_attiliq	SI	SI	SI	SI	SI
accatre_contratti	SI	SI	SI	SI	SI
accatre_decreti	SI	SI	SI	SI	SI
accatre_deliberazioni	SI	SI	SI	SI	SI
accatre_determinazioni	SI	SI	SI	SI	SI

Tipologia documentale	Download	Conserva	Rettifica	Elimina	Ricerca
accatre_docfisc	SI	SI	SI	SI	SI
accatre_docinterna	SI	SI	SI	SI	SI
accatre_docprot	SI	SI	SI	SI	SI
accatre_docrisum	SI	SI	SI	SI	SI
accatre_faelel	SI	SI	SI	SI	SI
accatre_listeel	SI	SI	SI	SI	SI
accatre_ordinanze	SI	SI	SI	SI	SI
accatre_regprot	SI	SI	SI	SI	SI
fata_pa	SI	SI	SI	SI	SI
fatp_pa	SI	SI	SI	SI	SI

3. Policy associate

3.1. P48443 - Policy standard

Formati di file ammessi alla conservazione:

File Mime	Descrizione
application/msword;2007	DOCX
application/odb;NA	ODB
application/odg;NA	ODG
application/pdf;NA	PDF
application/pkcs7;NA|application/msword;2007	DOCX firmato
application/pkcs7;NA|application/odb;NA	ODB firmato
application/pkcs7;NA|application/odg;NA	ODG firmato
application/pkcs7;NA|application/pdf;NA	PDF firmato
application/pkcs7;NA|application/vnd.ms-excel;2007	XLSX firmato
application/pkcs7;NA|application/vnd.ms-outlook;NA	MSG firmato
application/pkcs7;NA|application/vnd.ms-powerpoint;2007	PPTX firmato
application/pkcs7;NA|application/vnd.oasis.opendocument.graphics;NA	ODG firmato
application/pkcs7;NA|application/vnd.oasis.opendocument.presentation;NA	ODP firmato
application/pkcs7;NA|application/vnd.oasis.opendocument.spreadsheet;NA	ODS firmato
application/pkcs7;NA|application/vnd.oasis.opendocument.text;NA	ODT firmato
application/pkcs7;NA|image/gif;NA	GIF firmato
application/pkcs7;NA|image/jpeg;NA	JPG firmato
application/pkcs7;NA|image/tiff;NA	TIFF firmato
application/pkcs7;NA|message/rfc822;NA	EML firmato
application/pkcs7;NA|text/plain;NA	TXT firmato
application/pkcs7;NA|text/xml;1.0	XML firmato
application/pkcs7;na|application/msword;2007	
application/pkcs7;na|application/vnd.ms-excel;2007	
application/pkcs7;na|application/vnd.ms-outlook;na	
application/pkcs7;na|application/vnd.ms-powerpoint;2007	
application/pkcs7;na|application/vnd.oasis.opendocument.graphics;na	
application/pkcs7;na|application/vnd.oasis.opendocument.presentation;na	
application/pkcs7;na|application/vnd.oasis.opendocument.spreadsheet;na	
application/pkcs7;na|application/vnd.oasis.opendocument.text;na	
application/pkcs7;na|image/gif;na	
application/pkcs7;na|image/jpeg;na	
application/pkcs7;na|image/tiff;na	
application/pkcs7;na|text/plain;na	
application/pkcs7;na|text/xml;1.0	

File Mime	Descrizione
application/timestamp-reply;NA|application/msword;2007	docx marcato
application/timestamp-reply;NA|application/pdf;NA	PDF marcato
application/timestamp-reply;NA|application/pkcs7;NA|application/msword;2007	DOCX firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|application/pdf;NA	PDF firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|application/vnd.ms-excel;2007	XLSX firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|application/vnd.ms-outlook;NA	MSG firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|application/vnd.ms-powerpoint;2007	PPTX firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|application/vnd.oasis.opendocument.graphics;NA	
application/timestamp-reply;NA|application/pkcs7;NA|application/vnd.oasis.opendocument.presentation;NA	ODP firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|application/vnd.oasis.opendocument.spreadsheet;NA	ODS firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|application/vnd.oasis.opendocument.text;NA	ODT firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|image/gif;NA	GIF Firmato e Marcato
application/timestamp-reply;NA|application/pkcs7;NA|image/jpeg;NA	JPG firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|image/tiff;NA	TIFF firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|text/plain;NA	TXT firmato e marcato
application/timestamp-reply;NA|application/pkcs7;NA|text/xml;1.0	XML firmato e marcato
application/timestamp-reply;NA|image/jpeg;NA	JPG marcato
application/timestamp-reply;NA|image/tiff;NA	TIFF marcato
application/timestamp-reply;NA|message/rfc822;NA	EML marcato
application/timestamp-reply;NA|text/plain;NA	TXT marcato
application/timestamp-reply;NA|text/xml;1.0	XML marcato
application/timestamped-data;NA|application/odb;NA	ODB MARCATO
application/timestamped-data;NA|application/vnd.oasis.opendocument.graphics;NA	ODG MARCATO
application/timestamped-data;NA|application/vnd.oasis.opendocument.presentation;NA	ODP MARCATO
application/timestamped-data;NA|application/vnd.oasis.opendocument.spreadsheet;NA	ODS MARCATO
application/timestamped-data;NA|application/vnd.oasis.opendocument.text;NA	ODT MARCATO
application/timestampreply;NA|application/pkcs7;NA|application/pdf;NA	PDF firmato e marcato 2 - accatre
application/timestampreply;NA|application/pkcs7;NA|image/tiff;NA	

File Mime	Descrizione
application/timestampreply;NA|application/pkcs7;NA|text/plain;NA	
application/timestampreply;NA|application/pkcs7;NA|text/xml;1.0	
application/vnd.ms-excel;2007	XLSX
application/vnd.ms-outlook;NA	MSG
application/vnd.ms-powerpoint;2007	PPTX
application/vnd.oasis.opendocument.graphics;NA	ODG
application/vnd.oasis.opendocument.presentation;NA	ODP
application/vnd.oasis.opendocument.spreadsheet;NA	ODS
application/vnd.oasis.opendocument.text;NA	ODT
application/vnd.openxmlformats-officedocument.presentationml.presentation	PPT MS openxml
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet;NA	XLS MS openxml
image/gif;NA	GIF
image/jpeg;NA	JPG
image/tiff;NA	TIFF
message/rfc822;NA	EML
text/plain;NA	TXT
text/xml;1.0	XML

Formati di file indice ammessi:

File Mime	Descrizione
text/xml;1.0	XML

Tipologie documentali:

Nome	Descrizione	Controllo
accatre_contratti	Contratti	nessuno
accatre_deliberazioni	Deliberazioni	nessuno
accatre_regprot	Registro Giornaliero Protocollo	nessuno
fatp_pa	Fattura ricevuta PA	nessuno
accatre_faelel	Fascicolo Elettorale Elettronico	nessuno
fata_pa	Fattura emessa PA	nessuno
accatre_determinazioni	Determinazioni	nessuno
accatre_listeel	Liste elettorali	nessuno
accatre_attiliq	Atti di liquidazione	nessuno
accatre_decreti	Decreti	nessuno

Nome	Descrizione	Controllo
accatre_ordinanze	Ordinanze	nessuno
accatre_docinterna	Documentazione interna	nessuno
accatre_docprot	Documenti protocollati	nessuno
accatre_docfisc	Documenti fiscali	nessuno
accatre_docrisum	Documenti Risorse Umane	nessuno

Firmatario:

Nessun firmatario associato.

4. Campi di indice e controlli predefiniti per le Tipologie documentali

4.1. CONTRATTI - accatre_contratti

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
reg_importo	Importo_registrazione_d	NO	NO	-
Data documento	__data_documento_dt	SI	NO	-
Codice identificativo dell'amministratore	cod_amm_s	SI	NO	-
Codice identificativo AOO	cod_aoo_s	SI	NO	-
Contraente	contraente_s	SI	NO	-
Data stipula	data_stipula_dt	SI	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Indice di classificazione	id_class_s	NO	NO	-
Importo registrazione	importo_registrazione_d	NO	NO	-
Numero di repertorio	num_repertorio_s	SI	NO	-
Oggetto	oggetto_s	SI	NO	-
Data registrazione	reg_data_dt	NO	NO	-
Numero registrazione	reg_num_s	NO	NO	-
Serie registrazione	reg_serie_s	NO	NO	-

4.2. DELIBERAZIONI - accatre_deliberazioni

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
id_accatre	ID_univoco_ACCATRE_s	NO	NO	-
Data documento	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Codice identificativo dell'amministrazione	cod_amm_s	SI	NO	-
Codice Identificativo AOO	cod_aoo_s	SI	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Id registro	datregid_s	NO	NO	-
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Dirigente	dirigente_s	NO	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Indice di classificazione	id_class_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Numero di repertorio	num_repertorio_s	SI	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
Oggetto	oggetto_s	SI	NO	-
Organo deliberante	organo_delib_s	SI	NO	-
Responsabile procedimento	responsabile_s	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.3. REGISTRO GIORNALIERO PROTOCOLLO - accatre_regprot

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data chiusura	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Anno	anno_i	NO	NO	-
Codice fiscale soggetto prod	ccodice_fiscale_soggetto_prod_s	NO	NO	-
Codice identificativo dell'amministrazione	cod_amm_s	SI	NO	-
Codice identificativo AOO	cod_aoo_s	SI	NO	-
Codice fiscale destinatario	codice_fiscale_destinatario_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Codice fiscale responsabile	codice_fiscale_responsabile_s	NO	NO	-
Codice fiscale soggetto prod 2	codice_fiscale_soggetto_prod_2_s	NO	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Data prima registrazione	data_prima_reg_dt	NO	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Denominazione Amministrazione	denominazione_amm_s	NO	NO	-
Destinatario	destinatario_s	NO	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Indice di classificazione	id_class_s	NO	NO	-
Codice identificativo del registro	id_registro_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Numero fine	num_fine_s	SI	NO	-
Numero inizio	num_inizio_s	SI	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
Oggetto	oggetto_s	SI	NO	-
Numero progressivo del registro	progr_registro_i	NO	NO	-
Responsabile	responsabile_s	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice 2	soggcod_2_s	NO	NO	-
Soggetti - Codice 3	soggcod_3_s	NO	NO	-
Soggetti - Codice 4	soggcod_4_s	NO	NO	-
Soggetti - Codice 5	soggcod_5_s	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetto produttore 2	soggetto_prod_2_s	NO	NO	-
Soggetto produttore	soggetto_prod_s	NO	NO	-
Soggetti - Nominativo 2	soggnom_2_s	NO	NO	-
Soggetti - Nominativo 3	soggnom_3_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Soggetti - Nominativo 4	soggnom_4_s	NO	NO	-
Soggetti - Nominativo 5	soggnom_5_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo 2	soggru_2_s	NO	NO	-
Soggetti - Ruolo 3	soggru_3_s	NO	NO	-
Soggetti - Ruolo 4	soggru_4_s	NO	NO	-
Soggetti - Ruolo 5	soggru_5_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto 2	soggtip_2_s	NO	NO	-
Soggetti - Tipo soggetto 3	soggtip_3_s	NO	NO	-
Soggetti - Tipo soggetto 4	soggtip_4_s	NO	NO	-
Soggetti - Tipo soggetto 5	soggtip_5_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.4. FATTURA RICEVUTA PA - fatp_pa

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Periodo di imposta	__anno_fiscale_i	SI	NO	-
Data documento	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Allegati - Descrizione	allegdesc_s	NO	NO	-
Codice Identificativo Gara	cig_s	NO	NO	-
Codice Identificativo Gara	codice_cig_s	NO	NO	-
Codice Unitario Progetto	codice_cup_s	NO	NO	-
Codice fiscale emittente	codice_fiscale_emittente_s	SI	NO	-
Codice Fiscale	codice_fiscale_s	SI	NO	-
Codice Ufficio IPA	codice_pa_s	NO	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Codice Unitario Progetto	cup_s	NO	NO	-
Data protocollo	data_protocollo_dt	NO	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Denominazione emittente	denominazione_emittente_s	SI	NO	-
Denominazione	denominazione_s	SI	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-
Indentificativo univoco dato da SDI	identificativoSdi_s	SI	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Nome file SOGEI	nome_file_sogei_s	NO	NO	-
Numero documento - Numero Fattura	numero_documento_s	SI	NO	-
Numero protocollo attribuito dal ricevente	numero_protocollo_s	NO	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
Partita IVA emittente	partita_iva_emittente_s	SI	NO	-
Partita IVA	partita_iva_s	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice 1	soggcod_1_s	NO	NO	-
Soggetti - Codice 2	soggcod_2_s	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetti - Nominativo 1	soggnom_1_s	NO	NO	-
Soggetti - Nominativo 2	soggnom_2_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo 1	soggru_1_s	NO	NO	-
Soggetti - Ruolo 2	soggru_2_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto 1	soggtip_1_s	NO	NO	-
Soggetti - Tipo soggetto 2	soggtip_2_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Stato della Fattura	stato_fattura_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Parametro interno per identificare il flusso di alimentazione	token_flusso_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.5. FASCICOLO ELETTORALE ELETTRONICO - accatre_faelel

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Codice identificativo dell'amministrazione	cod_amm_s	SI	NO	-
Codice identificativo AOO	cod_aoo_s	SI	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Destinatario	dest_s	SI	NO	-
Cognome e Nome elettore	el_cne_s	SI	NO	-
Data di cancellazione elettore	el_dce_dt	NO	NO	-
Data di cancellazione elettore	el_dce_s	NO	NO	-
Data di nascita elettore	el_dne_dt	NO	NO	-
Data di nascita elettore	el_dne_s	SI	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Indice di classificazione	id_class_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Mittente	mitt_s	SI	NO	-
Modalita di formazione	modform_s	NO	NO	-
Numero protocollo	num_prot_s	SI	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
Oggetto	oggetto_s	NO	NO	-
Data protocollo	prot_data_dt	SI	NO	-
Numero protocollo	prot_num_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.6. FATTURA EMESSA PA - fata_pa

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Periodo di imposta	__anno_fiscale_i	SI	NO	-
Data documento	__data_documento_dt	SI	NO	-
Data inizio periodo di imposta	__data_inizio_numerazione_dt	SI	NO	-
Serie numerazione	__serie_s	NO	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Allegati - Descrizione	allegdesc_s	NO	NO	-
Codice CIG	codice_cig_s	NO	NO	-
Codice CUP	codice_cup_s	NO	NO	-
Codice fiscale emittente	codice_fiscale_emittente_s	SI	NO	-
Codice fiscale	codice_fiscale_s	SI	NO	-
Codice PA	codice_pa_s	NO	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Denominazione emittente	denominazione_emittente_s	SI	NO	-
Denominazione	denominazione_s	SI	NO	-
Indirizzo e-mail	email_destinatario_em	NO	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Identificativo SDI	identificativoSdi_s	NO	NO	-
Localita	localita_s	NO	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Nome file SOGEI	nome_file_sogei_s	NO	NO	-
Note	note_s	NO	NO	-
Numero documento	numero_documento_s	SI	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
Partita IVA emittente	partita_iva_emittente_s	SI	NO	-
Partita IVA	partita_iva_s	SI	NO	-
Provincia	provincia_s	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice 2	soggcod_2_s	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetti - Nominativo 2	soggnom_2_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo 2	soggru_2_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto 2	soggtip_2_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Parametro interno per identificare il flusso di alimentazione	token_flusso_s	NO	NO	-
Totale importo	totale_importo_d	NO	NO	-
Versione del documento	vers_i	NO	NO	-
Via	via_s	NO	NO	-

4.7. DETERMINAZIONI - accatre_determinazioni

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Codice identificativo dell'amministrazione	cod_amm_s	SI	NO	-
Codice identificativo AOO	cod_aoo_s	SI	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Id registro	datregid_s	NO	NO	-
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Dirigente	dirigente_s	NO	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Indice di classificazione	id_class_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Numero registro particolare	nr_reg_s	SI	NO	-
Numero di repertorio	num_repertorio_s	NO	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
Oggetto	oggetto_s	SI	NO	-
Responsabile procedimento	responsabile_s	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.8. LISTE ELETTORALI - accatre_listeel

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	__data_documento_dt	SI	NO	-
Responsabile procedimento	cod_amm_s	NO	NO	-
Codice identificativo AOO	cod_aoo_s	SI	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Descrizione lista	descr_lista_s	NO	NO	-
Descrizione verbale	descr_verb_s	NO	NO	-
destinatario	destinatario_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Numero verbale	nr_verb_s	SI	NO	-
oggetto	oggetto_s	SI	NO	-
Soggetto produttore	produttore_s	NO	NO	-
Responsabile procedimento	responsabile_s	NO	NO	-
sesso	sesso_s	SI	NO	-
Numero sezione	sezione_s	SI	NO	-
tipo	tipo_s	NO	NO	-
tipologia	tipologia_s	NO	NO	-

4.9. ATTI DI LIQUIDAZIONE - accatre_attiliq

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Codice identificativo amministrazione	cod_amm_s	SI	NO	-
Codice identificativo amministrazione	cod_aoo_s	SI	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Id registro	datregid_s	NO	NO	-
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Dirigente	dirigente_s	NO	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Indice di classificazione	id_class_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Verifica marca temporale	marc_b	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Numero registro particolare	nr_reg_s	NO	NO	-
Numero di repertorio	num_repertorio_s	NO	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
oggetto	oggetto_s	SI	NO	-
Responsabile procedimento	responsabile_s	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.10. DECRETI - accatre_decreti

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Codice identificativo amministrazione	cod_amm_s	SI	NO	-
Codice identificativo amministrazione	cod_aoo_s	SI	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Id registro	datregid_s	NO	NO	-
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Dirigente	dirigente_s	NO	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Indice di classificazione	id_class_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Numero registro particolare	nr_reg_s	NO	NO	-
Numero di repertorio	num_repertorio_s	NO	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
oggetto	oggetto_s	SI	NO	-
Responsabile procedimento	responsabile_s	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.11. ORDINANZE - accatre_ordinanze

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Codice identificativo amministrazione	cod_amm_s	SI	NO	-
Codice identificativo AOO	cod_aoo_s	SI	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Id registro	datregid_s	NO	NO	-
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Dirigente	dirigente_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Indice di classificazione	id_class_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Numero registro particolare	nr_reg_s	SI	NO	-
Numero di repertorio	num_repertorio_s	NO	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
oggetto	oggetto_s	SI	NO	-
Responsabile procedimento	responsabile_s	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.12. DOCUMENTAZIONE INTERNA - accatre_docinterna

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Data documento	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Allegati - Descrizione	allegdesc_s	NO	NO	-
Allegati - Indice IdDOC	allegiddoc_s	NO	NO	-
Codice identificativo amministrazione	cod_amm_s	SI	NO	-
Codice identificativo amministrazione	cod_aoo_s	SI	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Id registro	datregid_s	NO	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Descrizione	descrizione_s	NO	NO	-
Destinatario	destinatario_s	NO	NO	-
Dirigente	dirigente_s	NO	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
Prodotto software Nome	formnom_s	NO	NO	-
Prodotto software Produttore	formprod_s	NO	NO	-
Prodotto software Versione	formvers_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Indice di classificazione	id_class_s	NO	NO	-
Id - Aggregazione	idagg_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-
Identificativo Documento Principale	iddocprinc_s	NO	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Note	note_s	NO	NO	-
Numero registro particolare	nr_reg_s	NO	NO	-
Numero di repertorio	num_repertorio_s	NO	NO	-
oggetto	oggetto_s	SI	NO	-
Soggetto produttore	produttore_s	NO	NO	-
Responsabile procedimento	responsabile_s	NO	NO	-
Riservato	riservato_b	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice 1	soggcod_1_s	NO	NO	-
Soggetti - Codice 2	soggcod_2_s	NO	NO	-
Soggetti - Nominativo 1	soggnom_1_s	NO	NO	-
Soggetti - Nominativo 2	soggnom_2_s	NO	NO	-
Soggetti - Ruolo 1	soggru_1_s	NO	NO	-
Soggetti - Ruolo 2	soggru_2_s	NO	NO	-
Soggetti - Tipo soggetto 1	soggtip_1_s	NO	NO	-
Soggetti - Tipo soggetto 2	soggtip_2_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.13. DOCUMENTI PROTOCOLLATI - accatre_docprot

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
id_accatre	ID_univoco_ACCATRE_s	NO	NO	-
Data documento	__data_documento_dt	SI	NO	-
Allegati - Numero	alleg_i	NO	NO	-
Indice di classificazione	classificazione_s	NO	NO	-
Codice identificativo AOO	cod_aoo_s	NO	NO	-
Codice identificativo AOO	codice_aoo_s	NO	NO	-
Verifica conformita copie	cop_b	NO	NO	-
Data protocollo	data_prot_dt	SI	NO	-
Dati di registrazione - Data registrazione	datregdata_dt	NO	NO	-
Dati di registrazione - Tipologia di flusso	datregflusso_s	NO	NO	-
Dati di registrazione - Numero documento	datregnum_s	NO	NO	-
Dati di registrazione - Tipo registro	datregtipreg_s	NO	NO	-
Destinatario	dest_s	NO	NO	-
Verifica firma digitale	firm_b	NO	NO	-
Identificativo del formato	formid_s	NO	NO	-
ID doc algoritmo	iddocalg_s	NO	NO	-
ID doc identificativo	iddocid_s	NO	NO	-
ID doc Impronta	iddocimp_s	NO	NO	-
Indice fascicolo	indice_fascicolo_s	NO	NO	-
Verifica marca temporale	marc_b	NO	NO	-
Mittente	mitt_s	NO	NO	-
Modalita di formazione	modform_s	NO	NO	-
Numero protocollo	num_prot_i	SI	NO	-
Chiave descrittiva Oggetto	ogg_s	NO	NO	-
Oggetto	oggetto_s	NO	NO	-
Verifica sigillo	sig_b	NO	NO	-
Soggetti - Codice	soggcod_s	NO	NO	-
Soggetti - Nominativo	soggnom_s	NO	NO	-
Soggetti - Ruolo	soggru_s	NO	NO	-
Soggetti - Tipo soggetto	soggtip_s	NO	NO	-
Tipologia documentale	tipdoc_s	NO	NO	-
Tipo protocollo E-U-I	tipo_prot_s	NO	NO	-
Versione del documento	vers_i	NO	NO	-

4.14. DOCUMENTI FISCALI - accatre_docfisc

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Periodo di imposta	__anno_fiscale_i	SI	NO	-
Data documento	__data_documento_dt	SI	NO	-
Indice fascicolo	__indice_fascicolo_s	NO	NO	-
Codice identificativo AOO	codice_aoo_s	NO	NO	-
Codice Fiscale	codice_fiscale_s	SI	NO	-
Data protocollo	data_prot_dt	NO	NO	-
Denominazione	denominazione_s	SI	NO	-
Descrizione	descrizione_s	NO	NO	-
Destinatario	dest_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Mese di imposta	mese_fiscale_i	SI	NO	-
Mittente	mitt_s	NO	NO	-
Numero protocollo	num_prot_i	NO	NO	-
Oggetto	oggetto_s	SI	NO	-
Partita IVA	partita_iva_s	SI	NO	-
Numero di repertorio o registro	repertorio_i	SI	NO	-
Tipo allegato	tipo_allegato_s	SI	NO	-
Tipo documento	tipo_documento_s	SI	NO	-

4.15. DOCUMENTI RISORSE UMANE - accatre_docrisum

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Periodo di imposta	__anno_fiscale_i	SI	NO	-
Data documento	__data_documento_dt	SI	NO	-
Indice fascicolo	__indice_fascicolo_s	NO	NO	-
Codice identificativo AOO	codice_aoo_s	NO	NO	-
Codice Fiscale	codice_fiscale_s	SI	NO	-
Data protocollo	data_prot_dt	NO	NO	-
Denominazione	denominazione_s	SI	NO	-
Descrizione	descrizione_s	NO	NO	-
Destinatario	dest_s	NO	NO	-
ID univoco ACCATRE	id_accatre_s	NO	NO	-
Mese di imposta	mese_fiscale_i	SI	NO	-

Label	Indice	Controllo obbligatorietà	Controllo numerazione	Controllo continuità numerazione rispetto a
Mittente	mitt_s	NO	NO	-
Nominativo	nominativo_s	NO	NO	-
Numero protocollo	num_prot_i	NO	NO	-
Oggetto	oggetto_s	SI	NO	-
Numero di repertorio o registro	repertorio_i	NO	NO	-
Tipo allegato	tipo_allegato_s	SI	NO	-
Tipo documento	tipo_documento_s	SI	NO	-