Manuale di Conservazione
di Uni IT Srl

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	30/11/2018	Nadia Piazza	*Archivista del servizio di conservazione*
Verifica	30/11/2018	Rospocher Mauro	*Resp. della sicurezza dei sistemi per la conservazione*
Verifica	30/11/2018	Cazzanelli Stefano	*Resp. dei sistemi informativi per la conservazione*
Verifica	30/11/2018	Cazzanelli Stefano	*Resp. dello sviluppo e della manutenzione del sistema di conservazione*
Approvazione	30/11/2018	Benvenuti Carlo	*Resp. del servizio di Conservazione*

Codice documento: **IO0024**

Distribuzione: **Pubblica**

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	27/07/2015	Prima versione documento	
1.1	10/09/2015	Integrazione ai paragrafi 7.1 – 7.2 – 7.3 – 7.4 – 7.5 – 9.2.1 – 9.3	
1.2	01/10/2015	Integrazione al paragrafo 7.4	
1.3	06/06/2016	Rivisto layout manuale	
1.4	19/08/2016	Apportate modifiche richieste da AgID riguardanti aspetti formali	
1.5	01/07/2017	Revisione manuale	
1.6	09/02/2018	Integrazioni ai paragrafi 1 - 3.1 – 7.6 – 7.7.3 – 7.11 – 8.7 – 9.2 – 9.2.1	
1.7	20/11/2018	Cambio logo, correzione link pagina AgID, aggiornamento ruoli e organigramma	
1.8	30/11/2018	Aggiornamento ruoli e organigramma	

Sommario

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale del sistema di conservazione erogato da Uni IT Srl (di seguito per brevità chiamato anche "Manuale") ed è possibile reperirlo collegandosi alla pagina di Uni IT Srl del sito di AgID (https://www.agid.gov.it/it/piattaforme/spid/identity-provider-accreditati/it-srl). Illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, i processi inerenti al servizio, in particolare le modalità di versamento, archiviazione e distribuzione, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione ed alla verifica del funzionamento, nel tempo, del sistema di conservazione digitale di documenti informatici.

Il servizio pur essendo nativamente predisposto per la conservazione di ogni documento che rispetti i formati previsti, è rivolto principalmente agli Enti della Pubblica Amministrazione e non, ed alle Banche che utilizzano l'Ordinativo Informatico – per l'espletamento del servizio di Tesoreria

Il Manuale è costituito dalla versione corrente del presente documento.

In particolare, nel presente Manuale sono riportati:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del servizio di conservazione, descrivendo in modo puntuale, in caso di affidamento, i soggetti, le funzioni e gli ambiti oggetto dell'affidamento stesso;
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 dei documenti informatici sottoponibili a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti 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 della descrizione dei controlli effettuati su ciascuno specifico formato adottato;
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 documenti informatici devono essere oggetto di scarto/cancellazione;
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 i documenti.

Il Manuale recepisce le disposizioni di cui al D.Lgs. 7 marzo 2005, n. 82, e s.m.i. (Codice dell'amministrazione digitale), di seguito per brevità chiamato anche "Codice" o "CAD", oltre alle indicazioni riportate nei provvedimenti di legge o di prassi richiamati nel capitolo "Riferimenti normativi e di prassi" nonché i provvedimenti di natura tecnica richiamati nel capitolo "Riferimenti tecnici".

Il Cliente è tenuto a leggere con la massima attenzione il presente Manuale predisposto da Uni IT Srl ed in qualità di unico Responsabile della Conservazione, ne approva e ne fa propri i contenuti.

Torna al sommario

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale, i termini e le espressioni sotto elencate avranno il significato descritto nelle definizioni in esso riportate. Qualora le definizioni adottate dalla normativa di riferimento non fossero riportate nell'elenco che segue, si rimanda ai testi in vigore per la loro consultazione.
I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.
Ai fini della fruizione del Servizio di conservazione digitale dei documenti informatici descritto nel presente Manuale, valgono ad ogni effetto anche le definizioni contenute nel Contratto, da intendersi, pertanto, qui interamente riportate e trascritte, nonché le seguenti:

Torna al sommario

2.1 Glossario dei termini e Acronimi

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
Accesso	Operazione che consente a chi ne ha diritto di prendere visione dei documenti informatici conservati
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato che svolge attività di conservazione o di certificazione del processo di conservazione
Agente di alterazione	Qualsiasi codice contenuto in un documento informatico potenzialmente idoneo a modificare la rappresentazione dell'informazione senza alterarne il contenuto binario (in via meramente esplicativa e non esaustiva: macro, codici eseguibili nascosti, formule di foglio di lavoro occulte in tutto o in parte, sequenze di caratteri occultate all'interno dei documenti informatici)
Aggregazione documentale informatica	Raccolta di documenti informatici o 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 organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività

Archivio informatico	Archivio logico abbinato ad un codice fiscale/partita IVA, corrispondente ad una organizzazione pubblica o privata aderente al servizio, costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 e s.m.i
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 di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Base di dati	Collezione di dati registrati e correlati tra loro
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dell'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Chiusura del pacchetto di archiviazione	Operazione consistente nella sottoscrizione del pacchetto di archiviazione con firma digitale apposta da un Firmatario Delegato di Uni IT Srl e apposizione di una validazione temporale con marca temporale alla relativa impronta
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice o CAD	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
Codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto,

	dall'Agenzia per l'Italia Digitale o da un certificatore accreditato, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
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 e descritto nel Manuale di conservazione
Contrassegno a stampa	Contrassegno generato elettronicamente, apposto a stampa sulla copia analogica di un documento amministrativo informatico per verificarne provenienza e conformità all'originale
Coordinatore della Gestione Documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 e s.m.i. nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione
Descrittore evidenze	Vedi pacchetto informativo
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
DIRT	Documenti informatici rilevanti ai fini delle disposizioni tributarie
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
Documento analogico originale	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi
Documento originale unico	E' quel documento analogico il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta, anche presso terzi e che non soddisfa, dunque, alcuna

	delle condizioni elencate nella definizione di "Documento analogico originale"
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Il documento informatico ottenuto mediante la memorizzazione, sullo stesso supporto o su supporti diversi, della medesima sequenza di valori binari del documento originario
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia;
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
Fascicolo informatico	Raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo, nell'ambito della pubblica amministrazione. Per i soggetti privati è da considerarsi fascicolo informatico ogni aggregazione documentale, comunque formata, funzionale all'erogazione di uno specifico servizio o prestazione
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Firmatario delegato	Responsabile del servizio di conservazione o Persona formalmente delegata ad apporre la propria firma digitale sui Pacchetti di Archiviazione per conto di Uni IT Srl; questa persona può essere interna o esterna ad Uni IT Srl, laddove è giuridicamente possibile
Fruibilità di un dato	La possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione
Formato	Modalità di rappresentazione del documento informatico mediante codifica binaria; comunemente è identificato attraverso l'estensione del file e/o il tipo MIME

Fornitore esterno	Organizzazione che fornisce ad Uni IT Srl servizi relativi al suo sistema di conservazione dei documenti
Funzionalità aggiuntive	Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
Funzionalità interoperative	Le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Funzionalità minime	La componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Funzione di Hash	Una funzione matematica che genera, a partire da una evidenza informatica, una sequenza di bit (impronta) in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
idPdV	Indice del Pacchetto di Versamento
Immodificabilità	Caratteristica che rende la rappresentazione del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash

Insieme minimo di metadati del documento informatico	Complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato

Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di gestione	Strumento che descrive il sistema di gestione informatica dei documenti
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione
Normativa regolante la conservazione digitale di documenti informatici	Si intende: il D.lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione Digitale "CAD") e i relativi decreti attuativi, le regole tecniche e aggiungendo, per il documento informatico a rilevanza tributaria, le disposizioni di cui al DMEF 17 giugno 2014 e s.m.i., il DPR 26 ottobre 1972 n. 633 e s.m.i., il DPR 29 settembre 1973 n. 600 e s.m.i., i provvedimenti interpretativi emessi dagli organi competenti
Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e 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

Pacchetto di invio documenti	Pacchetto informativo utilizzato per inviare i documenti fisici al sistema di conservazione a seguito dell'avvenuta accettazione di un pacchetto di versamento;
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di conservazione
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei 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 e s.m.i.
Piano generale della sicurezza	Documento per la pianificazione delle 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
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici
Processo/servizio di marcatura temporale	E' il processo/servizio che associa in modo affidabile un'informazione e un particolare momento, al fine di stabilire prove attendibili che indicano il momento in cui l'informazione esisteva
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce – in proprio o attraverso specifico delegato

	- il *PdV (pacchetto di Versamento)* ed è responsabile del trasferimento del suo contenuto nel Sistema di Conservazione. Nelle pubbliche amministrazioni, tale ruolo è ricoperto dalle figure indentificate dal comma 3 dell'art 6 delle *Regole tecniche*
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
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
Registro particolare	Registro informatico specializzato per tipologia o per oggetto; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.
Registro di protocollo	Registro informatico della corrispondenza in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
Referente/i del Cliente	E'/sono le persone fisiche che il Cliente indica ad Uni IT Srl quali punti di riferimento tecnico ed organizzativo per gli aspetti che riguardano le comunicazioni relative all'erogazione del servizio di conservazione
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche che trattano il procedimento, ordinati secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi
Responsabile della Conservazione	E' il soggetto responsabile dell'insieme delle attività elencate dall'art. 7 comma 1 delle Regole tecniche
Responsabile del Servizio di Conservazione	E' la persona designata da Uni IT Srl a gestire il *SdC* affidato in outsourcing alla stessa dal *Titolare dei documenti informatici*. L'attività del *RSC* consiste nel gestire ed erogare il servizio di con-

	servazione come definito nel *contratto* e nel presente *Manuale di Conservazione* utilizzando strumenti e metodi conformi alla normativa vigente
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse culturale
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
Sistema di conservazione(SdC)	Insieme di hardware, software, politiche, procedure, linee guida, regolamenti interni, infrastrutture fisiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti del Cliente per il periodo di tempo specificato nel Contratto. Detto sistema tratta i documenti informatici in conservazione in pacchetti informativi che si distinguono in pacchetti di versamento, pacchetti di archiviazione e pacchetti di distribuzione
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.; per i privati è il sistema che consente la tenuta di un documento informatico
Staticità	Caratteristica che indica l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
Testo unico	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni;
Titolare/i	E' il Titolare dei Documenti Informatici

Titolare dei Documenti Informatici	E' il soggetto che, sottoscrivendo apposito contratto, affida ad Uni IT Srl le attività di conservazione dei propri documenti informatici (autoprodotti o acquisiti da terzi), che per legge o regolamento o per propria volontà è tenuto o comunque intenzionato a conservare. Tale figura generalmente va anche a ricoprire (direttamente o tramite proprio personale interno) il ruolo di *Produttore* previsto dalle *Regole tecniche*
Titolare del trattamento	La/e persona/e fisica/che o giuridica/che o altro tipo di società o ente che è/sono giuridicamente responsabili/e, anche unitamente ad altro titolare, delle decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza
Ufficio utente	Riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi
Versamento agli archivi di stato	Operazione con cui il responsabile della conservazione di un'amministrazione statale effettua l'invio 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

Torna al sommario

2.2 Abbreviazioni e termini tecnici

Abbreviazioni e termini tecnici	
Agenzia per L'Italia Digitale (già DigitPA)	Ente pubblico non economico, con competenza nel settore delle tecnologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione. L'Ente, che ha ereditato le funzioni di DigitPA che, a sua volta, ha ereditato le funzioni del CNIPA, opera secondo le direttive per l'attuazione delle politiche e sotto la vigilanza del Ministro per la pubblica amministrazione e l'innovazione, con autonomia

	tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale
ASP - Application Service Provider	Fornitore di Servizi Applicativi
CAD	Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni - "Codice dell'amministrazione digitale"
CA - Certificatore Accreditato	Soggetto autorizzato dall'Agenzia per l'Italia Digitale che garantisce l'identità dei soggetti che utilizzano la firma digitale
CC - Common Criteria	Criteri per la valutazione della sicurezza nei sistemi informatici, con riconoscimento internazionale in quanto evoluzione dei criteri europei (ITSEC), statunitensi (Federal Criteria), e canadesi (Canadian Criteria)
C.M. - Circolare Ministeriale;	
CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione	Creato con l'articolo 176 del DL 196/03, il CNIPA ha incorporato le strutture e le funzioni dell'AIPA e del Centro Tecnico della RUPA ed è stato quindi sostituito da DigitPA e quindi dall'AgID - Agenzia per l'Italia Digitale
CSCD - contratto di servizio di conservazione dei documenti	Contratto di servizio di conservazione dei documenti, ove sono esplicitate chiaramente l'ambito della delega conferita, le specifiche funzioni, le attività e le responsabilità affidate dal Cliente ad Uni IT Srl
D.LGS. - Decreto Legislativo;	
D.M. - Decreto Ministeriale;	
DNS – Domain Name System	Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet. Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http//www.....it) / in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3)
D.P.C.M.	Decreto del Presidente del Consiglio dei Ministri
D.P.R.	Decreto Presidente della Repubblica
DPS	Documento Programmatico per la Sicurezza
ETSI	European Telecommunications Standards Institute;
HSM - Hardware Security Module	Dispositivi hardware dedicati per la sicurezza crittografica e la gestione delle chiavi in grado di garantire un elevato livello di protezione
HTTP (Hypertext Transfer Protocol)	Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web
HTTPS (Secure Hypertext Transfer Protocol)	Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifratura dei dati trasmessi durante la consultazione di siti e pagine Internet.

	Corrisponde ad un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL
ICT - Information and Communication Technology	Tecnologia dell'Informazione e delle Telecomunicazioni. Il dipartimento che gestisce i sistemi informatici e telematici
INTERNET	Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. Lo sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW)
ISO – International Organization for Standardization	Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO
ITSEC – Information Technology Security Evaluation Criteria	Criteri europei per la valutazione della sicurezza nei sistemi informatici
MEF	Ministero dell'Economia e delle Finanze
NTP – Network Time Protocol	Protocollo per la sincronizzazione del tempo
OID – Object IDentifier	Sequenza numerica univoca che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO
PdV	Pacchetto di Versamento
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PU	Pubblico Ufficiale
PIN – Personal Identification Number	Codice di sicurezza riservato che permette l'identificazione del soggetto abbinato ad un dispositivo fisico. Permette ad esempio l'attivazione delle funzioni del dispositivo di firma;
POP – Point of Presence	Punto di accesso alla rete internet
PSCD - Prestatore di Servizi di Conservazione dei Dati	Nella fattispecie, Uni IT Srl
SSL – Secure Socket Layer	Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica
TSA - Time Stamping Authority;	
TSS - Time Stamping Service;	
TUDA - DPR 28 dicembre 2000, n. 445, e successive modificazioni - "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";	

URL – Uniform Resource Locator	Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http, ftp, file, telnet, news) specifica il protocollo di accesso all'oggetto
XML - Extensible Markup Language;	
WWW – World Wide Web	Insieme di risorse interconnesse da hyperlink accessibili tramite Internet

Torna al sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Il sistema di conservazione digitale di UNI IT Srl, è stato realizzato in conformità alla normativa vigente in materia di conservazione dei documenti informatici. Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990**, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000**, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo 30 giugno 2003, n. 196** e s.m.i. – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004, n. 42** e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82** e s.m.i. – Codice dell'amministrazione digitale (CAD);
- **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;
- **D.M. 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **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.
- **Il DPR nr. 1409 del 30 settembre 1963 -** (Legge archivistica) all'art. 30 prevede che le cartelle cliniche siano conservate illimitatamente. Secondo le norme vigenti, inoltre, gli originali cartacei delle cartelle cliniche in quanto originali unici, non possono essere distrutti;
- **Circolare Ministero della Sanità 19 dicembre 1986, n. 61 -** Circolare avente per oggetto il periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura
- **DM 14.2.1997 -** Norma di attuazione del D.lgs n.230/95, "Determinazione delle modalità

affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche, ai sensi dell'art. 111, comma 10, del decreto legislativo 17 marzo 1995, n. 230"

- **D.lgs 26 maggio 2000, n. 187 -** Attuazione della direttiva 97/43/Euratom in materia di protezione sanitaria delle persone contro i pericoli delle radiazioni ionizzanti connesse ad esposizioni mediche
- **Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere, 2005**
  Atto di indirizzo che reca indicazioni sui tempi di conservazione dei documenti generati e/o custodita Aziende Sanitarie pubbliche ed accreditate, redatto dal Ministero per i Beni e la Attività Culturali
- **Consiglio dei Ministri – Conferenza Stato Regioni 02 Marzo 2012 -** Linee Guida per la dematerializzazione della documentazione clinica in diagnostica per immagini. Normativa e prassi.

Torna al sommario

3.2 Standard di riferimento

Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato:

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)**Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **Dicom 3.0** (Digital Imaging and COmmunications in Medicine, immagini e comunicazione digitali in medicina)
- **Health Level 7 (HL7)** versione 2.3.1 e 2.5
- **Integrating the Healthcare Enterprise (IHE)**

Torna al sommario

4 RUOLI E RESPONSABILITÀ

Nel sistema di conservazione si individuano i seguenti ruoli principali:

Ruolo	Organizzazione di appartenenza
Produttore	Cliente
Responsabile della conservazione	Cliente
Referenti del Cliente	Cliente
Responsabile del servizio di conservazione	Uni IT Srl
Utente	Cliente/Terzi autorizzati

Uni IT Srl, quale **Responsabile del servizio di conservazione** digitale dei documenti informatici del Cliente, agisce nei limiti della delega ad essa conferita e nell'osservanza degli obblighi ivi previsti nonché nel rispetto della normativa regolante la conservazione digitale di documenti informatici e delle presenti prescrizioni; in particolare, essa agirà attraverso persone fisiche dalla stessa formalmente incaricate.

L'attività di Uni IT Srl riguarda la sola conservazione digitale dei documenti informatici del Cliente, senza alcuna responsabilità e/o possibilità di intervento sul contenuto degli stessi.

A carico del Responsabile del servizio di conservazione, non è posto alcun obbligo/dovere di elaborare i documenti informatici versati in conservazione al fine di estrarre i relativi metadati che, pertanto, dovranno essere forniti e associati ai rispettivi documenti a cura e carico del Cliente.

Il Responsabile del servizio di conservazione opera altresì nell'osservanza di quanto stabilito nel presente *Manuale*, al quale, se necessario, è sin da ora autorizzato ad apportare le modifiche, le integrazioni e gli aggiornamenti ritenuti necessari e/o conseguenti al mutato contesto tecnico-giuridico della normativa in materia.

L'utente è il soggetto che richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste nel presente *Manuale*.

Come già anticipato, il processo di conservazione impone al Cliente l'istituzione di una struttura ed una organizzazione interna, coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza alle disposizioni normative di riferimento e di quanto previsto dal presente *Manuale,* dal *Contratto* e dai rispettivi allegati.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla conservazione digitale dei propri documenti informatici sia dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro all'interno della propria organizzazione affinché esso venga svolto secondo i principi stabiliti dalla normativa in materia nonché dalle specifiche regole tecniche.

Torna al sommario

4.1 Profili professionali all'interno della struttura organizzativa Uni IT

Il processo di conservazione prevede una serie di attività che implicano il concorso di numerosi soggetti, a differenti livelli e con diverse responsabilità; in particolare prevede le seguenti **figure responsabili**:

1. Responsabile del servizio di conservazione;
2. Responsabile della funzione archivistica di conservazione;
3. Responsabile esterno del trattamento dei dati personali;

4. Responsabile della sicurezza dei sistemi per la conservazione;
5. Responsabile dei sistemi informativi per la conservazione;
6. Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Di seguito le **attività associate a ciascuna delle figure sopra elencate**:

1. **Responsabile del servizio di conservazione**
   - 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 del sistema di conservazione in conformità alla normativa vigente;
   - corretta erogazione del servizio di conservazione all'ente produttore;
   - gestione delle convenzioni, 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;
   - ogni altra attività affidata, con Atto di affidamento, dal Responsabile della Conservazione del Cliente

2. **Responsabile della funzione archivistica di conservazione**
   - definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, 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 col Cliente ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

3. **Responsabile del trattamento dei dati personali**
   - garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;
   - garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

4. **Responsabile della sicurezza dei sistemi per la conservazione**
   - Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;
   - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

5. **Responsabile dei sistemi informativi per la conservazione**

- gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore e segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive;
- pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione;
- controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

6. **Responsabile dello sviluppo e della manutenzione del sistema di conservazione**

- coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;
- pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;
- monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;
- interfaccia col Cliente relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

Ciascuno dei responsabili sopra elencati potrà eventualmente avvalersi, per lo svolgimento delle attività al medesimo attribuite, di addetti ed operatori formalmente incaricati.

Nella pagina seguente sono riportati i dati dei soggetti che nel tempo hanno assunto particolari funzioni e responsabilità con riferimento al sistema di conservazione.

Ruoli e responsabilità

Cognome	Nome	Ruolo	Responsabilità	Data nomina (gg/mm/aaaa)	Data cessazione (gg/mm/aaaa)
Benvenuti	Carlo	Responsabile del servizio di conservazione	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 del sistema di conservazione in conformità alla normativa vigente; corretta erogazione del servizio di conservazione al Cliente; gestione delle convenzioni, 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.	15/11/2018	
Pisoni	Elisabetta	Responsabile del servizio di conservazione	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 del sistema di conservazione in conformità alla normativa vigente; corretta erogazione del servizio di conservazione al Cliente; gestione delle convenzioni, 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.	02/08/2007	30/11/2018
Piazza	Nadia	Responsabile della funzione archivistica di conservazione	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, 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;	01/11/2018	

			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 col Cliente ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.		
Stecchini	Simona	Responsabile della funzione archivistica di conservazione	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, 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 col Cliente ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	21/07/2015	31/10/2018
Benvenuti	Carlo	Responsabile del trattamento dei dati personali	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con	01/12/2018	

			garanzia di sicurezza e di riservatezza.		
Pisoni	Elisabetta	Responsabile del trattamento dei dati personali	Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	02/08/2007	30/11/2018
Rospocher	Mauro	Responsabile della sicurezza dei sistemi per la conservazione	Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	26/06/2015	
Cazzanelli	Stefano	Responsabile dei sistemi informativi per la conservazione	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore; segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	26/06/2015	
Cazzanelli	Stefano	Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;	26/06/2015	

			interfaccia col Cliente relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.		

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

In questo capitolo sono indicate le strutture organizzative coinvolte nel servizio di conservazione comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione

5.1 Organigramma

La figura in basso riporta le strutture organizzative coinvolte nel servizio di conservazione dalla data 01/12/2018:

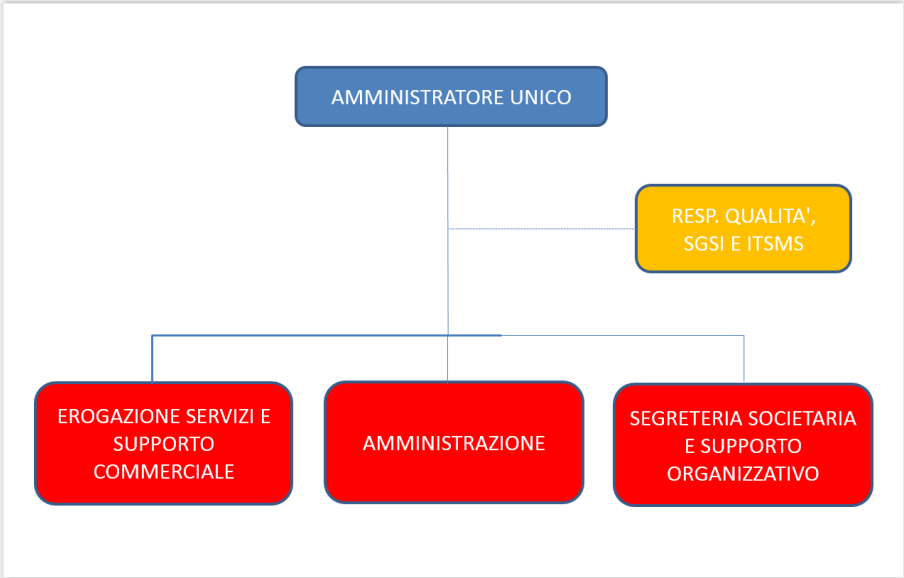

Figura 1: Rappresentazione grafica delle strutture organizzative della Società coinvolte nel servizio di conservazione.

In colore Azzurro sono evidenziati i Ruoli decisionali, in Giallo le Funzioni di Qualità e Controllo, in Rosso quelle direttamente coinvolte nell'erogazione del Servizio.

Torna al sommario

5.2 Strutture organizzative e Ruoli

Nello specifico le strutture funzionali dell'organizzazione operano in sinergia come segue:

Le attività relative al servizio di conservazione coinvolgono vari settori dell'organizzazione di **Uni IT Srl** che interagiscono tra loro al fine di garantire la gestione di tutte le esigenze del produttore dei documenti. Specificamente, le attività impattano sulle seguenti strutture organizzative/ruoli:

- *Amministratore Unico: per la formalizzazione delle procedure interne per la gestione dei rischi dell'organizzazione. A valle della fase di analisi dei rischi approva il piano di mitigazione e sicurezza presentato dal Responsabile della Sicurezza. L'Amministratore Unico definisce i parametri contrattuali relativi al servizio di conservazione;*
- *Amministrazione per la fase di definizione e predisposizione della contrattualistica, nonché per il seguimento amministrativo/contabile del servizio stesso;*
- *Erogazione Servizi e Supporto Commerciale* per lo sviluppo, mantenimento e monitoraggio del sistema, Help Desk e, coadiuvata dal *Responsabile del Servizio di Conservazione* e dal *Responsabile della Funzione Archivistica di Conservazione,* per le fasi di setup dell'integrazione tra i sistemi del produttore ed il sistema di conservazione. Il Direttore Tecnico ricopre anche il ruolo di *Responsabile dei Sistemi Informativi per la Conservazione* e *Responsabile per lo Sviluppo del Sistema di Conservazione*;
- *Responsabile del Servizio di Conservazione:* per la definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;
- *Responsabile dei Sistemi Informativi per la Conservazione* per il monitoraggio complessivo del sistema di conservazione;
- *Responsabile per lo Sviluppo del Sistema di Conservazione* per la correzione di eventuali anomalie applicative che dovessero emergere nel processo di conservazione;
- *Responsabile della Funzione Archivistica di Conservazione*, per la 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;
- *Responsabile della sicurezza dei sistemi per la Conservazione* per il rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione. Ricopre anche il ruolo di *Responsabile del Sistema di Gestione della Sicurezza Informatica* e del *Sistema di Gestione della Qualità*.

Torna al sommario

5.3 Responsabilità e funzioni nel processo di conservazione

Di seguito sono indicati i compiti, le responsabilità e le funzioni di firma in relazione alle diverse fasi del processo di conservazione digitale.

Fasi del processo	Descrizione delle fasi del processo di conservazione		COMPITI	RESPONSABILITA'	FIRMA
FASE 1	**Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico**				
	Descrizione sintetica	Il sistema di conservazione riceve l'indice del pacchetto di versamento contenente le informazioni sugli oggetti digitali che saranno inviati in conservazione.	**SC**	**DT**	**==**
FASE 2	**Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione**				
	Descrizione sintetica	Viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard della procedura. Viene verificato che il PdV venga versato nei termini contrattuali e di servizio stabiliti col produttore	**SC**	**DT**	**==**
FASE 3	**Preparazione del rapporto di conferma**				
	Descrizione sintetica	Il sistema, una volta effettuate le verifiche dell'IPdV rimane in attesa dell'invio dei documenti	**SC**	**DT**	**==**
FASE 4	**Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o**				

	non conformità				
	Descrizione sintetica	Il sistema scarta l'intero pacchetto e invia notifica in automatico	**SC**	**DT**	**==**
FASE 5	**Ricezione e verifica dei documenti**				
	Descrizione sintetica	Per ognuno di documenti inviati viene verificato che l'hash del documento informatico sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata. Vengono inoltre effettuati controlli di leggibilità, integrità e che i documenti non siano già presenti a sistema	**SC**	**DT**	**==**
FASE 6	**Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte**				
	Descrizione sintetica	Il sistema genera in automatico il rapporto di versamento per ognuno dei PdV che ha superato i controlli qualitativi	**SC**	**DT**	**==**
FASE 7	**Sottoscrizione del rapporto di versamento con firma digitale apposta da Uni IT Srl**				
	Descrizione sintetica	Il sistema provvede in automatico alla sottoscrizione digitale del rapporto di versamento con certificato del RSC e alla marcatura temporale del rapporto.	**SC**	**DT**	**RSC**

FASE 8	**Preparazione e gestione del pacchetto di archiviazione**				
	Descrizione sintetica	Il sistema genera il pacchetto di archiviazione secondo le modalità descritte al cap. 9	**SC**	**DT**	**==**
FASE 9	**Sottoscrizione del pacchetto di archiviazione con firma digitale apposta da Uni IT Srl e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del pacchetto di archiviazione"**				
	Descrizione sintetica	Come previsto da normativa l'indice del pacchetto di archiviazione, viene sottoscritto digitalmente dal RSC, una volta passato nello stato "conservato".	**SC**	**DT**	**RSC**
FASE 10	**Preparazione e sottoscrizione con firma digitale del Responsabile del servizio di conservazione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente**				
	Descrizione sintetica	Come previsto da normativa il PdD viene sottoscritto digitalmente dal RSC	**SC**	**DT**	**RSC**
FASE 11	**Produzione di duplicati informatici o di copie informatiche effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico**				
	Descrizione sintetica	Richieste di duplicati o copie informatiche vengono sottoscritte digitalmente dal RSC in modo da attestarne l'autenticità rispetto al documento sorgente	**SC**	**DT**	**RSC**
FASE 12	**Eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal contratto di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso**				
	Descrizione sintetica	Una volta scaduti i termini di conservazione previsti dal contratto, il sistema provvede a inviare una mail di notifica al cliente, il quale potrà decidere in autonomia se cancellarli dal sistema.	**SC**	**DT** **RP**	**==**

Legenda:
- **DT –** Direttore Tecnico Responsabile dell'Unità *Erogazione Servizi e Supporto Commerciale*
- **RP** - responsabile privacy
- **RSC** - Responsabile del servizio di conservazione
- **SC** - Sistema di conservazione

Torna al sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Descrizione delle tipologie dei documenti sottoposti a conservazione

Come chiaramente esplicitato nel *Contratto*, il servizio di conservazione digitale dei documenti informatici non riguarda la conservazione di documenti analogici di alcun tipo e genere.

Prima dell'attivazione del servizio il Cliente esplicita la tipologia di documenti che intende sottoporre a conservazione mediante il servizio offerto da Uni IT Srl, evidenziandone le caratteristiche nell'apposito allegato del *Contratto*.

Per ogni formato definito viene individuato anche il **software necessario per la visualizzazione** del documento informatico.

Uni IT Srl configura sul servizio un profilo di conservazione per ogni tipologia/classe di documenti su indicazione del Cliente, classificato come omogeneo in base ai dati da utilizzare per l'indicizzazione ed i termini di conservazione (vedi apposito allegato al *Contratto*).

Ogni variazione di formato di documento e di software associato per la visualizzazione oppure dei dati utilizzati per l'indicizzazione deve essere preventivamente concordato con Uni IT Srl e configurato sul servizio.

Il sistema di conservazione digitale dei documenti informatici è impostato per accettare le seguenti tipologie di documenti informatici:
- Documenti informatici;
- Documenti amministrativi;
- Documenti rilevanti ai fini tributari;
- Altri documenti in genere

Le diverse tipologie di documenti sono prodotte/formate/emesse a cura e sotto l'esclusiva responsabilità del Cliente mediante una delle seguenti principali modalità:
a) redazione tramite l'utilizzo di appositi strumenti software;
b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari;
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Al fine di garantire l'identificazione certa del soggetto che ha formato il documento, i documenti informatici versati in conservazione saranno in genere sottoscritti con firma digitale del Cliente e dovranno essere identificati in modo univoco e persistente.

E' prevista la possibilità di depositare in conservazione documenti informatici non sottoscritti. In tal caso deve necessariamente essere preventivamente dichiarata, per ogni classe/tipo di documento, nell'apposito allegato del *Contratto*.

Torna al sommario

6.2 Copie informatiche di documenti analogici originali unici

Come noto, l'art. 22 del CAD stabilisce che:

a) (comma 2) le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.
b) (comma 3) le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

Pertanto, alla luce di quanto sopra, il Cliente qualora intendesse depositare in conservazione copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico è tenuto, a propria cura e spese, a predisporre quanto necessario per ottemperare a quanto previsto dalle richiamate disposizioni.

In particolare, sarà cura e carico del Cliente:

1. produrre la copia per immagine su supporto informatico del documento analogico mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto;

successivamente, in alternativa:

2. dovrà sottoscrivere con firma digitale la copia per immagine del documento analogico (ai fini di quanto stabilito dall'articolo 22, co. 3, del CAD);
3. laddove richiesto dalla natura dell'attività, (art. 22, comma 2, del CAD), dovrà inserire nel documento informatico contenente la copia per immagine, l'attestazione di conformità all'originale analogico. Il documento informatico così formato dovrà poi essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata di pubblico ufficiale a ciò autorizzato.

Si tenga presente che l'attestazione di conformità delle copie per immagine su supporto informatico di uno o più documenti analogici, effettuata per raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia, può essere prodotta, sempre a cura e carico del Cliente, come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Tale documento informatico separato dovrà essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

In sostanza, in questi casi il Cliente dovrà alternativamente depositare in conservazione:

- la copia per immagine su supporto informatico dell'originale analogico contenente l'attestazione di conformità all'originale analogico debitamente sottoscritto come sopra riportato;

oppure

- le copie per immagine su supporto informatico unitamente all'attestazione di conformità prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni singola copia per immagine, debitamente sottoscritto come sopra riportato.

Torna al sommario

6.3 Formati gestiti

Come noto, la leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato. Il formato di un documento informatico è la convenzione usata per rappresentare il contenuto informativo mediante una sequenza di byte.

Il sistema di conservazione UNI IT Srl garantisce la conservazione dei documenti prodotti nei formati previsti dall'allegato 2 "Formati" del DPCM 03-12-2013.

I formati ammessi alla conservazione, devono essere specificati dal Cliente prima del versamento in conservazione e per tale ragione vengono esplicitati all'interno del Contratto di servizio stipulato con UNI IT Srl.

Torna al sommario

6.3.1 Caratteristiche generali dei formati

I formati scelti devono essere, puntualmente richiamati nel *Contratto*. UNI IT Srl, comunque raccomanda un insieme di formati che sono stati dalla stessa valutati in funzione di alcune caratteristiche quali:

	caratteristica	descrizione della caratteristica
1	**APERTURA**	Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse. In relazione a questo aspetto, Uni IT Srl ha privilegiato formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS.
2	**SICUREZZA**	La sicurezza di un formato dipende da due elementi: - grado di modificabilità del contenuto del file; - capacità di essere immune dall'inserimento di codice maligno.
3	**PORTABILITÀ**	Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto si ottiene mediante l'impiego fedele di standard documentati e accessibili e dalla loro diffusione sul mercato.
4	**FUNZIONALITÀ**	Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione del Cliente per la formazione e gestione del documento informatico.
5	**SUPPORTO ALLO SVILUPPO**	Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).

6	**DIFFUSIONE**	La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

Torna al sommario

6.3.2 Formati consigliati per la conservazione

Oltre al soddisfacimento delle caratteristiche suddette, nella scelta dei formati idonei alla conservazione, UNI IT Srl è stata estremamente attenta affinché i formati stessi fossero in grado di far assumere al documento le fondamentali caratteristiche di immodificabilità e staticità.

Pertanto, alla luce delle suddette considerazioni, **i formati consigliati da UNI IT SRL** per la conservazione delle diverse tipologie di documenti informatici sono i seguenti:

Formato	**Descrizione**	
XML	Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio: SVG usato nella descrizione di immagini vettoriali, XBRL usato nella comunicazione di dati finanziari, ebXML usato nel commercio elettronico, SOAP utilizzato nello scambio dei messaggi tra Web Service	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Contenuto di evidenze informatiche, dei pacchetti di versamento, archiviazione e distribuzione, ecc.
	Sviluppato da	W3C - http://www.w3.org/
	Estensione	.xml
	Tipo MIME	Application/xml Text/xml
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da W3C – http://www.w3.org/XML/
	Altre caratteristiche	E' un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	Qualsiasi editor di testo.

Formato	**Descrizione**
PDF/A	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. Questo formato è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.
	Caratteristiche e dati informativi

	Informazioni gestibili	Testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.
	Sviluppato da	Adobe Systems - http://www.adobe.com/
	Estensione	.pdf
	Tipo MIME	Application/pdf
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 19005-1:2005 (vesr. PDF 1.4)
	Altre caratteristiche	Assenza di collegamenti esterni
		Assenza di codici eseguibili
		Assenza di contenuti crittografati
		Il file risulta indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo
		Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A
		Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.
	Software necessario alla visualizzazione	Adobe Reader

Formato	**Descrizione**	
EML	Electronic Mail Message (EML) è un formato di testo che definisce la sintassi di messaggi di posta elettronica scambiati tra utenti	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Messaggi di posta elettronica e PEC
	Sviluppato da	Internet Engineering Task Force (IETF) - http://www.ietf.org/
	Estensione	.eml
	Tipo MIME	Message/rfc2822
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da IETF - http://www.ietf.org/rfc/rfc2822.txt
	Altre caratteristiche	E' un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	La maggior parte dei client di posta elettronica supportano la visualizzazione di file eml

Per quanto concerne il formato degli allegati al messaggio di posta elettronica, valgono le indicazioni di cui sopra. I formati EML sono accettati solamente per le classi documentali di tipo "PEC".

Torna al sommario

6.3.3 Identificazione

L'associazione del documento informatico al suo formato può avvenire, attraverso varie modalità, tra cui le più impiegate sono:

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].doc identifica un formato sviluppato dalla Microsoft;
2. il magic number: i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 identifica i file immagine di tipo .jpeg;
3. verifica della corrispondenza tra il tipo MIME ricavato dall'estensione del file ed il tipo MIME ricavato dal magic number;
4. l'utilizzo di tool automatici specifici come Apache TIKA

Per identificare il formato dei files posti in conservazione occorre procedere all'analisi di ogni singolo documento informatico contenuto all'interno dei pacchetti di versamento. Uni IT Srl procede come segue:

1	**Fase di IDENTIFICAZIONE**	Ogni documento che viene inviato al sistema di conservazione deve essere stato precedentemente ed espressamente indicato dal sistema versante. In questo modo tutti i documenti non noti vengono automaticamente non riconosciuti e quindi rifiutati
2	**Fase di RICEZIONE**	Il sistema Uni IT Srl, una volta noti i documenti che il Cliente vuole mettere in conservazione si mette in attesa, secondo i canali concordati, della loro ricezione
3	**Fase di VALIDAZIONE**	Una volta che i documenti vengono recepiti dal sistema di conservazione la prima elaborazione effettuata sugli stessi è quella del rilevamento della tipologia corretta del documento. Solo se questo esame restituisce esito positivo vengono realizzate ulteriori validazioni atte a garantire la correttezza formale del documento, secondo gli standard qui esposti e gli accordi convenuti col Cliente

Torna al sommario

6.3.4 Verifica della leggibilità dei documenti informatici

Per assicurare la leggibilità dei documenti informatici Uni IT Srl potrà adottare una delle seguenti misure:

a) conservare in sicurezza, per tutto il tempo in cui il documento informatico è mantenuto nel suo formato originale, il software necessario all'esibizione del dato. Dove necessario, Uni IT Srl dovrà avere la disponibilità anche del relativo hardware così come di qualsiasi altro dispositivo richiesto per la presentazione dei documenti informatici. Questo obiettivo può essere raggiunto acquisendo o conservando in proprio l'hardware e i dispositivi, come anche assicurandosene l'utilizzo presso fornitori esterni;
b) conservare le specifiche del formato del documento informatico, garantendo che esisteranno applicazioni software in grado di esibire i documenti nei formati ammessi. Questo secondo modo può essere utilizzato solo se le specifiche del formato in questione sono disponibili.

Uni IT Srl, dal canto suo, deve avere in essere procedure idonee a verificare l'effettiva leggibilità dei documenti informatici conservati; tali procedure sono eseguite a intervalli idonei a garantire l'individuazione tempestiva di un degrado nella leggibilità, almeno come previsto dalla normativa regolante la conservazione digitale di documenti informatici.

Esempi di "degrado" sono:

c) danneggiamento del supporto usato per la memorizzazione del dato;
d) alterazione di alcuni bit del dato.

Il controllo di leggibilità eseguito da Uni IT Srl è di due tipologie:

- controllo di leggibilità: consiste nel verificare che i singoli bit degli oggetti siano tutti correttamente leggibili. Questo fornisce garanzia del buono stato del supporto di memorizzazione.
- controllo di integrità: consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema. Questo fornisce una ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

La combinazione dei due tipi di controllo descritti non fornisce però garanzia di poter visualizzare correttamente il documento e che lo stesso sia effettivamente intellegibile dall'uomo.

Infatti questa garanzia non può essere fornita senza entrare nel merito del documento stesso. La garanzia della corretta visualizzazione del documento è d'altro canto garantita dalla scelta del formato PDF/A per i documenti conservati. Questo formato possiede infatti la caratteristica intrinseca di fornire leggibilità a lungo termine oltre all'ulteriore garanzia di essere basato su specifiche pubbliche (ISO 19005-2005).

Pertanto, il Cliente, preso atto che depositare in conservazione documenti informatici in formati diversi da quelli indicati nel presente capitolo potrebbe pregiudicare la corretta visualizzazione dei documenti medesimi nonché il loro contenuto semantico, se ne assume ogni responsabilità.

Torna al sommario

6.3.5 Migrazione dei formati

Particolarmente delicata è l'operazione di migrazione dei formati, operazione, questa, che potrà essere necessaria nei casi di obsolescenza dei formati.

Il problema che si pone è quello di capire se il contenuto del file di partenza e di arrivo è rimasto inalterato. In altre parole è necessario capire se le *significant properties* si sono conservate.

E' necessario quindi impostare dei test di controllo che, inevitabilmente dovranno essere automatici. Sulla base dello specifico formato divenuto obsoleto e sulla base del nuovo formato di destinazione scelto per l'operazione di migrazione verranno scelti quanti e quali controlli sul buon esito della conversione inserire.

Le specifiche dei formati di partenza e di destinazione saranno decisive e determinanti per l'individuazione dei controlli da attuare.

Torna al sommario

6.4 Metadati da associare alle diverse tipologie di documenti

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento

informatico, escluse quelle che costituiscono il contenuto del documento stesso. I metadati riguardano principalmente, ma non esclusivamente, i modi, i tempi ed i soggetti coinvolti nel processo della formazione del documento informatico, della sua gestione e della sua conservazione.

Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento. I metadati che seguono devono essere associati al documento dal Cliente prima del versamento in conservazione.

I metadati forniti dal Cliente restano di proprietà del Cliente medesimo.

I metadati, seppur chiaramente associati al documento informatico, possono essere gestiti indipendentemente dallo stesso. In relazione ai diversi tipi di documenti informatici posti in conservazione, è previsto un "**set minimo"** di metadati conformi a quello indicato dal DPCM del 3 dic. 2013.

Oltre al set minimo di metadati, il Cliente potrà decidere di associare al documento informatico eventuali ulteriori metadati c.d. "*extrainfo*" che, al pari del set minimo di metadati, saranno oggetto di indicizzazione da parte del sistema. I metadati *extrainfo* dovranno essere puntualmente individuati nello spazio ad essi riservato nell'apposito allegato del *Contratto* e verranno opportunamente gestiti da Uni IT Srl come in esso concordato.

Torna al sommario

6.5 Modalità di assolvimento dell'imposta di bollo sui documenti posti in conservazione

Il Cliente è tenuto al pagamento dell'imposta di bollo eventualmente dovuta sui documenti depositati in conservazione.

Pertanto, il versamento dell'imposta dovuta dovrà essere effettuata dal Cliente nei termini previsti dall'art. 6 del DMEF 17 giugno 2014 e nei modi di cui all'art. 17 del D.Lgs. 9 luglio 1997, n. 241 e loro successive modificazioni e/o integrazioni.

Tutti i relativi e conseguenti obblighi, adempimenti e formalità per l'assolvimento dell'imposta di bollo sui documenti informatici posti in conservazione sono ad esclusivo onere e carico del Cliente, il quale dovrà attenersi alle disposizioni di legge ed ai documenti di prassi emanati ed emanandi.

Allo stesso modo, sono ad esclusivo onere e carico del Cliente tutte le comunicazioni da presentare al competente Ufficio delle entrate in forza di quanto stabilito dalla normativa regolante la conservazione digitale di documenti informatici.

Torna al sommario

6.6 Pacchetto di versamento

In questo paragrafo sono fornite le tipologie di pacchetto di versamento gestite e per ciascuna di esse descritta la struttura dati.

Il nostro standard prevede l'indice di un pacchetto di versamento che si caratterizza per le seguenti parti:

- area di identificazione del PDV;

- area di identificazione dei documenti costituenti il pacchetto e composta dai seguenti elementi:
  - metadati obbligatori;
  - metadati extra-info.

Nella prima parte il dato importante e obbligatorio è il *pdvid* ovvero l'identificativo del PDV. Esso deve essere unico all'interno dello spazio gestito dal produttore, quindi indipendentemente dall'archivio.

La seconda parte prevede una lista di elementi, uno per ogni documento da versare. Ogni singolo file deve essere per prima cosa identificato. A questo scopo sono necessari i seguenti dati:
- nome file
- algoritmo di hashing per la generazione dell'impronta
- impronta del documento

Inoltre, poiché il sistema deve controllare la tipologia di documento per valutarne l'aderenza alle condizioni espresse in fase di contratto, deve essere indicato il MIME type del documento.

Per rimanere poi aderenti alla norma vigente devono essere passati anche un id unico dei singoli documenti del pacchetto e la data di chiusura degli stessi.

L'ultima parte dell'Indice contiene un insieme di metadati extra-info, così come definiti in fase contrattuale col Produttore.

Torna al sommario

6.6.1 Specifiche Pacchetto di Versamento

Le specifiche del Pacchetto di Versamento secondo lo standard definito da Uni IT Srl, sono disponibili all'interno del manuale tecnico inviato al Cliente in fase di attivazione del servizio.

Torna al sommario

6.7 Pacchetto di archiviazione

In questo paragrafo viene resa la struttura del pacchetto di archiviazione nonché il trattamento dei pacchetti di archiviazione.

Specifiche Pacchetto di archiviazione

Il Pacchetto di Archiviazione è composto da varie parti:

- insieme degli elementi (documenti e/o altri PdA) che compongono il pacchetto;
- IPdA ovvero l'Indice del Pacchetto di Archiviazione che elenca tutti gli elementi del pacchetto.

Il formato dell'IPdA è aderente allo standard UNISInCRO ed è marcato temporalmente e firmato elettronicamente con certificato del Responsabile del servizio di conservazione.

Torna al sommario

6.8 Pacchetto di distribuzione

Il pacchetto di distribuzione contiene l'insieme degli elementi (documenti e/o PdA) precedentemente ricercati e selezionati dall'utente.

Viene offerto sotto forma di un archivio .zip che per ogni elemento contiene:

- una cartella contenente l'elemento stesso. Nel caso di un documento il documento stesso, nel caso di un PdA l'intero PdA, ovvero tutti gli elementi di cui è costituito
- un'altra cartella che contiene l'indice relativo all'elemento individuato, marcato temporalmente e firmato elettronicamente con certificato del Responsabile del servizio di conservazione

Torna al sommario

6.9 Documenti rilevanti ai fini delle disposizioni tributarie

In considerazione di quanto previsto dall'art. 21, co. 5, del CAD[1], i documenti informatici rilevanti ai fini delle disposizioni tributarie (di seguito, per brevità chiamati anche "**DIRT**") sono conservati nel rispetto di quanto previsto dalle disposizioni in materia, attualmente riconducibili al Decreto del 17 giugno 2014 del Ministero dell'Economia e delle Finanze e successive modificazioni ed integrazioni.

Il Cliente, pertanto, è tenuto a conoscere le disposizioni relative alla normativa regolante la conservazione digitale di documenti informatici in vigore ed a controllare l'esattezza dei risultati ottenuti con l'utilizzo del Servizio di conservazione fornito da Uni IT Srl.

Formazione, emissione e trasmissione dei documenti fiscalmente rilevanti

Ai fini tributari, la formazione, l'emissione, la trasmissione, la copia, la duplicazione, la riproduzione, l'esibizione, la validazione temporale e la sottoscrizione dei documenti informatici, deve avvenire a cura del Cliente nel rispetto delle regole tecniche adottate ai sensi dell'art. 71 del decreto legislativo 7 marzo 2005, n. 82, e dell'art. 21, comma 3, del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633, in materia di fatturazione elettronica

Immodificabilità, integrità, autenticità e leggibilità dei documenti fiscalmente rilevanti

I documenti informatici rilevanti ai fini tributari devono avere le caratteristiche dell'immodificabilità, dell'integrità, dell'autenticità e della leggibilità, e devono essere utilizzati i formati previsti dal decreto legislativo 7 marzo 2005, n. 82 e dai decreti emanati ai sensi dell'art. 71 del predetto decreto legislativo nonché quelli individuati nel presente Manuale. Detti formati devono essere idonei a garantire l'integrità, l'accesso e la leggibilità nel tempo del documento informatico.

Pertanto, tutti i DIRT che vengono versati in conservazione devono essere statici ed immodificabili, ossia privi di qualsiasi agente di alterazione.

[1] Art. 21, co. 5 del CAD: "Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.";

Il Cliente dovrà assicurarsi e garantire che i DIRT che versa in conservazione abbiano le suddette caratteristiche sin dalla loro formazione e, in ogni caso, prima che siano depositati nel sistema di conservazione.

A tale fine, i DIRT, salvo diverso e circostanziato accordo col Responsabile del servizio di conservazione, devono essere prodotti nel formato PDF/A in conformità a quanto previsto dal presente *Manuale* e dal Manuale Tecnico inviato al Cliente al momento dell'attivazione del servizio.

Ordine cronologico e non soluzione di continuità per periodo di imposta

Posto che l'art. 3 del Decreto MEF 17.06.2014 stabilisce che i documenti informatici devono essere conservati in modo tale da rispettare le norme del codice civile, le disposizioni del codice dell'amministrazione digitale e delle relative regole tecniche e le altre norme tributarie riguardanti la corretta tenuta della contabilità, il Cliente deve farsi carico di versare in conservazione i propri documenti informatici assicurando, ove necessario e/o previsto dalle norme e/o dai principi contabili nazionali, l'ordine cronologico dei medesimi e senza che vi sia soluzione di continuità in relazione a ciascun periodo d'imposta o anno solare.

In altre parole, gli obblighi richiamati dall'art. 3 del DM 17.06.2014, essendo riferibili a norme riguardanti la corretta tenuta della contabilità, sono posti a completo ed esclusivo carico del Cliente.

Ciò comporta che il Cliente, nell'eseguire il versamento in conservazione dei DIRT, dovrà rispettare le regole di corretta tenuta della contabilità e procedere secondo regole uniformi, nell'ambito del medesimo periodo d'imposta o anno solare.

Funzioni di ricerca

Uni IT Srl non fornisce, in fase di formazione dei documenti, alcuna funzionalità di indicizzazione degli stessi che, quindi, è posta ad esclusivo carico e sotto la responsabilità del Cliente il quale dovrà associare, al documento informatico immodificabile ed in relazione ad ogni classe/tipologia documentale, i metadati previsti dalla legge (anche tributaria) e dalle regole tecniche di cui all'art. 71 del CAD e, più in generale, dalla vigente normativa in materia o gli eventuali ulteriori metadati riportati nell'Elenco documenti in conservazione; i suddetti metadati dovranno essere generati dal Cliente durante la fase di produzione/formazione/emissione dei documenti informatici.

Pertanto, è il Sistema di Gestione documentale del Cliente che deve assicurare l'indicizzazione dei DIRT in merito al formato, allo stato, alle caratteristiche (fiscali) di ogni singolo DIRT ed ai metadati "minimi" previsti dal Decreto MEF del 17 giugno 2014 (nome, cognome, denominazione, codice fiscale, partita IVA, data e associazioni logiche di questi) e dal presente *Manuale* nel capitolo 6.4.

Per sfruttare appieno le potenzialità del processo di conservazione dei DIRT non è sufficiente attenersi alle regole tecniche previste dalla norma, ma è necessario che il Cliente si attenga scrupolosamente ad un progettato ciclo di gestione dei DIRT, con il fine di predisporli ed organizzarli sin dalla loro formazione in modo tale da massimizzare la facilità del loro reperimento, prestando particolare attenzione alla fase di classificazione ed organizzazione. Dal puntuale svolgimento di quanto sopra dipende la facilità del loro reperimento.

A tale fine, è necessario che, in relazione ad ogni classe documentale, il Cliente associ ad ogni DIRT i metadati previsti dal presente *Manuale* (ed, eventualmente, degli ulteriori previsti nell'apposito allegato del *Contratto*) necessari per adempiere agli obblighi imposti dalle disposizioni in materia.

Il sistema di conservazione garantisce, le necessarie funzioni di ricerca dei DIRT conservati sulla scorta dei metadati ad essi associati.

Classificazione dei DIRT secondo aggregazioni per "Tipo documento"

Il Sistema di Gestione documentale del Cliente, oltre ad assicurare il formato, l'indicizzazione, l'apposizione del riferimento temporale, la sottoscrizione con firma digitale di ogni DIRT dallo stesso prodotto, deve provvedere altresì alla classificazione per tipologia di documento in conformità a quanto previsto dall'apposito allegato al Contratto.

Torna al sommario

6.9.1 Modalità di assolvimento dell'imposta di bollo sui DIRT

Come precisato nel precedente paragrafo 6.5L'imposta di bollo nonché tutti gli obblighi e le formalità per l'assolvimento dell'imposta sui DIRT, qualora dovuta, sono ad esclusivo onere e carico del Cliente, il quale dovrà attenersi alle disposizioni di legge (art. 6, del DMEF del 17 giugno 2014) ed ai documenti di prassi emanati ed emanandi.

Torna al sommario

6.10 Trattamento dei pacchetti di archiviazione contenenti documenti rilevanti ai fini delle disposizioni tributarie

Il processo di conservazione dei DIRT è effettuato nel rispetto delle regole di cui al DMEF del 17 giugno 2014 e successive modificazioni ed integrazioni.

Nello specifico, il processo di conservazione prende avvio con il versamento in conservazione del pacchetto di versamento prodotto dal Cliente e termina (ergo, "*viene chiuso in conservazione*") con l'apposizione di una marca temporale sul pacchetto di archiviazione.

Con riferimento ai DIRT, il processo di conservazione, in forza di quanto stabilito dall'art. 3 del DMEF del 17 giugno 2014, è effettuato entro il termine previsto dall'art. 7, comma 4-ter, del decreto-legge 10 giugno 1994, n. 357, convertito con modificazioni dalla legge 4 agosto 1994, n. 489 e s.m.i..

Pertanto, il Cliente dovrà provvedere a trasmettere ad Uni IT Srl il pacchetto di versamento, contenente i DIRT da sottoporre a conservazione, rigorosamente entro i termini stabiliti nell'apposito allegato del *Contratto*; tale termine è necessario ad Uni IT Srl per "chiudere" in conservazione il pacchetto di archiviazione entro i termini perentori previsti dalla legge.

Torna al sommario

7 IL PROCESSO DI CONSERVAZIONE

In questo capitolo sono riportate tutte le fasi inerenti il processo di conservazione dei documenti informatici

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Come già anticipato in altre parti del presente *Manuale*, unico responsabile del contenuto del pacchetto di versamento è il Cliente (Produttore), che deve formarlo, sottoscriverlo con firma digitale (ove previsto) e trasmetterlo al sistema di conservazione secondo le modalità operative di versamento definite nel presente *Manuale,* nel *Contratto* e nei rispettivi allegati.

L'operazione di versamento consiste nella trasmissione dei documenti da conservare e dei metadati che li specializzano, così come già accennato precedentemente.

La ricezione e presa in carico di un pacchetto di versamento segue uno schema logico di funzionamento che si articola in due fasi distinte: ricezione dell'Indice del Pacchetto di Versamento (IPdV) e ricezione dei documenti che fanno parte del Pacchetto di Versamento (PdV).

L'uno e gli altri possono essere trasmessi al sistema di conservazione attraverso canali diversi. Alternativamente essi possono essere:

- interfaccia web;
- invocazione di metodi tramite web service REST;
- invio in allegato a una mail PEC;
- trasferimento via protocollo FTP.

Ogni canale messo a disposizione è provvisto di opportuni accorgimenti per la trasmissione dei dati in modalità sicura:

- interfaccia web che viaggia su protocollo HTTPS;
- web service REST contattabile tramite protocollo HTTPS;
- PEC che, nativamente, garantisce l'autenticità della provenienza e la notifica di consegna in modalità sicura;
- server FTP raggiungibile via SFTP.

Per il completamento delle operazioni di conservazione di un PdV non è necessario scegliere esclusivamente uno dei canali sopra citati. La ricezione, anche in maniera asincrona, dei singoli componenti di un PdV possono arrivare anche da canali diversi.

Il sistema di conservazione prende in carico un PdV solo dopo che tutte le sue parti (IPdV e relativi documenti) vengono correttamente ricevute e superano con esito positivo i relativi controlli.

Tale operazione viene ufficialmente sancita dalla produzione del cosiddetto Rapporto di Versamento (RdV) che viene inviato o reso disponibile al cliente secondo le modalità previste dall'accordo contrattuale.

Poiché la produzione del RdV rappresenta formalmente la presa in carico del PdV da parte del sistema di conservazione, il RdV viene marcato temporalmente e firmato digitalmente direttamente dal Responsabile del servizio di conservazione o da altro soggetto da questi appositamente delegato.

Torna al sommario

7.1.1 Registrazioni log

I log relativi ai singoli versamenti riportano l'oggetto (indice o documento), il risultato dell'operazione (ok o errore), data e ora e l'utente che ha fatto l'operazione. In particolare vengono loggate le seguenti operazioni:

1. creazione di un nuovo PdA;
2. ricezione di un nuovo indice di versamento che viene accettato e/o rifiutato – con esito e motivazione del rifiuto (es. classe non prevista, DocID duplicati, etc.);
3. ricezione di un nuovo documento che viene accettato e/o rifiutato – con esito e motivazione del rifiuto (es. file name o Hash non corrispondenti, file type non previsto, etc.);
4. validazione di un pacchetto di versamento che avviene a pacchetto completo (indice + documenti);
5. conservazione del Pacchetto di Archiviazione.

Nel caso di errore vengono inviati via PEC al produttore messaggi dettagliati. Vi è la possibilità anche di configurare una callback e ricevere alcuni degli eventi sopra riportati in formato json.

Inoltre sempre via PEC viene inviato il Rapporto di Versamento (di fatto è la presa in carico ufficiale del pacchetto) e il Rapporto di Conservazione, al Responsabile della Conservazione.

Se il versamento viene fatto tramite canale WEB per i casi 2 e 3 il rifiuto è immediato e reso disponibile all'utente tramite interfaccia WEB. Nel caso di versamenti effettuati tramite canale Web service/FTP l'esito è messo a disposizione nell'apposito log scaricabile con richiesta effettuabile via WS/FTP. Nel caso in cui un pacchetto di versamento risulta incompleto e non viene quindi validato vengono mandati messaggi PEC (o altro canale sicuro definito nel contratto) che segnalano la problematica che ne impedisce la validazione. Tale messaggio viene inviato ogni 8 ore per un massimo di 7gg dalla data di creazione del PdA. Il pacchetto rimane a sistema e viene "marcato" come incompleto. Il produttore riceve una segnalazione via PEC per ogni PdA incompleto

Se dopo 7gg i PdA incompleti non vengono corretti o completati si procede alla parziale conservazione dei pacchetti di versamento corretti o alla rimozione totale nel caso non ci siano PDV validi. Il produttore riceve via PEC il dettaglio delle cancellazioni effettuate su un PdA incompleto.

Torna al sommario

7.1.2 Ricezione dell'indice del pacchetto di versamento

L'IPdV è un'evidenza informatica, ovvero un file, che descrive il versamento stesso e i documenti che ne fanno parte attraverso l'uso di metadati. Questi sono di carattere diverso a seconda che descrivano proprietà e qualità del pacchetto in genere o dei singoli documenti.

E' bene sottolineare che ogni PdV può contenere esclusivamente documenti della stessa tipologia, ovvero della stessa Classe Documentale. In questo senso l'elenco dei metadati dei singoli documenti è in qualche modo omogeneo.

Per consentire l'elaborazione automatica dei metadati il sistema di conservazione di Uni IT Srl richiede l'incapsulamento degli stessi in un determinato formato XML, che di fatto costituisce l'IPdV.

In tale file sono contenute sezioni diverse che identificano la qualità dei metadati. Essi infatti possono essere caratteristici del PdV e del soggetto versante, rappresentare direttive speciali di elaborazione per la conservazione e, infine, essere descrittivi dei singoli documenti che si vogliono conservare.

La struttura dell'indice del pacchetto di versamento, come indicato al paragrafo 6.6.1 è descritta nel manuale tecnico inviato al Cliente in fase di attvazione del servizio.

La funzione di ricezione degli indici dei pacchetti di versamento nel sistema di conservazione effettua, per ogni indice, i seguenti controlli:

- abilitazione alla conservazione da parte del sistema di gestione documentale versante e in particolare dell'utente che effettua il versamento. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- controllo formale dell'indice versato. In particolare viene verificato che sia un formato XML valido per una delle Classi Documentali registrate a sistema. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- verifica, tramite l'id univoco contenuto nell'indice, dell'eventuale presenza del PdV già nel sistema. In caso di esito positivo il nuovo indice sostituisce in toto il vecchio. Di conseguenza vengono aggiornati tutti i metadati, tutti i documenti eventualmente versati e non più presenti nel nuovo indice vengono cancellati dal sistema e viene restituito un warning al Cliente
- controllo sulla completezza e correttezza formale dei metadati, in relazione alla Classe Documentale rilevata. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- controllo sulla tipologia di documenti che si vuole versare. Ogni documento deve appartenere ad almeno uno dei formati ammessi dalla tipologia di Classe Documentale. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- eventuali controlli supplementari definiti insieme al Cliente. La gestione degli esiti negativi va formalizzato in sede contrattuale

Torna al sommario

7.1.3 Ricezione documenti associati ad un pacchetto di versamento

La ricezione dell'IPdV permette al sistema di conservazione di registrare i metadati del PdV e di mettersi in attesa dei documenti per la conservazione del pacchetto.

Relativamente al singolo documento tra i metadati indicati nell'IPdV sono di particolare importanza quelli utili all'identificazione dello stesso. Essi sono principalmente due: un identificativo univoco utile all'identificazione human readable del documento e un hash del file stesso, ovvero una stringa di caratteri che normalizza con un particolare algoritmo in maniera univoca il documento stesso.

In particolare l'hash, che per il sistema di conservazione Uni IT Srl deve essere in formato SHA256 base64, garantisce la riconoscibilità e incorruttibilità del documento in forma automatica e univoca.

Nel momento in cui un documento viene ricevuto da uno qualsiasi dei canali esposti precedentemente, ne viene calcolato l'hash in SHA265 e base64. Se il risultato è tra quelli precedentemente comunicati in uno dei IPdV ricevuti e non ancora in conservazione, allora il file viene accettato.

Successivamente la funzione di ricezione dei documenti informatici nel sistema di conservazione effettua una serie di controlli atti a verificare formalmente leggibilità, integrità e corrispondenza del documento alle regolamentazioni stabilite per la Classe Documentale di appartenenza. Per operare ciò il sistema determina il formato dello stesso sulla base di quanto esposto in precedenza (estensione e mime type).

La mancata identificazione del formato del file causa il rifiuto dello stesso con conseguente restituzione di un errore.

Una volta individuato il formato del documento viene controllato che questo sia tra i formati ammessi per la Classe Documentale di appartenenza. Nel caso di esito negativo il file viene

rifiutato e viene restituito un errore. Superati i primi controlli, ne vengono operati degli altri relativamente alla qualità dello stesso.

In relazione a ciascun documento informatico infine viene verificato:

- che non sia già presente nel sistema di conservazione;
- che il salvataggio avvenga correttamente all'interno del sistema di conservazione.

Tutti i documenti informatici che non superano anche uno solo dei precedenti controlli **vengono rifiutati**. In questo caso non viene salvata alcuna informazione sul sistema di conservazione ed il documento non conforme viene immediatamente eliminato.

Quando tutti i documenti di un pacchetto di versamento vengono ricevuti correttamente viene reso disponibile il rapporto di versamento sottoscritto con firma digitale dal Responsabile del servizio di Conservazione.

Tale rapporto viene anche inviato o reso disponibile al cliente secondo l'accordo contrattuale.

Torna al sommario

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Le funzionalità attivate nel processo di versamento/acquisizione del pacchetto di versamento prevedono dei controlli sia nella fase di ricezione dell'indice del PdV che sui singoli documenti inviati e corrispondenti a quanto previsto nell'indice stesso. La tabella riportata in basso elenca le diverse tipologie di controlli effettuati e per ognuna di esse indica l'azione prevista dal sistema. Quest'ultima può tradursi in una operazione di scarto o notifica di un warning.

Controlli dell'indice del Pacchetto di versamento

Un pacchetto di versamento può contenere unicamente documenti informatici omogenei (ossia aventi la stessa classe documentale). Pertanto, a classi documentali diverse corrispondono diversi PdV e versamenti, uno per ogni classe.

Controlli nella fase di ricezione dell'indice del PdV

ID	Oggetto del controllo	Azione in caso di check negativo
Verifica Autorizzazioni		
1.01	Viene verificato che l'utente che effettua il versamento sia abilitato all'invio dei PdV	Il sistema scarta l'intero pacchetto
Verifica formale indice del PdV		
2.01	Viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard convenuto	Il sistema scarta l'intero pacchetto

2.02	Viene verificato che il PdV sia versato nei termini contrattuali e di servizio stabiliti col produttore	WARNING: Il sistema accetta il PdV ma non garantisce la conservazione nei termini concordati
Verifica presenza dati-documenti nell'indice del PdV		
3.01	Viene verificato che l'indicazione del sistema di conservazione sia corretta	Il sistema scarta il PdV poiché il metadato contenuto nell'indice indica un sistema di conservazione diverso
3.02	Viene verificato che l'identificativo specificato nel Pdv non sia già presente nel sistema di conservazione	Il sistema verifica se il PdV (che contiene lo stesso ID) non sia già stato conservato. In questo caso il sistema considera il nuove indice in sostituzione del precedente. Viene invece scartato qualora il PdV risulti essere in stato 'conservato'
3.03	Viene effettuato un controllo semantico sui metadati presenti nell'indice del PdV	Il sistema scarta il PdV poiché uno o più' metadati non rispettano il formato condiviso nei contratti di servizio
3.04	Viene controllato che per ciascun documento dichiarato e descritto all'interno dell'indice del Pdv che: **a**. tutti i metadati minimi obbligatori siano presenti e nel formato corretto; **b**. il formato del documento è un formato ammesso **c**. l'estensione del documento sia tra quelle ammesse per il tipo documento; **d**. il formato dichiarato sia corrispondente all'estensione del nome file	Il sistema scarta il PdV perché le verifiche formali sui documenti dichiarati nell'indice del PdV hanno avuto esito negativo
Verifiche Paternità		
4.01	Viene verificato che il Pdv, nel caso abbia estensione P7M, sia firmato con certificato valido	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo
4.02	Viene verificato che tutte le firme apposte al Pdv siano valide	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo

Controlli nella fase di ricezione dei documenti

A seguito della corretta ricezione dell'indice del PdV, il sistema di conservazione è pronto per la ricezione dei relativi documenti informatici (files) descritti nel pacchetto stesso

Controlli nella fase di ricezione dei documenti (files)

Controllo ricezione documenti		
1.01	Viene verificato che l'hash del documento informatico inviato sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto, al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata	Il sistema scarta il documento poiché non atteso
1.02	In caso di file P7M viene verificata la validità della firma apposta su ogni singolo documento: o Controllo di conformità o Controllo Crittografico o Controllo Catena Trusted o Controllo Certificato o Controllo CRL.	SCARTO: Il sistema scarta il documento qualora il certificato di firma non sia valido WARNING: in caso di documenti firmati e il certificato di firma utilizzato sia prossimo alla scadenza, il sistema evidenzia un warning
1.03	Viene verificato che il documento sia leggibile	Il sistema scarta il documento nel caso questo non sia leggibile
1.04	Viene verificato che il formato del documento informatico sia effettivamente valido e corrispondente a quanto dichiarato nel pacchetto di versamento. In tal caso i controlli eseguiti variano in funzione del formato atteso per ciascuno specifico documento	Il sistema scarta il documento poiché il formato non è quello atteso
1.05	Viene verificato che i documenti ricevuti non siano già presenti nel sistema di conservazione	WARNING: il documento viene accettato e il sistema invia una notifica
1.06	Viene verificato che la ricezione dei documenti si sia correttamente conclusa entro la data limite di ricezione stabilita col produttore nel contratto di servizio	WARNING: il documento viene accettato ma il sistema non garantisce la conservazione nei termini concordati

Le eventuali anomalie e/o scarti riscontrate durante le verifiche effettuate sull'indice del pacchetto di versamento e documenti contenuti al suo interno, saranno comunicate via PEC o altro canale concordato con il Cliente ed esplicitato nel contratto sia al Responsabile della conservazione indicato dal cliente (nel contratto di servizio) che all'utente che ha effettuato l'operazione di versamento.

Tali comunicazioni saranno conservate per tutta la durata del contratto sottoscritto dal cliente.

Per quanto riguarda la registrazione a log si rimanda a quanto descritto al punto 7.1.1

Torna al sommario

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Il sistema di conservazione predispone, per ciascun pacchetto di versamento, un **rapporto di versamento** che viene firmato dal Responsabile del servizio di conservazione. Lo schema del rapporto di versamento è illustrato nel paragrafo successivo (par. 7.3.1).

In particolare il rapporto di versamento contiene, tra l'altro, le seguenti informazioni:

- identificativo unico del PdV, come indicato nel relativo IPdV;
- identificativo unico del PdV fornito dal sistema di conservazione;
- data di ricezione dell'IPdV;
- per ogni documento accettato viene indicato:
  - id univoco, come indicato nell'IPdV;
  - id univoco fornito dal sistema di conservazione;
  - hash;
  - data di ricezione;
  - esito della ricezione (accettato o warning);
  - descrizione warning, ove necessario.

Per quanto riguarda la registrazione a log si rimanda a quanto descritto al punto 7.1.1

Torna al sommario

7.3.1 Specifiche rapporto di versamento

Il Rapporto di Versamento è basilare nel processo di conservazione, in quanto è il documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

Esso viene prodotto nel momento in cui tutti gli elementi utili per la conservazione del pacchetto di versamento sono stati consegnati al sistema.

In esso sono presenti sempre i seguenti dati:

- id del Pacchetto di Versamento;
- id del Rapporto di Versamento;
- lista dei documenti afferenti al pacchetto. Per ognuno di essi sono distinguibili:
  - id come indicato nell'Indice del PdV
  - id assegnato dal sistema
  - impronta del documento
  - nome del documento
  - data di ricezione del file
  - esito controllo firma digitale (ove previsto)
  - esito controllo marca temporale (ove previsto).

Il rapporto di versamento viene sempre firmato digitalmente con certificato del Responsabile del servizio di conservazione e marcato temporale.

Torna al sommario

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Per la gestione dei rifiuti dei pacchetti di versamento e le modalità di comunicazione delle anomalie si rimanda al paragrafo 7.2.

I log registrano tutti le operazioni transitate dal sistema di conservazione e per la descrizione dettagliata si rimanda al paragrafo 7.1.1.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Il pacchetto di archiviazione (PdA) è quello conservato dal sistema di conservazione e possiede un insieme completo di metadati utili alla conservazione a lungo termine.

Il pacchetto di archiviazione viene realizzato secondo lo standard di riferimento SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che rappresenta lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Uno più pacchetti di versamento vengono trasformati in un pacchetto di archiviazione (PdA) in base alle regole tecniche standard del sistema conservazione previste e agli accordi contrattuali.

Il sistema di conservazione a lungo termine ha, fra le altre, la prerogativa di conservare l'autenticità dei documenti in esso contenuti.

La preservazione della suddetta autenticità non può però basarsi esclusivamente sulla firma digitale in quanto quest'ultima:
- ha una validità slegata dall'architettura e dalla struttura del sistema di conservazione;
- ha una validità limitata nel tempo e pari al certificato emesso dalla CA;
- vede la propria sicurezza legata ad algoritmi soggetti ad obsolescenza tecnologica.

E' pertanto fondamentale che il sistema di conservazione a lungo termine verifichi la validità ed il valore delle firme digitali apposte dal Cliente sui documenti informatici oggetto di conservazione.

A tale fine, il Cliente dovrà accertarsi che le firme digitali apposte sui documenti informatici inviati in conservazione:

a) siano valide al momento di sottoscrizione del documento informatico;

b) mantengano piena validità sino al termine ultimo convenuto con Uni IT Srl per la "chiusura" del pacchetto di archiviazione.

Con la sottoscrizione dei pacchetti di archiviazione Uni IT Srl non sottoscrive il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto della normativa regolante la conservazione digitale di documenti informatici.

Torna al sommario

7.5.1 Chiusura anticipata (in corso d'anno) del pacchetto di archiviazione.

In caso di accessi, verifiche ed ispezioni in corso d'anno, il sistema consente, dietro specifica richiesta del Cliente, l'anticipata chiusura del pacchetto di archiviazione rispetto ai tempi programmati.

Torna al sommario

7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

Nel modello OAIS e in linea con la normativa vigente, il pacchetto di distribuzione è strutturato nel modello dati come il pacchetto di archiviazione. La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).

In questo caso, un PdD può anche non coincidere con il pacchetto di archiviazione originale conservato. Molto spesso però, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un PdA, ma può anche verificarsi il caso di PdD (pacchetto di distribuzione) contenenti documenti provenienti da più PdA che vengono "spacchettati" e reimpacchettati per un più fruibile utilizzo da parte dell'utente.

Un utente autorizzato da un soggetto produttore, quindi, è in grado di interrogare il sistema per ricevere in uscita uno specifico pacchetto di distribuzione. L'utente utilizzerà le funzionalità di richiesta di esibizione di un documento o di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.

In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema di conservazione risponderà restituendo un PdD che nel caso più completo conterrà:

- i file/documenti richiesti così come sono stati archiviati dal sistema al momento della messa in conservazione
- gli Indici dei Pacchetti di Archiviazione, marcati temporalmente e firmati come all'origine, con cui sono stati conservati i documenti richiesti. Al loro interno sono contenuti tutti i metadati di tutti i documenti messi in conservazione nello stesso PdA

A fronte di una richiesta di produzione del pacchetto di distribuzione, il sistema effettua delle verifiche di coerenza e correttezza del pacchetto e dei documenti in esso contenuti. A tal proposito, il sistema di conservazione verifica che le impronte dei documenti restituiti nel PdD corrispondano a quelle presenti nel relativo indice del pacchetto di archiviazione; in modo da garantire che i documenti stessi non abbiano subito alterazioni o modifiche nei contenuti.

La richiesta di produzione di un PdD implica l'invio di una comunicazione via PEC o per altro canale secondo quanto previsto dagli accordi contrattuali, all'utente finale e agli altri destinatari eventualmente comunicati dal cliente nel contratto di servizio. Le comunicazioni via PEC, relative alle ricevute di invio e consegna, vengono conservate al fine di tracciare l'intera trasmissione.

La richiesta di esibizione può avvenire da due tra i canali messi a disposizione: interfaccia web e web service.

In entrambi i casi il flusso di selezione dei documenti da esibire è il medesimo:

1. ricerca dei documenti attraverso opportuni filtri
2. selezione e spostamento dei riferimenti dei documenti individuati all'interno di un' area di lavoro
3. richiesta di esibizione a partire dai documenti nell'area di lavoro
4. produzione del link di download da cui scaricare il Pacchetto di Distribuzione.

La ricerca dei documenti avviene tramite la selezione di filtri sui metadati. Una volta individuata la classe documentale di interesse, l'utente può effettuare le ricerche inserendo i valori su cui filtrare per uno o più metadati di riferimento.

La ricerca contemporanea su più metadati implica un filtro più forte, ovvero una restrizione del numero dei documenti risultanti.

Inoltre è possibile effettuare una ricerca tra documenti di classi documentali differenti ma che sono accomunati per un particolare metadato.

Se ad esempio si volessero cercare tutti i documenti afferenti a un determinato numero pratica, dotando classi documentali di tipo differente dello stesso metadato "numero pratica" è possibile effettuare una ricerca di questo tipo.

Tutti i documenti di interesse risultanti dalle ricerche vengono quindi spostati in un'area di lavoro. Finita l'operazione di selezione l'utente può ulteriormente chiedere di esibire solo una parte dei documenti messi nell'area di lavoro.

Il Pacchetto di Distribuzione risultante dalla richiesta di esibizione contiene:

- i documenti da esibire
- gli indici dei PdA, marcati temporalmente e firmati elettronicamente così come al momento della conservazione, del flusso di conservazione relativo ai documenti scelti.

Nel caso in cui tra i documenti figurino interi PdA, il Pacchetto di Distribuzione contiene tutti i documenti che lo compongono.

Torna al sommario

7.6.1 Funzioni svolte alla conclusione del contratto

In tutti i casi di cessazione del Contratto Uni IT Srl consentirà al Cliente di recuperare i propri documenti, entro e non oltre 60 (sessanta) giorni dalla data in cui detta cessazione è divenuta efficace e previo pagamento ad Uni IT Srl di tutti gli importi contrattualmente dovuti.

I documenti informatici dovranno essere prelevati dal Cliente – quindi non incombe su Uni IT Srl alcun obbligo di provvedere alla materiale restituzione dei documenti informatici conservati – secondo le modalità stabilite di seguito:

1. accedendo al sistema, il Cliente effettua esplicita richiesta di chiusura dell'intero Archivio
2. il sistema in automatico genera il pacchetto di versamento contenente tutte le evidenze dei PdA (Pacchetti di Archiviazione) conservati.

3. il Cliente riceve comunicazione via mail PEC o altro canale previsto dal contratto del buon esito della procedura
4. il Cliente, da sistema, richiede la produzione del pacchetto di distribuzione relativo all'intero archivio
5. entro i termini stabiliti da contratto o dalla documentazione collegata, il sistema rende disponibile il pacchetto di distribuzione che potrà essere scaricato dal cliente

Torna al sommario

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

Nei successivi paragrafi vengono descritte le procedure adottate per la produzione di duplicati o copie.

7.7.1 Produzione di duplicati

La produzione di duplicati informatici dei documenti conservati può avvenire a seguito di una richiesta proveniente dal settore tecnico a supporto del servizio di conservazione oppure da una richiesta effettuata direttamente all'interno del sistema di conservazione.

In entrambe le situazioni, il passo iniziale consiste nella ricerca del documento informatico di interesse sfruttando le funzionalità messe a disposizione dal sistema di conservazione. Individuato il documento informatico di interesse, una apposita funzione consente di effettuare il download del documento stesso, producendo quindi un duplicato.

Il documento informatico richiesto viene infatti estratto dal sistema in formato binario controllando che l'estrazione sia eseguita senza errori e quindi inviata all'utente che ne ha fatto richiesta.

Torna al sommario

7.7.2 Produzione di copie

La produzione di copie si rende necessaria solamente a seguito di obsolescenza tecnologica di un formato accettato in conservazione e determina, quale diretta conseguenza, l'avvio di una procedura di riversamento sostitutivo.

In tale contesto Uni IT Srl, previo perfezionamento di specifico accordo scritto (dove saranno concordati ruoli, modalità, tempi e corrispettivi), si renderà disponibile a collaborare col Cliente nell'effettuare le copie informatiche dei documenti informatici depositati in conservazione secondo quanto stabilito dalle regole tecniche vigenti.

Torna al sommario

7.7.3 Produzione copie o duplicati su supporti rimuovibili

In caso di richiesta di produzione di copie o duplicati su supporto rimuovibile, viene prodotto un insieme di DVD (o altro supporto), ognuno autoconsistente, e consegnati al Responsabile della Conservazione che ne ha fatto richiesta.

Il processo prevede l'uso di un apposito applicativo che permette la generazione di immagini complete o parziali degli archivi di conservazione che poi vengono riversate su supporto ottico da un operatore. Il software richiede in input l'identificativo dell'archivio di conservazione, le classi documentali desiderate e il periodo temporale coinvolto. L'output generato è dato dal contenuto selezionato dagli archivi di conservazione, lottizzato in pacchetti di dimensione compatibile alla capienza del supporto ottico. I supporti creati vengono etichettati con una codifica generata automaticamente che in nessun modo riporta informazioni sul contenuto.
In ogni singolo pacchetto sono presenti i documenti protetti con *criptazione* e il software di ricerca e accesso. Il software di ricerca e accesso permette previo inserimento di una password da parte dell'utente, di poter visionare l'indice di quanto contenuto nei pacchetti prodotti, eseguire ricerche su metadati e decriptare e visionare i singoli documenti.
La protezione dei documenti è quindi ottenuta tramite criptazione con un certificato pubblico, generato allo scopo. La decriptazione è eseguita tramite la chiave privata, abbinata al certificato, rilasciata col software di ricerca e accesso, e un PIN che viene recapitato a mezzo telematico al Responsabile della Conservazione. Insieme al PIN viene anche recapitata una descrizione del contenuto di ogni supporto: codice del supporto, evidente sull'etichetta dello stesso, archivio, classi documentali data conservazione primo pacchetto di archiviazione, data conservazione ultimo pacchetto di conservazione.

Torna al sommario

7.7.4 Intervento del Pubblico Ufficiale

Uni IT Srl richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento assicurando allo stesso l'assistenza tecnica necessaria per l'espletamento delle attività al medesimo attribuite.

Ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovranno essere garantite e sostenute dal Cliente; pertanto, qualora il Cliente non se ne sia fatto carico direttamente, Uni IT Srl è sin da ora autorizzata ad addebitare al Cliente tutti i costi e le spese, compresi gli onorari inerenti le attività prestate dal Pubblico Ufficiale, qualora la normativa ne richieda obbligatoriamente la presenza.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

7.8.1 Trasferimento dei documenti informatici in conservazione

Nel contratto di servizio o nella documentazione collegata , sono indicati i tempi entro i quali le diverse tipologie di documenti vanno trasferite in conservazione.

Torna al sommario

7.8.2 Scarto dei documenti informatici conservati

Relativamente alla possibilità di scarto, ossia di eliminare legalmente i documenti informatici conservati digitalmente a norma di legge, occorre distinguere preliminarmente la tipologia dei soggetti (Clienti) produttori, pubblici o privati.

Va preliminarmente osservato, che in ambito privato, con l'eccezione degli "archivi che rivestono interesse storico particolarmente importante", che divengono archivi specificamente disciplinati, l'obbligo di conservazione dei documenti è disciplinato dall'ordinamento vigente e, in particolare, dai termini prescrittivi del codice civile nonché, per le scritture contabili, le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti, segnatamente dall'art. 2220 del c.c., il quale stabilisce l'obbligo di conservazione di dieci anni dalla data dell'ultima registrazione.

In ambito pubblico, oltre alle prescrizioni civilistiche, si rendono applicabili una serie di altre disposizioni specifiche, una su tutte, il Codice dei beni culturali e ambientali, emanato con il D.Lgs. 10 gennaio 2004, n. 42.

Inoltre, con riferimento agli archivi pubblici o privati, che rivestono interesse storico-artistico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero per i beni e le attività culturali rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

Pertanto, alla luce di quanto sopra sinteticamente rappresentato, una volta scaduti i termini previsti dalla legge il Cliente riceve una notifica via PEC dal sistema di conservazione e in autonomia può decidere di eliminare i documenti conservati attraverso le funzionalità previste dal sistema di conservazione.

Torna al sommario

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

Al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, la struttura dell'indice del pacchetto di archiviazione viene realizzata da Uni IT Srl in conformità con quanto previsto dallo standard "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali", (c.d. SInCRO), ossia dalla norma UNI 11386 dell'ottobre 2010.

I pacchetti di archiviazione generati dal sistema di conservazione vengono trattati al solo scopo di soddisfare i requisiti della conservazione digitale dei documenti e delle richieste di produzione di pacchetti di distribuzione e di esibizione.

Il soddisfacimento dei requisiti della conservazione digitale implica che i pacchetti di archiviazione vengano firmati digitalmente dal responsabile del servizio di conservazione o da un suo delegato e marcati temporalmente per assicurarne la validità nel corso del tempo.

La produzione di pacchetti di distribuzione o l'esibizione di pacchetti di archiviazione comporta invece la produzione di duplicati degli stessi che sono successivamente utilizzabili in altri processi. Il pacchetto di archiviazione memorizzato all'interno del sistema non subisce più alcuna modifica successiva alla firma digitale e all'apposizione della marca temporale.

Torna al sommario

7.10 Tabella riepilogativa delle fasi del processo di conservazione

Il processo di conservazione si articola nelle seguenti fasi:

FASE 1	**Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico**

	Descrizione sintetica	Consiste nella ricezione dell'IPdV

FASE 2	**Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione**	
	Descrizione sintetica	In questa fase vengono condotti i controlli sull'IPdV

FASE 3/a	**Preparazione del rapporto di conferma**	
	Descrizione sintetica	A seconda dell'esito del controllo sull'IPdV viene prodotto un rapporto di conferma che viene restituito al sistema versante. **NOTA BENE:** il rapporto di conferma non implica la presa in carico del versamento da parte del sistema

FASE 3/b	**Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o non conformità**	
	Descrizione sintetica	Alternativamente alla fase 3 viene restituito al sistema versante l'indicazione di eventuali anomalie. In tale caso il versamento viene rifiutato

FASE 4	**Ricezione dei documenti**	
	Descrizione sintetica	Il sistema si mette in attesa dei documenti del PdV.

FASE 5	**Verifica dei documenti**	
	Descrizione sintetica	In questa fase vengono condotti i controlli specifici del documento ricevuto

FASE 6	**Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte**	
	Descrizione sintetica	Una volta ricevuti correttamente, o con warning, tutti i documenti del PdV viene prodotto il PdV

FASE 7	**Sottoscrizione del rapporto di versamento con firma digitale apposta da Uni IT Srl**

Descrizione sintetica	Il RdV viene firmato digitalmente dal Responsabile del servizio di Conservazione o da un suo delegato. Infine il RdV viene inviato al Cliente via email PEC. In questa fase Uni IT Srl prende in carico il versamento ufficialmente

FASE 8	**Preparazione e gestione del pacchetto di archiviazione**
Descrizione sintetica	Il Pacchetto di Archiviazione è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualificata, corroborata da una marca temporale. La struttura del Pacchetto di Archiviazione è costruita sulla base delle specifiche della struttura dati (UNI 11386:2010) contenute nell'allegato 4 alle regole tecniche e secondo le modalità riportate nel manuale della conservazione

FASE 9	**Sottoscrizione del pacchetto di archiviazione con firma digitale apposta da Uni IT Srl e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del pacchetto di archiviazione"**
Descrizione sintetica	Il Pacchetto di Archiviazione (PdA), che viene costruito dal versamento di uno o più PdV, viene "chiuso" nel momento in cui tutti i PdV sono stati presi in carico dal sistema. La chiusura viene sancita dall'apposizione di opportuna marca temporale, per stabilirne l'istante di creazione, e firma digitale del Responsabile del servizio di Conservazione o di un suo delegato, per garantirne l'immodificabilità. Con la suddetta firma apposta in calce al Pacchetto di Archiviazione e la suddetta dichiarazione il conservatore NON SOTTOSCRIVE il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto delle norme giuridiche e delle indicazioni contrattuali di servizio.

FASE 10	**Preparazione e sottoscrizione con firma digitale di Uni IT Srl del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente**
Descrizione sintetica	Il pacchetto di distribuzione (PdD) è definito in base alle esigenze del richiedente e può contenere anche un set parziale di metadati. È generato a partire dai pacchetti di archiviazione. Nel caso più semplice il PdD contiene dei duplicati del PdA. In alternativa esso può essere costituito da una scelta di documenti conservati selezionati attraverso una o più interrogazioni. I risultati di tali ricerche possono essere raccolti in un'area di lavoro e da qui può essere prodotto il PdD voluto.

FASE 11	**Produzione di duplicati informatici effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico**

	Descrizione sintetica	Per duplicato informatico si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche in materia di formazione del documento informatico, ovvero se contiene la stessa sequenza di bit del documento informatico di origine.

FASE 12	**Eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal *Contratto* di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso**	
	Descrizione sintetica	Alla scadenza dei termini di conservazione, il cliente in autonomia può decidere di cancellar ei documenti in conservazione.

Torna al sommario

7.11 Audit Log

Il sistema di conservazione registra ogni evento rilevante del processo di conservazione.

In particolare sono gestiti i seguenti eventi:

- Creazione PdA
- Conservazione PdA
- Invio Rapporto di Versamento
- Invio Rapporto di Conservazione
- Esibizione PdD
- Download Documento
- Scarto PdA
- Verifica Integrità PdA

Il log di audit è consultabile tramite l'applicazione DocHome e attraverso il sistema di back office da chi gestisce il servizio o da un pubblico ufficiale che ne faccia richiesta.

Il log viene salvato in apposito database e rimane disponibile nel tempo per consultazione.

Oltre al log di audit sono presenti altri log di servizio relativi ad altri eventi generati dal sistema durante il processo di conservazione.

Torna al sommario

8 IL SISTEMA DI CONSERVAZIONE

8.1 Infrastruttura informatica datacenter

Il servizio di Conservazione erogato da Uni IT Srl si avvale di un fornitore esterno per i servizi di Data Center e sviluppo/manutenzione software. I Data Center dal quale sono erogati i servizi si trovano sul territorio nazionale e sono conformi ai requisiti della normativa ISO/IEC 27001:2005.

Nelle due strutture che sono messe a disposizione dal Fornitore per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo è presente tutta una serie di sistemi che permette di garantire integrità degli ambienti e dei servizi.

Torna al sommario

8.2 Caratteristiche generali della soluzione di conservazione

La soluzione, come meglio descritto in seguito, presenta le seguenti caratteristiche peculiari:

- architettura di produzione implementata su infrastruttura virtuale e storage dedicati - predisposta e totalmente ridondata (HA) presso il Data Center del Fornitore, che rispetta le caratteristiche proprie della certificazione Tier IV dell'Uptime Institute - sito in via Gobetti 96, Arezzo;

- architettura secondaria predisposta per consentire la doppia scrittura del dato, effettuata applicativamente, con replica sincrona storage based della piattaforma virtuale, inclusi i DB documentali e di gestione, situata presso il Data Center sempre di proprietà del Fornitore, sito in via Ramelli, Arezzo.

Il Sistema di Conservazione è sviluppato in modo modulare consentendo una facile scalabilità semplicemente aggiungendo unità e potenza elaborativa ai moduli sottoposti al maggior carico. L'esperienza del Fornitore nell'ambito della gestione di grandi volumi di dati ha permesso di creare architetture che si possono definire elastiche: "espandibili" in caso di aumento del carico di lavoro oppure "limitabili" nel caso di una riduzione delle necessità.

L'intera soluzione è stata progettata per essere quindi in grado di gestire l'elaborazione di grandi volumi di dati, scalando sia verticalmente che orizzontalmente in ognuna delle sue singole componenti, con un elevato livello di affidabilità, distribuendo su più server fisici nodi con il medesimo ruolo ed evitando single point of failure.

L'architettura modulare del sistema è implementata al 100% su infrastruttura di virtualizzazione con hypervisor vMWare e garantisce in sintesi i seguenti vantaggi:

Affidabilità - Totale ridondanza ai guasti HW

- funzionalità di HA implementata dall'architettura virtuale;
- almeno due moduli con il medesimo ruolo posizionati su server fisici separati;
- DBMS in configurazione Master-Master;
- sistemi documentali duplicati "gemelli";
- doppia scrittura dei documenti;
- utilizzo di sistemi di firma e marca ad alte prestazioni in HA.

Architettura scalabile

- nodi di Front-End ed Application multipli e contemporaneamente attivi;
- storage di livello Enterprise ad alte prestazioni per la piattaforma VMware e le componenti DB;
- funzionalità di replica.

Torna al sommario

8.3 Componenti Logiche

Di seguito riportiamo l'immagine rappresentativa delle componenti logiche del sistema di conservazione:

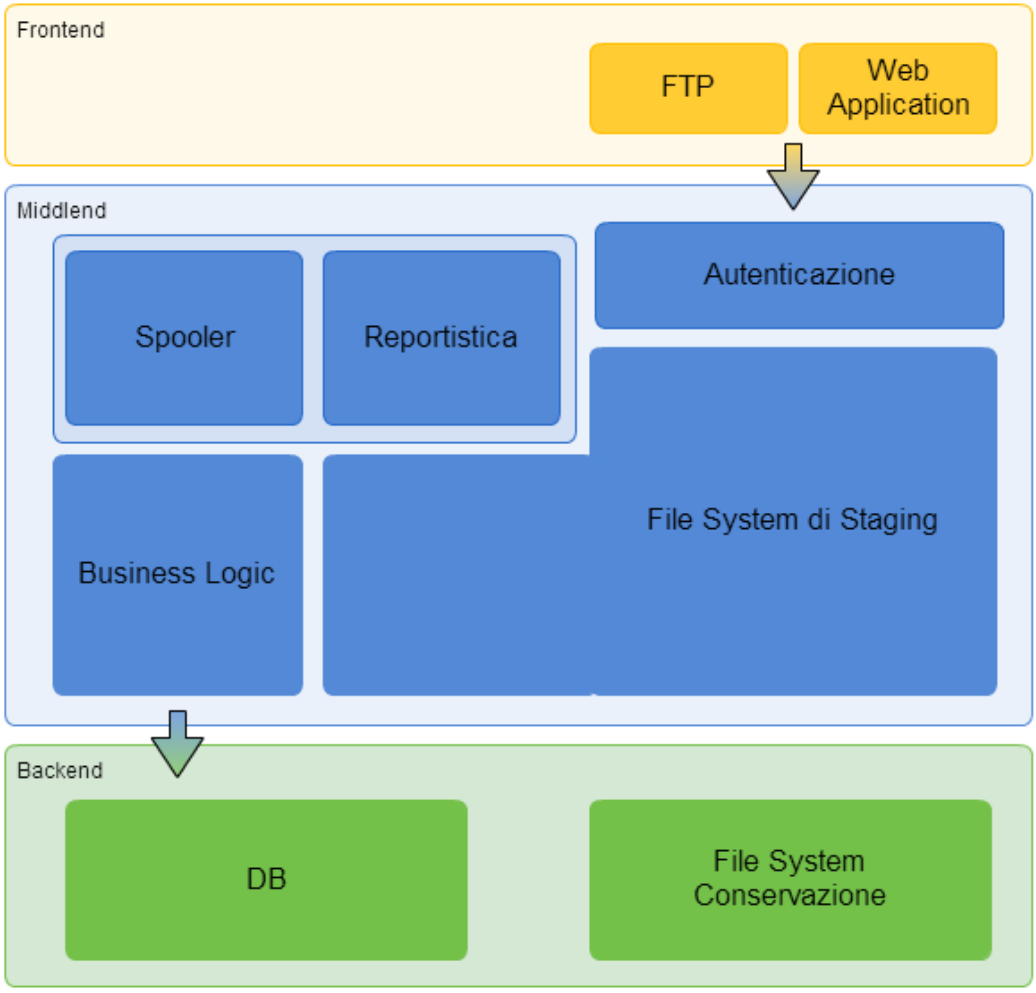

Figura 2: Rappresentazione delle componenti logiche

Come si evince dalla figura l'architettura è basata su una soluzione multi-tier a 3 livelli:

- **Presentation layer**: l'applicazione è pensata per essere scalabile, aumentando il numero dei Web container attraverso una logica di server clustering, gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client;

- **Business logic (o application) layer**: la Business Logic implementa l'intelligenza necessaria per gestire le varie istanze di backend sia in scrittura, sia in fase di ricerca, distribuendo le query sulle varie istanze disponibili. Tutte le istanze backend sono sempre disponibili almeno in lettura

- **Store (& Database) layer**: la parte di back end è composta da diverse istanze. Ogni istanza è costituita dal DB e dal relativo file system. Il DB è duplicato in modalità Master-Master su due nodi predisposti sull'ambiente virtuale e contiene i metadati conservati; il FS contiene l'archivio (dati conservati) e viene replicato con strumenti di basso livello.

Torna al sommario

8.4 Componenti tecnologiche

Il sistema di conservazione è composto da varie parti e tecnologie, con l'obiettivo di trarre il meglio dalla loro sinergia.

Le principali componenti software che interagiscono all'interno del sistema sono:

- sistema documentale quale CMS di riferimento;
- DB per la gestione dei dati di sistema e dei metadati legati ai documenti in conservazione;
- sistema LDAP per le operazioni di registrazione, autenticazione e controllo degli accessi degli utenti al sistema, indipendentemente dall'interfaccia scelta;
- Web server e servlet container per le interfacce di frontiera (Web e Web Service);
- un sistema di message broker per la gestione delle code in ingresso dei documenti in conservazione sulle interfacce di caricamento massivo (FTP e Web Service);
- motore di Ricerca per la gestione dei dati di audit.

Torna al sommario

8.5 Componenti fisiche

La soluzione è composta da due infrastrutture fra loro interconnesse:

- un sito di Produzione completamente autosufficiente e con tutte le componenti ridondate in HA e collegato tramite fibre ottiche dedicate e di proprietà, con doppia via, al sito secondario,
- un sito Secondario di DR predisposto alla replica dei dati e con le componenti necessarie ad una ripartenza del servizio.

Tutte le componenti utilizzate sono di tipologia enterprise e, come tutte le soluzioni implementate dal Fornitore di Uni IT Srl, utilizzano prodotti di marche ampiamente riconosciute e leader del mercato di riferimento.

Torna al sommario

8.5.1 Sito Primario (Produzione)

Il sito di produzione ospita una infrastruttura virtuale basata su soluzione VMware sul quale vengono istallati:

- i nodi di Front-End (almeno due) per le interfacce di caricamento, esibizione e gestione;
- gli Application o Business Logic server (almeno due);
- i backend server, un singolo nodo per ogni istanza;
- un nodo virtuale dedicato al DB server di ogni istanza di backend con la seconda copia in Master-Master installata sul sito secondario;
- un nodo virtuale per la gestione delle code del sistema di caricamento;
- un nodo virtuale che implementa il DB che contiene tutte le informazioni per la gestione dell'infrastruttura (configurazione, accounting, etc.)con la seconda copia in Master-Master installata sul sito secondario;
- Storage di livello enterprise per l'archiviazione dei documenti;
- Link ed interfacce verso i sistemi di Firma e Marcatura presenti nel medesimo Data Center.

La figura sottostante schematizza quanto implementato sul sito principale senza entrare nelle specifiche modalità di replica.

Al fine di garantire la ridondanza ed il bilanciamento del traffico vengono utilizzati dispositivi di load balancing in grado di distribuire il carico di lavoro su un numero di macchine virtualmente illimitato. Questo meccanismo permette di risolvere oltre a problemi prestazionali con la semplice aggiunta a caldo di nuove macchine, anche problemi relativi ad eventuali guasti delle componenti bilanciate, nonché la manutenzione programmata dei singoli nodi.

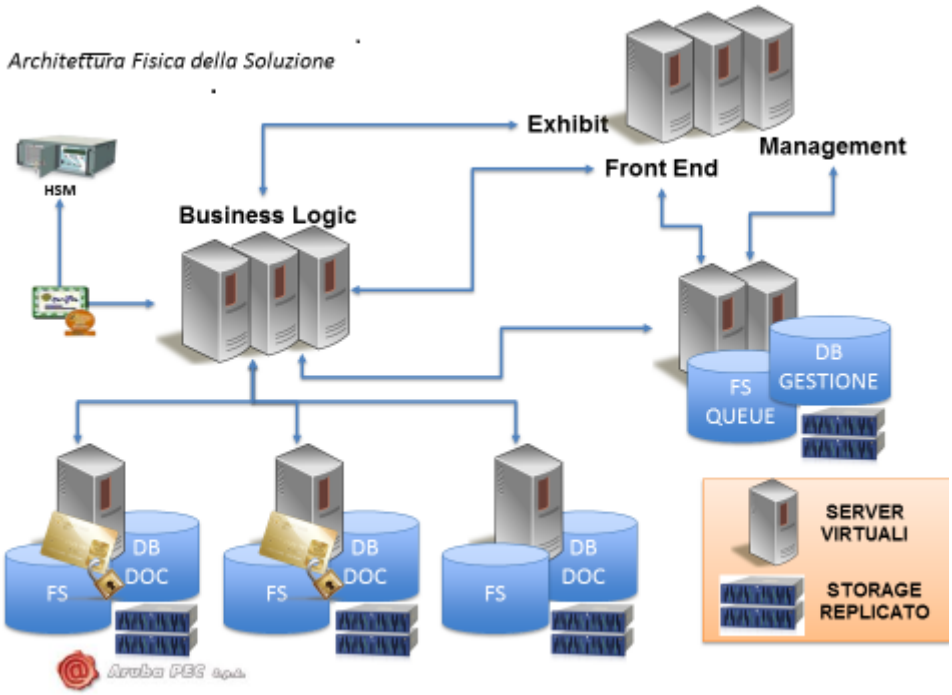

Figura 3: Rappresentazione architettura fisica della soluzione

Torna al sommario

8.5.2 Sito Secondario (DR)

Il sito secondario ospita un'infrastruttura virtuale basata su VMWare sulla quale vengono installati:

- server di backend corrispondente ad uno dei nodi ridondati dell'ambiente di produzione;
- server DB sincronizzato in maniera sincrona (master-master) con i DB di produzione;
- storage enterprise su cui vengono sincronizzati i dati in maniera asincrona che saranno resi disponibili ai server del sito secondario per ripristinare il servizio;
- collegamenti verso i sistemi esterni di firma e Marcatura temporale (sempre situati nel sito secondario);
- macchine virtuali replicate dal sito primario (1 per ciascuna tipologia).

Nello specifico le macchine replicate dal sito primario sono quelle che forniscono i seguenti servizi:

- Frontend Web
- Frontend WS
- Business Logic
- Indicizzazione
- Audit
- Autenticazione

La procedura di switch tra il sito primario ed il secondario è basata tramite il cambio dei puntamenti a livello di DNS.

La figura sottostante schematizza la modalità di replica delle componenti non replicate applicativamente, ad esclusione quindi dei dati archiviati, replicati con doppia scrittura e DB MySQL, configurati in Master-Master.

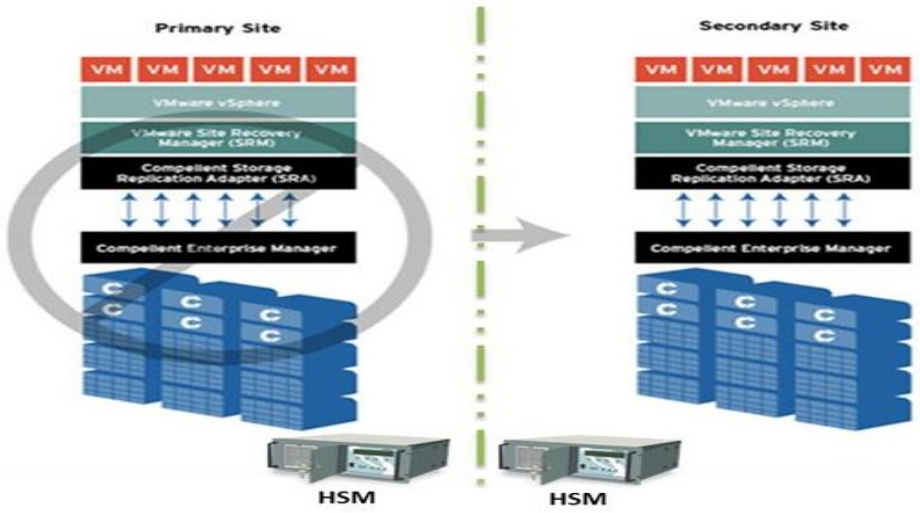

Figura 4: Schema logico della soluzione di Disaster Recovery

In caso di problemi sul sito di Produzione è possibile effettuare la riattivazione del servizio, senza perdita di dati entro 24 ore.

Torna al sommario

8.6 Politica di gestione degli accessi applicativi

L'accesso al sistema è garantito attraverso credenziali di autenticazione (Username e Password) le cui caratteristiche principali sono di seguito riportate:

- **Robustezza password;** le password che il sistema accetta devono rispettare le seguenti regole:
  - Lunghezza minima 8 caratteri
  - Contenere maiuscole e minuscole
  - Contenere almeno un numero
  - Contenere almeno un carattere speciale tra:

    !#$%&'()+,\-.:;<=>?@[]{|}/*

- **Scadenza password**

  Tutte le utenze applicative comprese quelle amministrative richiedono il cambio obbligatorio della password dopo 90 giorni. La durata della password è configurabile a livello di prodotto, ma è uguale per tutte le tipologie di utenza: produttore, titolare e amministratore.
  Il profilo amministratore può impostare delle utenze "speciali", utilizzate dalle procedure automatiche di versamento, per le quali non è prevista la scadenza della password.
  L'utente all'approssimarsi della scadenza della password riceve un email contenente l'invito a rinnovare la password con le seguenti tempistiche:
  - 10 gg prima della scadenza
  - 5 gg prima della scadenza
  - 1 gg prima della scadenza

  Nel caso in cui la password sia scaduta al primo accesso al sistema tramite pannello web il sistema obbliga a cambiare la password. Nel caso invece l'accesso avvenga tramite web service il sistema genera un messaggio di "*password expired*". Il cambio password può essere fatto solo tramite pannello web.

- **Blocco utenza**

  Nel caso in cui venga superato il numero massimo di tentativi consecutivi di inserimento errato della password viene bloccato l'accesso al sistema. Il valore di default è 5.
  L'utenza risulta bloccata sia per tentativi di accesso tramite web service che tramite pannello web.
  Nel caso di utenza bloccata alla pagina di login compare il messaggio: "*Login fallito: Utente disabilitato*".
  Lo sblocco dell'utenza può essere fatto tramite pannello web da un utente con profilo amministrativo. Quando viene sbloccata un'utenza il sistema genera una password temporanea che deve essere obbligatoriamente cambiata al primo accesso.

- **Gestione password precedenti**

  Al fine di garantire uno standard di sicurezza adeguato non è consentito dal sistema utilizzare le 5 password precedenti.

Torna al sommario

8.7 Procedure di gestione e di evoluzione

In linea con quanto previsto dalla circolare n° 65, nell'allegato "REQUISITI DI QUALITÀ E SICUREZZA PER L'ACCREDITAMENTO E LA VIGILANZA", sono descritte le procedure in riferimento a:

- conduzione e manutenzione del sistema di conservazione;
- gestione e disponibilità dei log(vedi paragrafo 7.11);
- monitoraggio del sistema di conservazione(vedi paragrafo 9);
- change management (vedi paragrafo 8.7.2);
- verifica periodica di conformità a normativa e standard di riferimento (vedi paragrafo 8.7.3).

Torna al sommario

8.7.1 Conduzione e manutenzione del sistema di conservazione

L'argomento è trattato nel documento tecnico "MGA_A_38-01 Politica per la gestione dei beni, delle capacità e delle modifiche" che descrive le strategie di continuità, considerando tutte le componenti organizzative, operative, del business, tecnologiche, infrastrutturali che contribuiscono all'intero sistema e processo di conservazione.
Il documento prevede tra l'altro quanto segue:
Il monitoraggio viene svolto dal gruppo di operatori appartenenti al Network Operation Centre, 24 ore su 24/7/365, il quale procede non solo per monitorare la gestione delle capacità ma anche per monitorare qualsiasi evento anomalo.

I sistemi sono infatti configurati per inviare agli operatori allarmi nel caso in cui il livello di utilizzo delle risorse superi una certa soglia oppure in caso di altri eventi anomali, compresi quelli che possono indicare una potenziale violazione di sicurezza. Gli allarmi vengono definiti sui sistemi tenendo in conto anche della criticità degli stessi o delle informazioni in essi eventualmente contenute.
Ove ciò avvenga, e quindi quando una risorsa è vicina alla saturazione oppure in caso di eventi anomali, è necessario aggiungere risorse (comunque da gestire come Change Request) o intraprendere le attività di verifica delle anomalie dei sistemi, anche al fine di verificare se si renda necessaria l'attivazione delle procedure.

L'organizzazione del Centro prevede la figura dei capoturno e dei turnisti; inoltre per garantire che nessun alert venga perso, viene fatta espressa raccomandazione ai turnisti di non lasciare mai il Centro non presidiato. Pertanto deve esserci sempre almeno un operatore davanti agli schermi.

Gli strumenti automatici di segnalazione, che vengono costantemente controllati dal personale del Centro, permettono l'impostazione di controlli "ad hoc" per ciascun servizio da monitorare, rilevando automaticamente le anomalie e segnalandole visivamente (e opzionalmente via email, sms, ecc.).

Per tutti i sistemi sono inseriti appositi controlli su tali strumenti atti a verificare i vari aspetti del servizio preso in esame, in modo da evidenziare qualsiasi tipo di anomalia.

Non appena compare un alert sullo strumento di monitoraggio, il personale addetto avvia immediatamente le opportune verifiche.

Ciascun alert è stato creato in modo da identificare in maniera precisa e rapida il sottostante servizio monitorato e ottenere:

- una breve descrizione del servizio monitorato;
- le verifiche e le ulteriori prove da compiere per assicurarsi dell'effettiva presenza di anomalie e raccogliere ulteriori dettagli;
- le operazioni da compiere nel caso si presenti una reale anomalia;
- le condizioni per cui è necessario avviare l'escalation.

I controlli periodici schedulati vengono invece inseriti in uno strumento per la pianificazione delle attività.

Il personale addetto controlla tale strumento e si assicura che i task che vi sono indicati vengano presi in carico dagli assegnatari (che poi invieranno il relativo report).

L'impianto elettrico (Power Center/UPS) e antincendio dei Data Center, sono dotati di controlli che generano l'invio di email di avviso in caso di anomalie e sono dotate di avvisatori acustici ed ottici che si attivano in caso di emergenza o malfunzionamento.

Torna al sommario

8.7.2 Change management

Per ogni operazione di upgrade - per evoluzione o bug fixing - di una qualsiasi componente del sistema di conservazione viene seguita una procedura standardizzata al fine di garantire il minimo impatto su eventuali fermi del servizio ed avere la massima sicurezza possibile riguardo ai dati e documenti a sistema.
Tale procedura si basa sui seguenti assunti:

- ogni componente sviluppata è conservata in opportuno sistema di versionamento del codice
- i file di configurazione di ogni componente sono separati dai compilati in maniera da garantire un accesso più flessibile e veloce al personale addetto;
- sono state predisposte apposite macchine di deploy per la compilazione e creazione dei pacchetti delle varie componenti da installare;

Ogni aggiornamento del sistema passa da un flusso ben definito che consente contemporaneamente di mantenere stabile e sicura l'intera soluzione in uso dall'esterno e di sviluppare senza ostacoli nuove funzionalità.

Tale procedura risulta di particolare importanza anche per garantire l'accesso controllato e limitato a pochi addetti agli ambienti di produzione.

In particolare vengono messi a disposizione 4 ambienti di lavoro: sviluppo, test, collaudo e produzione.
Tutti gli sviluppi vengono condotti e testati nell'ambiente sviluppo che è in uso esclusivo agli sviluppatori per le sue caratteristiche di continua trasformazione.

Qualsiasi altro attore esterno al team di sviluppo non ha nessun accesso a tale ambiente.

Il codice sviluppato viene conservato all'interno di un sistema di versionamento organizzato in maniera da permettere, qualora sia necessario, l'estrazione di una qualsiasi versione del software. Una volta che un nuovo modulo software è pronto, esso viene registrato nel sistema di versionamento associandogli un tag/versione.

Per operare l'installazione sull'ambiente di test, deputato ai test pre-collaudo, i sorgenti vengono scaricati su un ambiente di deploy, esterno all'ambiente di test stesso, direttamente dal sistema di versionamento, insieme a eventuali script automatici di compilazione, installazione e configurazione.

Sull'ambiente di test il team della QA (Quality Assurance) effettua i test per verificare la corretta implementazione dei moduli rilasciati ed effettua anche i test regressione.

Solo se il processo di testing va a buon fine si procede con il rilascio dei nuovi moduli nell'ambiente di collaudo e produzione con la medesima procedura utilizzata per l'ambiente di test.

Torna al sommario

8.7.3 Verifica periodica di conformità a normativa e standard di riferimento

Uni IT Srl, in qualità di conservatore, svolge una verifica periodica della conformità alle normative ed agli standard di riferimento. A tal proposito, viene effettuata una volta l'anno, una verifica sulla rispondenza ai requisiti di qualità e sicurezza avvalendosi dello strumento di check list, sulla base dell'allegato della circolare n° 65, attraverso il quale viene registrata l'aderenza o meno alla conformità richiesta.

Torna al sommario

9 MONITORAGGIO E CONTROLLI

In questo capitolo si riporta 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.

Torna al sommario

9.1 Procedure di monitoraggio

Uni IT Srl, con l'ausilio e supporto del fornitore della piattaforma tecnologica ospitante la soluzione, assicura la verifica periodica del funzionamento, nel tempo, del sistema di conservazione. Il controllo della buona funzionalità del sistema di conservazione avviene tramite apposite funzionalità di monitoraggio del software. Esse mostrano l'esito delle operazioni automatiche eseguite sul sistema di conservazione come la generazione dei pacchetti di archiviazione, la chiusura dei pacchetti di archiviazione e la verifica dell'integrità degli archivi.

Il monitoraggio avviene inoltre anche a livello di processi di elaborazione sul sistema di conservazione. Questo permette di individuare eventuali casi di processi bloccati che potrebbero inficiare il funzionamento del sistema stesso.

Un ultimo controllo del buon funzionamento del sistema avviene tramite il monitoraggio delle tracciature che vengono effettuate a livello di database. Tutte le operazioni eseguite determinano infatti la creazione di apposite revisioni che registrano tutte le modifiche intervenute sul sistema permettendo eventualmente di ripristinare i dati a seguito di situazioni anomale.

Torna al sommario

9.2 Verifiche sull'integrità degli archivi

Come previsto dalla normativa, Uni IT Srl, con l'ausilio e supporto del fornitore della piattaforma tecnologica ospitante la soluzione, assicura la verifica periodica, con cadenza non superiore a 36 mesi, dell'integrità degli archivi e della leggibilità degli stessi; assicura, inoltre, agli organismi competenti previsti dalle norme vigenti, l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Il sistema di conservazione esegue periodicamente ed automaticamente le operazioni di controllo dell'integrità degli archivi. Tali operazioni vengono eseguite solo su una certa percentuale dell'archivio che viene definita nella configurazione del sistema di conservazione.

Il controllo eseguito è di due tipologie:

- controllo di leggibilità: consiste nel rendere disponibile attraverso una macchina virtuale un viewer per la visualizzazione dei documenti conservati. Il viewer specifico viene fornito sulla base dell'estensione del documento (mime type) e della versione del formato associato. Il dettaglio di tutte. La lista delle tipologie supportate è definita nella procedura "Registro dei formati supportati da DocHome". Per ogni formato presente nel registro è individuato il relativo programma che ne permette la corretta visualizzazione(viewer). Il registro viene tenuto aggiornato sulla base dei nuovi formati o di quelli che diventano

obsoleti. Conseguentemente sono aggiornati i viewer presenti sulla macchina virtuale per la corretta leggibilità dei documenti conservati. Ulteriori dettagli operativi sulla verifica della leggibilità sono disponibili sulla procedura IO0037 Conservazione - procedura leggibilità documenti in conservazione a norma, definendo il processo, i tempi e gli attori coinvolti per garantire la leggibilità nel tempo dei documenti presenti nel sistema di conservazione a norma.

- controllo di integrità: consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema. Questo fornisce una ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

La combinazione dei due tipi di controllo descritti non fornisce però garanzia di poter visualizzare correttamente il documento e che lo stesso sia effettivamente intellegibile dall'uomo.

Infatti questa garanzia non può essere fornita senza entrare nel merito del documento stesso. La garanzia della corretta visualizzazione del documento è d'altro canto garantita dalla scelta del formato PDF/A per i documenti conservati. Questo formato possiede infatti la caratteristica intrinseca di fornire leggibilità a lungo termine oltre all'ulteriore garanzia di essere basato su specifiche pubbliche (ISO 19005-2005).

Torna al sommario

9.2.1 Pianificazione delle verifiche periodiche da effettuare

La verifica dell'integrità degli archivi viene effettuata sui filesystems in cui i documenti sono replicati, controllando tutti i file presenti in nei PdA conservati.

Viene verificato che i file distribuiti nei filesystems siano identici mediante:

- controllo del nome e della dimensione dei file presenti sui filesystems;
- calcolo dell'hash di ogni singolo file. Il valore viene confrontato con l'hash del corrispondente file censito nell'IPdV del PdA.

Il controllo su ciascun PdA conservato viene effettuato a intervalli temporali. La prima verifica dell'integrità del PdA viene effettuata entro 36 mesi dalla conservazione del PdA. Le successive verifiche vengono effettuate entro 36 mesi dalla conclusione dell'ultima verifica effettuata.

Torna al sommario

9.2.2 Mantenimento della firma per il periodo di conservazione

Il sistema di conservazione si avvale di un altro fornitore terzo (Certificatore accreditato) per le attività di firma digitale e di marcatura temporale. Questo fornitore garantisce che gli elaboratori che offrono il servizio di marcatura temporale e di firma digitale sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali. Non è infatti consentito l'accesso e la permanenza di una sola persona. I locali ove si svolgono le procedure di firma e marca sono dotati di sofisticati impianti di allarme, telecamere, microfoni, rilevatori di movimento (che si attivano soltanto quando nessuna persona vi è presente), al fine di controllare ogni movimento all'interno degli stessi.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Nell'ambito dell'Infrastruttura che ospita la soluzione di conservazione viene conservata e periodicamente esaminata dall'Amministratore una traccia (audit log) delle operazioni svolte dagli utenti e dai processi, in modo che tali azioni possano essere documentate ed attribuite a chi le ha eseguite o causate (accountability), anche allo scopo di rilevare eventi di sicurezza, incidenti e vulnerabilità associati ai sistemi coinvolti nel processo di conservazione. Tali log vengono archiviati su supporto permanente e non è permesso agli utenti non autorizzati di accedervi.

In caso di anomalie riscontrate a seguito del monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi, sono presenti apposite procedure di emergenza (contingency) da applicare in attesa del ripristino del servizio.

Torna al sommario

9.3.1 Procedura di ripristino in caso di corruzione o perdita dei dati:

Nel caso di errore in fase di Conservazione del PdA il processo scatena un alert verso gli addetti al monitoraggio del servizio di conservazione i quali intervengono per la soluzione del problema occorso. Nel caso di errori riscontrati in fase di verifica – invece – si procede come indicato al paragrafo 7.1.

Torna al sommario

9.3.2 Gestione dei log

Il log più rilevante è ovviamente quello applicativo e che registra tutti gli accessi al sistema e le operazioni di amministrazione e conservazione che vengono effettuate: creazioni di aziende, archivi ed utenze, assegnamento risorse, creazione di PdA, caricamenti di indici e files, validazioni, conservazioni ed errori durante questo tipo di operazioni.
Tali dati, memorizzati in un apposito data base vengono salvati e storicizzati periodicamente e quindi messi essi stessi in conservazione. La periodicità di default stabilita è mensile, ma dipende anche dalla numerosità dei log generati dal sistema stesso.
Seppur messi in conservazione i log restano comunque presenti nel DB per le consultazioni online tramite l'interfaccia amministrativa e non è prevista ad oggi alcuna cancellazione.

I log che registra gli accessi amministrativi ai server dell'infrastruttura sono invece salvati su un apposito server di riferimento, marcati temporalmente e archiviati sul file WORM per 6 mesi.

Gli altri log di sistema, utili esclusivamente per analizzare eventuali errori o comportamenti anomali dell'applicazione nel momento in cui questa avviene, sono viceversa in configurazione "*rotate*" sulle macchine, con una retention massima di 10 giorni.

Torna al sommario