Grammelot Srl
Via Casale, 5 - 20144 - Milano – Italy
Tel: +39 02 89075413 – Fax: +39 02 32066978
www.grammelot.eu - info@grammelot.eu

DESCRIZIONE DEL SERVIZIO DI CONSERVAZIONE DIGITALE KLOUDARCHIVE

Il servizio KloudArchive consente di conservare i documenti in ottemperanza alle normative vigenti in temini di conservazione sostitutiva. Permette all'utente di caricare in autonomia i propri documenti aziendali a rilevanza fiscale e non, associandoli univocamente alla relativa tipologia di appartenenza: fatture emesse, fatture ricevute, libri contabili, registri e altre tipologie eventualmente contrattualizzate con Grammelot Srl. Il sistema permette il caricamento in modalità massiva tramite Webservices su canale sicuro HTTPS oppure tramite canale FTPS.
Nel caso delle fatture emesse, il sistema consente a fronte del caricamento manuale, oltre all'archiviazione del documento, la possibilità di inviare contestualmente un'e-mail al destinatario del documento – il cliente a cui è indirizzata la fattura - contenete come allegato la fattura emessa e con la descrizione di come questo documento debba essere trattato dal destinatario ai fini del rispetto delle norme.
Ogni documento inserito nel sistema deve essere corredato degli indici di ricerca, inseriti direttamente dell'utente con apposita procedura guidata. Tali indici sono indispensabili alla ricerca del singolo documento in archivio dopo la sua conservazione (chiavi di ricerca). I documenti archiviati possono essere eliminati e sostituiti sino alla esecuzione mensile, da parte del Responsabile della Conservazione di KloudArchive, della procedura di "chiusura dei lotti" (vedi paragrafi successivi). I documenti che sono contenuti in un "lotto chiuso" non potranno essere in alcun modo modificati. Potranno invece essere annullati e sostituiti da una copia dello stesso documento che sarà contenuta in uno dei lotti successivi.
Mensilmente il servizio KloudArchive prevede la chiusura dei lotti di conservazione, eseguita dal delegato del responsabile della Conservazione, tramite firma digitale e marca temporale apposte sull'insieme delle impronte dei documenti presenti nei lotti generati. L'utente riceverà una e-mail di conferma della chiusura del lotto al termine della procedura.
Da quel momento l'utente potrà utilizzare le funzioni di ricerca dei documenti nell'archivio di conservazione. E' possibile la visualizzazione, il download e la verifica/validazione del singolo documento contenuto in ogni lotto. In particolare la verifica della corretta conservazione visualizzerà tutte le informazioni utili alla validazione del documento stesso quali: l'identità del firmatario (il delegato del responsabile della conservazione), la marca temporale, e il risultato del confronto fra l'hash del documento ricalcolato in fase di verifica e quello presente nell'elenco delle impronte del lotto archiviato. Contestualmente è possibile eseguire il download del documento, del file di chiusura firmato e della marca temporale del lotto. Questa funzione assicura agli organi competenti una validazione autonoma della coerenza delle informazioni prodotte e conservate dal servizio.
La funzione di download, inoltre, consente il prelievo dall'archivio di una copia del singolo documento o dell'intero lotto. La visualizzazione e validazione dei lotti di cui è stato compiuto il download è garantita dal software "client" – scaricabile autonomamente dall'utente - che consente le funzionalità base di ricerca e validazione dei documenti scaricati.
Al cliente, su richiesta, può essere messa a disposizione un area FTPS per lo scarico massivo dei propri documenti.
L'utente può permettere al proprio commercialista l'accesso ai documenti conservati semplicemente inserendo la sua email. Il commercialista riceverà così - via email - le proprie credenziali di accesso e di consultazione autonoma – in sola lettura – dei documenti inviati in conservazione dal cliente. L'utente del servizio può annullare in ogni

momento l'e-mail del commercialista impedendo, da quel momento, ogni successiva consultazione al proprio archivio. Modificando invece l'indirizzo e-mail del commercialista si potrà permettere la consultazione del proprio archivio a un altro commercialista. Ogni commercialista può avere visibilità su più clienti e società, a patto che questi lo abilitino alla visualizzazione dei propri archivi.

MODALITA' DI ACQUISTO DEL SERVIZIO

Il servizio è fornito in modalità SaaS (Software as a Service) e può essere acquistato con la tipica modalità di ricarica credito tramite pagamento on-line con PayPal o carta di credito dal sito https://www.kloudarchive.it/ o ordinando la relativa attivazione al fornitore del servizio.
L'utente in ogni caso acquista un "pacchetto di documenti" che vengono accreditati sul suo account al termine del pagamento. Il credito così ottenuto assicura l'accesso al servizio per un anno solare a partire dall'ultima data di acquisto. Al nuovo utente vengono associate le credenziali al servizio e inviate all'indirizzo e-mail fornito.
L'estensione temprale del servizio o l'aumento del numero dei documenti da conservare è subordinata all'acquisto di un qualsivoglia "pacchetto" diverso da quello free. Se un utente acquista contemporaneamente più pacchetti, i crediti relativi sono cumulati e i documenti trattabili risulteranno dalla somma dei pacchetti acquistati (ad esempio se un utente acquista 2 pacchetti da 500 documenti verranno accreditati 1.000 documenti trattabili).
Ogni volta che un documento è immesso nel sistema, il contatore del "numero di documenti disponibili" è decrementato di un'unità fino all'esaurimento del credito.
Allo scadere del credito l'utente avrà l'accesso ai propri documenti fino a che non scadrà il suo account o acquisterà un nuovo pacchetto.

MODALITA' DI DISMISSIONE DEL SERVIZIO

L'utente ha la facoltà di dismettere il servizio semplicemente non acquistando più alcun pacchetto e lasciando scadere il proprio account (cosa che avviene automaticamente dopo un anno solare dall'ultimo "credito" acquistato). Fino allora potrà scaricare i suoi archivi con il relativo visualizzatore "client". Allo scadere dell'account Grammelot S.r.l. si riserva la possibilità di eliminare definitivamente i lotti e i documenti appartenenti all'account, previa comunicazione al cliente stesso, dopo 6 mesi dalla scadenza e di garantire al cliente la possibilità di mantenere i dati per 10 anni con la sottoscrizione di un contratto di mantenimento dello storico da pattuire separatamente.

GRAMMELOT

POLICY DI UTILIZZO

Premesse

La mancata ottemperanza a questa PDU comporterà l'immediata sospensione o interruzione del Servizio KloudArchive (di seguito "Servizio") in conformità con le condizioni di fornitura ad esso relative. Tutte le richieste d'informazioni riguardo al contenuto del presente documento dovranno essere indirizzate aprendo apposito ticket tramite l'invio di una email all'indirizzo di posta: support@Grammelot.eu.

Violazioni

E' vietato l'uso dei servizi Grammelot per porre in essere e/o promuovere comportamenti illegali, abusivi o irresponsabili, tra cui:

- L'accesso non autorizzato o l'uso non autorizzato di dati, sistemi o reti, ivi incluso ogni tentativo di sondare, esaminare o testare la vulnerabilità di un sistema o di una rete o di violare le misure di sicurezza o di autenticazione senza l'espressa autorizzazione del proprietario del sistema o della rete;
- porre in essere attività che rechino interferenze con l'utilizzo del Servizio a qualsiasi utente del medesimo, compresi, a titolo esemplificativo ma non esaustivo, attacchi mediante software pirata, cracks, keygenerators, serials, attacchi informatici di ogni tipologia ivi compresi gli attacchi DOS, virus o altri componenti dannosi o tentativi deliberati di sovraccaricare un sistema di trasmissione;
- utilizzare applicazioni e/o script non consentiti. Resta inteso che nell'ipotesi in cui Grammelot rilevi che applicazioni e/o script, anche non inseriti nel suddetto elenco, provochino malfunzionamento al server, Grammelot si riserva la facoltà di intervenire nella maniera più opportuna al fine di far cessare tale malfunzionamento;
- l'uso di un account Internet o di un personal computer senza l'autorizzazione del proprietario;
- la raccolta o l'utilizzo di indirizzi e-mail, nomi o altri identificativi senza il consenso della persona interessata (inclusi, senza limitazione, spamming, phishing, truffe internet, furto di password, spidering);
- la raccolta o l'utilizzo di informazioni di terzi senza il consenso del proprietario delle informazioni;
- l'uso e/o la diffusione di qualsiasi informazione falsa, fuorviante, ingannevole anche, a titolo esemplificativo ma non esaustivo, mediante e-mail o newsgroup;
- l'utilizzo del servizio per la distribuzione di software che raccolga fraudolentemente informazioni su un utente o trasmetta fraudolentemente informazioni sull'utente;
- l'utilizzo del servizio per la distribuzione di software c.d. "adware".
- Offrire informazioni al pubblico (testuali o grafiche) nocive dell'immagine di Grammelot tramite i servizi messi a disposizione.

Uso delle risorse del sistema

L'utente non potrà utilizzare il servizio in modo che interferisca con il normale funzionamento dei servizi di Grammelot. In tali circostanze, Grammelot potrà richiedere di ripristinare il livello di normalità qualora tale utilizzo non conforme confligga, ad insindacabile giudizio della stessa, con l'utilizzo degli altri utenti. L'utente si impegna a non utilizzare apparecchiature difettose o non omologate secondo gli standard europei, oppure che presentino delle disfunzioni che possano danneggiare l'integrità della rete e/o disturbare i Servizi e/o creare rischi per l'incolumità fisica delle persone. Grammelot, infatti, non presta alcuna garanzia circa la compatibilità degli apparati e dei programmi (hardware e software) utilizzati dal Cliente con il Servizio, essendo tutte le relative verifiche a carico esclusivo del Cliente.

E-mail commerciali.

E' vietata la diffusione di messaggi commerciali se non si è in grado di dimostrare che:
• i destinatari abbiano dato il loro preventivo consenso a ricevere posta elettronica tramite espressa procedura opt-in;
• le procedure di raccolta del consenso comprendano strumenti opportuni a garantire che la persona che presta il proprio consenso sia il titolare dell'indirizzo e-mail per il quale è stato fornito il consenso;
• si conservi la prova del consenso del destinatario in una forma che possa essere prontamente prodotta su richiesta, con l'onere del destinatario delle richieste di Grammelot al riguardo di produrre prova del consenso entro 72 ore dalla ricezione della richiesta della medesima;
• siano applicate procedure che consentano ad un destinatario di revocare il proprio consenso, come, a titolo esemplificativo e non esaustivo, un collegamento nel corpo della e-mail od istruzioni per rispondere con la parola "Rimuovi" nella riga dell'oggetto, e si sia in grado di ottemperare alla revoca del consenso entro 48 ore dal ricevimento, informando i destinatari che la revoca del loro consenso sarà lavorata in 48 ore al massimo;
• sia sempre evidenziato un indirizzo e-mail per i reclami in un luogo ben visibile su ogni sito web associato alla e-mail, e si riscontrino tempestivamente i messaggi inviati a tale indirizzo.
Non è consentito oscurare in qualsiasi forma il mittente della e-mail. L'indirizzo e-mail mittente dovrà comparire nel corpo del messaggio o nella linea "Da" della e-mail;
Queste disposizioni si applicano ai messaggi inviati tramite il Servizio, o per i messaggi inviati da qualsiasi rete da parte dell'utente o da qualsiasi persona per suo conto che direttamente o indirettamente si riferisca al recipient di un sito ospitato tramite i Servizi. Inoltre, non sarà possibile utilizzare un servizio "terzo" di posta elettronica che non applichi procedure simili a tutti i propri clienti. Questi requisiti si applicheranno nella stessa misura alle liste di distribuzione create da terze parti come se la lista fosse stata creata dal Cliente. Grammelot si riserva il diritto di verificare e monitorare in qualsiasi momento il rispetto delle disposizioni sopra elencate, anche con richiesta di informazioni a campione mediante metodo opt-in. Grammelot potrà sospendere la trasmissione di messaggi di posta elettronica che violino le presenti disposizioni.

Autenticazione SMTP – Policy

A completamento delle disposizioni sopra riportate, non sarà consentito inviare attraverso i server SMTP Grammelot messaggi e-mail di contenuto analogo a più di duecentocinquanta (250) destinatari. I tentativi di aggirare questa limitazione mediante la creazione di più account o mediante qualsiasi altro mezzo saranno intesi come una violazione di tale restrizione.
Grammelot si riserva il diritto di sospendere la trasmissione dei messaggi che violino queste disposizioni. Inoltre, i servizi di posta potranno essere sospesi o interrotti qualora venisse ravvisata una violazione di questa AUP, in conformità con le condizioni generali di fornitura.

Mail Relay

In generale non sono consentite trasmissioni di massa o trasmissioni di informazioni commerciali via e-mail per un volume di più di 5.000 (cinquemila) utenti al giorno con una media di 250 messaggi ogni 20 minuti. Se si desidera inviare più di 5.000 messaggi al giorno, si prega di contattare il nostro team di supporto per ulteriori informazioni.
Test di vulnerabilità
L'utente non potrà in alcun modo tentare di sondare, esaminare, penetrare o testare la vulnerabilità del sistema di rete Grammelot o di violare la sicurezza di Grammelot o delle relative procedure di autenticazione, sia con tecniche passive che invasive, senza l'espresso consenso scritto di Grammelot, né, allo stesso modo, potrà effettuare dette attività mediante il servizio fornito da Grammelot nei confronti delle reti e/o delle informazioni di Terzi senza il loro esplicito consenso.

Newsgroup, forum di discussione, altre reti

Il Cliente prende atto ed accetta che i contenuti dei messaggi commerciali, i messaggi su qualsiasi bacheca elettronica, chat di gruppo od altri forum cui partecipi come, a titolo esemplificativo ma non esaustivo, IRC e gruppi USENET, saranno subordinati al rispetto delle leggi e dei regolamenti vigenti in materia. Altresì, lo stesso dovrà rispettare le regole di qualsiasi altro network (rete o circuito) cui acceda o partecipi utilizzando i servizi Grammelot.

Contenuti offesivi

E' vietato pubblicare, trasmettere o memorizzare su o tramite la rete e gli apparati Grammelot qualsiasi contenuto o link a contenuti che Grammelot ritenga ragionevolmente:
• costituire, raffigurare, favorire, promuovere o riferirsi in qualsiasi modo alla pedofilia, al razzismo, al fanatismo, o a contenuti di pornografia che non siano inseriti nel rispetto delle normative vigenti in materia ed accessibili solo alle persone di maggiore età;
• essere eccessivamente violenti, incitare alla violenza, contenere minacce, molestie o espressioni di odio;
• essere sleali o ingannevoli in relazione alle leggi di tutela dei consumatori di qualsiasi giurisdizione, inclusi lettere a catena e schemi a piramide;
• essere diffamatorio o violare la privacy di una persona;
• creare un rischio per la sicurezza della persona o della salute, un rischio per la sicurezza pubblica o la salute pubblica, compromettere la sicurezza nazionale o interferire con indagini dell'Autorità giudiziaria;
• divulgare in modo improprio segreti commerciali o altre informazioni riservate o di proprietà di terzi;
• avere lo scopo di aiutare terzi ad eludere diritti di copyright;
• violare il copyright di terzi, i marchi, i brevetti o altro diritto di proprietà altrui;
• promuovere droghe illegali, violare le leggi sul controllo delle esportazioni, si riferiscano al gioco d'azzardo illegale o illegale traffico di armi;
• essere altrimenti illegali o sollecitare un comportamento illegale secondo le leggi applicabili nella relativa giurisdizione, del Cliente o di Grammelot;
• essere altrimenti dannosi, fraudolenti o poter portare ad azioni legali contro Grammelot.
Per contenuto "pubblicato o trasmesso" tramite la rete o le infrastrutture Grammelot si includono contenuti Web, e-mail, chat e qualsiasi altro tipo di pubblicazione o trasmissione che si basi sulla rete Internet.

Materiale protetto da copyright

E' vietato l'uso dei servizi Grammelot per scaricare, pubblicare, distribuire, copiare o utilizzare in qualsiasi modo qualsiasi opera di testo, musica, software, arte, immagine o altro protetti dal diritto d'autore ad eccezione del caso in cui:
• sia stato espressamente autorizzato dal titolare del diritto;
• sia altrimenti consentito dalle vigenti leggi sul copyright nella pertinente giurisdizione.

Disposizioni finali

 Il Cliente si impegna a comunicare ad Grammelot i propri dati personali necessari all'integrale e corretta esecuzione del contratto; garantisce, altresì, sotto la propria personale ed esclusiva responsabilità, che i predetti dati sono corretti, aggiornati e veritieri e che consentono di individuare la sua vera identità. Il Cliente si impegna a comunicare a Grammelot ogni variazione dei dati forniti, tempestivamente e comunque entro e non oltre 15 (quindici) giorni dal verificarsi della predetta variazione, ed altresì a fornire in qualsiasi momento, previa richiesta di Grammelot, prova adeguata della propria identità, del proprio domicilio o residenza e, se del caso, della propria qualità di legale rappresentante della persona giuridica richiedente o intestataria del Servizio. Al ricevimento della suddetta
comunicazione, Grammelot potrà richiedere al Cliente documentazione aggiuntiva diretta a dimostrare le variazioni comunicate. Nel caso in cui il Cliente ometta di fornire ad Grammelot la predetta comunicazione o la documentazione richiesta, oppure nel caso in cui abbia fornito ad Grammelot dati che risultino essere falsi, non attuali o incompleti o dati che Grammelot abbia motivo, a suo insindacabile giudizio, di ritenere tali, Grammelot si riserva il diritto di:
a) rifiutare la richiesta inoltrata dal Cliente avente ad oggetto operazioni da eseguire in riferimento al Servizio;
b) sospendere i servizi con effetto immediato, senza preavviso ed a tempo indeterminato;
c) annullare e/o interrompere senza preavviso eventuali operazioni di modifica dei dati associati al Servizio;
d) risolvere il contratto
• il Cliente accetta che possano essere messi in quarantena o cancellati i dati memorizzati su un sistema condiviso qualora i suddetti dati siano infettati da un virus o altrimenti corrotti, e abbiano, ad insindacabile giudizio di Grammelot, un potenziale per infettare o danneggiare il sistema o i dati di altri Clienti che vengano immessi sulla stessa infrastruttura.
 Il Cliente si impegna ad osservare le norme di buon uso delle risorse di rete comunemente definite "Netiquette",

SLA

Nessun rimborso previsto nell'allegato "Service Level Agreement" di Grammelot sarà concesso per interruzioni del servizio derivanti da violazioni della presente PDU.

PRIVACY POLICY

Informativa di carattere generale

La presente Policy Privacy ha lo scopo di descrivere le modalità di trattamento dei dati personali degli utenti dei servizi Grammelot. Si tratta di un'informativa resa a coloro che acquistano servizi Grammelot o si collegano al sito www.kloudarchive.it ed alle pagine o domini di terzo livello ad esso collegate. La procedura prevista dalla legislazione vigente prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. A norma della stessa, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza tutelando la riservatezza e i diritti del sottoscrittore. Il trattamento dei dati personali che Grammelot intende effettuare ha la finalità di concludere, gestire ed eseguire i contratti di fornitura dei servizi richiesti; di organizzare, gestire ed eseguire la fornitura dei servizi anche mediante comunicazione dei dati a terzi Fornitori o a società collegate a Grammelot; di assolvere agli obblighi di legge o agli altri adempimenti richiesti dalle competenti Autorità;
Il trattamento sarà effettuato con le modalità informatizzato/manuale;
I dati raccolti saranno altresì utilizzati da Grammelot per l'integrale e la corretta esecuzione del contratto e saranno resi conoscibili a Terzi per la difesa dei diritti nonché in adempimento agli obblighi previsti dalla legge o dai regolamenti e su richiesta dalle competenti Autorità, ed il loro trattamento sarà improntato ai principi di correttezza, liceità e trasparenza tutelando la riservatezza e i diritti del Cliente e di terzi. Il titolare del trattamento è Grammelot S.r.l. con sede in Via Casale, 5 – 20144 Milano (MI), la quale, a norma del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (GDPR) potrà rispettivamente nominare uno o più Responsabili Esterni del trattamento che operino sotto la propria diretta autorità sulla base delle istruzioni ricevute, identificati all'interno del territorio dell'Unione Europea e nel rispetto delle cautele previste dalla stessa in materia di protezione di dati personali. In ogni momento il Cliente potrà rivolgersi al Titolare del trattamento (Grammelot S.r.l.) contattando gli Uffici del Titolare del trattamento - per esercitare i propri diritti, così come previsto dalla legislazione vigente.

Dati di navigazione e di accesso

I sistemi informatici e le procedure software preposte al funzionamento dei servizi Grammelot acquisiscono, nel normale esercizio, alcuni dati personali che vengono trasmessi implicitamente nell'uso di protocolli di comunicazione internet. Si tratta di dati relativi al traffico telematico che per loro natura non sono immediatamente associabili ad interessati identificati, ma tramite elaborazioni o associazioni con dati detenuti da terzi potrebbero permettere di identificare gli utenti/visitatori del sito (es. indirizzi IP). Questi dati vengono utilizzati soltanto per informazioni statistiche anonime relative all'utilizzo del servizio o per verificare la corretta funzionalità dello stesso. Tali dati sono conservati dalla Società Grammelot S.r.l. per il periodo strettamente necessario e comunque in conformità alle vigenti disposizioni normative in materia. Il Cliente prende espressamente atto dell'esistenza del Registro dei Collegamenti (LOG - dati relativi al traffico telematico), compilato e conservato da Grammelot nei termini e con le modalità stabilite dalla legge. Il predetto registro costituisce piena ed incontrovertibile prova dei fatti e degli atti compiuti dal Cliente medesimo di fronte ad Grammelot e/o a Terzi; esso ha carattere di riservatezza assoluta e potrà essere esibito e/o fornito esclusivamente su richiesta dei Soggetti espressamente indicati dalla Legge. Grammelot adotta tutte le misure tecniche ed organizzative necessarie a garantire la riservatezza dei registri di collegamento. Grammelot si riserva la facoltà di conservare i "Log di accesso" (cd. LOG FTP) generati dal Cliente in occasione degli accessi al servizio oggetto di contratto, per un periodo di tempo pari o superiore alla durata del rapporto contrattuale. Trascorso il periodo di conservazione previsto dalla legge i predetti dati verranno distrutti e non sarà più garantita la possibilità di ottenere copia di tale documentazione.

Cookies

Sui siti web di Grammelot sono utilizzati dei "cookies" (marcatori temporanei) che permettono di accedere più velocemente ai medesimi. Per "cookie" si intende un dato informativo, attivo solamente per la durata della singola sessione-utente, che sarà trasmesso dal sito web al computer dell'Utilizzatore al fine di permetterne una rapida identificazione. L'Utilizzatore potrà sempre richiedere la disattivazione dei cookies modificando le impostazioni del browser, tale disattivazione, però, potrà rallentare o impedire l'accesso ad alcune parti del sito. I cookies di sessione utilizzati evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente. Dati forniti dagli utenti Qualora il Cliente intenda registrarsi nella banca dati di Grammelot S.r.l., al fine di accedere ai servizi dalla stessa forniti, dovrà compilare un "form" nel quale rilascerà il proprio espresso consenso al trattamento dei dati. La comunicazione dei dati sarà indispensabile ma non obbligatoria, e l'eventuale rifiuto non avrà alcuna conseguenza ma potrà comportare il mancato puntuale adempimento delle obbligazioni assunte da Grammelot S.r.l. per la fornitura del servizio richiesto.

Immissione di dati da parte del Cliente

Il Cliente effettua autonomamente da remoto via internet, attraverso apposita login, password e/o tramite relativi programmi FTP l'inserimento e/o l'aggiornamento del materiale immesso nello spazio a sua disposizione, Grammelot non effettua né potrebbe effettuare alcun controllo su tali informazioni. Pertanto, il Cliente si impegna a farsi carico della protezione dei dati immessi ed a ottemperare autonomamente e direttamente a tutte le disposizioni normative in materia di protezione di dati personali compreso acquisire il consenso da parte di terzi quando necessario.

Siti e servizi di Terzi

Sulle pagine web di Grammelot si possono trovare collegamenti ipertestuali con altri siti web, proposti per fornire un migliore servizio ai propri utenti. Grammelot non è in alcun modo responsabile del contenuto dei siti web ai quali gli utenti dovessero eventualmente accedere tramite il proprio sito. L'esistenza di un link verso un altro sito non sottintende quindi approvazione od accettazione di responsabilità da parte di Grammelot circa il contenuto del nuovo sito cui si accede, anche in relazione alla politica adottata per il trattamento dei dati personali, nonché alla sua utilizzazione.

Sicurezza delle informazioni

Tutte le informazioni raccolte vengono memorizzate e mantenute in strutture sicure che limitano l'accesso esclusivamente al personale autorizzato. I servizi vengono costantemente mantenuti per verificare l'eventuale presenza di violazioni della sicurezza ed assicurare che tutte le informazioni raccolte siano al riparo da eventuali intrusioni di terzi che intendessero prenderne possesso senza autorizzazione.
Grammelot S.r.l. si attiene a tutte le misure di sicurezza descritte dalle leggi e dalle normative applicabili e vigenti nell'Unione Europea, ed adotta tutte le misure adeguate secondo i criteri attualmente più all'avanguardia per assicurare e garantire la riservatezza dei dati personali degli utenti e ridurre al minimo, per quanto possibile, i pericoli costituiti dall'accesso non autorizzato, dalla rimozione, perdita o dal danneggiamento dei dati personali degli utenti.

Diritto di accesso ai dati personali ed altri diritti (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio - GDPR):

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Contatti

Tutte le richieste dovranno essere indirizzate ad Grammelot S.r.l. con sede in Via Casale, 5 – 20144 Milano (MI) Tel. 0289075413 Fax 0232066978.

GRAMMELOT

SERVICE LEVEL AGREEMENT

1 Oggetto e scopo del documento

Obiettivo del presente “Service Level Agreement” (in seguito per brevità "SLA") è quello di definire i parametri di riferimento per l'erogazione del servizio Kloud Archive (in seguito per brevità "Servizio") e per il monitoraggio del livello di qualità effettivamente erogato.
Obiettivo dello SLA è anche quello di definire le regole di interazione tra Grammelot ed il Cliente. Il presente SLA è parte integrante del Contratto perfezionatosi tra Grammelot e Cliente con le modalità previste all'art. 3 delle Condizioni Generali di Fornitura del Servizio. Il presente SLA si applica separatamente a ciascun Cliente e per ciascun Contratto.

2 Validità e durata dello SLA - modifiche o sostituzioni dello SLA

Il presente SLA entra in vigore a tempo indeterminato per ciascun Cliente a decorrere dal perfezionamento di ciascun Contratto e termina con la cessazione del Contratto cui si riferisce. Grammelot si riserva la facoltà di modificarlo o sostituirlo più volte nel corso del Contratto ed in qualsiasi momento. Le modifiche apportate allo SLA ovvero il nuovo SLA - sostitutivo di quello precedente - entrano in vigore, sempre a tempo indeterminato ovvero fino alla prossima modifica o sostituzione, dalla data della loro pubblicazione alla pagina http://computing.cloud.it/it/termini-condizioni; In tale ipotesi tuttavia è data facoltà al Cliente di recedere dal Contratto con le modalità previste in Contratto entro trenta giorni dalla pubblicazione della modifica e/o dalla sostituzione dello SLA. In caso di recesso da parte del Cliente si applica la disciplina prevista all'art. 11.1. e 11.3. delle Condizioni di Fornitura del Servizio.

3 SLA di funzionalità operativa

Grammelot farà ogni ragionevole sforzo per garantire la massima disponibilità dell'Infrastruttura virtuale creata ed allocata dal Cliente e, contestualmente, l'osservanza dei seguenti parametri di funzionalità operativa:
A) Risorse del Data Center attraverso il quale viene erogato il Servizio
- Uptime del 100% su base annuale per alimentazione elettrica e/o climatizzazione ambientale ;
- lo spegnimento della Infrastruttura virtuale creata ed allocata dal Cliente causato dalla mancanza generalizzata dell'alimentazione elettrica e/o della climatizzazione ambientale costituisce disservizio per il quale, in base alla sua durata, è dovuto al Cliente, a titolo di indennizzo, il credito determinato ai sensi del successivo art. 6 del presente SLA.
- Uptime del 99,90% su base annuale, di accessibilità tramite rete internet alla Infrastruttura virtuale creata ed allocata dal Cliente.
- la completa inaccessibilità tramite rete internet alla Infrastruttura virtuale creata ed allocata dal Cliente per un tempo complessivo superiore a quello determinato dal parametro di Uptime garantito da Grammelot costituisce disservizio per il quale, in base alla sua durata, è dovuto al Cliente, a titolo di indennizzo, il credito determinato ai sensi del successivo art. 6 del presente SLA.
B) Infrastruttura virtuale creata ed allocata dal Cliente
- Uptime del 99,90% su base annuale, per la disponibilità dei nodi fisici (server) che ospitano l'Infrastruttura virtuale;

- il mancato funzionamento della Infrastruttura virtuale creata ed allocata dal Cliente - per un tempo complessivo superiore a quello determinato dal parametro di Uptime garantito da Grammelot - causato da guasti e/o anomalie dei suddetti nodi fisici costituisce disservizio per il quale, in base alla sua durata, è dovuto al Cliente, a titolo di indennizzo, il credito determinato ai sensi del successivo art. 6 del presente SLA.

4 Manutenzione programmata

4.1. Il tempo di manutenzione programmata non viene conteggiato ai fini del calcolo degli Uptime. La manutenzione programmata riguarda le attività svolte regolarmente da Grammelot per mantenere la funzionalità delle risorse del Data Center attraverso il quale viene erogato il Servizio e dei nodi fisici che ospitano l'Infrastruttura virtuale; essa è ordinaria e straordinaria.
4.2. L'esecuzione degli interventi di manutenzione sarà comunicata da Grammelot al Cliente con un preavviso minimo di 24 ore a mezzo e mail inviata all'indirizzo di posta elettronica indicato in fase d'ordine. Grammelot si impegna a compiere ogni ragionevole sforzo per eseguire le attività di manutenzione programmata in orari di minimo impatto per l'Infrastruttura virtuale del Cliente.

5 Rilevamento guasti e/o anomalie

5.1.Eventuali guasti e/o anomalie alle risorse del Data Center attraverso il quale viene erogato il Servizio ovvero ai nodi fisici che ospitano l'Infrastruttura virtuale creata ed allocata dal Cliente saranno segnalate dal Cliente aprendo un ticket tramite invio di email a support@Grammelot.eu; ai fini del riconoscimento dei crediti di cui al successivo art. 6 saranno tuttavia presi in considerazione soltanto i disservizi confermati anche dal sistema di monitoraggio di Grammelot.
5.2. Guasti o anomalie possono essere segnalati dal Cliente al servizio assistenza Grammelot dalle ore 9 alle ore 18 dal Lunedì al Venerdì ad esclusione dei giorni calendariali festivi,. Ogni segnalazione pervenuta sarà tempestivamente inoltrata al supporto tecnico rispettando rigorosamente l'ordine cronologico di suo ricevimento;
5.3. Il monitoraggio da parte di Grammelot viene effettuato tramite software specifici che rilevano ed indicano eventuali guasti o anomalie dandone comunicazione in tempo reale al servizio assistenza operativo 24/7/365;

6 Crediti

6.1. Ai sensi del presente SLA Grammelot riconosce al cliente, a titolo di indennizzo, un credito pari al 2,5% della spesa complessiva generata - nei trenta giorni precedenti al disservizio - dalla parte di infrastruttura virtuale da esso interessata per ogni frazione completa da quindici minuti di disservizio oltre i limiti previsti dal presente SLA, fino ad un massimo di trecento minuti.
6.2. Per farsi riconoscere il/i Credito/i il Cliente deve rivolgere richiesta al Servizio di Assistenza Grammelot aprendo un ticket tramite invio di email a support@Grammelot.eu entro 10 giorni dalla fine del Disservizio.
6.3. Fermo quanto sopra resta in ogni caso inteso che durante il periodo di sua inattività il Servizio non genera spesa pertanto per tale periodo dalla Ricarica non sarà detratto il corrispondente importo previsto nel Listino prezzi
7. Limiti di applicabilità dello SLA
Qui di seguito sono riportate le condizioni in presenza delle quali, nonostante il verificarsi di eventuali disservizi, al Cliente non è dovuto l'indennizzo previsto dallo SLA:
- cause di Forza Maggiore e cioè eventi che, oggettivamente, impediscano al personale di Grammelot di intervenire per eseguire le attività poste dal Contratto a carico della stessa Grammelot (in via meramente esemplificativa e non esaustiva: scioperi e manifestazioni con blocco delle vie di comunicazione; incidenti stradali; guerre e atti di terrorismo; catastrofi naturali quali alluvioni, tempeste, uragani etc);
- interventi straordinari da effettuarsi con urgenza ad insindacabile giudizio di Grammelot per evitare pericoli alla sicurezza e/o stabilità e/o riservatezza e/o integrità dell'Infrastruttura virtuale creata ed allocata del Cliente e dei dati e/o informazioni in essa contenuti. L'eventuale esecuzione di tali interventi sarà comunque comunicata al Cliente a mezzo e mail inviata all'indirizzo di posta elettronica indicato in fase d'ordine con preavviso anche inferiore alle 24 ore oppure contestualmente all'avvio delle operazioni in questione o comunque non appena possibile;
- indisponibilità o blocchi dell'Infrastruttura virtuale creata ed allocata dal Cliente imputabili a; a) errato utilizzo, errata configurazione o comandi di spegnimento, volontariamente o involontariamente eseguiti dal cliente; b) anomalie e malfunzionamenti dei software applicativi/gestionali forniti da terze parti; c) inadempimento o violazione del Contratto imputabile al Cliente;
- anomalia o malfunzionamento del Servizio, ovvero loro mancata o ritardata rimozione o eliminazione imputabili ad inadempimento o violazione del Contratto da parte del Cliente ovvero ad un cattivo uso del Servizio da parte sua;
- mancato collegamento della/e infrastruttura/e virtuale/i alla rete pubblica per volontà o per fatto del Cliente;
- cause che determinano l'inaccessibilità, totale o parziale, dell'Infrastruttura virtuale creata e allocata dal Cliente imputabili a guasti nella rete internet esterna al perimetro di Grammelot e comunque fuori dal suo controllo

GRAMMELOT

Manuale di Conservazione Digitale

di Grammelot Srl

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	28/10/2014	Riccardo Sirtori	Direttore Tecnico
Verifica	05/11/2014	Massimo Maronati	CEO
Approvazione	07/11/2014	Massimo Maronati	CEO

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	28/10/14	Prima emissione	Prima stesura
1.1	20/10/17	Aggiornamento normativo	
2.0	01/10/20	Aggiornamento normativo	
3.0	10/10/2021	Aggiornamento normativo e rielaborazione puntuale in base alle nuove LLGG AgID (di Maggio 2021)	

GRAMMELOT

INDICE

1 SCOPO E AMBITO DEL DOCUMENTO

Scopo di questo documento è di descrivere tutte le procedure e informazioni relative al Sistema di Conservazione Digitale in uso e di dare evidenza di tutte le componenti presenti, sia in termini di software utilizzato sia di personale e ruoli associati.

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Glossario dei termini e Acronimi ricorrenti nel testo o comunque giudicati significativi in relazione alla materia trattata. Di seguito si riporta la tabella.

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
CA	Certification Authority
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
TSA	Time stamping authority di riferimento per la marca temporale
OAIS	ISO 14721:2012; Space Data information transfer system
PdV	Pacchetto di Versamento
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

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

Contesto nazionale

- Codice Civile – "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 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 11 febbraio 2005 n. 68 . Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del 2 novembre 2005 - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (Gazzetta Ufficiale n. 266 del 15-11-2005) del Ministro per l'Innovazione e le Tecnologie;

- Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici;
- Deliberazione Cnipa del 21 maggio 2009, n. 45 (come modificata dalla determinazione dirigenziale DigitPA n. 69/2010). Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013 - Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- 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;
- Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (Maggio 2021) (LLGG AgID)

Altre normative

- Decreto Legislativo 1 settembre 1993 n.385 - "Testo unico delle leggi in materia bancaria e creditizia";
- Decreto Legislativo 6 settembre 2005, n. 206 - Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229;
- Decreto Legislativo 9 aprile 2008, n. 81 - Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- Decreto Legislativo 10 agosto 2018, n. 101 e s.m.i. - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018).
- Regolamento (UE) 2016/679 (General Data Protection Regulation o GDPR) del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018).
- Legge 22.04.1941 n. 633 , G.U. 16.07.1941 e s.m.i. - Legge sul diritto d'autore.

3.2 Standard di riferimento

ISO/IEC

- UNI EN ISO 9000:2015 - Sistemi di gestione per la qualità - Fondamenti e vocabolario;
- UNI EN ISO 9001:2015 - Sistemi di gestione per la qualità - Requisiti;
- UNI EN ISO 19011:2018 - Linee guida per audit di sistemi di gestione;
- ISO 14721:2012 - Space data and information transfer systems - Open archival information system (OAIS) - Reference model; Sistema informativo aperto per l'archiviazione;
- UNI ISO 31000:2010 - Gestione del rischio - Principi e linee guida;
- ISO/IEC 27000:2012 - Overview and vocabulary;
- ISO/IEC 27001:2017 - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO/IEC 27002:2013 - Code of practice for information security controls;
- ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management;
- UNI ISO 15489-1:2006 - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management;
- UNI ISO 15489-2:2007 - Informazione e documentazione - Gestione dei documenti di archivio - Linee Guida sul record management;
- UNI 11386 - 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 metadati del Dublin Core.

ETSI (European Telecommunications Standards Institute)

- 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) - Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors; Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI GS ISI 001-1 V1.1.1 (2013-04) - Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operation al indicators for organizations to use to benchmark their security posture;
- ETSI GS ISI 001-2 V1.1.1 (2013-04) - Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1;
- ETSI GS ISI 002 V1.1.1 (2013-04) - Information Security Indicators (ISI); Event Model A security event classification model and taxonomy;
- ETSI GS ISI 003 V1.1.2 (2014-06) – Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection;
- ETSI GS ISI 004 V1.1.1 (2013-12) - Information Security Indicators (ISI); Guidelines for event detection implementation.

OAIS(Open Archival Information System)

- Consultative Committee for Space Data Systems (CCSDS) – Audit and Certification of Trustworthy Digital Repositories – Recommended Practice – CCSDS 652.0-M-2-2012;
- Consultative Committee for Space Data Systems (CCSDS) – Reference Model for an Open Archival Information System (OAIS).
- EIDAS
- Regolamento UE n° 910/2014 – eIDAS (electronic IDentification Authentication and Signature)

4 RUOLI E RESPONSABILITA'

Nel presente capitolo s'indicano le attività svolte e i nomi delle persone che ricoprono i ruoli elencati nella tabella seguente.

Ruoli	Nome	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del Servizio di Conservazione	Massimo Maronati	- definizione e attuazione delle politiche complessive del sistema di Conservazione, 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 regole operative di erogazione dei servizi di Conservazione.	10 anni	Riccardo Sirtori

Responsabile Sicurezza dei sistemi per la Conservazione	Riccardo Sirtori	- 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.	10 anni	

Responsabile funzione archivistica di conservazione	Riccardo Sirtori	- Definizione e gestione del processo di conservazione, incluse le regole di trasferimento da parte dell'ente produttore, di acquisizione, verifica, integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di Conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di Conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di Conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in Conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	10 anni	

Responsabile trattamento dati personali	Massimo Maronati	- 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	10 anni	

Responsabile sistemi informativi per la conservazione	Riccardo Sirtori	- Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; - monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - segnalazione delle eventuali difformità degli SLA al Responsabile del Servizio di Conservazione. - 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.	10 anni	

Responsabile sviluppo e manutenzione del sistema di conservazione	Riccardo Sirtori	- 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 con l'ente produttore riguardo alle regole 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.	10 anni	

Ruoli esterni al SdC

Nella presente sezione sono riportati, a titolo non esaustivo, i ruoli principalmente individuabili nelle strutture organizzative dei soggetti produttori.

Produttore

- Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che, avvalendosi dei servizi di gestione degli archivi informatici erogati dal service provider, produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.

Responsabile della conservazione

Il Responsabile della conservazione è una figura, interna al perimetro del soggetto produttore, che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo adottato.

Utente

Il ruolo di utenti del sistema di conservazione è ricoperto dai soggetti che, opportunamente autorizzati, accedono al SdC e, tramite l'interazione con esso, ricercano le informazioni di interesse, le consultano e ottengono uno o più Pacchetti di Distribuzione (PdD).

Certification Authority e fornitori di servizi di Firma Digitale

I certificati crittografici utilizzati nel processo di firma sono certificati rilasciati da Certificatori accreditati dall'AGID.

I dispositivi HSM eventualmente utilizzati per la gestione massiva di operazioni di firma digitale è conforme al DPCM. 22 febbraio 2013 e viene mantenuto in un Data Center, sito presso il certificatore accreditato, con certificazioni ISO 27001:2017, ISO 9001:2015, ISO 14001:2015, OHSAS 18001:2007.

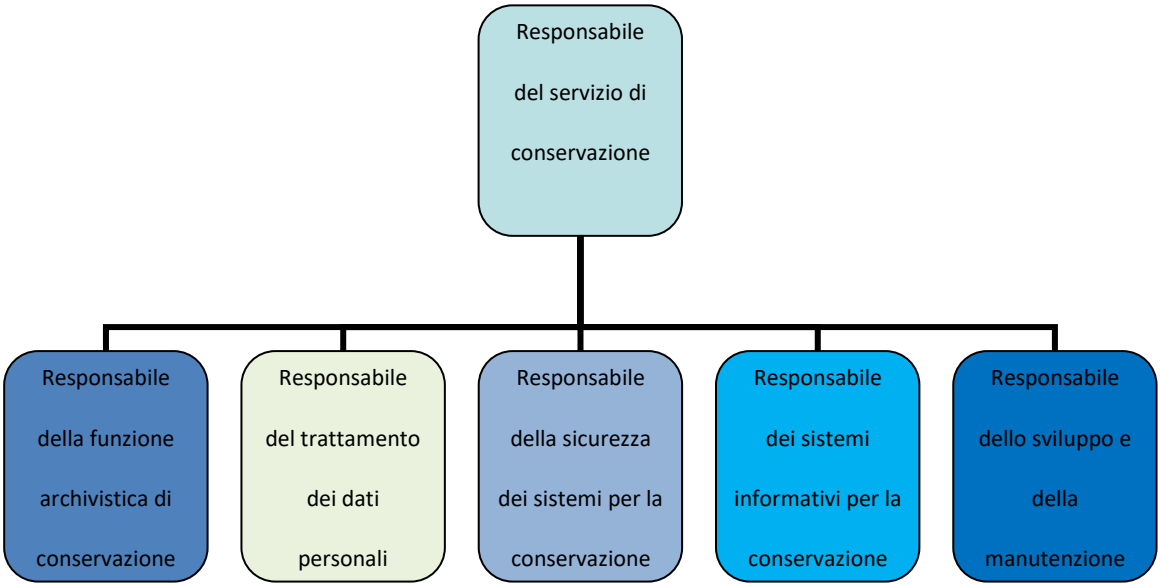
Time Stamping Authority

Le marche temporali utilizzate nel processo di apposizione dela marca temporale sono rilasciate da Certificatori accreditati dall'AGID.

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Indicazione delle strutture organizzative coinvolte nel servizio di conservazione:



5.2 Strutture organizzative

Di seguito sono descritte le strutture organizzative e le responsabilità delle principali funzioni relative al Servizio di Conservazione:

- attività specifiche per ciascun contratto di Servizio di Conservazione:
  - attivazione del Servizio di Conservazione (a seguito della sottoscrizione di un contratto)
    - Responsabile del servizio di conservazione
    - Responsabile Sicurezza dei sistemi per la conservazione
    - Responsabile funzione archivistica di conservazione
    - Responsabile trattamento dati personali
    - Responsabile sistemi informativi per la conservazione
    - Responsabile sviluppo e manutenzione del sistema di conservazione
  - acquisizione, verifica e gestione dei Pacchetti di Versamento presi in carico e generazione del rapporto di versamento:
    - Responsabile del Servizio di Conservazione
    - Responsabile Sicurezza dei Sistemi per la Conservazione
    - Responsabile funzione archivistica di Conservazione
    - Responsabile sistemi informativi per la Conservazione
  - preparazione e gestione del Pacchetto di Archiviazione:
    - Responsabile del servizio di conservazione
    - Responsabile Sicurezza dei Sistemi per la Conservazione
    - Responsabile funzione archivistica di Conservazione
    - Responsabile sistemi informativi per la Conservazione

- preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta:
    - Responsabile del Servizio di Conservazione
    - Responsabile Sicurezza dei sistemi per la Conservazione
    - Responsabile funzione archivistica di Conservazione
    - Responsabile sistemi informativi per la Conservazione

- scarto dei Pacchetti di Archiviazione:
    - Responsabile del Servizio di Conservazione
    - Responsabile Sicurezza dei sistemi per la Conservazione
    - Responsabile funzione archivistica di Conservazione
    - Responsabile sistemi informativi per la Conservazione

- chiusura del Servizio di Conservazione (al termine di un contratto).
    - Responsabile del servizio di Conservazione
    - Responsabile Sicurezza dei sistemi per la Conservazione
    - Responsabile funzione archivistica di Conservazione
    - Responsabile trattamento dati personali
    - Responsabile sistemi informativi per la Conservazione
    - Responsabile sviluppo e manutenzione del sistema di Conservazione

- attività proprie di gestione dei sistemi informativi:
  - conduzione e manutenzione del sistema di Conservazione:
    - Responsabile del servizio di Conservazione
    - Responsabile Sicurezza dei sistemi per la Conservazione
    - Responsabile funzione archivistica di Conservazione
    - Responsabile sistemi informativi per la Conservazione
  - monitoraggio del sistema di Conservazione:
    - Responsabile del servizio di Conservazione
    - Responsabile Sicurezza dei sistemi per la Conservazione
    - Responsabile funzione archivistica di Conservazione
    - Responsabile trattamento dati personali
    - Responsabile sistemi informativi per la Conservazione
    - Responsabile sviluppo e manutenzione del sistema di Conservazione
  - change management:
    - Responsabile del servizio di Conservazione
    - Responsabile Sicurezza dei sistemi per la Conservazione
    - Responsabile funzione archivistica di Conservazione
    - Responsabile trattamento dati personali
    - Responsabile sistemi informativi per la Conservazione
    - Responsabile sviluppo e manutenzione del sistema di Conservazione

- verifica periodica di conformità a normativa e standard di riferimento:
    - Responsabile del servizio di Conservazione
    - Responsabile Sicurezza dei sistemi per la Conservazione
    - Responsabile funzione archivistica di Conservazione
    - Responsabile trattamento dati personali
    - Responsabile sistemi informativi per la Conservazione
    - Responsabile sviluppo e manutenzione del sistema di Conservazione

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Descrizione delle tipologie degli oggetti - e dei pacchetti in essi contenuti - sottoposti a Conservazione.

6.1 Oggetti conservati

Di seguito sono elencati i formati gestiti:

Visualizzatore	Produttore	Formato del file	Versione del formato	Sistema operativo	Riferimenti licenza e relativa scadenza
Adobe reader	Adobe	PDF e PDF/A (.pdf)		Windows	Free
Alternatiff	Medical informatics engineering	Tiff (.tif)		Windows	Free
Visualizzatore foto	Microsoft	JPG (.jpg, .jpeg)		Windows	Free
Chrome	Google	Office Open XML (OOXML) (.docx, .xlsx, .pptx)		Windows	Free
OpenOffice	Apache	Open Document Format (.ods, .odp, .odg, .odb)		Windows	Free
Browser embedded	Google Microsoft	XML (.xml)		Windows	Free
Browser embedded	Google Microsoft	TXT (.txt)		Windows	Free
Thunderbird	Apache	Posta elettronica (.eml)		Windows	Free
Dike	Infocert	P7M (.p7m) (tutti i file sopra elencati firmati digitalmente)		Windows	Free

Nell'ALLEGATO A, che è parte integrante del presente Manuale della Conservazione, sono indiciate le tipologie documentali oggetto del servizio di conservazione e i metadati associati ad ognuna delle suddette tipologie.

L'ALLEGATO A potrà essere variato soltanto in forma scritta e accettato dal Responsabile della Conservazione ovvero da suoi delegati anche di altre ragioni sociali a cui il l'erogazione del servizio è assegnato.

6.2 Pacchetto di versamento

Il PdV è il pacchetto informativo, inviato dal produttore al sistema di conservazione, il cui formato e contenuto sono concordati con il soggetto produttore.

I PdV contengono insiemi informativi da sottoporre al procedimento di conservazione e sono generati tramite procedura interna appositamente implementata per i procedimenti gestiti dal sistema di conservazione.

I PdV sono trasmessi al conservatore tramite:

- appositi web service
- tramite canale sicuro concordato con il conservatore,
- tramite interfaccia web-based e/o mediante una azione di "upload" dei documenti informatici,
- tramite altri strumenti software eventualmente sviluppati e messi a disposizione dal sistema di conservazione.

Le informazioni e le specifiche di carattere tecnico, relative alle diverse tipologie di pacchetti di versamento trattati, sono concordate, specificate ed approfondite nei contratti di servizio stipulati.

I PdV sono composti da un singolo file con estensione convalidata appartenente alle tipologie previste dall'allegato 2 delle LLGG AgID e da un descrittore XML che ne definisca i metadati associati secondo la seguante stuttura (Oltre ai metadati minimi dell'allegato 5 delle LLGG AgID):

```
<?xml version="1.0" encoding="UTF-8"?>
<DocumentoInformatico>
  <index id="Doc_id" value="#VALUE" />
  <index id="#Indice1" value="#VALUE " />
  <index id="#indice2" value="#VALUE " />
…
  <index id="#IndiceN" value="#VALUE"  />
  <Karchive_AnnoFiscale value="#VALUE" />
  <Karchive_Azienda value="#VALUE" />
  <Karchive_TipoDoc value="#VALUE" />
…
</DocumentoInformatico >
```

Dove

- **Doc_Id** è l'identificativo univoco del documento e lo identifica inequivocabilmente da qualunque altro documento che non ne sia una sua versione.
- **#Indice1..N** contiene la descrizione del metadato
- **#VALUE** contiene il valore del metadato
- **Karchive_AnnoFiscale** Anno fiscale di riferimento
- **Karchive_Azienda** azienda di riferimento
- **Karchive_TopoDoc** tipologia documentale di riferimento

6.3 Pacchetto di Archiviazione

Il Pacchetto di Archiviazione consiste nell'insieme dei Pacchetti di Versamento che sono associabili alla medesima Figura Giuridica (azienda) e alla medesima tipologia documentale. Ogni Pacchetto di Archiviazione consiste in un folder in cui sono presenti due sottocartelle:

- **Docs**: dove sono inseriti tutti i documenti derivanti dai Pacchetti di Versamento;
- **Index**: dove sono inseriti tutti gli xml descrittori presenti in ogni Pacchetto di Versamento.

Nella root di ogni Pacchetto di Archiviazione è presente il Rapporto di Versamento in formato XML contenente tutti gli HASH dei documenti dei Pacchetti di Versamento, firmato digitalmente, con riferimento temporale e l'Indice del Pacchetto di Archiviazione (IPdA) secondo le regole tecniche definite nella norma UNI 11386 Standard SInCRO (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali), firmato digitalmente con riferimento temporale e sul quale viene apposta anche una Marca Temporale.

Non sono presenti aggiunte al IPdA nel campo <moreInfo>

Le informazioni più rilevanti che il sistema di conservazione gestisce, in relazione ad ogni PdA prodotto, sono:

- Identificativo univoco dell'IPdA generato automaticamente dal sistema di conservazione;
- Informazioni sull'applicazione che ha generato il PdA (produttore del software, nome e versione);
- Informazioni sui PdV contenuti nell'indice;
- Informazioni su documenti (ID, Impronta di hash, formato, percorso);
- Informazioni relative al processo di conservazione (elementi identificativi del responsabile del servizio di conservazione);
- Informazioni relative alla data di produzione del pacchetto stesso (marca temporale);
- Informazioni relative alla firma digitale.

6.4 Pacchetto di Distribuzione

Il Pacchetto di Distribuzione coincide con il Pacchetto di Archiviazione e può essere scaricato dall'applicativo con il suo Viewer Standalone per la Consultazione/Esibizione offline.

La richiesta di esibizione dei documenti conservati da parte dell'utente viene soddisfatta attraverso la generazione di un PdD formato secondo le regole tecniche definite nello Standard SInCRO e con struttura analoga a quella del PdA.

Il PdD è corredato dalle seguenti informazioni a titolo non esaustivo:

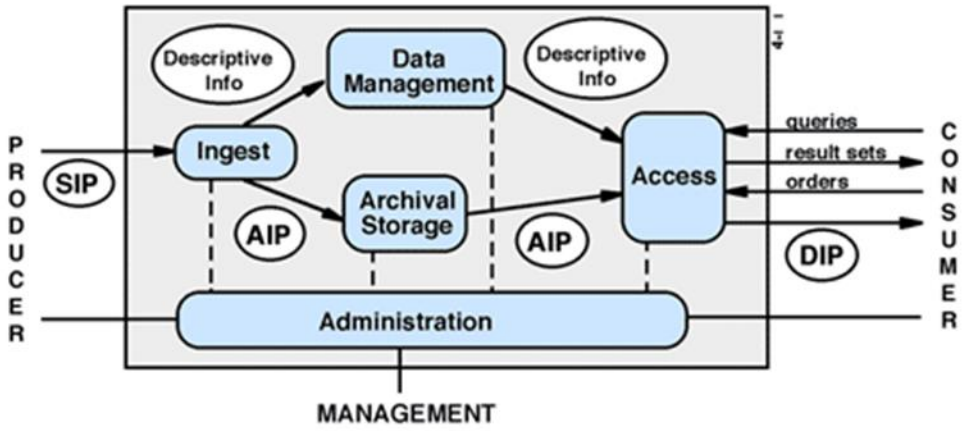
- Identificativo univoco dell'PdD generato automaticamente dal SdC;
- Informazioni sull'applicazione che ha generato il PdD (produttore del software, nome e versione);
- Informazioni sui PdV contenuti nel PdD;
- Informazioni sui documenti (ID, Impronta di hash, formato, percorso);
- Informazioni relative al processo di conservazione (elementi identificativi del responsabile del servizio di conservazione);
- Informazioni relative alla data di produzione del pacchetto stesso (marca temporale);
- Informazioni relative alla firma digitale.

Le richieste di esibizione dei PdD sono accettate solamente se provenienti dai soggetti autorizzati.

7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione si svolge sulla base delle modalità previste dalle LLGG AgID ed è realizzato sulla base del modello funzionale OAIS (Open Archival Information System) normato dallo standard ISO 14721:2003 a cui si fa riferimento. Il modello OAIS ha introdotto nella gestione degli archivi informatici i concetti fondamentali relativi alle modalità di transazione dei pacchetti informativi (PdV, PdA, PdD) contemplati e descritti nel presente manuale.

Nello schema che segue si evidenziano le modalità che regolano il flusso informativo di pacchetti informativi generati da un soggetto produttore (nello schema: Producer) sotto forma di PdV (nello schema: SIP) ad un sitema di conservazione (nello schema: management) che lo trasforma in PdA (nello schema: AIP) e ne cura la conservazione ed il mantenimento nel tempo. Il sistema di conservazione provvede anche a mettere a disposizione dell'utente (nello schema: consumer) il contenuto del PdA tramite opportune modalità di accesso (nello schema: Access) e sotto forma di PdD (nello schema DIP).



7.1 Modalità di acquisizione dei Pacchetti di Versamento per la loro presa in carico

I Pacchetti di Versamento, come già anticipato, sono da considerarsi elementi atomici composti di un solo documento con relativi metadati che formano il Descrittore o Indice.

La coppia di file documento-indice costituisce quindi il PdV da conservare. Il PdV è preso in carico dal momento del suo deposito all'interno della directory d'ingresso del software di Conservazione Karchive/Kloudarchive. Il software si fa carico di svolgere il processo di Conservazione secondo le norme vigenti. L'elaborazione e la predisposizione del Rapporto di Versamento (RdV), così come file XML, sono associate alla forma giuridica e alla tipologia documentale a cui il documento appartiene. In base a queste discriminanti il PdV è inserito nel corretto RdV del relativo PdA con identificativo univoco. All'interno del Rapporto di Versamento per ogni PdV è inserita l'Impronta del documento (l'intero contenuto del PdV) e il nome del file di riferimento.

Al termine dell'elaborazione dei PdV, il RdV è firmato digitalmente con riferimento temporale a cura del Responsabile del servizio di Conservazione o da un suo delegato.

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

Sui PdV sono eseguite le verifiche di coerenza dei formati dei file previsti. Qualora non siano conformi a tali standard, i PdV vengono scartati.

Il controllo e l'identificazione certa del produttore sono date dal canale stesso di caricamento che è legato ad una autenticazione con userid e password, sia sul canale FTP/S sia sul caricamento da portale web sia dal caricamento tramite web services.

Log dei pacchetti di versamento controllati

Le verifiche effettuate sui PdV consentono di evidenziare nel log del SdC almeno le seguenti possibili anomalie determinate da:

- Controlli di formato: se non presenti nell'elenco dei formati accettati dal sistema di conservazione i PdV vengono rifiutati e nel log riportate le relative informazioni

Tutte le informazioni vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente, processo informatico, tipo di operazione, identificativo univoco dei PdV.

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

Il processo di Conservazione prevede l'accettazione del PdV con la generazione del Rapporto di Versamento contenente gli estremi identificativi dei documenti processati e appartenenti ad un Pacchetto di Archiviazione firmato digitalmente dal responsabile del servizio di conservazione o da un suo delegato. Il Rapporto di Versamento è un file XML contenente il nome del file conservato e la sua impronta hash SHA-256.

Il RdV è firmato digitalmente con riferimento temporale come "signing time" della firma.

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

Nel caso in cui un Pacchetto di Versamento sia rifiutato il responsabile del servizio di conservazione è avvisato dall'interfaccia grafica, consentendogli di adottare tempestivamente le misure adatte per poter rendere il PdV idoneo alla conservazione. Il PdA generato contiene nell'RdV l'indicazione del/i PdV che sono stati scartati.

Il RdV è firmato digitalmente con riferimento temporale come "signing time" della firma.

7.5 Preparazione e gestione del pacchetto di archiviazione

I Pacchetti di Versamento in input al software di Conservazione, opportunamente verificati e validati come descritto nelle sezioni precedenti, vengono accorpati in PdA e corredati delle ulteriori caratteristiche necessarie a soddisfare i requisiti previsti dalla normativa. Sono così generati PdA univocamente identificati all'interno del sistema (identificativo univoco).

Il PdA è costituito dai seguenti elementi:

- File XML del **RdV** (.xml)
- File XML del **RdV firmato digitalmente** (.xml.p7m)
- File **IPdA** [come da standard SInCRO] (.xml)
- File **IPdA firmato digitalmente** con riferimento temporale (.xml.p7m)
- **Marca temporale** dell' IPdA (.xml.p7m.tsr)
- Cartella **Docs** con al suo interno tutti i file derivanti dai PdV
- Cartella **Index** con al suo interno tutti i file indice dei documenti derivanti dai PdV

I PdA sono sottoscritti dal responsabile del servizio e, ad essi, sono associate le relative marche temporali.

I PdA, così sottoposti al processo di conservazione digitale, sono custoditi, per i tempi previsti dalla normativa, nell'archivio informatico facente parte del sistema di conservazione. Il sistema è implementato e sviluppato allo scopo di garantire e mantenere la disponibilità, la fruibilità, l'immodificabilità e l'autenticità dei documenti informatici in esso contenuti.

7.6 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'Esibizione

Il processo di preparazione del PdD è attivato dalla ricezione di una richiesta di esibizione da parte dell'utente. Il sistema di conservazione si occupa di verificare che il profilo dell'utente che accede abbia le necessarie autorizzazioni per effettuare l'estrazione.

L'utente, guidato dal sistema, opera la selezione dei documenti informatici da estrarre e consente di produrne un duplicato corredato dal relativo IPdA.

Il SdC prevede la possibilità di scaricare in autonomia il PdD dall'applicazione accessibile tramite web; la rappresentazione informatica del PdD è un duplicato del PdA.

I IPdA contengono le impronte dei documenti richiesti per consentire all'utente la verifica autonoma e completa delle caratteristiche che determinano la corretta conservazione dei documenti.

Tutte le informazioni relative ai PdD richiesti, generati, esportati dal sistema di conservazione vengono storicizzate su appositi log (si menzionano, a titolo non esaustivo: data e ora di ogni singola operazione, utente/processo, tipo di operazione).

L'interfaccia del sistema di distribuzione rende inoltre disponibile per il download un software visualizzatore stand-alone per la consultazione offline dei PdD.

Le transazioni dei dati relativi ai documenti conservati avvengono tramite autenticazione del profilo utente del soggetto interessato alla consultazione, in questo contesto, la sicurezza è garantita dalla tecnologia di cifratura del canale di comunicazione basata sul protocollo HTTPS.

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

Il Responsabile del servizio Conservazione o un suo delegato si preoccupa di eseguire la copia su supporti più moderni e all'avanguardia qualora l'evolversi del contesto tecnologico renda obsoleti i dispositivi utilizzati fino a quel momento. I supporti saranno cambiati solo se il Responsabile del servizio di Conservazione lo riterrà opportuno riversando tutti i Pacchetti di Archiviazione sul nuovo dispositivo di archiviazione.

I documenti trattati sono normalmente di tipo NON unico. Per questa tipologia documentale non è mai richiesta la presenza del Pubblico Ufficiale.

Nel caso sia richiesto il trattamento di documenti UNICI il Responsabile della Conservazione predisporrà le opportune procedure operative per l'apposizione della Firma Digitale da parte di un Pubblico Ufficiale.

Produzione di duplicati informatici

Il procedimento di produzione di duplicati informatici consente di ottenere dal sistema di conservazione i duplicati informatici aventi il medesimo valore giuridico, ad ogni effetto di legge, dei documenti informatici dai quali sono tratti in conformità con le regole tecniche vigenti. I duplicati di documenti informatici hanno il medesimo contenuto e la medesima rappresentazione informatica degli originali dai quali sono tratti.

Il procedimento di produzione di duplicati si attiva automaticamente:

- ogni volta che l'utente accede al sistema di selezione per ottenere uno o più PdD contenenti i documenti informatici di interesse;
- in occasione dei backup e delle repliche perpetrate sui PdA allo scopo di garantirne la permanenza dei requisiti essenziali di fruibilità e verificabilità.

7.8 Scarto dei pacchetti di archiviazione

Allo scadere del tempo di archiviazione dei PdA il Responsabile della Conservazione si fa carico di richiedere al responsabile del servizio della conservazione di eliminare i PdA che sono obsoleti, dandone evidenza e comunicazione al produttore.

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

Al fine di garantire l'interoperabilità del sistema di conservazione e la trasferibilità di archivi informatici ad altri eventuali soggetti conservatori il sistema di conservazione prevede le seguenti misure:

- Adozione dallo standard SInCRO, di tracciati XML omogenei relativi ai PdD e PdA;
- Generazione di tracciati XML (conformi allo standard SInCRO) privi di informazioni non standardizzate e/o arbitrariamente definite e/o ridondanti;
- Mantenimento, per i PdD, della medesima struttura di dati dei PdA;
- Mantenimento di identità tra indice IPdA del PdA ed il medesimo presente nel PdD;
- Gestione dei metadati dei documenti informatici esterna al PdA.

In caso di conclusione del contratto di servizio sono resi disponibili al produttore i PdD, coincidenti con i PdA conservati.

8 IL SISTEMA DI CONSERVAZIONE

Il sistema adottato si avvale delle opportune tecniche crittografiche per la realizzazione delle funzionalità di Firma Digitale, fornisce supporto per la gestione dei certificati/chiavi dei Responsabili di Archiviazione, Operatori e Pubblici Ufficiali che operano all'interno del Sistema di Conservazione e per il trattamento e custodia delle informazioni concernenti le quantità crittografiche che dovranno essere integrate negli archivi digitali su opportuni supporti di memorizzazione.

Il sistema si configura come un servizio a disposizione di qualsiasi piattaforma, sia esso applicativo o Sistema di Document Management (DMS). Fornisce le funzionalità di gestione delle strutture aggiuntive necessarie alla Conservazione Digitale, rende disponibili le interfacce verso infrastrutture PKI per la Firma Digitale (Certification Authority), e le interfacce per l'integrazione tra il DMS e il servizio stesso.

Un'ulteriore caratteristica del sistema è quello di fornire una interfaccia tra le procedure crittografiche standard e i client destinati alla produzione dei documenti elettronici consentendo la gestione di documenti firmati PKCS#7

Affinché l'archiviazione possa essere terminata, il sistema garantisce inoltre che:

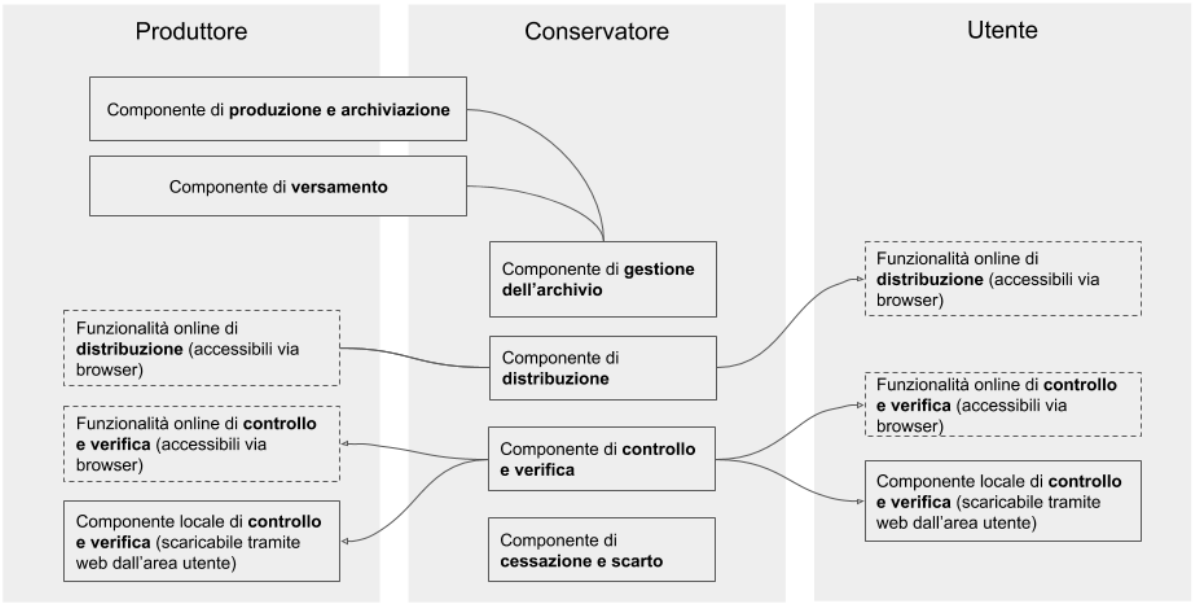
- Sia generato un **Rapporto di Versamento** firmato digitalmente con riferimento temporale,
- Il **Pacchetto di Archiviazione** sia corredato dall'IPdA,
- Sull'IPdA venga apposta la ***Firma Figitale*** *del Responsabile o di un suo delegato* e che siano registrati su idoneo supporto di memorizzazione.
- Venga apposta sull'IPdA una ***Marca Temporale*** rilasciata da una TimeStamping Authority riconosciuta all'albo AgID.
- Si preveda, nel caso di Conservazione di documenti analogici unici, l'apposizione della Firma Digitale di un Pubblico Ufficiale.

8.1 Componenti Logiche

La logica del sistema è strutturata sulle indicazioni dello standard OAIS e prevede componenti che ne consentono l'applicazione nel sistema di conservazione.

Si individuano pertanto le seguenti componenti logiche:

- produttore: effettuano il versamento dei nuovi PdV generati al SdC;
- Componente di produzione e archiviazione che ha la funzionalità di archiviare i PdV inviati dal produttore e li struttura per la gestione successiva, con la generazione dei PdA, effettuando tutte le azioni di monitoraggio e controllo previste nonché la produzione dei rapporti di versamento;
- Componente di gestione dei versamenti: prende in carico i PdV validati e gestisce l'inoltro al sistema di conservazione;
- Componente di gestione dell'archivio: gestisce la trasformazione da PdV a PdA utilizzando i servizi di firma digitale dei documenti da CA accreditate ed attendibili;
- Componente di gestione della distribuzione: mette a disposizione gli strumenti per la ricerca dei documenti da parte degli utenti abilitati alla generazione dei PdD;
- Componente di gestione della cessazione e dello scarto: presidia il periodo di esistenza dei documenti informatici all'interno del sistema di conservazione in base a quanto previsto dal quadro normativo vigente;
- Utenti: fruiscono del sistema di conservazione.



Alla base del funzionamento delle componenti logiche, operano le componenti software del SdC composte da una parte applicativa Web Based (basato su tecnologia IIS e sviluppato in .Net C#), di una parte applicativa client/server (sviluppata in .Net C#) e di un servizio/applicazione (sviluppato in tecnologia .Net C#) di upload su DB dei metadati.

La parte applicativa (KarchiveEngine) si occupa di:

- prendere in carico i PdV,
- dare evidenza all'operatore (Responsabile o suo delegato) dei PdV scartati,
- generare il RdV e firmarlo digitalmente con riferimento temporale
- generare i PdA,
- generare l'IPdA e firmarlo con riferimento temporale e marca temporale.

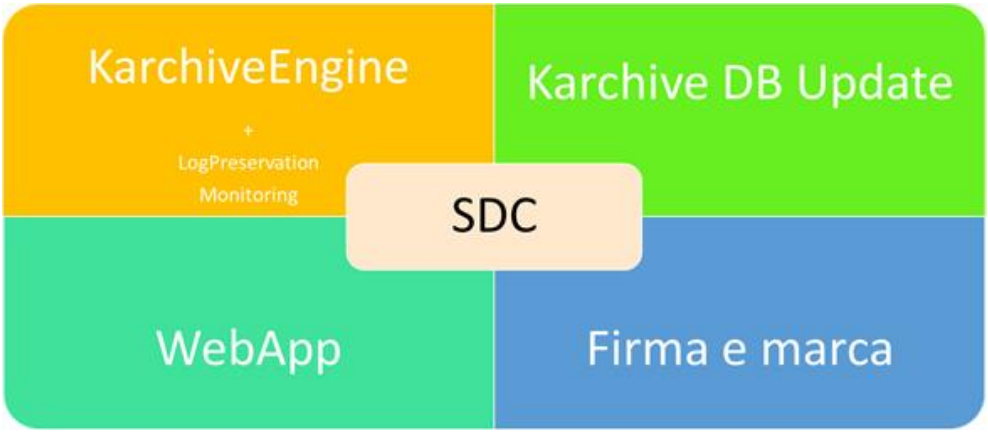
Il servizio di upload su DB (KarchiveDBUpdate) dei metadati si occupa di:

- caricare i metadati di tutti i documenti presenti nei nuovi PdA generati,
- eventualmente creare le versioni di documenti già presenti.

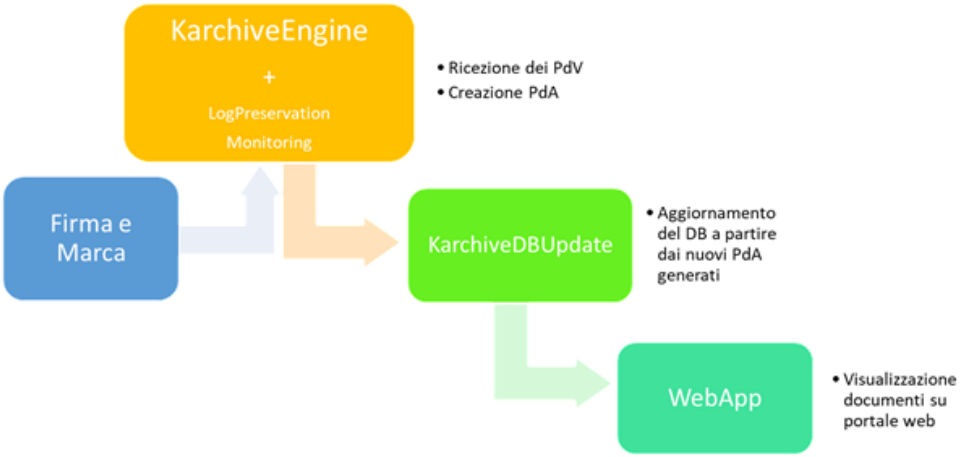
L’ applicativo WebBased (WebApp - Karchive) consente di:

- prendere visione dei PdA generati,
- scaricare i PdD generati come copia esatta del PdA di riferimento,
- Scaricare il visualizzatore per la fruizione, ricerca ed esibizione in locale dei PdD,
- Eseguire ricerche puntuali sui documenti basandosi sui metadati associati,
- Visionare i documenti informatici on-line,
- Scaricare in locale il documento di riferimento,
- Esibire il documento con tutte le informazioni legate alla conservazione dello stesso con evidenza della loro validità:
    - RdV,
    - Firme associate al IPdA e al RdV,
    - Marca temporale dell’IPdA,
    - Validazione dell’impronta contenuta nell RdV e nel IPdA.
- Creare utenti (funzionalità consentita ai soli profili amministrativi),
- Profilare gli utenti (funzionalità consentita ai soli profili amministrativi),
- Visionare le statistiche di elaborazione (funzionalità consentita ai soli profili amministrativi).

Schema delle componenti software:



Rappresentazione funzionale delle componenti software:



8.2 Componenti Tecnologiche

Il Sistema di Conservazione può utilizzare **SmartCard/Token** di **Firma Digitale** rilasciate da ognuna delle Certification Authority (CA) riconosciute dall'AgID.

In alternativa posso essere utilizzati i **webservices di firma** per l'accesso a **HSM** (hardware security module) presenti presso la CA di riferimento con un certificato di firma massiva rilasciato da una CA riconosciuta dal AgID.

All'approssimarsi della scadenza dei certificati di firma il responsabile del servizio della conservazione provvede al rinnovo degli stessi o alla loro sostituzione con altri dispositivi di firma.

Per l'apposizione della **Marca Temporale** si fa affidamento alle Time Stamping Authority (TSA) riconosciute dall'AgID.

8.3 Componenti Fisiche

Gli elementi dell'infrastruttura fisica per i servizi di Conservazione - nel solo caso di Kloudarchive – sono presso il datacenter di Aruba, sul territorio nazionale Italiano per i server primari e nella unione europea per i backup. Su richiesta possono essere mantenuti anche i backup sul territorio nazionale Italiano.

Aruba è una **Certification Authority** Italiana con massimi livelli di sicurezza:

- **Tier IV**: il data center è stato progettato e realizzato secondo le specifiche di ridondanza Tier IV, il livello più alto disponibile
- **Uptime**: il data center ha un uptime del 100% dalla sua entrata in funzione a Luglio 2011
- Gestione riservata degli accessi.
- Presenza di Network Operation Center (NOC) presidiato 24 ore su 24, 365 giorni all'anno (due ad Arezzo ed uno a Ktiš).
- Ridondanza tra i NOC.

Prevenzione dei rischi

- Conformità alle normative sismiche.
- Separazione dell'impianto elettrico e delle batterie in edifici appositi (monitorati, refrigerati e protetti contro l'incendio).
- Separazione fisica tra Power Center e sala dati.
- Dotazione di due PDU (Power Distribution Unit) per ciascun armadio rack.
- Oltre 100.000 litri di capacità di stoccaggio del carburante (autonomia a pieno carico di oltre 48 ore).

Sicurezza Logica

- Rispetto delle normative vigenti in materia di sicurezza informatica e di rete.
- Piano di gestione degli incidenti informatici.

- Troubleshooting.
- Escalation.
- Incident Management.

Sicurezza Fisica

- Sistemi automatici di rilevamento fumi ed incendi posizionati nelle sale dati, sotto al pavimento flottante e sopra al controsoffitto.
- Sistemi di spegnimento a gas inerte posizionati nelle aree sensibili.
- Sistemi di intercettazione ed interruzione del carburante ai gruppi elettrogeni in caso di incendio.
- Sistema di rilevazione liquidi: per garantire tempestività in caso di fuoriuscite liquidi o allagamento.

Certificazioni Aruba:

- **Certificazione ISO 9001:2008:** Certificazione conseguita per "Erogazione servizi di Data Center (Server Dedicati, Server Virtuali, Cloud Computing, Housing, Hosting, Posta elettronica, Backup da remoto, Disaster Recovery e Conservazione Sostitutiva) e relativa assistenza specialistica anche tramite Call Center. Progettazione e sviluppo software per soluzioni Web e Cloud Oriented."
- **Certificazione ISO 27001:2005:** Erogazione servizi di Data Center (Server Dedicati, Server Virtuali, Cloud Computing in modalità IaaS, SaaS e PaaS, Housing, Hosting, Posta elettronica, Backup da remoto, Disaster Recovery e Conservazione Sostitutiva) e relativa assistenza specialistica. Gestione e manutenzione di server, postazioni di lavoro, reti informatiche e relativi apparati e sistemi di sicurezza logica.
- **Certificazione GO:** Aruba e Romagna Energia hanno sviluppato una partnership con la finalità di ricercare soluzioni di risparmio energetico sfruttando tutte le possibilità di ottimizzazione dei consumi.

8.4 Procedure di gestione e di evoluzione

Sono di seguito descritte le procedure di gestione e di evoluzione, e la relativa documentazione prevista, per le componenti logiche, tecnologiche e fisiche del sistema di conservazione relativamente a:

- **Conduzione e manutenzione del sistema di conservazione;**

  In relazione alle componenti del sistema di conservazione specificate nel capitolo che precede, l'aggiornamento e l'evoluzione delle stesse rientrano nei compiti previsti dalle LLGG AgID per il responsabile del servizio di conservazione che effettua le necessarie verifiche sulla base dei seguenti elementi:

  - Panorama normativo vigente,
  - Componenti logiche, tecnologiche e fisiche del sistema di conservazione (così come illustrato nelle sezioni precedenti)

- **Gestione e conservazione dei log (anche in accordo con l'ente Produttore);**

  Il sistema di "log management" del sistema di conservazione traccia tutte le operazioni e le transazioni informatiche inerenti a:

  - versamento di pacchetti informativi;
  - trasformazioni di pacchetti informativi in PdA;
  - conservazione dei PdA;
  - gestione della firma digitale e della marcatura temporale;
  - produzione e distribuzione dei PdD;
  - controllo e verifica dei PdA;

- **Monitoraggio del sistema di conservazione:**

  Il sistema di conservazione è costantemente monitorato per valutarne l'efficienza per tutte le parti logiche, tecnologiche e fisiche.

- **Change management**

Ogni modifica al software di Conservazione genera una sua nuova release che va ad aggiungersi all'archivio delle release precedenti. Ogni release è "retrocompatibile" con tutte le parti precedenti, inclusi i PdV, PdA e PdD.

- **Verifica periodica di conformità a normativa e standard di riferimento.**

  Il Responsabile del servizio di Conservazione e i suoi delegati sono aggiornati sui cambiamenti normativi, organizzativi e procedurali da attuare. Ogni cambiamento che impatta uno qualunque degli elementi del sistema di conservazione è riportato nel presente manuale in modo da darne evidenza e garantire una costante aderenza alle normative di riferimento.

9 MONITORAGGIO E CONTROLLI

Descrizione generale della strategia della conservazione e dei conseguenti obiettivi di monitoraggio e controllo

9.1 Procedure di monitoraggio

Il Sistema di Conservazione è monitorato dal Responsabile del servizio di Conservazione o da un suo delegato che verifica periodicamente la sua funzionalità ed efficienza e valuta con attenzione le possibili implicazioni derivanti dal ogni possibile degrado di performance o di integrità del dato presente nello storage primario. In caso di problematiche riscontrate sul sistema dovute alla perdita di dati o alla loro non perfetta leggibilità, è richiesta una copia dal back-up. Se anche questo non fosse sufficiente, è prevista la sostituzione dello storage primario.

Nel caso in cui un malfunzionamento del sistema, dovuto a blackout o altro, dovesse non consentire la conservazione secondo le tempistiche previste, si terrà traccia, in un documento opportunamente allegato al presente Manuale di Conservazione, dell'avvenuto disservizio indicando le cause, le azioni correttive intraprese e i risultati ottenuti.

Ove previsto il sistema di monitoraggio può comprendere automatismi sulle verifiche delle caratteristiche dei pacchetti di archiviazione con notifiche al personale di servizio via email e gestisce le seguenti casistiche:

- **Gestione della granularità del controllo**

I controlli effettuati sui pacchetti di archiviazione possono essere gestiti in termini di granularità di verifica, per quanto concerne il confronto degli hash.

- **Gestione della frequenza**

Il monitoraggio può essere gestito in base a frequenze di elaborazione predefinite schedulando l'attività in determinate date specifiche.

- **Gestione dell'esclusione dei pacchetti monitorati nel breve periodo**

La gestione di esclusione dei pacchetti da monitorare si basa su una parametrizzazione del sistema di monitoraggio che consente di indicare la data da cui considerare i pacchetti da escludere dal processamento.

- **Gestione del numero di controlli effettuati su ciascun pacchetto**

Per ogni elaborazione di monitoraggio viene generato un report che rendiconta l'esito del monitoraggio eseguito (tenendo traccia della data di effettuazione del monitoraggio, del nome del PdA, della data di monitoraggio, della validità delle firme apposte, della validità delle marche temporali associate, della validità del confronto delle impronte Hash).

- **Verifica dell'integrità degli archivi: gestione della validità delle impronte hash**

Il monitoraggio prevede che per ogni file/pacchetto di versamento venga rielaborato l'hash SHA256 e confrontato con quello presente nell'IPdA per validare la sua integrità nel tempo.

- **Monitoraggio dei formati**

Nel report generato dal processo di monitoraggio viene inserita l'informazione relativa a quali formati sono presenti nel sistema di conservazione raggruppandoli per pacchetto di archiviazione. Questo consente un constante monitoraggio dei formati che vengono ad essere gestiti all'interno del sistema di conservazione.

- **Monitoraggio delle caratteristiche di firma digitale e validità temporale**

Il monitoraggio della validità della firma associate al rapporto di versamento e all'indice del pacchetto di archiviazione fa parte integrante del processo di monitoraggio.

9.2 Verifica dell'integrità degli archivi

Periodicamente è compiuta una verifica di tutte delle funzionalità del sistema, controllando in particolare che tutte le operazioni possano essere svolte con efficienza ed efficacia nei tempi previsti dalla normativa specifica sui documenti trattati.

Con periodicità inferiore ai 5 anni il Responsabile del servizio di Conservazione o un suo delegato esegue la verifica della leggibilità dei supporti di memorizzazione utilizzati effettuando un riversamento diretto nel caso in cui il Supporto risulti danneggiato o non più leggibile utilizzando la copia di sicurezza (back-up).

Il Responsabile della Conservazione o un suo delegato verifica regolarmente che i Supporti di Memorizzazione siano leggibili e non vi sia alcun degrado di affidabilità del sistema di memorizzazione e delle registrazioni.

Tutti i Pacchetti di Archiviazione sono registrati su file system ridondato e qualunque degrado dei dischi primari è gestito rispristinando i back-up e/o sostituendo i dischi danneggiati.

Qualora un formato sia divenuto obsoleto, il Responsabile ne prevede la conversione e la rielaborazione nel Sistema di Conservazione.

9.3 Soluzioni adottate in caso di anomalie

Anomalie

Le eventuali anomalie sono prese in carico dal responsabile del servizio di conservazione, coadiuvato dagli ulteriori responsabili coinvolti, che provvede all'adozione delle necessarie misure commisurate all'entità e alle caratteristiche dell'incidente per il ripristino della corretta operatività del sistema.

Procedura di Back up del database

La procedura di back-up del database è eseguita automaticamente grazie ad uno specifico piano di manutenzione che prevede la generazione di un back-up dell'intero database eseguito durante la notte.

Procedura di recovery: Applicativo

Il Software di conservazione è conservato, nelle sue differenti versioni e con relativi file d'installazione e applicativi complementari. E' possibile quindi ripristinare l'applicativo eseguendo una re-installazione del software in ogni momento.

Procedura di recovery: Database

La procedura di recovery del Data Base è effettuata ripristinando dalle copie di back up i suoi contenuti.

Procedura di recovery : Pacchetti di archiviazione

I PdA sono presenti in duplice copia e in due locazioni fisiche diverse. In caso di non leggibilità degli stessi è possibile compiere il ripristino del contenuto dei Pacchetti di Archiviazione primari eseguendo un riversamento diretto dei supporti di back-up. Si ripristinano così, come in origine, le due copie dei pacchetti di archiviazione.

9.4 Politiche di conservazione a lungo termine (Long Preservation policy e obsolescenza)

Al fine mantenere nel lungo periodo l'autenticità, l'integrità e la leggibilità dei documenti posti in conservazione il responsabile del servizio di conservazione predispone e attua il piano della sicurezza, volto ad individuare e correggere eventuali difetti e non congruità dei documenti conservati e dei pacchetti di archiviazione con gli standard tecnologici e la normativa vigente.

I processi di monitoraggio approfonditi nella sezione precedente costituiscono parte integrante delle politiche di conservazione a lungo termine. Oltre ad essi, al fine di garantire il perdurare della validità legale, integrità, leggibilità e riservatezza dei documenti informatici conservati, il sistema prevede alcune procedure di verifica di seguito meglio dettagliate.

- Gestione dell'obsolescenza dei formati:
    - Verifiche periodiche sui formati presenti nel sistema,

    - Mantenimento dei software di visualizzazione.

- Gestione dell'obsolescenza dei metadati:

Il sistema di conservazione consente di prendere in carico almeno le seguenti casistiche:

- Aggiornamento degli standard di rappresentazione informatica dei documenti: la gestione dei metadati dei pacchetti di versamento avviene con uno schema XML che è in grado di recepire gli eventuali aggiornamenti della rappresentazione informatica dei documenti;
- Aggiornamento applicativo in base al contesto normativo vigente: il sistema di conservazione garantisce una flessibilità di gestione dei metadati che consente di aggiungerne di nuovi o modificarne la lunghezza, permettendo così di adeguare lo standard di ricezione e gestione dei metadati a nuove esigenze sia legate al panorama normativo che ad esigenze specifiche.
- Gestione dell'obsolescenza tecnologica dei supporti informatici e degli apparati

10 SOTTOSCRIZIONE E TEMPISTICHE DI ATTUAZIONE

I ruoli vengono così assegnati:

Responsabile della conservazione

Con l'acquisto del servizio Kloudarchive il cliente dichiara esplicitamente di essere pienamente informato che il Responsabile della Conservazione è il Legale Rappresentante del soggetto passivo di imposta che acquista il servizio. Il cliente è quindi responsabile a tutti gli effetti delle attività di Conservazione Digitale svolte per suo conto e sotto espressa delega dal fornitore del servizio. Il fornitore del servizio è manlevato da ogni eventuale responsabilità presente e futura per ogni dato, documento o informazione erronea o difforme dalle norme tributarie, civilistiche e penali in vigore. Il cliente, con l'acquisto del servizio, delega la Società Grammelot S.r.l., in persona del suo legale rappresentante, allo svolgimento delle attività di Delegato del Servizio di Conservazione che potrà essere, per ragioni di organizzazione relativa all'erogazione del servizio, delegata a personale qualificato di Grammelot S.r.l. come specificato in questo documento.

Delegato Responsabile Grammelot S.r.l:

Nome e Cognome: **Massimo Roberto Maronati**

Compiti delegati: Tutte le funzionalità operative del responsabile di conservazione

Delegato1:

Nome e Cognome: **Riccardo Sirtori**

Compiti delegati: Tutte le funzionalità operative del responsabile di conservazione

ALLEGATO A

Nella seguente tabella sono indicate le tipologie documentali che sono trattate dal Sistema di Conservazione per ogni Figura Giuridica e i metadati associati

(altre tipologie e metadati potranno essere concordate con Grammelot Srl):

Oggetti sottoposti a conservazione	Metadati associati
Fattura emessa	• Numero fattura • Partita IVA/CF • Ragione Sociale/Nome/Cognome • Data emissione • Altre chiavi aggiuntive
Fattura ricevuta	• Numero Registrazione • Partita IVA/CF • Ragione Sociale/Nome/Cognome • Data emissione • Data registrazione • Altre chiavi aggiuntive
Libri e registri iva	• Codice protocollo • Tipologia • Mese • Anno • Altre chiavi aggiuntive
Fattura_EmessaPA	• AnnoDoc • Numero • DataFattura(gg/mm/yyyy) • IdTipoDoc • RagioneSociale

	• Cognome • Nome • CodiceFiscale • PartitaIVA • Cedente
Fatture_Elettroniche_Passive	• AnnoDoc • Numero • DataFattura(gg/mm/yyyy) • IdTipoDoc • RagioneSociale • Cognome • Nome • CodiceFiscale • PartitaIva • Azienda • ProtocolloIVA • Sezionale • DataRegistrazione(gg/mm/yyyy)
RicevutePA	• AnnoDoc • Numero • DataFattura(gg/mm/yyyy) • IdTipoDoc • RagioneSociale • Cognome • Nome • CodiceFiscale • PartitaIVA • Cedente

LUL	• Nome • Cognome • CF • Mese • Anno • Altre chiavi aggiuntive

Il servizio di Conservazione Digitale ha inizio dalla data di sottoscrizione del contratto da parte del Responsabile della Conservazione