Sommario

CARATTERISTICHE PRINCIPALI DEL SOFTWARE APPLICATIVO OFFERTO J-IRIDE

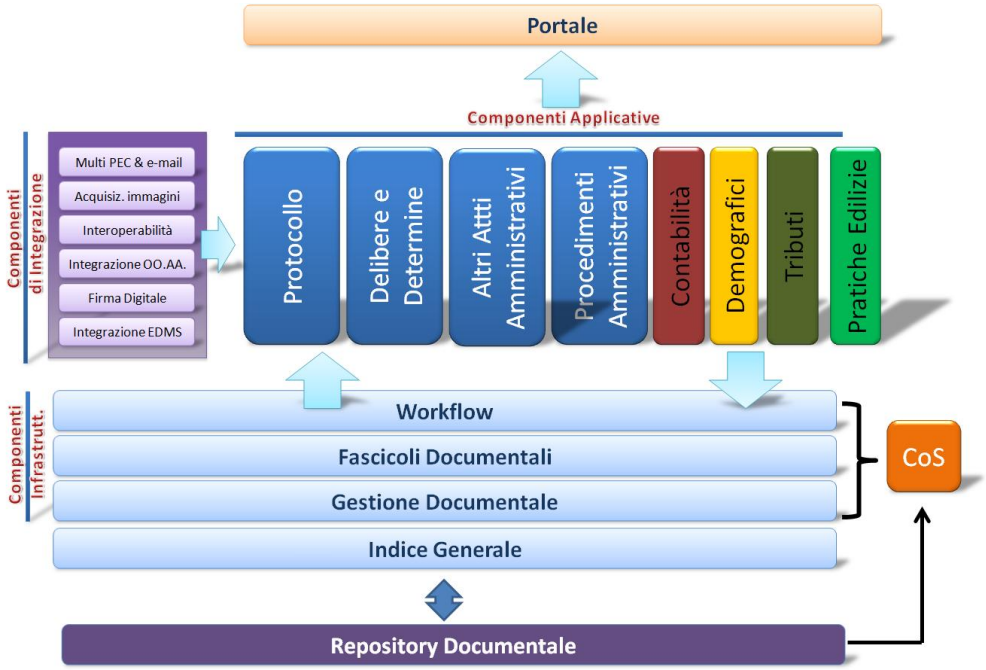
La gestione delle informazioni, dei documenti, dei processi e dei procedimenti amministrativi, dal Protocollo Informatico alla gestione dei flussi documentali, rappresentano elementi essenziale per realizzare le prescrizioni contenute nelle leggi di riforma della Pubblica Amministrazione italiana

J-IRIDE mette in grado le Pubbliche Amministrazioni di avere un totale controllo di tutti i cicli di creazione, acquisizione, gestione, distribuzione, condivisione, scambio ed archiviazione dei dati, delle informazioni e dei documenti di tutti i principali procedimenti amministrativi degli Enti Pubblici, il tutto garantendo sicurezza, autenticità, archiviazione, conservazione a norma e salvaguardia dei dati in conformità alle normative di riferimento.

Consente la creazione, la modellazione e la gestione dinamica dei procedimenti amministrativi.

In questo senso J-IRIDE permette una gestione integrata dei procedimenti amministrativi informatici dell'ente, la creazione di report, statistiche, etc.

La soluzione software J-IRIDE è un sistema integrato di Gestione Documentale e si presenta come una piattaforma modulare che realizza il tracciamento e l'esecuzione automatica dei flussi di lavoro (Work-Flow) e di Gestione Documentale. La suite è composta da un'ampia gamma di moduli applicativi, a partire dal Protocollo Informatico, immediatamente fruibili a supporto dei processi amministrativi dell'Ente. Negli applicativi si accede alle informazioni in modo semplice e intuitivo con l'utilizzo di logiche di tipo multimediale. Tutte le informazioni sono convalidabili con l'apposizione della Firma Digitale e sono rigorosamente protette da accessi non autorizzati (Access Control List). La Suite di prodotti è dotata di un nucleo minimo al quale si possono aggiungere: una serie di componenti applicative ed una serie di componenti di integrazione. Di seguito uno schematico quadro di riepilogo delle componenti del Sistema Informativo.



. Fra i servizi di infrastruttura si possono evidenziare:

- ***Workflow management system*** per la definizione degli iter documentali relativi a procedimenti amministrativi
- ***Generatore di report*** per la produzione e personalizzazione di tutte le stampe a corredo dell'applicativo. Il motore per la generazione di report utilizzato dal sistema è di tipo open source con interfaccia grafica che consente la definizione e personalizzazione dei layout da parte dell'utente
- ***Gestione documentale*** per tutti i servizi specifici alla gestione dei documenti informatici
- ***Integrazione sistemi Office automation*** offre la possibilità di interfacciarsi indifferentemente sia con OpenOffice che con Microsoft Office, in modo da consentire all'Ente la massima libertà nella scelta del sistema di office automation
- ***Gestione della sicurezza e dei log*** il modulo si incarica di tracciare tutte le operazioni svolte, memorizzando sul database e rendendo accessibile all'utente tutte le interazioni utente/sistema avvenute per il monitoraggio delle attività. Sicra@Web consente per ogni area applicativa di configurare dinamicamente il livello di dettaglio con cui tracciare il log al quale si potrà accedere da applicativo o editor esterno.
- ***Firma digitale, e-mail, PEC*** per gestire i documenti prodotti dal sistema senza dover fare uso di programmi esterni per firmare digitalmente documenti e connettersi direttamente ai server SMTP per l'invio via posta elettronica.

Tutto il software applicativo viene concesso in licenza d'uso non esclusiva e non trasferibile, a tempo indeterminato. Tutto il software applicativo proposto è di proprietà di Maggioli SpA e sviluppato dalla stessa.

Moduli Applicativi proposti

La soluzione proposta prevede la copertura funzionale delle seguenti Aree Funzionali:

- "Gestione Documentale"
- "Atti Amministrativi"
- "Protocollo Informatico"
- "Workflow Management"
- "Gestione Pubblicazioni"
- "JCity.Gov Albo Pretorio e storico Atti"
- "JCity.Gov Amministrazione Trasparenza"

PROTOCOLLO INFORMATICO

Funzionalità di protocollazione di documenti in formato cartaceo ed elettronico

Il sottosistema del Protocollo Informatico permette di svolgere le operazioni di acquisizione e segnatura di protocollo di documenti cartacei e informatici integrando firma digitale e servizi di marcatura temporale, la classificazione d'archivio e la gestione dei fascicoli, nonché la gestione e il monitoraggio dei processi amministrativi dell'Ente. La procedura prevede la protocollazione di documenti in formati diversi, sia in ingresso sia in uscita, in particolare di documenti cartacei acquisiti da scanner, posta elettronica con gestione degli allegati, fax. Tutti i tipi di documento, in particolare quelli in formato elettronico, possono essere acquisiti automaticamente ed e' possibile scegliere se protocollarli o No. I flussi informatici gestiti in maniera automatica, prevedendo da parte dell'operatore la possibilità di non protocollare, sono almeno i seguenti: Fax in entrata e/o uscita tramite fax server; Posta elettronica con gestione degli allegati; Flusso documentale interno.
Le funzionalità minime previste sono le seguenti:

- Registrazione puntuale dei protocolli in ingresso, in uscita, e interni;
- Segnatura di protocollo con la possibilità di stampa diretta sul documento;
- Gestione degli allegati;

- Gestione dei collegamenti tra protocolli diversi (antefatto) con possibilità di visualizzazione dei documenti collegati sia in avanti sia indietro nel tempo;
- Possibilità di ricerche secondo criteri diversi (numero, data, mittente, destinatario, corrispondente interno, fascicolo, …);
- Rilascio quietanza o ricevuta di avvenuta protocollazione;
- Integrazione con firma digitale e servizi di marcatura temporale;
- Gestione di più AOO all'interno della stessa Amministrazione;
- Servizio installato e configurato nel server, che crea giornalmente il Registro di Protocollo, per tutte le AOO presenti nel Sistema, in un formato standard;
- Registro di emergenza;
- Registro di protocollo: stampe e salvataggi secondo le regole imposte dalla normativa.
- Il Sistema di Protocollo proposto espone un'interfaccia di programmazione verso altre applicazioni, in modo da permettere l'automazione di operazioni di consultazione ed inserimento delle registrazioni quando effettuate direttamente dall'interno di altre applicazioni.

Fasi di protocollazione

Le macrofasi gestite dall'applicazione sono le seguenti:

- Ricezione;
- Registrazione;
- Classificazione;
- Fascicolazione;
- Assegnazione;
- Trasmissione.

Ricezione: è la fase di ricezione ed identificazione del tipo di documento da trattare, che può essere di tipo cartaceo o informatico. Il flusso di documenti in entrata può essere prodotto da varie sorgenti: la posta ordinaria, la casella di posta elettronica certificata dell'ente, il fax server, etc. I sistemi esterni depositano i messaggi in un'area a cui l'operatore accederà per eseguire la protocollazione dei documenti.

Registrazione: identifica tutte le operazioni relative alla protocollazione quali: registrazione del documento (assegnazione del numero e della data di protocollo), l'inserimento di tutte le informazioni obbligatorie compresa l'impronta nel caso di un documento informatico. Viene effettuata anche l'operazione di segnatura del documento: operazione diversa a seconda che il documento sia di tipo informatico o di tipo cartaceo.

Assegnazione: attribuisce la responsabilità del documento protocollato (competenza) ad un solo ufficio/servizio dell'ente e individua gli altri uffici/servizi (uno o più di uno) a tale documento interessati (conoscenza). Può essere eseguita anche nella fase di protocollazione. La possibilità di eseguire questa funzione da parte dell'utente è disciplinata da una specifica abilitazione a livello di permessi utente.

Classificazione: la classificazione definisce la posizione del documento relativamente al titolario di classificazione definito dalla AOO. Può essere eseguita anche nella fase di protocollazione. La possibilità di eseguire questa funzione da parte dell'utente è disciplinata da una specifica abilitazione a livello di permessi utente.

Fascicolazione: ogni documento viene prima individuato attraverso la classificazione e poi viene inserito obbligatoriamente in un fascicolo. L'inserimento nel fascicolo è effettuato dall'operatore che ha preso in carico il documento. Questa operazione può essere eseguita anche nella fase di protocollazione, previa assegnazione e classificazione. La possibilità di eseguire questa funzione da parte dell'utente è disciplinata da una specifica abilitazione a livello di permessi utente.

Trasmissione: il sistema gestisce le trasmissione dei documenti informatici secondo le specifiche delle circolare 7 maggio 2001, AIPA/CR/28 che stabilisce come costruire il messaggio da inviare, nonché il file XML per la segnatura ed eventualmente gli allegati relativi a tale documento.

Descrizione Funzionalità minime del protocollo informatico

Il sistema di protocollo informatico offerto, in coerenza con il DPR 445/2000, prevede in dettaglio le seguenti funzionalità minime:

- Configurazione del sistema;
- Ricezione;
- Registrazione;
- Segnatura;
- Assegnazione;
- Classificazione;
- Generazione o lettura dell'impronta del documento;
- Annullamento o modifica;
- Funzionalità di base ricerca dei documenti;
- Stampe;
- Gestione protocollo di emergenza;
- Gestione dell'archivio;

- Interoperabilità con altri sistemi di protocollo;
- Firma digitale
- Back up dei dati.

Tutte le funzioni di accesso ai dati del sistema nonché la ricerca, la visualizzazione e la stampa delle informazioni sono disciplinate da criteri di abilitazione stabiliti dal responsabile del protocollo.

OLTRE LA NORMATIVA

Sicr@Web va oltre il livello minimo previsto dal DPR 445/2000 e offre una serie di funzionalità aggiuntive, in più a quelle minime obbligatorie. La procedura consente infatti l'inserimento di ulteriori informazioni che riportiamo di seguito:

- **classificazione parametrica fino a cinque livelli**
- **riferimenti agli allegati e inserimento di allegati**
- **ufficio mittente/ricevente**
- **uffici per conoscenza nel caso di documenti in entrata**
- **riferimenti a pratica con responsabile di procedimento**
- **note**
- **protocollo "origine"; riferimento a tutti i protocolli collegati padri e figli con lo stesso protocollo "origine" tramite la costruzione di un albero**
- **link dinamico ad eventuale protocollo collegato**
- **identificativo dell'operatore "protocollatore"**

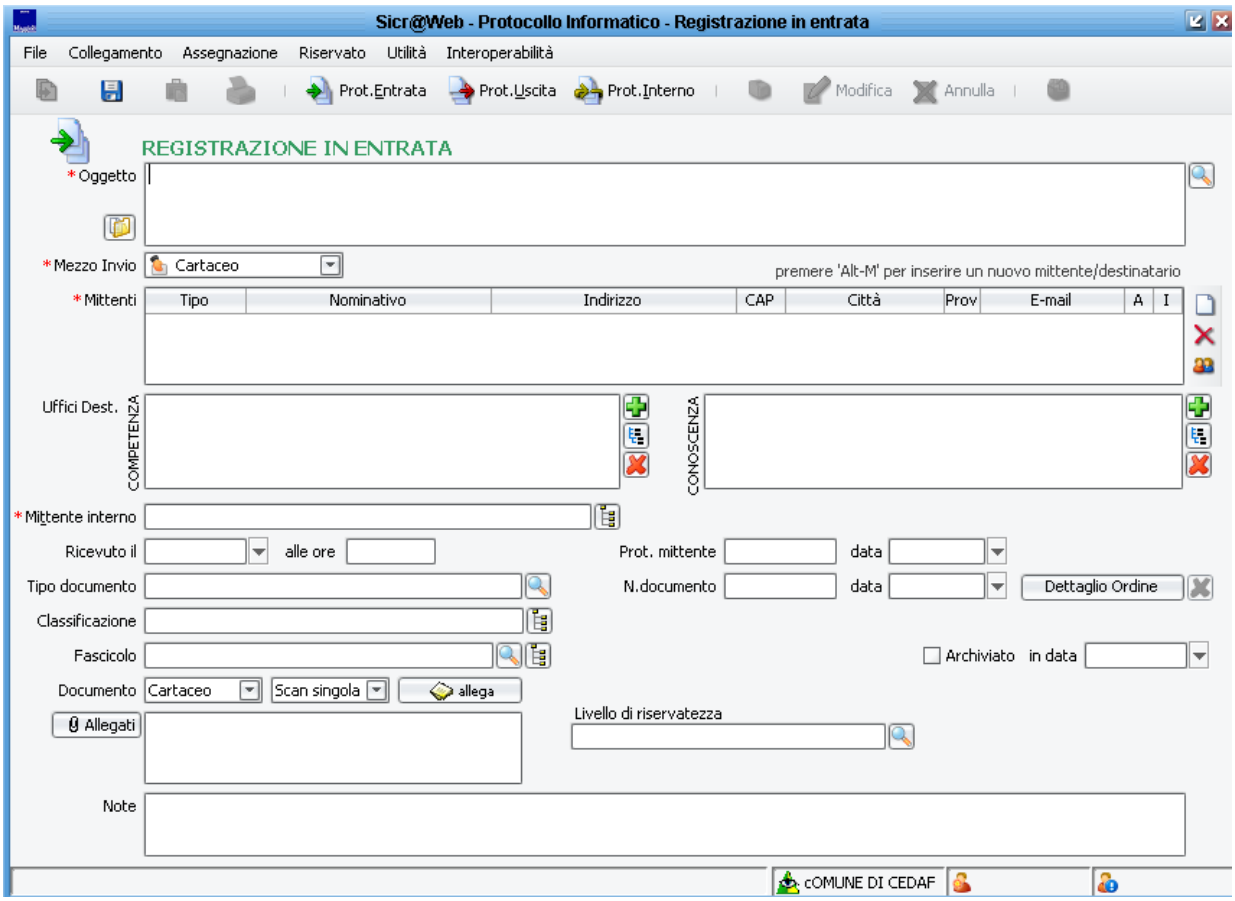
Ricezione: E' la fase di identificazione del tipo di documento che deve essere trattato, che può essere di tipo cartaceo: con la possibilità di acquisire i documenti via scanner;
informatico: con accesso al contenitore dei messaggi smistati e ancora da protocollare ed estrazione, in fase di registrazione, delle seguenti informazioni: documento primario, eventuali allegati, segnatura informatica (automatizzando così in fase di registrazione l'inserimento dei dati).Per quanto riguarda i documenti informatici il flusso di documenti in entrata verso l'ente pubblico può essere prodotto in diversi modi, a seconda delle tecnologie utilizzate per la trasmissione del documento. La procedura permette la ricezione dei documenti da diversi tipi di sorgenti di ingresso (posta elettronica certificata con gestione degli allegati, un fax server, ecc.). L'integrazione dell'applicazione protocollo con tali sistemi potrà essere personalizzata a seconda delle specifiche esigenze dell'Ente, come per esempio nel supporto di uno specifico fax server.

Registrazione: Relativamente al sistema di protocollo informatico possiamo distinguere i documenti in base al loro stato di trasmissione: Spediti(documenti prodotti dal soggetto produttore e trasmessi all'esterno); Ricevuti (documenti ricevuti da altri soggetti produttori);

Interni (documenti prodotti/acquisiti e mantenuti solo all'interno del soggetto produttore). Per ciascuna di queste tipologie è predisposta una specifica procedura di registrazione, in quanto le informazioni necessarie per ciascun tipo di operazione sono differenti. La registrazione di ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione in un archivio informatico, oltre ai dati identificativi dell'AOO protocollante (ente, denominazione AOO, codice identificativo AOO) forniti automaticamente dal sistema sulla base dei parametri di configurazione, delle seguenti informazioni:

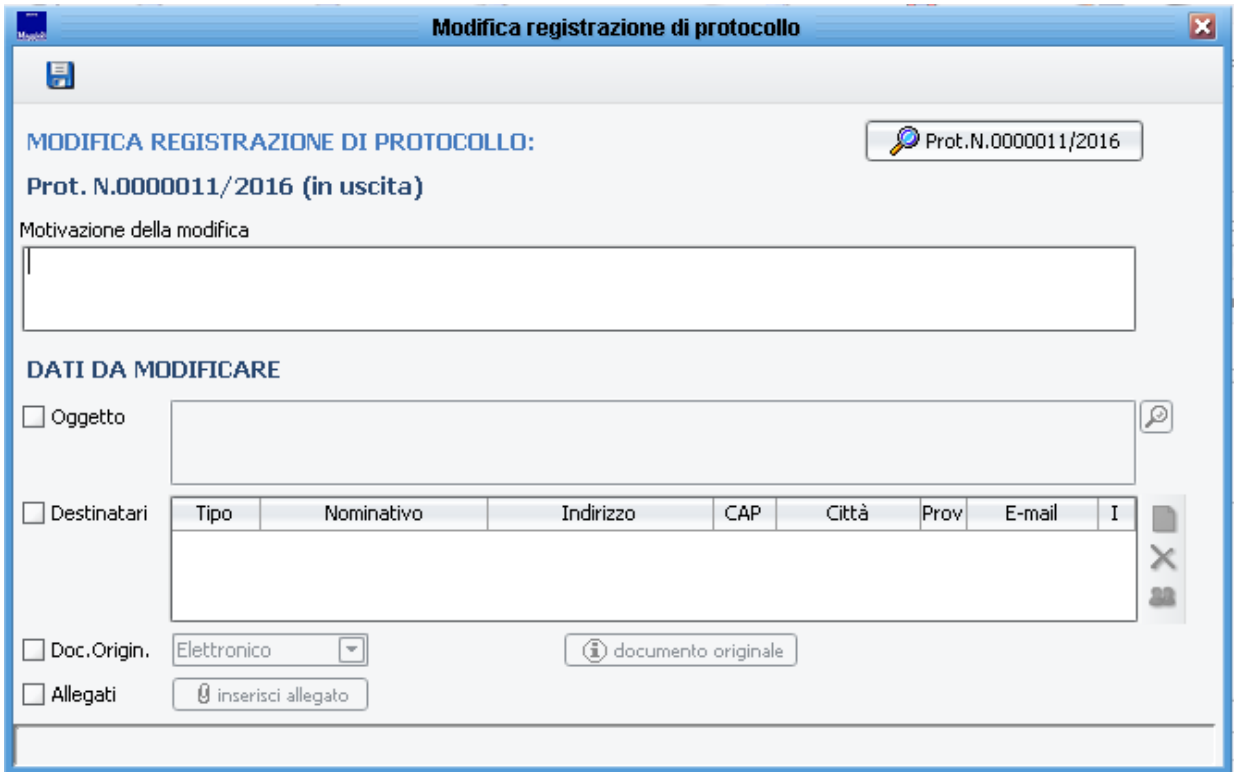
- numero di protocollo del documento; il progressivo di protocollo è un numero ordinale, costituito da sette cifre numeriche. La numerazione è rinnovata ogni anno solare. Può essere composto da un numero di cifre inferiore a sette, in tal caso si appongono degli zeri (assegnato automaticamente dal sistema e non modificabile);
- data di registrazione di protocollo (assegnata automaticamente dal sistema e non modificabile);
- mittente per i documenti ricevuti o, in alternativa, il destinatario o destinatari (dato obbligatorio);
- ufficio mittente e destinatario (nel caso dei documenti interni) (dato obbligatorio);
- eventuali informazioni identificative del mittente, quali codice fiscale, indirizzo, numero di telefono, indirizzo di posta elettronica, identificativo se persona fisica o ente/società;
- la data o il numero di protocollo del mittente (dati obbligatori se disponibili);
- oggetto del documento (dato obbligatorio);
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto (dato obbligatorio per i documenti informatici);
- l'ufficio al quale il documento è assegnato ovvero l'ufficio che lo ha prodotto;
- l'eventuale riferimento a documenti collegati, protocollati in precedenza;
- la classifica ed eventuale sottoclassifica, con particolare riferimento alle categorie degli atti esclusi dall'accesso;
- la data di arrivo o di spedizione;
- la collocazione del documento nell'archivio dell'amministrazione, anche in relazione all'identificativo del fascicolo in cui è inserito;
- l'eventuale numero e tipologia degli allegati;
- il riferimento ad eventuali allegati redatti su supporto informatico.

Di seguito un esempio di registrazione in partenza o uscita



Una volta eseguita l'operazione di protocollazione le informazioni, per le quali e' prevista la registrazione in forma non modificabile, non sono più alterabili ed in caso di errore nell'introduzione di questi dati, deve essere eseguito l'annullamento parziale ed effettuata una modifica con log, a correzione dei dati errati con richiesta della modifica e successiva autorizzazione da parte del Responsabile del protocollo.

L'annullamento dell'intera registrazione di protocollo annulla invece il protocollo e non consente altre operazioni. Per ulteriori dettagli su modifica ed annullamento della registrazione di protocollo si rimanda ad un paragrafo successivo. Esempio di maschera per la richiesta di modifica di informazioni non modificabili dopo la registrazione.



Le seguenti informazioni vengono prodotte automaticamente dal sistema:

- Progressivo del protocollo;
- Data di protocollo;
- Impronta del documento informatico;

Identificativo della AOO.

L'applicazione mette a disposizione dell'utente diverse procedure di registrazione dei documenti a seconda della direzione del flusso documentale relativamente all'ente: registrazione di documenti in ingresso, di documenti in uscita e di documenti ad uso interno. Le informazioni comuni a tutti i tipi di registrazione, con inserimento a carico dell'operatore, sono le seguenti:

- oggetto del documento
- classificazione
- protocollo originario (protocollo apicale)
- eventuale collegamento ad un altro numero di protocollo
- note

Oltre alle informazioni comuni, la registrazione dei documenti in ingresso prevede l'inserimento a carico dell'operatore delle seguenti ulteriori informazioni:

- nome del mittente
- indirizzo del mittente
- eventuale responsabile dell'assegnamento
- ufficio per competenza
- uffici per conoscenza
- data e ora di ricezione
- n. e data di protocollo del documento in entrata (protocollo mittente) se presente
- impronta (per i documenti informatici)

Oltre alle informazioni comuni, la registrazione dei documenti in uscita prevede l'inserimento a carico dell'operatore delle seguenti ulteriori informazioni:

- nome del destinatario
- indirizzo del destinatario
- uffici per conoscenza
- ufficio mittente

Se il documento è trasmesso per via telematica viene prodotta e memorizzata anche l'impronta del documento.

Oltre alle informazioni comuni, la registrazione dei documenti interni prevede l'inserimento a carico dell'operatore delle seguenti ulteriori informazioni:

- ufficio mittente
- ufficio destinatario
- uffici per conoscenza

Segnatura:

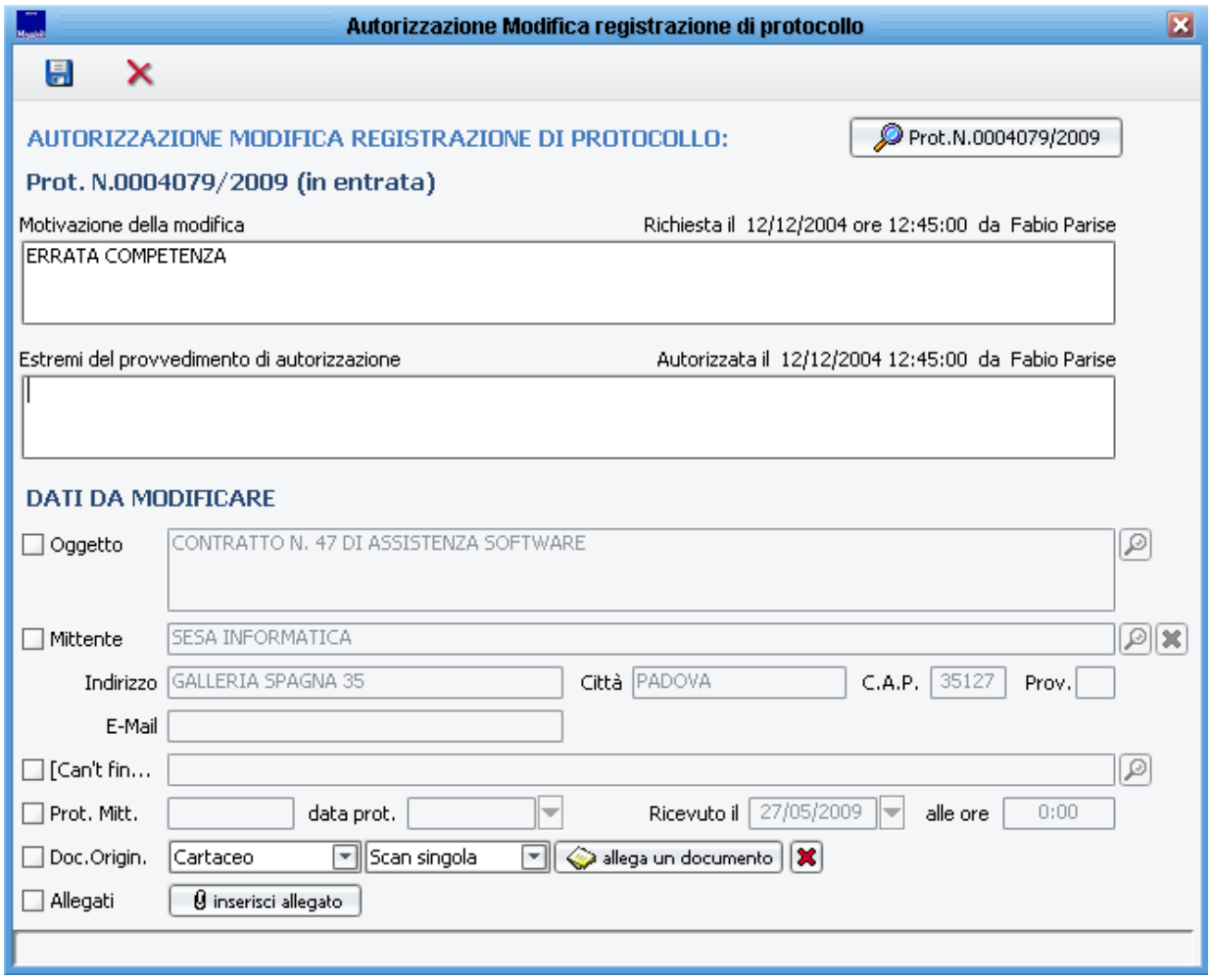
Le funzionalità di segnatura del protocollo informatico hanno uno scopo duplice a seconda che i documenti siano cartacei o che siano informatici (identificata dalle regole tecniche).

Segnatura dei documenti cartacei: il sistema prevede la stampa di un'etichetta autoadesiva contenente tutte le informazioni previste dalla normativa. La segnatura dei documenti di protocollo viene gestita mediante la stampa di etichette autoadesive, bianche o trasparenti, su stampanti a trasferimento termico (ad es. ELTRON 2742, Zebra TLP 2844, INTERMEC EASYCOADER PC4 o simili). Per la caratteristica delle etichette, si suggerisce debbano essere indelebili ed antistrappo e la dimensione tipica è di 34mmX54mm che consente anche la stampa di un codice a barre.

Segnatura dei documenti informatici: il sistema prevede la possibilità di effettuare la segnatura informatica (a norme "AIPA"), secondo la struttura descritta dettagliatamente nel DTD relativo.

La segnatura informatica si compone di tre sezioni: la sezione intestazione contiene i dati identificativi e le informazioni fondamentali del messaggio; la sezione riferimenti contiene le informazioni relative al contesto generale di cui il messaggio fa parte; la sezione descrizione contiene le informazioni descrittive riguardanti il contenuto del messaggio. Intestazione: la sezione intestazione contiene gli elementi essenziali di identificazione e caratterizzazione amministrativa del messaggio protocollato. Tale sezione riporta anche le informazioni relative alla trasmissione del messaggio. In particolare, la sezione contiene l'identificazione della registrazione relativa al messaggio protocollato in uscita. Tale identificazione, ai sensi del DPR n. 445/2000, riporta i seguenti dati: numero progressivo di protocollo; data di registrazione; indicazione della amministrazione mittente; indicazione della AOO mittente. Riferimenti: nella sezione riferimenti sono riportati gli eventuali riferimenti ad altri messaggi protocollati e/o relativi a contesti procedurali o procedimenti. Per i documenti informatici in entrata che provengano da altre AOO o Amministrazioni è prevista una funzione di lettura del file XML associato e la relativa funzione di compilazione in maniera automatica dei campi nella fase di protocollazione. E' prevista inoltre una funzione di ricerca che a partire dal documento individua tutte le informazioni di protocollazione relative ad esso. Per i documenti informatici in uscita è prevista la relativa funzione di generazione e compilazione del file XML.

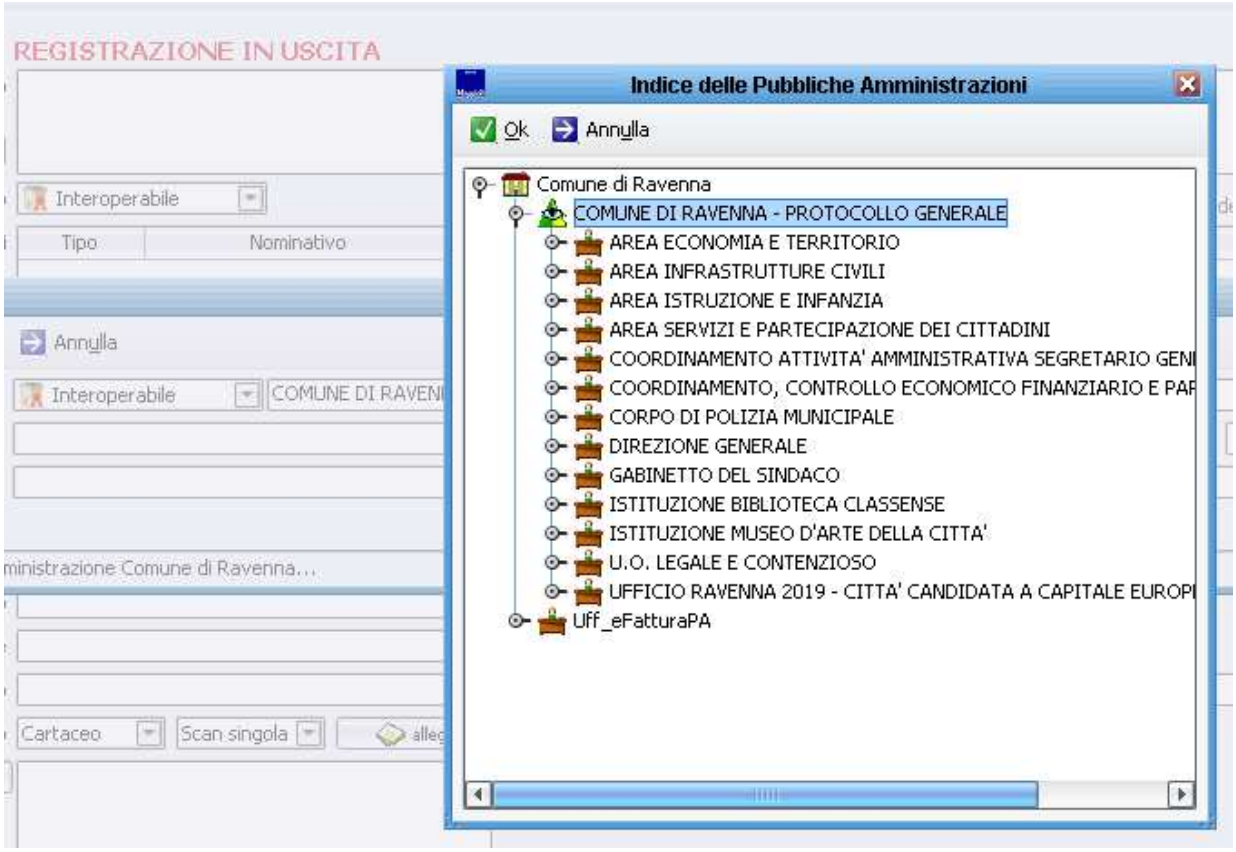
Annullamento o modifica: Le modalità di annullamento e modifica sono regolate dagli art.54 DPR n.445/2000, art.5 DPR n.428/98, regole tecniche art.8. Fra le informazioni generate o assegnate automaticamente dal sistema e registrate in forma non modificabile l'annullamento di una sola di esse determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo. Per le altre informazioni, registrate in forma non modificabile, l'annullamento anche di un solo campo, che si rendesse necessario per correggere errori intercorsi in sede di immissione di dati, comporta la rinnovazione del campo stesso con dati corretti e la contestuale memorizzazione, in modo permanente. L'annullamento totale prevede che le informazioni relative ad un protocollo annullato rimangano comunque memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché gli estremi dell'autorizzazione all'annullamento del protocollo quali: Data; Identificativo dell'operatore; Estremi del provvedimento di autorizzazione.



La procedura di annullamento prevede l'inoltro della richiesta di autorizzazione al Responsabile del protocollo; in caso di accettazione il protocollo assumerà lo stato "annullato". E' comunque consentita, la lettura di tutte le informazioni. Solo il responsabile del protocollo può autorizzare l'annullamento di documenti protocollati. Le procedura di annullamento parziale per i dati non alterabili mette il documento registrato in uno stato particolare "Richiesta di modifica": il Responsabile del protocollo accetta o nega la richiesta. Per le richieste autorizzate la procedura rende disponibili all'operatore le funzioni di modifica. Le modifiche effettuate vengono salvate nella base dati tenendo traccia del dato modificato. E' previsto anche un log in cui sono memorizzati i dati relativi a tutte le modifiche effettuate.

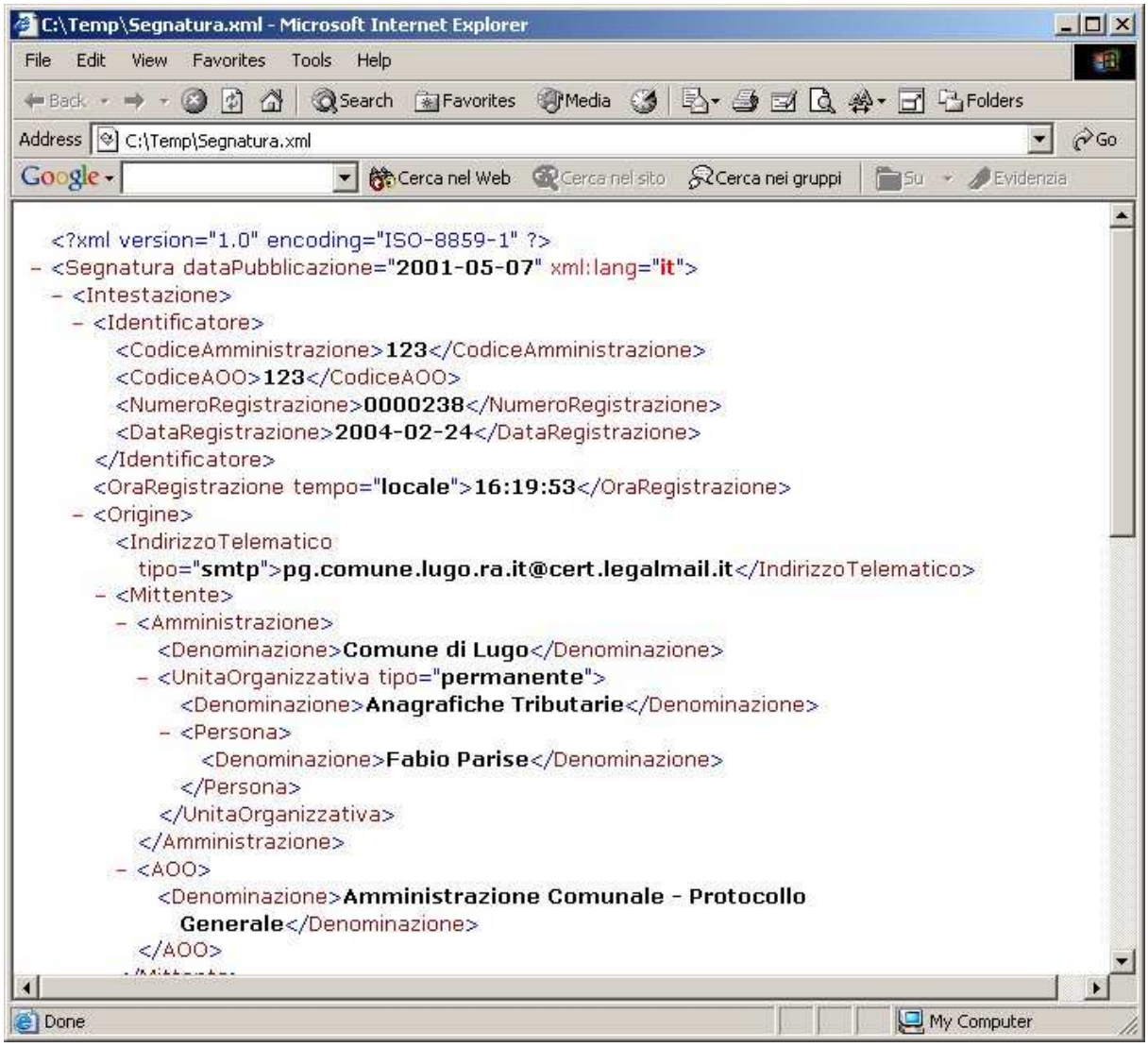
Interoperabilità con altri sistemi di protocollo

La procedura prevede uno specifico modulo di interoperabilità con altri sistemi di protocollo informatico, che prevede la possibilità di trattamento automatico della ricezione/trasmissione di documenti informatici protocollati da/per altri sistemi di protocollo, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti. La procedura opera in conformità alla circolare AIPA del 7 maggio 2001 (n. AIPA/CR/28), che indica in maniera dettagliata le modalità di trasmissione dei documenti informatici, il tipo ed il formato delle informazioni archivistiche di protocollo minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai messaggi di posta elettronica protocollati.



Nella figura precedente vi è un esempio di connessione tramite protocollo LDAP con l'indice delle pubbliche amministrazioni (IPA) per selezionare l'unità organizzativa di una specifica AOO di una certa Amministrazione a cui spedire un documento protocollato secondo le specifiche AIPA.

Nella figura che segue viene mostrato un esempio di generazione del file di segnatura in formato standard XML prodotto secondo lo schema DTD fornito dalle specifiche AIPA.



Come è previsto dalla Circolare AIPA 7 maggio 2001, n° 28 e DTD allegata la produzione della segnatura informatica XML viene generata per tutti i documenti informatici in uscita.
Il messaggio da inviare all'Amministrazione destinataria, tramite, posta certificata, contiene il documento informatico con eventuali allegati e la segnatura informatica di protocollo.
La spedizione del messaggio all'indirizzo di posta elettronica, istituzionale o comunque certificata, dell'Amministrazione destinataria viene composto interagendo con l'indice

nazionale IPA o con un indice locale appositamente costituito per il recupero di informazioni relative alla AOO destinataria.
Il sistema prevede la gestione automatizzata dei messaggi di ritorno provenienti dal sistema di protocollo informatico dell'Amministrazione destinataria:

- Messaggio di conferma di ricezione(non obbligatorio e su richiesta del Mittente)
- Messaggio di notifica di eccezione (obbligatorio)
- Messaggio di aggiornamento di conferma (non obbligatorio)
- Messaggio di annullamento di protocollazione (obbligatorio)

Il sistema prevede la verifica delle firme elettroniche associate ai documenti informatici ricevuti presso l'indirizzo istituzionale dichiarato e ricevuti per via telematica.

Funzioni di backup:
La procedura, nel nucleo minimo, implementa le funzionalità che permettono al Responsabile del protocollo informatico di effettuare le attività di backup del sistema.

Funzionalità di scansione massiva dei documenti

La procedura mette a disposizione specifiche funzionalità per l'acquisizione ottica, via scanner, dei i documenti (uno o più fogli per documento). Tali funzioni permettono la trasformazione dei documenti cartacei in documenti elettronici (in formato immagine); il salvataggio in particolari cartelle di sistema o in un repository documentale; l'attribuzione dei diritti di accesso, in modo che siano rispettate le regole di sicurezza e di riservatezza (privacy), quando gli utenti accedono a tali file.
Sono previste due modalità di acquisizione ottica dei documenti: modalità interattiva (acquisizione ottica di singoli documenti effettuata contestualmente alla protocollazione); modalità differita (acquisizione ottica batch dei documenti effettuata tipicamente in modo massivo in tempi successivi alla protocollazione). Per la modalità di acquisizione ottica interattiva la procedura mette a disposizione delle funzionalità minime native (per scanner TWAIN compatibili) oppure prevede la possibilità di utilizzare le funzionalità messe a disposizione a tale scopo da sistemi di gestione documentale esterni specifici, di società leader di mercato, per i quali è prevista una completa integrazione.
Per la modalità di acquisizione ottica differita la procedura prevede l'utilizzazione (integrata) di prodotti proprietari Maggioli quale J-IRIDE Scan Express presente nel presente progetto/offerta

Archiviazione ottica sostitutiva

Il sistema di gestione documentale proposto può integrare sia sistemi di archiviazione ottica sostitutiva di mercato sia soluzioni sviluppabili ad hoc, la cui scelta può essere differita ad una fase successiva del progetto. La funzione di "archiviazione ottica sostitutiva" sarà disponibile "a menu", consentirà di attivare il sottosistema dedicato allo scopo e al termine delle operazioni di archiviazione aggiornerà il sistema di gestione documentale con le informazioni di riferimento a tali azioni (log, data e ora, operatore, link al documento, ecc.)

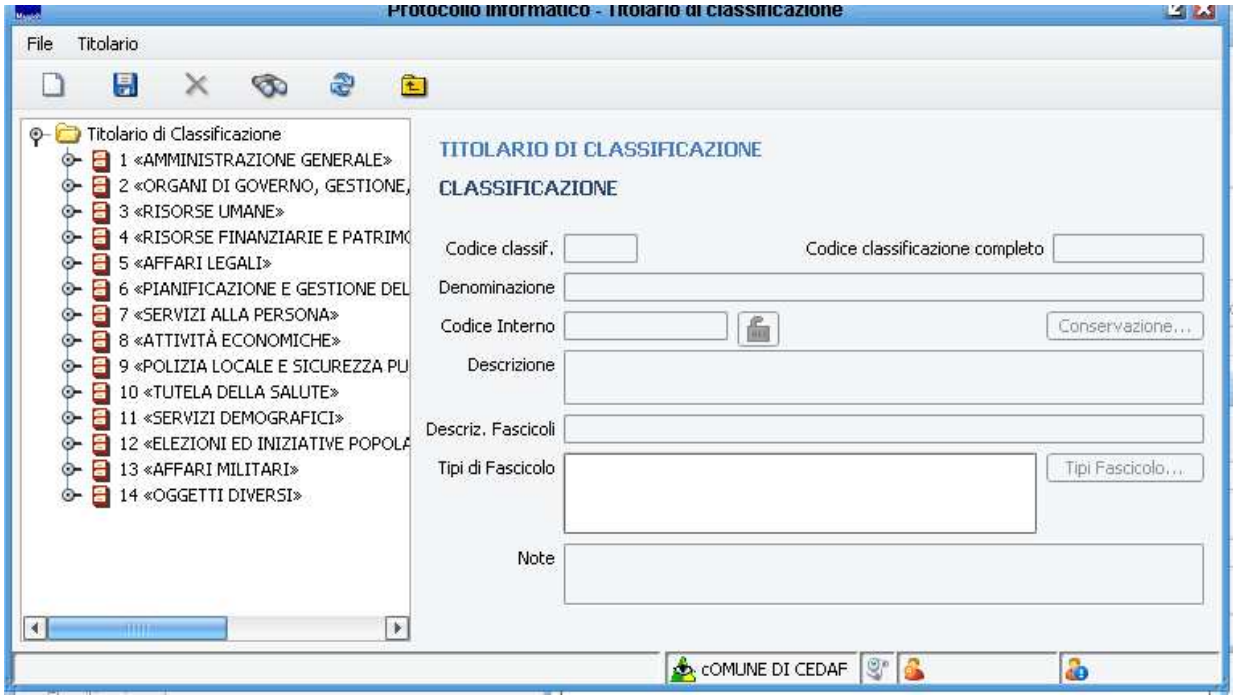
Protocollo di emergenza

La procedura prevede una funzione specifica per la gestione del protocollo di emergenza in conformità a quanto previsto dall'art. 14 del DPR n. 428/98 e dall'art. 63 del DPR n. 445/2000. Le informazioni relative ai documenti protocollati manualmente / automaticamente possono essere reinserite nel sistema informatico utilizzando un'apposita funzione di recupero dei dati. I documenti protocollati con la procedura di emergenza recano due numerazioni: quella di emergenza (numero e data) e quella ordinaria ottenuta dopo il riavvio del sistema dalla registrazione nel sistema dei documenti protocollati manualmente.

MAGGIOLI S.p.A. ha sviluppato un modulo software aggiuntivo per la protocollazione nel registro di emergenza.

Gestione del Titolario

Il nucleo minimo predispone delle funzioni di classificazione del documento protocollato tramite l'associazione del documento protocollato ad un elemento foglia dell'albero di classificazione.



La possibilità di eseguire questa funzione da parte dell'utente è disciplinata da una specifica abilitazione a livello di permessi utente.

Piano di classificazione: la procedura prevede un sistema di classificazione flessibile e adattabile alle esigenze dell'Ente sulla base del piano di classificazione adottato. Il responsabile del protocollo potrà definire il livello di profondità dell'albero di classificazione. L'albero di classificazione definito dall'ente può avere fino a 5 livelli di profondità. La procedura permette di definire la denominazione di ciascun grado divisionale del piano di classificazione. (Ad esempio titolo come primo grado divisionale, classe come secondo, sottoclasse come terzo, categoria come quarto e sottocategoria come quinto). L'Ente potrà redigere l'intero piano di classificazione definendo tutti i criteri di classificazione adottati. Tutti i documenti soggetti a protocollazione vengono classificati secondo il piano di classificazione definito dall'ente. La classificazione avviene tramite l'associazione del documento protocollato ad un elemento foglia dell'albero di classificazione. Le funzionalità di gestione del titolario di classificazione esporranno all'operatore una serie di funzioni quali la navigazione nell'albero di classificazione, l'automatizzazione nella creazione del Repertorio dei fascicoli, ecc. La procedura consente la gestione del Massimario di Scarto, strumento di base per l'effettuazione della delicata operazione di Scarto Archivistico, mediante la quale vengono selezionati i documenti da conservare e distrutti i rimanenti, applicando quanto previsto dal DPR 1409/63. Il massimario di scarto è costituito da un elenco, per ciascuna tipologia di documento riportata nel titolario

d'archivio, dei tempi di conservazione e di scarto espressi in mesi ed anni. Nella definizione del massimario di scarto sono previste per ogni tipologia di documento le seguenti informazioni: descrizione del tipo di documento; periodo di conservazione espresso in anni, oppure l'indicazione di conservazione illimitata; eventuali commenti riguardanti i criteri da applicare per lo scarto.

Gestione dell'archivio:

La funzione di assegnazione di un documento protocollato ad una UOR costituisce la prima fase del flusso documentale. La UOR competente è incaricata della gestione del documento, della sua classificazione, della tenuta del fascicolo archivistico e della eventuale apertura e/o associazione ad un procedimento amministrativo. La possibilità di eseguire questa funzione da parte dell'utente è disciplinata da una specifica abilitazione a livello di permessi utente.

Fascicolazione:

'unità archivistica di base è costituita dal fascicolo, all'interno del quale possono essere contenuti uno o più documenti. La procedura prevede, dopo la fase di classificazione, di assegnare il documento ad un fascicolo (nuovo o esistente). L'inserimento nel fascicolo è effettuato dall'operatore a cui è stato assegnato il documento (operatore che ha preso in carico il documento). Il fascicolo è individuato da tre elementi: l'anno di apertura (o di istruzione); il numero di fascicolo, cioè un numero sequenziale all'interno dell'ultimo grado divisionale, da 1 a n con cadenza annuale; l'oggetto del fascicolo, cioè una stringa di testo atta a descriverne compiutamente il significato. Ogni documento, dopo la sua classificazione, va inserito nel fascicolo di competenza. L'operazione va effettuata dal responsabile del documento. I documenti sono archiviati all'interno di ciascun fascicolo secondo l'ordine logico di registrazione. Quando si verificano tutte le condizioni previste dall'ente per la chiusura (ad es. termine di un procedimento amministrativo nel caso in cui il fascicolo coincida con il procedimento, o a fronte del licenziamento di un dipendente nel caso in cui il fascicolo sia relativo al dipendente) il fascicolo viene chiuso da parte del relativo responsabile, il quale procede poi alla sua archiviazione.

La procedura prevede le seguenti funzionalità nella gestione dei fascicoli: creazione di nuovi fascicoli; gestione dei fascicoli (inserimento/cancellazione documenti, modifica dello stato del fascicolo, modifica della classificazione del fascicolo); ricerche.

Repertorio dei Fascicoli

La procedura consente la tenuta del Repertorio dei fascicoli.

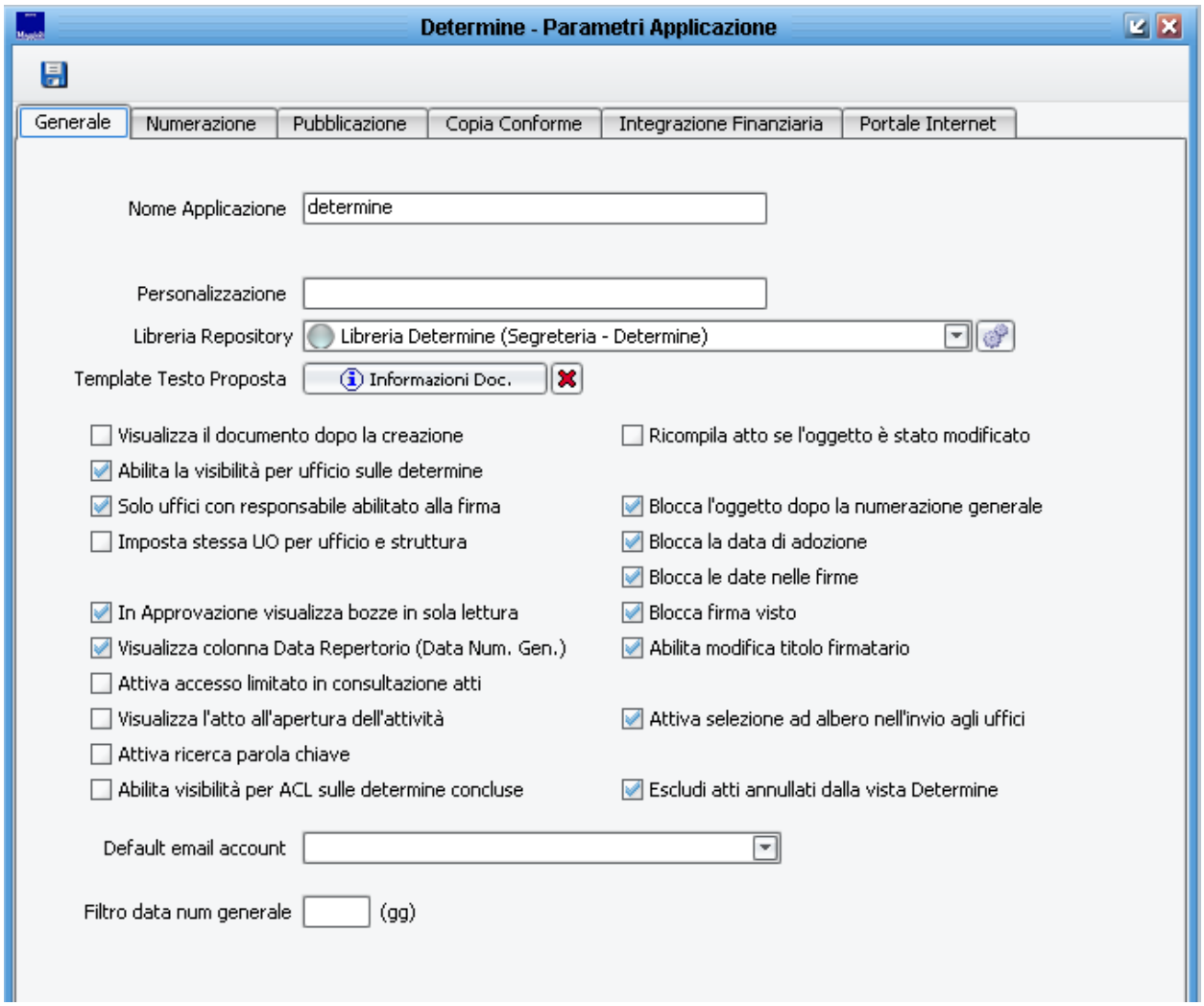
Il Repertorio dei Fascicoli è un registro annuale che inizia il 1° gennaio e termina il 31 dicembre ed è costituito da un elenco ordinato ed aggiornato dei fascicoli istruiti all'interno di ciascuna classe o sottoclasse e riportante tutti i dati del fascicolo. Esso è costituito dai seguenti elementi: anno di istruzione; classificazione completa; numero di fascicolo; anno di chiusura; oggetto del fascicolo; status relativo all'età (corrente o versamento in archivio di deposito); stato di archiviazione (passaggio all'archivio storico o eventuale scarto);

Gestione Archivistica dei Documenti : da un punto di vista prettamente archivistico i documenti si distinguono in: correnti: i documenti del soggetto produttore relativi ad affari correnti e necessari allo svolgimento delle attività; semicorrenti o di deposito: i documenti del soggetto produttore ancora utili per finalità amministrative e giuridiche, ma non necessari allo svolgimento delle attività correnti; storici : documenti relativi ad affari esauriti da oltre 40 anni e selezionati per la conservazione permanente. Il sistema di protocollo informatico e gestione dei flussi documentali opera in maniera integrata con il sistema di gestione documentale. La gestione archivistica dei documenti prevedere il fatto che alcuni documenti possono essere spostati dall'archivio corrente (on line), all'archivio di deposito o storico (off line). Questa operazione fisicamente si traduce nel trasferimento dei documenti dal document repository (archivio on line) verso un supporto di memorizzazione magnetico od ottico (archivio off line). Il sistema tiene traccia dello stato di archiviazione del documento (on line/off line), della data di archiviazione e delle coordinate archivistiche. In caso di richiesta di consultazione di un documento off line, il sistema permette di risalire al supporto di archiviazione in cui è memorizzato il documento, consentendone una semplice consultazione.

ATTI AMMINISTRATIVI

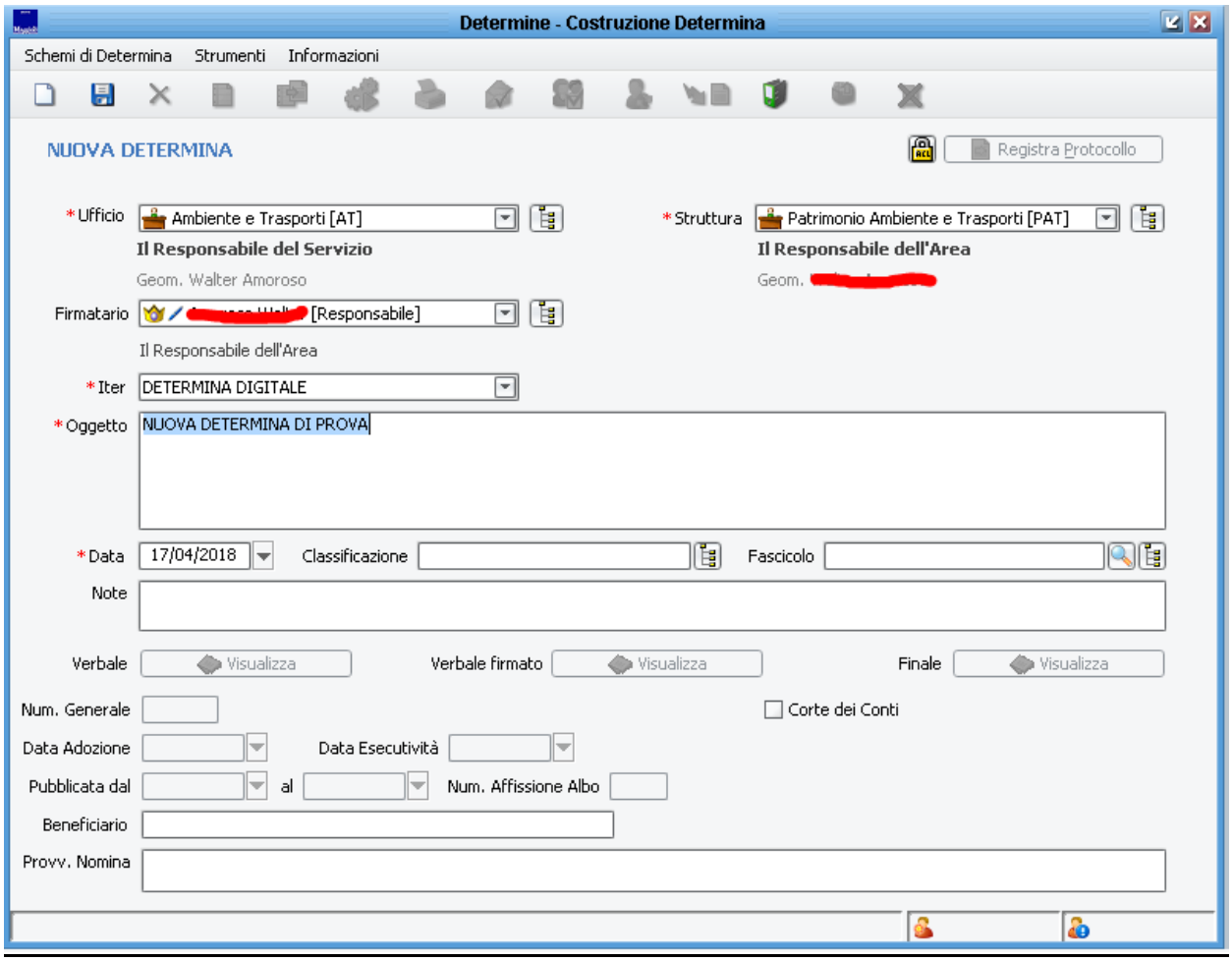
Il modulo applicativo consente la gestione di tutti gli atti amministrativi dell'Ente. Per quanto riguarda ad esempio delle Determinazion: produzione dei documenti, firma dei documenti, validazione dei documenti, possibile integrazione con la procedura di contabilità (impegni), iter dei documenti (workflow), pubblicazione, tenuta dei registri.

Esistono numerosi parametri che consentono di configurare l'applicativo con grande flessibilità in base alle esigenze proprie dell'Ente.



Si citano solo alcuni dei parametri che ad esempio possono essere impostati:

- attivare la visibilità in fase di preparazione all'ufficio
- gestire la numerazione di settore
- impedire modifiche durante la fase di approvazione
- inviare delle notifiche via mail
- bloccare alcuni informazioni chiave dell'atto

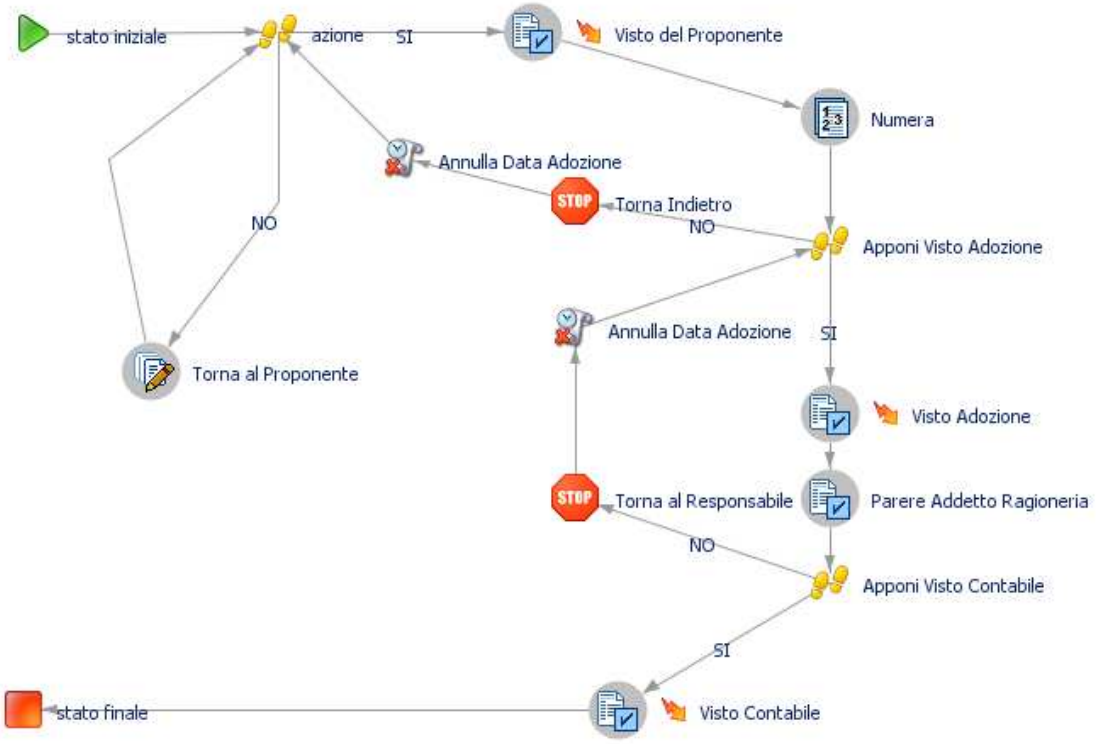


Determine e Delibere di Sicr@web si caratterizzano per le seguenti peculiarità:

- Per ciascun tipo di atto è previsto un modello standard del documento (frontespizio, certificato di pubblicazione e simili, retro) basato sull'associazione di segnalibri e tabelle. Tale formato viene concordato con l'Amministrazione e può essere modificato anche dagli amministratori del sistema.
- L'iter dell'atto viene definito e gestito tramite un motore di Worflow che permette di definire un tipo di iter da seguire per ciascuna tipologia di atto.
- Il tipo di iter viene progettato attraverso la connessione di azioni di Workflow (WKF) specificatamente predisposte per gestire le fasi principali di vita dell'atto: alla stesura del testo segue la compilazione dell'atto sulla base del modello predisposto, l'avvio dell'iter di WKF, l'approvazione tramite firme e/o visti, azioni utenti di scelta, la gestione

della numerazione, il flusso di ritorno in redazione, la sottoscrizione con la firma digitale P7M, ecc…

- Lo stato dell'atto, in corso di approvazione, è visibile tramite l'accesso all'istanza di workflow. L'amministrazione di Workflow e la storia presente nelle azioni permettono di tener traccia di tutti i passaggi effettuati dal documento e dei relativi tempi impiegati tramite l'utilizzo di elementi grafici.



Esempio di un flusso documentale.

Esistono delle griglie che dividono gli atti in tre stati differenti:

1. determine in preparazione, fase della stesura del testo, prima dell'avvio dell'iter di WKF
2. determine in approvazione, fase di iter di WKF in corso
3. determine a iter concluso

Sono previste, tra le altre, le seguenti funzionalità:

- Gestione storico atti con varie possibilità di ricerca;
- Gestione degli allegati (documenti collegati) in vari formati (documenti elettronici di formati diversi, documenti cartacei acquisiti tramite scanner);
- Gestione, all' interno del testo, di dati strutturati con campi formattati e/o segnalibri;

Tipi di determinazioni dirigenziali gestite:

Atti con implicazioni finanziarie (tabella degli impegni e accertamenti):
In fase di predisposizione del documento il sistema può interagire con la procedura di contabilità Sicra e/o Sicraweb. (possibile interfacciamento con altri sistemi contabili)
L'applicativo consente di popolare una tabella degli impegni e degli accertamenti, dispone di un modulo di integrazione che effettua la prenotazione d' impegno, richiamando le maschere della contabilità. Il sistema provvederà, in base all'iter predisposto, alla numerazione dell' atto al momento della trasmissione al Servizio Economico Finanziario riportando il numero all' interno del testo unitamente ai dati contabili.
Al momento dell'apposizione del visto di regolarità contabile i dati verranno automaticamente formalizzati dal sistema e l'atto, reso esecutivo, sarà trasmesso al Servizio Segreteria per la pubblicazione.
L'applicativo è integrato sia con la finanziaria di Sicra che con la finanziaria di SicraWeb.
La tabella impegni/accertamenti può essere usata anche senza integrazioni con la finanziaria per un utilizzo manuale.

Atti senza implicazioni finanziarie:
Saranno trasmessi al Servizio Segreteria senza passaggi intermedi.
Atti che comportano liquidazione di spesa:
Sicr@web permette di gestire gli atti di liquidazione come una tipologia specifica delle determine dette appunto di liquidazione oppure come una applicazione con numerazione separata dalle determine e dette Liquidazioni.

JCITY.GOV ALBO PRETORIO E AMMINISTRAZIONE TRASPERENTE

Modulo J-City.gov-AMT: Amministrazione trasparente:

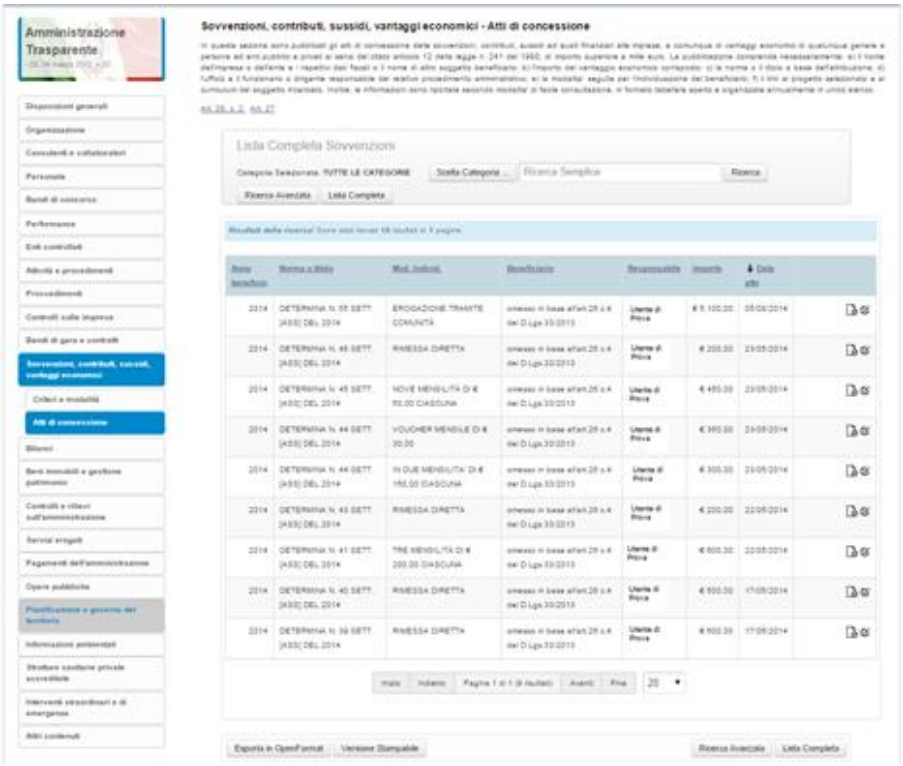
All'interno delle funzionalità del modulo J-City.gov-Amministrazione Trasparente sono ricomprese tutte le esigenze di pubblicazione di piani, informazioni, documenti e atti previsti dal Decreto Legislativo 33. In particolare il modulo **Amministrazione Trasparente** permette ad un ente di pubblicare, secondo la tassonomia prevista dall'Allegato 1 al citato DL.33/2013:

- *Sovvenzioni*, secondo quanto disposto dagli Art. 26 e 27 del citato decreto trasparenza, anch'esso da interfacciare con il relativo sistema di back-end J-Iride o Iride.
- *Incarichi*, secondo quanto disposto dagli Art. 15 del citato decreto trasparenza, anch'esso da interfacciare con il relativo sistema di back-end J-Iride o Iride.
- *Provvedimenti* secondo quanto previsto dall'Art.23 del DL33/2013, da interfacciare con il relativo sistema di back-end J-Iride o Iride
- *Pubblicazione generica atti e documenti*

La soluzione proposta mette a disposizione dell'utente le seguenti caratteristiche:

- l'articolazione di tutte le sezioni documentali, come previsto dal Decreto, nell'Allegato 1;
- un sistema di navigazione che permette di esplorare le diverse sezioni documentali:
- un potente motore di ricerca che permette di individuare in modalità *full text* qualsiasi informazione anche nel caso la stessa sia contenuta all'interno di un documento, a prescindere dalla sezione in cui è archiviato;
- per ogni sezione, i riferimenti alle relative norme, come previsto dall'Art. 12

La modalità principale con cui vengono caricati i dati sul modulo Amministrazione Trasparente è il collegamento con l'applicativo di back office J-Iride. Ciascun atto di determina (o di altro tipo) caricato nel BO può essere pubblicato su una o più sezioni tra quelle previste da Amministrazione Trasparente, specificando quindi fin dal back office la sezione di destinazione, i documenti aggiuntivi allegati ed il periodo di pubblicazione. Il BO guida l'utente attraverso una configurazione che permette di associare a ciascun tipo

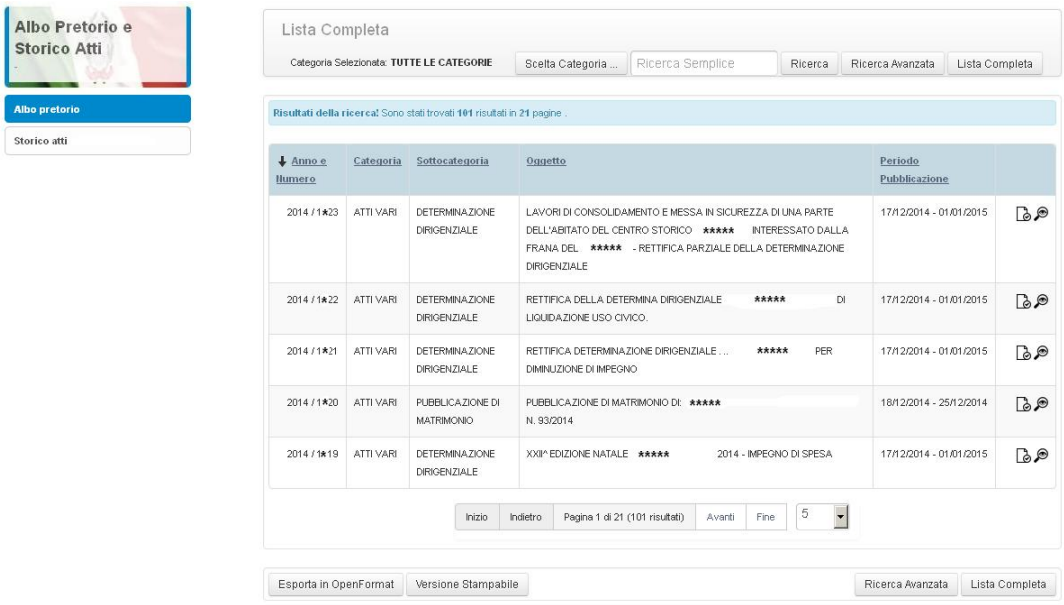


documento la o le sezioni di pubblicazione in modo permanente, semplificando notevolmente la fase di pubblicazione vera e propria.
I servizi verso il front office sono resi attraverso un web service che interrogherà il sistema di BO acquisendo dati e documenti.
A fianco della modalità "automatica" sopra descritta, il modulo Amministrazione Trasparente prevede una funzionalità specifica dedicata al caricamento ed alla gestione documenti attraverso il quale è possibile alimentare il sistema indipendentemente dal back office J-Iride, inserendo nuovi documenti e aggiornando quelli esistenti. Il modulo di gestione documenti non è chiaramente disponibile come accesso pubblico, ma è accessibile solo agli utenti opportunamente autenticati e autorizzati. Questa funzionalità è utile in tutti quei casi dove i documenti da pubblicare provengono dall'esterno del sistema dell'Ente gestore, come ad esempio documenti inviati dalla Corte dei Conti, oppure che non hanno un nesso diretto con l'operatività dell'applicativo J-Iride, come ad esempio il Piano Triennale della Trasparenza o gli Oneri informativi per i cittadini e le imprese.
Non sono previste altre modalità di caricamento e pubblicazione dei dati oltre alle due sopra elencate. Se si desidera pubblicare su J-City.gov dati e documenti presenti su altri sistemi di Amministrazione Trasparente gestiti dall'Ente prima di adottare la soluzione J-City.gov, occorre che l'Amministrazione pubblichi nuovamente i documenti con J-Iride o con J-City.gov secondo le modalità sopra descritte.

Modulo J-City.gov-APS: Pubblicazione albo pretorio e storico atti

Il Cittadino per consultare l'elenco degli atti messi in pubblicazione dall'Amministrazione ha a disposizione tre pagine:

- la pagina di Elenco degli Atti, che ha il compito di esporre l'elenco di tutti gli atti in pubblicazione e attraverso la quale è possibile effettuare delle semplici ricerche di tipo full-text sull'intero archivio. Tutte le colonne presenti all'interno di questa pagina sono ordinabili in modo ascendente o discendente con un semplice click.
- la pagina di dettaglio del singolo atto, che permette di accedere a tutte le informazioni relative all'atto, compresi gli eventuali allegati.
- la pagina di Ricerca Avanzata, attraverso la quale è possibile impostare in modo puntuale dei criteri di ricerca nel caso la semplice ricerca effettuata sulla pagina di Elenco Atti abbia bisogno di una maggiore precisione.
- Il modulo Albo Pretorio e Storico Atti è alimentato direttamente dalle funzionalità di back office, che permettono il caricamento degli atti da pubblicare all'albo pretorio, classificandoli in base a due attributi chiamati categoria e sottocategoria.



SERVIZIO DI CONSERVAZIONE A NORMA DEI DOCUMENTI

Obbiettivo

La presente offerta riguarda il rinnovo e l'estensione del servizio di conservazione attualmente in essere, le classi documentali da conservare sono le seguenti:

- Contratti informatici sottoscritti digitalmente
- Protocollo Generale (PEC)
- Registro Giornaliero di Protocollo
- Fatture Elettroniche

Altre Classi documentali potranno essere aggiunte in seguito.

Il servizio garantisce la leggibilità a lungo termine dei i documenti digitali ed è conforme alla normativa vigente. **Maggioli è Conservatore Accreditato AGID**.

descrizione dei servizi

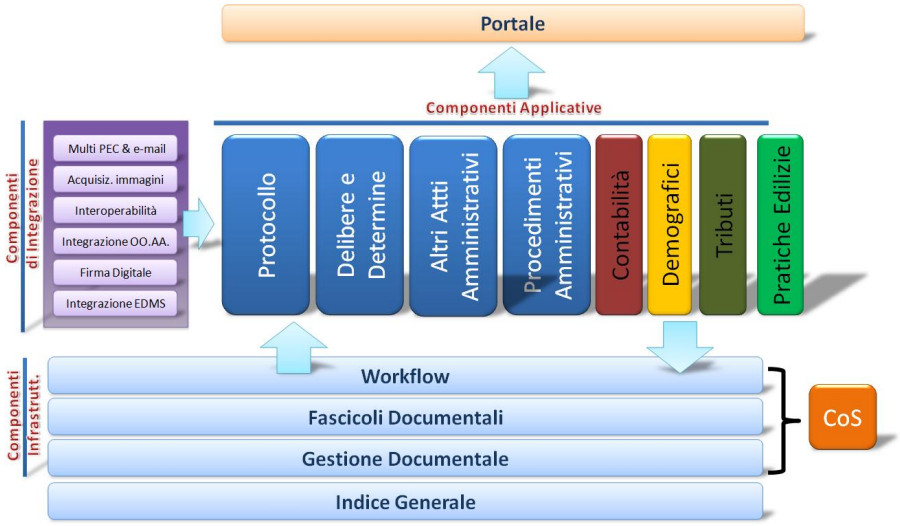
Il Servizio di Conservazione a Norma Maggioli prevede:

- Assunzione della Delega per la gestione del processo di Conservazione da parte di MAGGIOLI.
- Consultazione dei documenti Conservati tramite portale WEB a cui si accede dopo autenticazione di User Name e Password.
- Firma digitale e Marcatura Temporale dei lotti di Conservazione (conservazione mensile, giornaliera per il registro di protocollo)
- Integrazione con il software IRIDE e J-IRIDE (Sicr@web) per il "versamento" automatizzato in conservazione dei documenti informatici.
- E' disponibile il Modulo Sicr@web per la gestione dei contratti, completo di integrazione ed automatismo per la Conservazione. Qualora il Modulo Contratti non fosse attivo presso l'Ente, i file PDF (o PDF/A) firmati digitalmente relativi ai Contratti informatici e ad eventuali allegati, dovranno essere singolarmente indicizzati e caricati (upload) sul portale di Conservazione direttamente dall'operatore dell'Ente che avrà in carico la procedura di invio in Conservazione.

Si consiglia che i documenti firmati digitalmente inviati in conservazione abbiamo firma digitale con validità residua di almeno 45 giorni.

modello di integrazione per il versamento automatico in conservazione

Di seguito la sintesi grafica dei modelli di integrazione operativi fra gli applicativi Maggioli per il versamento automatico in Conservazione sulla piattaforma Maggioli:



SUPPORTO REDAZIONE MANUALE DI GESTIONE DOCUMENTALE E CONSERVAZIONE

Il servizio di redazione del Manuale della Gestione Documentale prevede: 1) Verifica stato dell'arte della gestione documentale e delle azioni previste per la transizione al digitale della PA 2) Elaborazione e condivisione di una prima bozza standard di manuale della gestione documentale 3) Verifica e personalizzazione del modello di manuale di gestione documentale e predisposizione degli allegati tecnici previsti dalla normativa, secondo le esigenze e le specifiche dell'Ente. 4) La produzione del manuale di gestione andrà parallelamente ad una serie di attività di analisi e interviste presso gli uffici per conciliare il piano con le risorse tecniche e organizzative dell'Ente. Il manuale sarà oggetto di costante aggiornamento, verrà infatti rivisitato nelle varie fasi di attuazione dell'intero progetto. Pag. 8 Programma dei lavori 1) Incontro preliminare e propedeutico per la raccolta di informazioni generali per la definizione dello stato dell'arte della gestione documentale e per la presentazione di una bozza standard di manuale di gestione documentale. L'incontro sarà da remoto (previste max 2 sessioni da max 4 ore cad.) Durante l'incontro sarà presentato anche il contesto normativo (CAD e Regole Tecniche) che obbliga alla stesura del manuale di gestione documentale e gli adempimenti normativi relativi alla Conservazione a Norma dei documenti informatici. Saranno raccolte anche le specifiche particolarità dell'Ente. All'incontro dovranno essere presenti i responsabili del servizio protocollo e archivio 2) Predisposizione di una Bozza di Manuale della Gestione Documentale e relativi allegati. L'attività sarà svolta degli esperti Maggioli presso la ns. sede. Sarà compito dell'Ente far pervenire la documentazione e le informazioni specifiche necessarie alla personalizzazione di ogni singola bozza di manuale. 3) Verifica e redazione conclusiva del Manuale della Gestione Documentale e suoi allegati. L'attività prevede la presentazione delle bozze personalizzate del Manuale per la loro verifica, integrazione e completamento. L'incontro sarà da remoto (previste max 2 sessioni da max 4 ore cad.) All'incontro dovranno essere presenti i responsabili del servizio protocollo, archivio e gestione documentale. 4) Presentazione della versione finale del Manuale di Gestione Documentale e della sua gestione operativa, saranno inoltre approfonditi i seguenti ambiti: Gestione della fascicolazione Operatività del software gestionale Maggioli in funzione del Manuale di Gestione Documentale Conservazione a norma dei documenti informatici L'incontro sarà da remoto o in presenza (prevista sessione da max 4 ore) All'incontro dovranno essere presenti i responsabili del servizio protocollo, archivio e gestione documentale. Eventuali attività previste da remoto potranno essere svolte anche in presenza presso il cliente per una maggiore efficacia degli interventi

INSTALLAZIONE

Le attività di installazione e di configurazione dei prodotti offerti saranno effettuate da nostro personale specializzato direttamente presso la vostra sede.
I tecnici Maggioli si occuperanno delle seguenti fasi:

- Configurazione del software di base, limitatamente agli aspetti di corretto funzionamento del sistema applicativa proposto;
- Installazione e configurazione del software applicativo sul server e sui client previsti da progetto.
- Impostazione della sicurezza con l'identificazione dei profili utenti per l'accesso alla applicazione;
- Impostazione dei parametri base della procedura software proposta;
- Effettuare le verifiche ed i test necessari a garantire il corretto funzionamento di tutto il sistema applicativo.

FORMAZIONE SOFTWARE

La formazione del personale da Voi designato all'uso delle procedure sarà svolta da nostri tecnici qualificati presso la Vostra sede.
Durante lo svolgimento del corso sarà effettuata la simulazione delle reali condizioni operative, al fine di garantire la perfetta preparazione del personale addetto.
Il corso avrà una durata massima giornaliera di **6 ore** di lavoro/uomo, non frazionabili in ½ giornate.
L'attività formativa verrà pianificata secondo un calendario che verrà definito in accordo fra le parti, sulla base delle specifiche esigenze di servizio.

CONTRATTO DI ASSISTENZA SOFTWARE

Maggioli S.p.A. offre un servizio di assistenza software a tutti gli Enti che sottoscrivono specifico contratto. Un gruppo di tecnici qualificati garantisce l'aggiornamento e manutenzione del software nonché il supporto telefonico o telematico necessario per la risoluzione di eventuali problemi segnalati dal Cliente.
Maggioli S.p.A. garantisce Assistenza ai programmi software forniti nel pieno rispetto della norma, previo apposito contratto da stipularsi tra le parti.

Per Assistenza Software si intende l'attività volta al ripristino del buon funzionamento dei programmi rispetto ad ogni difetto di progettazione o di realizzazione che dovesse rivelarsi durante l'utilizzo e che ne impedisca il corretto e regolare funzionamento.

SERVIZIO ASSISTENZA SOFTWARE

Il Servizio di Assistenza Software comprende :
1) Servizio di Assistenza Telefonica senza limitazioni di chiamata (servizio di Hot-Line attivo nei giorni feriali dal Lunedì al Venerdì dalle ore 8.30 alle 13.00 e dalle ore 14.00 alle 17.30);
2) Servizio di Teleassistenza ossia un servizio di Assistenza in Remoto che consente l'intervento di un tecnico a distanza direttamente sui PC dell'utente. I tecnici, utilizzando il canale Internet, potranno accedere alla procedura installata presso l'utente per identificare l'anomalia segnalata ed intervenire per la sua risoluzione;
3) Fornitura degli aggiornamenti (patch e/o nuove versioni eventuali) dei programmi installati.
4) Fornitura di eventuali aggiornamenti migliorativi periodici (patch e/o nuove versioni eventuali).
5) Ripristino del buon funzionamento dei programmi per errori e difetti dovuti alla progettazione e/o realizzazione degli stessi.

SERVIZIO SAAS

Il Cloud nelle PA

Il piano triennale per l'informatica nella pubblica amministrazione 2020-2022, strumento fondamentale di guida per le Pubbliche Amministrazioni per indicare gli adeguamenti da seguire per una trasformazione digitale dell'amministrazione italiana e del Paese, si muove nell'ottica di un progressivo miglioramento della gestione interna dell'Ente e del rapporto Ente - cittadino, che deve essere sempre più ottimizzato in trasparenza ed efficienza. Per raggiungere questi traguardi la qualità dei servizi ICT di cui l'Ente è dotato rappresenta un tassello fondamentale. Nello specifico Il piano triennale indica le azioni che le PA devono intraprendere per l'adeguamento tecnologico e nello specifico viene fornito un Modello strategico evolutivo dell'informatica nella PA da adottare in relazione ad ogni componente della Infrastrutture ICT, ovvero nel dettaglio: Cloud della PA; data center e connettività.
Il piano detta pertanto delle direttrici fondamentali:

razionalizzazione e il consolidamento dei data center della Pubblica Amministrazione attraverso la progressiva dismissione dei data center obsoleti e inefficienti, con l'obiettivo di ridurre i costi di gestione delle infrastrutture IT in favore di maggiori investimenti in nuovi servizi digitali;
l'adeguamento del modello di connettività al paradigma Cloud, favorendo la razionalizzazione delle spese per la connettività delle pubbliche amministrazioni e la diffusione della connettività nei luoghi pubblici a beneficio delle PA, dei cittadini e delle imprese.
la razionalizzazione e il consolidamento dei data center della Pubblica.
Il Cloud, nell'ambito della trasformazione digitale, rappresenta infatti una delle tecnologie che comporta notevoli vantaggi in termini di incremento di affidabilità dei sistemi, qualità dei servizi erogati, risparmi di spesa realizzabili attraverso l'opportunità della migrazione dei servizi esistenti verso il Cloud e la possibilità di pagare soltanto gli effettivi servizi utilizzati. L'adozione del paradigma Cloud rappresenta la chiave della trasformazione digitale consentendo una vera e propria rivoluzione del modo di pensare i processi di erogazione dei servizi della PA verso i cittadini. Al fine di incrementare l'adozione del Cloud nella PA, è stato introdotto il Modello Cloud della PA che descrive l'insieme di infrastrutture IT e servizi Cloud qualificati da AGID a disposizione della PA, secondo una strategia che prevede la realizzazione di tale modello, la definizione e attuazione del programma nazionale di abilitazione al Cloud della PA e l'applicazione del principio di Cloud first. La realizzazione di tale strategia consentirà il conseguimento di importanti benefici in termini di flessibilità e risparmio per le PA, oltre ad un significativo incremento di qualità, sicurezza e affidabilità dei servizi per gli utenti dei servizi offerti dalle PA (cittadini e imprese). In questo nuovo scenario secondo quanto definito dalle Circolari AgID n.2 e n.3 del 2018, che regolano la qualificazione dei servizi Cloud, dal 1 aprile 2019, le PA sono espressamente invitate a valutare prima di qualunque altra soluzione tecnologica, il paradigma Cloud e in particolare ad acquistare esclusivamente le soluzioni Cloud e SaaS (Software as a Service) presenti nel Catalogo dei servizi Cloud qualificati per la PA (Cloud Marketplace AgID).

I servizi Cloud Gruppo Maggioli

Mission aziendale del Gruppo Maggioli è da sempre promuovere e accompagnare l'innovazione nelle organizzazioni pubbliche e private attraverso prodotti e servizi che favoriscano evoluzioni tecnologiche e di processo, permettendo così di semplificare la vita a cittadini, professionisti e imprese.
Questa strategia perseguita attraverso divisioni tecniche specializzate in Informatica, Document Management, Editoria e Convegnistica, Gestione delle Entrate e Service, Formazione e Consulenza si è evoluta nel corso degli anni ampliando la propria offerta accreditandosi presso l'Agenzia per l'Italia Digitale AgID come Cloud Service Provider (CSP) AGID per le proprie soluzioni di servizi SaaS con offerta disponibile sul Marketplace della Pubblica Amministrazione consultabile all'indirizzo: https://cloud.italia.it/marketplace/

In questa ottica il Gruppo Maggioli una infrastruttura e servizi Cloud di proprietà (https://cloud.italia.it/marketplace/service/45), individuando e avvalendosi delle migliori soluzioni tecnologiche presenti sul mercato al fine di garantire ai propri clienti i massimi livelli di sicurezza, disponibilità, flessibilità e scalabilità.
Il Cloud Gruppo Maggioli vanta il rispetto di tutti i requisiti organizzativi, di sicurezza ed affidabilità, di performance e interoperabilità, fissati dalle norme definite nella circolare AGID n. 2 del 9 aprile 2018 e rappresentando un fornitore di riferimento organizzazioni pubbliche e private.
Il Cloud Gruppo Maggioli è stato progettato per erogare servizi di tipo Saas, IaaS e PaaS e la sua architettura modulare sottostante prevede l'uso di soluzioni flessibili e scalabili. Il Gruppo Maggioli gestisce, attraverso uno staff altamente qualificato, interamente tutti i livelli operativi dei servizi Cloud proposti su infrastrutture tecnologiche di proprietà, ospitate presso i più prestigiosi Data Center del panorama italiano.

Portafoglio di servizi Cloud Gruppo Maggioli

Il Cloud Gruppo Maggioli vanta un ampio portafoglio di servizi ed è supportato da tutte le funzionalità di base necessarie per garantire prestazioni e affidabilità di livello Enterprise.

I data center Gruppo Maggioli

Maggioli ha selezionato tre siti datacenter, situati su territorio italiano, su cui implementare il proprio Cloud:
Sito Primario: Data Center Campus DATA4 – Milano Cornaredo (MI)
Sito Secondario: Data Center Retelit Bologna Villanova di Castenaso (BO)

- Sito Secondario: Data Center Maggioli – Mantova (MN)

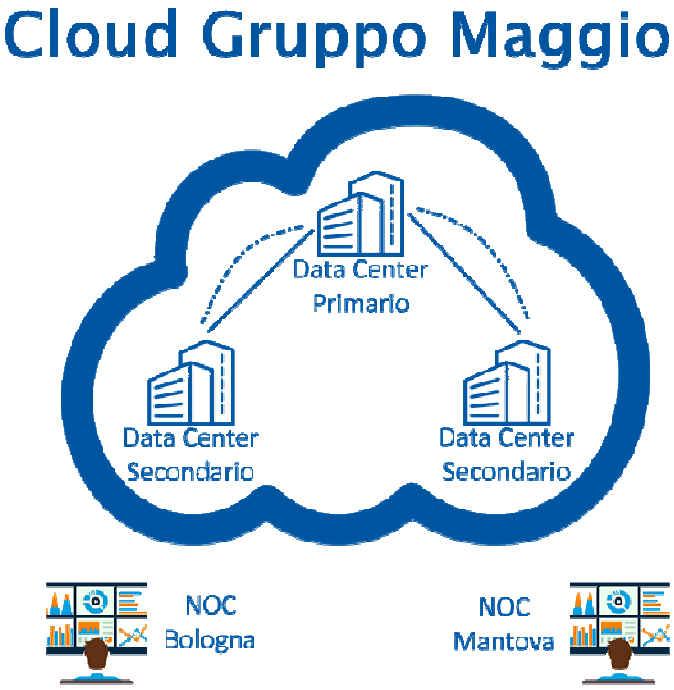


Figura 1- Distribuzione del Cloud Gruppo Maggioli

L'adozione di tre diversi Data Center permette l'erogazione di servizi ad altissima affidabilità con garanzia di integrità dei dati, il tutto grazie a soluzioni di replica dati, copie multiple di backup, molteplici punti di accesso a Internet, distribuzione dei servizi e nuove soluzioni in fase di continua evoluzione ad arricchimento del portafoglio Cloud Gruppo Maggioli.

I criteri di identificazioni dei Data Center hanno previsto una scrupolosa valutazione tra cui alcuni degli più qualificanti sono stati:

Gestione della sicurezza ISO 27001;

Livelli di affidabilità TIER IV (sito principale) e TIERIII (siti secondari);

Presenza operatori Internet Nazionali e Internazionali;

Vicinanza al MiX (Milan Internet Exchange);

Soluzioni di riduzione dell'impatto ambientale;

Esperienza e competenza nella gestione delle piattaforme tecnologiche e di sicurezza;

Neutralità verso operatori terzi;

Flessibilità e velocità di implementazione;

Scalabilità.

La scelta di Data Center di tipo TIER IV garantisce il massimo livello di affidabilità raggiungibile con garanzie di servizio di primordine. Sotto si riportano le caratteristiche di SLA con

caratteristiche di riferimento, percentuali di disponibilità e massimo fermo tollerabile su base annua.

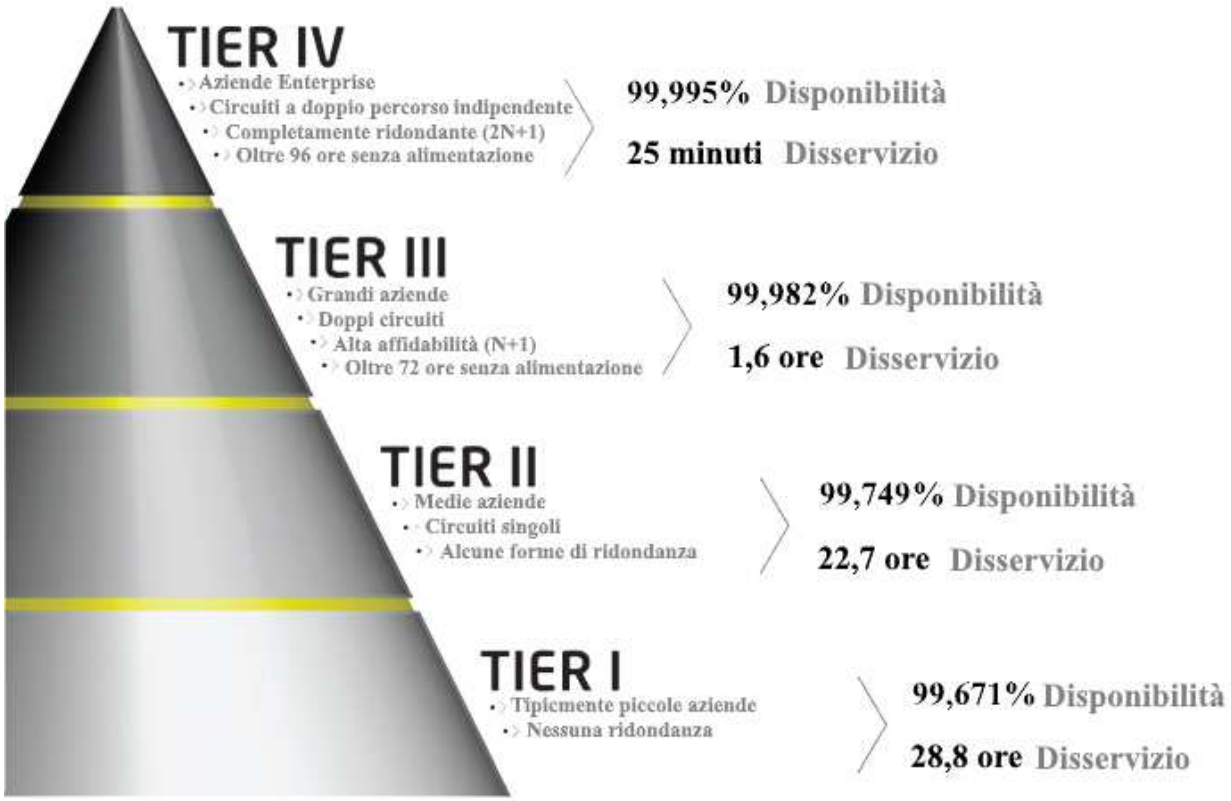


Figura 2- SLA Classificazione Data Center

Maggioli informazioni riguardanti l'infrastruttura Cloud Gruppo Maggioli sono disponibili nel documento di allegato tecnico: "MAGGIOLI SPA - Infrastruttura Cloud Gruppo Maggioli - Allegato Tecnico.pdf"

Modalità di erogazione suite Maggioli in ambiente Cloud

Questa modalità di fornitura prevede che il software sia fruito direttamente attraverso Internet in quanto erogato dall' infrastruttura Cloud Gruppo Maggioli. I servizi Cloud Gruppo Maggioli sono certificati AGID e disponibili sul marketplace Cloud della PA come da Catalogo dei servizi Cloud per la PA qualificati, disponibile al seguente URL: https://cloud.italia.it/marketplace/
Dettagli relativi alle caratteristiche del servizio quali, attivazione e disattivazione del servizio, utilizzo del servizio, scalabilità, piattaforme e livelli di servizi garantiti, sono disponibili on line all'URL:

- **Sicr@web** https://cloud.italia.it/marketplace/service/53

I vantaggi del servizio Cloud

Un servizio Cloud prevede che il gestore del servizio (CSP) sia responsabile della predisposizione, configurazione, messa in esercizio e manutenzione della suite software erogata attraverso l'infrastruttura Cloud del fornitore i servizi lasciando al Cliente il solo ruolo di utilizzatore delle funzionalità software offerte.
L'adozione di un tale paradigma introduce diverse importanti considerazioni tecnico economiche per il Cliente, tra le principali è importante sottolineare:

- **Miglioramento dell'efficienza operativa degli ambienti ICT**: Il Cloud rende l'attività lavorativa del Cliente molto più rapida, agile e flessibile. La presenza di connessioni Internet con banda di dimensioni sempre più larghe e l'utilizzo di infrastrutture Cloud altamente specializzate, garantisce disponibilità, flessibilità e scalabilità dei servizi dell'Cliente nonché prestazioni superiori rispetto alla classica infrastruttura on-premise.
- **Riduzioni di costi** collocare all'esterno applicazioni e dati permette di ridurre i costi dell'hardware, del software e della loro manutenzione. I servizi in Cloud possono essere pagati in base ad un canone annuale flessibile.
- **Software sempre aggiornato**: Il supporto e gli aggiornamenti sono attività costose e complicate da gestire ed è molto difficile per qualsiasi organizzazione tenere il passo con la costante richiesta di aggiornamenti e patch di sicurezza. Un servizio software erogato in modalità Cloud garantisce, che tutte le componenti necessarie alla fruizione del

servizio stesso vengano mantenute, aggiornate, migliorate durante tutto la durata contrattuale direttamente dal fornitore senza costi aggiuntivi per l'Ente Cliente.

- **Garanzia di sicurezza e protezione dei dati:** I dati archiviati in ambiente Cloud sono sottoposti alle più avanzate tecniche protezione dati per prevenire possibilità di attacchi hacker e potenziali perdite di dati. Le workstation dell'Ente Cliente possono pertanto interconnettersi e lavorare senza il rischio di essere intaccate da fattori esterni.

Caratteristiche del servizio Cloud

La modalità di erogazione del servizio Sicr@web Cloud proposta dal Gruppo Maggioli include non solo l'erogazione delle funzionalità software ma anche la fornitura di diversi servizi di assistenza, manutenzione e supporto di seguito descritti:

- Attivazione del servizio Cloud: predisposizione dell'infrastruttura, software applicativo, dei suoi prerequisiti di base (e.g. database server) e configurazione della connettività verso l'Ente Cliente.
- Continuità di servizio, l'architettura Cloud Gruppo Maggioli si incarica di tutte le operazioni necessarie per garantire la disponibilità del servizio (e.g. architettura ridondata, monitoraggio del sistema, backup) secondo gli SLA di seguito riportati e pubblicati sul market-place AGID.
- Problem solving pro-attivo, il sistema è sottoposto a costante monitoraggio, questo consente di prevedere e risolvere pro-attivamente molti dei problemi che si possono presentare nell'erogazione del servizio.
- Performance e Scalabilità, la piattaforma Cloud Gruppo Maggioli dispone di tutte le tecnologie e le skill necessarie per garantire le performance del servizio.
- Manutenzione: gli specialisti tecnici del Gruppo Maggioli si incaricano di tutte le operazioni di manutenzione ed aggiornamento della piattaforma di base e del software specifico in uso all'Ente Cliente garantendo il minimo impatto sulla sua operatività.
- Sicurezza: il Cloud Gruppo Maggioli è dotato di tutta l'infrastruttura necessaria a garantire la sicurezza del sistema, sia da un punto di vista fisico (e.g. anti-incendio, sorveglianza) sia da un punto di vista software (e.g. firewall, sistemi di anti-intrusione).

L'Ente Cliente è quindi sollevato da tutti i problemi di sicurezza, ridondanza dell'architettura, controllo degli accessi fisici e remoti, amministrazione, manutenzione, backup e recovery dei sistemi fisici. Inoltre, può scalare capacità elaborativa, memoria volatile e permanente e connettività progressivamente in funzione del carico.

La soluzione Sicr@web Agile Cloud

La soluzione Sicr@web Agile SaaS si applica allo scenario in cui il Cliente dispone della soluzione Sicr@web in Cloud presso il Cloud Gruppo Maggioli.

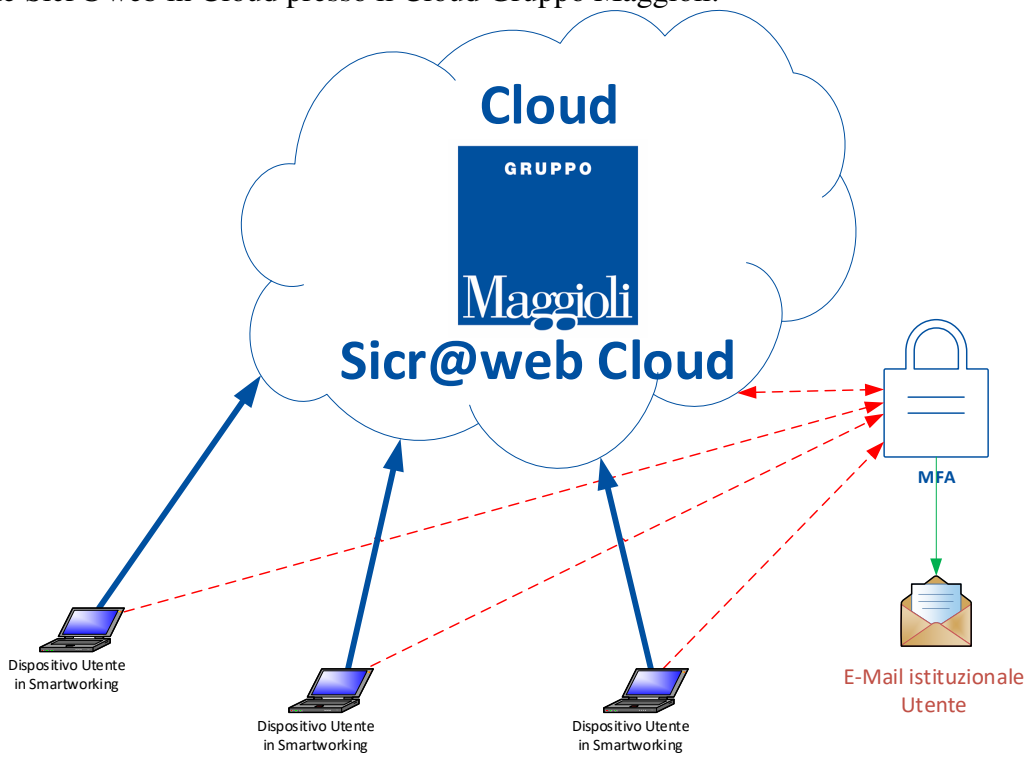


Figura 3 Sicr@web Agile Cloud

Oltre al tradizionale accesso previsto dalla sede del Cliente viene abilitato un accesso ulteriormente protetto da autenticazione MFA (Multi Factor Authentication) utile alla connessione da parte degli utenti in Smartworking.
L'MFA prevede la definizione da parte del cliente di una lista preautorizzata di utenti identificati da nome, cognome e indirizzo e-mail. Il servizio mette a disposizione un portale dove i soli utenti autorizzati dal cliente accedono identificandosi con le credenziali attivate col servizio.
L'utente riceve un messaggio e-mail nella propria casella istituzione contente un codice OTP (One Time Password) da riportare nel portale web MFA che, una volta verificato il codice, reindirizza sull'accesso alla suite Sicr@web in totale sicurezza.

Requisiti Sicr@web Agile Cloud

Ogni ***Postazione Utente*** in Smartworking deve:

- Disporre di una postazione conforme con i requisiti della suite Sicr@web (vedi https://wiki.maggioli.it/images/7/7a/Sicraweb-Requisiti_Client_SicraWeb_1.7.pdf);
- Disporre di una utenza MFA univoca (non è consentito l'uso di una stessa utenza MFA da più utenti o dispositivi);
- Accedere alla casella e-mail istituzionale dell'utente cui saranno consegnati gli accessi MFA;
- Essere connessa a Internet con una connessione stabile e disporre di almeno 700Kbps in upload e 7Mbps in download;
- Rispondere a tutti i requisiti minimi di sicurezza indicati dal Cliente;
- Seguire tutte indicazioni "Lavoro agile - Linee guida" (http://www.funzionepubblica.gov.it/lavoro-agile-linee-guida)
    - Assicurarsi che il sistema operativo sia aggiornato con le relative patch di sicurezza, antivirus, etc.;
    - Non memorizzare le password di accesso all'utilizzo delle risorse sulle postazioni personali, evitando di scrivere password su post-it e/o fogli lasciati in prossimità della postazione;
    - Non effettuare salvataggi su dispositivi personale e utilizzare le risorse cloud messe a disposizione dal titolare del trattamento, limitando il ricorso a dispositivi esterni opportunamente cifrati;
    - Bloccare la postazione in caso di assenza, seppur temporanea;
    - Non gettare nella spazzatura documenti cartacei utilizzati per l'attività lavorativa contenenti dati personali se non dopo averli triturati;
    - Comunicare senza ritardo ogni tipo di incidente da cui potrebbe derivare una violazione di dati personali;
- Disporre di una soluzione antivirus aggiornata e funzionante.

Limitazioni applicative Sicr@web Agile Cloud

L'erogazione dei servizi attraverso Sicr@web Smartworking consentirà di effettuare qualsiasi attività di backoffice, con le seguenti limitazioni di carattere tecnico-logistico:

- per gli Enti subentrati in ANPR sarà necessario certificare le postazioni locali, per poter operare sull'anagrafe relativamente a variazioni/interrogazioni sulla banca dati ANPR;
- per l'utilizzo dei dispositivi, stampanti, scanner, firme, si dovrà valutare la specifica attività di riconfigurazione sulla postazione locale;
- la postazione locale dovrà possedere il medesimo editor di testo (Word, Open Office, Libre Office) utilizzato per la configurazione dei modelli presenti sul Server;

- limitazione su acquisizione e/o produzione di specifica documentazione cartacea, in relazione alla logistica e/o all'utilizzo di stampanti adeguate (es. Atti di Stato Civile);
- La lettura di file con estensioni specifiche richiede l'installazione sulla postazione locale di software specializzati (es. Dike);
- Le prestazioni operative sono condizionate dalla capacità della linea Internet cui è connessa l'utenza.

Limitazioni generali Sicr@web Agile Cloud

Per l'attivazione e il funzionamento dei servizi di Sicr@web Agile sono inoltri richiesti:

- Definizione di un "Referente unico del Cliente per il delivery del servizio". Il referente dovrà essere reperibile in orario lavorativo per essere contattato dal nostro staff per la definizione dell'intervento di installazione e per il reperimento delle informazioni necessarie.
- Definizione dell'elenco utenze da abilitare nel sistema MFA (lista con nome, cognome ed e-mail istituzionale per ogni utente).

Servizio di replica geografica infrastruttura (opzionale)

Grazie alla sua infrastruttura tecnologica distribuita su più data center posizionati nel territorio italiano, il servizio Sicr@web Cloud può essere completato con l'opzione di **replica geografica infrastruttura** che prevede l'esecuzione di una replica giornaliera dei server fisici virtuali dal sito primario del Gruppo Maggioli (Milano) ad uno dei due siti secondari del gruppo (Mantova e/o Bologna).
La replica della VM è sempre disponibile per la riattivazione sul sito secondario e potrà essere raggiunta utilizzando indirizzamento IP pubblico differente compreso nel servizio.

Il servizio di replica geografica infrastruttura prevede le seguenti SLA garantite:

- RTO (recovery point objective): 36 H
- RPO (recovery point objective) – 24 H,

RTO e RPO più stringenti possono essere richieste dal Cliente a seguito di analisi tecnica e progettuale delle caratteristiche specifiche dell'applicazioni in uso (personalizzazioni e verticalizzazioni della stessa).

Caratteristiche principali servizio cloud Sicr@web

Nella modalità Cloud la suite software Sicr@web e relative verticalizzazioni e/o personalizzazioni presenti, sono erogate tramite l'infrastruttura Cloud Gruppo Maggioli.
Questa soluzione consente all'Cliente di non impegnare la propria infrastruttura tecnologica locale, ottenendo in tempi rapido la possibilità di:

- usare i moduli applicativi attraverso Internet (canale cifrato);
- immagazzinare in Cloud i dati necessari ai moduli applicativi;

- usufruire dalla manutenzione proattiva e correttiva;
- beneficiare di tutti i servizi di sicurezza, monitoraggio, controllo degli accessi, manutenzione dei sistemi, backup dei dati e recovery delle applicazioni offerti da Cloud Gruppo Maggioli
- servizio di raccolta di log di sistema con retention di 6 mesi
- replica geografica data base applicativo.

Prerequisiti internet consigliati per il servizio Cloud Sicr@web

Poiché le caratteristiche di erogazione in modalità Cloud della suite Sicr@web sono strettamente correlata alla connettività Internet in dotazione all'Ente Cliente, si fa presente che questo scenario tecnologico presenta produce i migliori risultati in presenza del rispetto dei seguenti requisiti consigliati:

- dotazione da parte del Cliente di due apparati firewall in HA;
- dotazione da parte del Cliente di doppia connettività Internet ridondata;
- gestione attraverso gli apparati firewall locali del failover e bandwith delle connettività.

Inoltre si riportano per completezza i requisiti di banda internet consigliati specifici per la suite Sicr@web:

Suite Maggioli	Caratteristiche di connettività Internet consigliate
Sicr@web	In presenza di postazioni di lavoro connesse tramite rete geografica occorre considerare che l'occupazione media di banda è pari a 300 kbps a postazione in fase di apertura sessione e 100 kbps a postazione durante una normale sessione di lavoro. Al fine di ottenere tempi di risposta ottimali, occorre avere a diposizione una linea con 2Mb/s sincroni ogni 15 client. Previa valutazione sistemistica è possibile dotarsi di WanAccelerator Sicr@Web per ridurre il consumo di banda, come da specifica documentazione.

Prerequisiti Client servizio Cloud Sicr@web

Si riportano per completezza i prerequisiti di Client consigliati specifici per la suite Sicr@web:

Suite Maggioli	Caratteristiche consigliate Client
Sicr@web	Workstation Client: • CPU: Intel Core i3/i5/i7 serie 4000 (anno 2014) • RAM: 4 GB (di cui liberi almeno 1GB) • HD: 10 GB spazio libero • SO: Ms Windows 7 64bit, Windows 8.1 64 bit, Windows 10 64 bit (Nota: si sconsigliano le versioni Home e/o Starter). Per quei sistemi operativi non più supportati dalla software house di produzione non verrà fornita assistenza: es. Microsoft Windows Vista, XP o 2000. Versioni JRE 32bit: 1.8 update 181 o superiore (verificare l'ultima versione certificata al seguente URL http://sicrawebhelp.saga.it/index.php/Java La versione di java deve essere comunque supportata dal sistema operativo client come da requisiti ufficiali Oracle. Per maggiori informazioni si prega di consultare il seguente URL: http://sicrawebhelp.saga.it/index.php/Requisiti_Client_e_Server_Sicr@web Prerequisiti: **in presenza di postazioni di lavoro connesse tramite rete geografica si consideri che l'occupazione media di banda è: 300 kbps a postazione in fase di apertura sessione e 100 kbps a postazione durante una normale sessione di lavoro Durante lo studio di fattibilità è bene considerare che per avere tempi di risposta accettabili è necessario prevedere una linea con 2Mb/s sincroni ogni 15 client.**

Tempi di attivazione dei servizi Cloud Gruppo Maggioli

Tempi di attivazione e disattivazione	Attivazione:5 giorni Disattivazione: 10 giorni
Processo di attivazione ambiente Cloud	Il processo di attivazione decorre dalla sottoscrizione contrattuale e prevede l'attivazione dell'istanza applicativa (nel caso di prima fornitura del servizio), l'abilitazione dei servizi acquisiti e la trasmissione delle

Maggioli	credenziali temporanee di primo accesso.
Processo di disattivazione ambiente Cloud Maggioli	Il processo di disattivazione parziale o totale del servizio si attiva automaticamente decorsi 30gg dal termine contrattuale o a seguito di esplicita richiesta dell'Ente Cliente.

Livello di servizio garantito SLA

Availability (in percentuale)	99.5 %
Support hours per il canale e-mail	Dal lunedì al venerdì, dalle 8.30 alle 17.30. Opzionale estensione di orario e giornate.
Support hours per il canale telefonico	Dal lunedì al venerdì, dalle 8.30 alle 17.30. Opzionale estensione di orario e giornate.
Support hours per il sistema di online ticketing	Dal lunedì al venerdì, dalle 8.30 alle 17.30. Opzionale estensione di orario e giornate.
Maximum First Support Response Time (in minuti)	120 min

Allegati

Titolo Allegato	Nome file	Versione aggiornata on-line
Infrastruttura Cloud Gruppo Maggioli - Allegato Tecnico	MAGGIOLI SPA - Infrastruttura Cloud Gruppo Maggioli - Allegato Tecnico.pdf	*link*
Servizi Cloud e sistemistici - SLA Tecnici di Riferimento	MAGGIOLI SPA - Servizi Cloud e sistemistici - SLA Tecnici di Riferimento.pdf	*link*

OFFERTA ECONOMICA : moduli software oggetto della fornitura

Moduli software proposti SAS	Prezzo
JIRIDE - Indice generale	
JIRIDE- Protocollo Informatico	
JIRIDE - Atti Amministrativi	
JIRIDE - Gestione documentale	
JIRIDE - Connettore conservazione Maggioli	
JCITY – Amministrazione Trasparente, Anac	
JCITY- Albo Pretorio on line	

Servizi di startup una tantum :

N.B. AVVIO DEI MODULI SOPRAINDICATI CON L'ATTIVITA' DI CONFIGURAZIONE E FORMAZIONE ENTRO IL 31 12 2022

Attività	Prezzo
Installazione procedure (attività erogate dalle sedi Maggioli)	€ 800,00
Attivazione conservazione a norma dei documenti (attività erogate dalle sedi Maggioli)	€ 400,00
Attività di configurazione da remoto a corpo , organigramma , titolario , iter atti Amminstrativi : • Protocollo Informatico • Atti amministrativi	€ 2.200,00 A CORPO
2 Giornate di formazione da remoto Protocollo e Atti	€ 900,00
2 Giornate di formazione on site presso l'ente per supporto all'avviamento Protocollo e atti	€ 1.160,00
Fornitura Sigillo Elettronico Namirial	€ 100,00
TOTALE Servizi :	**€ 5.560,00**

I prezzi indicati sono IVA esclusa

MANUALE DI GESTIONE DOCUMENTALE

N.B. CONSEGNA DEL MANUALE DI GESTIONE DOCUMENTALE DA CONCORDARE CON L'ENTE IN BASE AL QUESTIONARIO CHE L'ENTE DEVE RESTITUIRE A MAGGIOLI PER LA REDAZIONE DEL MANUALE

Attività	Prezzo
REDAZIONE DEL MANUALE DI GESTIONE DOCUMENTALE Raccolta informazioni per redazione manuale Presentazione e condivisione bozza manuale Redazione versione finale manuale .Supporto presentazione manuale	€ 2.800,00

Conversione archivi

N.B. CONSEGNA DA CONCORDARE CON L'ENTE IN BASE ALLA CONSEGNA DEGLI ARCHIVI

Attività	Prezzo
Conversione Protocollo	
Conversione Atti Ammnistrativi	
Conversione Albo Pretorio e Amministrazione Trasparente	
TOTALE:	**€ 5.550,00**

Canone annuo servizio SAAS a decorrere dall'avvio del Servizio

Attività	Prezzo
JIRIDE – JCITY AMT Albo – Sigillo Namirial COS conservazione a norma canone annuo servizio Saas	€ 8.600,00
IMPORTO TOTALE CANONE SAAS 2023 , 2024 , 2025	**€ 25.800,00**

I prezzi indicati sono IVA esclusa

N.B. Qualora l'ente IRPET decida di rescindere il contratto prima del triennio , Maggioli come da normativa AGID (vedi linee guida) si impegna a fornire dump del data base di JIRIDE nei tempi richiesti da IRPET

CONDIZIONI GENERALI

I moduli software oggetto della presente offerta implementano le funzionalità a supporto dei processi contabili riferiti alla normativa di riferimento esplicitato nel paragrafo di descrizione funzionale del sistema. Eventuali richieste di variazione delle funzionalità e/o logiche già implementate sul sistema offerto dovranno essere analizzate e valutate a parte come richieste di personalizzazione soggette a preventivo. Allo stesso modo eventuali giornate on- site ulteriori rispetto a quanto previsto nella presente, saranno rendicontate sulla base di tariffe giornaliere a Voi riservate.

Termini di consegna

La presente proposta progettuale del sistema prevede l'avvio entro il 31 12 2022 , resta da concordare tra le parti la consegna del Manuale di Gestione Documentale e la consegna della conversione archivi .

Modalità di fatturazione

Le licenze del software applicativo a seguito della installazione del software presso la vostra infrastruttura.
Giornate di intervento presso di Voi (installazione, formazione, ecc.): a consuntivo mensile sulla base dei rapportini di intervento prodotti a seguito di ciascun intervento on-site.
Manutenzione: annuale anticipata.

Termini di pagamento

Accredito su nostro conto corrente bancario tramite bonifico bancario, a 30 giorni data fattura.
In caso di ritardato pagamento, Maggioli avrà diritto ad addebitare al cliente, senza necessità di costituzione in mora, gli interessi passivi, al tasso legale corrente, ferma restando la facoltà di interrompere la fornitura di tutti i prodotti/servizi non ancora erogati.

Oneri contrattuali

Eventuali spese e/o diritti inerenti il contratto, quali oneri di registrazione, diritti di stipula, di bollo, ecc. non sono compresi nei prezzi della presente proposta .

Diritti di Autore e Clausole di riservatezza

Prezzi

TUTTI I PREZZI SONO AL NETTO DI I.V.A. nella misura di legge se non diversamente specificato.

Validità Offerta

180 giorni dalla data della presente offerta.

Maggioli Informatica

è un marchio Maggioli Spa

Santarcangelo di Romagna, 25/05/2018

DICHIARAZIONE DI CONFORMITA SUITE SOFTWARE "SICRAWEB"
IN TEMA DI MISURE MINIME DI SICUREZZA (Circ. Agid 2/2017) E COMPLIANCE ALLA PRIVACY BY DESIGN (Reg. UE 2016/679)

Gentile Cliente,
in data 25 maggio 2018 diventa pienamente efficace Regolamento Generale sulla Protezione dei Dati (Reg. UE 2016/679).

I software della suite "Sicr@web" di Maggioli Spa aderiscono alle indicazioni della Circolare Agid n.2/2017 del 18 aprile 2017 in relazione alle «*Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015*)» , e garantiscono il pieno rispetto di quanto previsto dal Reg. UE 2016/679.

Sicurezza dei dati (art. 24 e 32 GDPR)
Tutti i processi produttivi (sviluppo, collaudo, manutenzione del software) e di assistenza (monitoraggio e tracciamento delle richieste, del loro stato ed evoluzione) sono eseguiti in osservanza ed in accordo con il Manuale della Qualità di cui alla certificazione ISO 9001:2015 posseduta, adottando sistemi atti a impedire la vulnerabilità dei codici sorgenti.

La soluzione proposta, tramite l'infrastruttura applicativa, garantisce la disponibilità e l'integrità di tutti i dati nel caso in cui si verifichino errori, assicurando l'isolamento e limitando la propagazione delle anomalie nei diversi moduli applicativi. Il prodotto utilizza un'infrastruttura di persistenza che garantisce l'atomicità delle transazioni effettuate assicurando l'integrità dei dati anche a fronte di errori e situazioni anomale.

Le attività di personalizzazione software di tipo "custom" sono progettate nel rispetto della totale compatibilità e integrazione con la linea di produzione standard, adottando sistemi parametrici con chiavi di attivazione / disattivazione delle funzionalità dedicate.

La soluzione applicativa è parte di una suite completa totalmente integrata ed assicura pertanto una totale interoperabilità tra i vari moduli che la compongono. La soluzione è inoltre aperta e predisposta all'interazione con altre applicazioni esterne, mediante scambio di flussi di dati e/o messaggi utilizzando una tecnologia sicura ed

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

efficiente: i Web Services SOAP (WS). I WS permettono l'invocazione funzionale sincrona da un applicativo all'altro e complementano le capacità di coordinamento asincrono basate sul workflow manager.

Ove si verificasse la situazione tale per cui parte degli archivi dell'Ente si trovassero in hosting presso il DataCenter, Maggioli Spa, si impegna a restituire tutti i dati nel loro formato nativo, strutturati e non, al momento della conclusione del contratto (attività di "phase out").

Servizio di assistenza e manutenzione

L'assistenza viene garantita mediante un servizio di help-desk, per fornire il supporto tecnico-operativo agli utenti dell'Ente interessati alla fruizione dei servizi dell'infrastruttura tecnologica ed applicativa. Il servizio di help-desk eroga le sue attività agli utenti al fine di risolvere le problematiche che si manifestano e per le quali il personale dell'Ente non sia autonomo nella soluzione. Il servizio di help desk viene erogato da personale altamente qualificato, preparato e di comprovata esperienza nel settore della Pubblica Amministrazione Locale ed è in grado di risolvere in modo rapido e puntuale il problema segnalato. Compiti ed attività del servizio di Help desk sono tali da:

- fornire direttamente la soluzione attraverso il canale telefonico e/o con collegamento da remoto, avvalendosi in caso di necessitò del supporto del 2° Livello e/o del reparto di Sviluppo software.
- attivare su richiesta del Cliente, previo acquisto di giornate, l'assistenza on-site di personale in modalità affiancamento nel caso di esigenza specifica dell'ente.

Misure Tecniche – Gestione Utenti e accessi

Il sistema di autenticazione degli utenti a Sicr@web permette di integrarsi in modo efficace con un sistema di autenticazione LDAP. Il sistema di autenticazione di Sicr@Web è ovviamente in grado di operare in autonomia anche se non collegato ad un sistema di autenticazione LDAP, in particolare per gestire le situazioni di servizio LDAP momentaneamente offline oppure quando non si voglia proprio fare uso di un LDAP. L'autenticazione degli utenti è prevista una sola volta, al momento dell'accesso all'applicazione. L'applicazione prevede funzionalità di tipo amministrativo, tali da consentire una profilazione centralizzata e granulare degli utenti.

Nello specifico Sicraweb recepisce le seguenti indicazioni previste nella Circolare Agid n.2/2017, con particolare attenzione alle seguenti indicazioni:

- [ABSC 5.1.2] Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

- [ABSC 5.7.1] Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri con la regola di avere almeno una maiuscola e un numero)
- [ABSC 5.7.3] Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging opzione 30-60-90 gg)
- [ABSC 5.7.4] Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history opzione 15-20-25 volte)
- [ABSC 5.4.1] Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa
- [ABSC 5.4.2] Generare un'allerta quando viene aggiunta un'utenza amministrativa
- [ABSC 5.4.3] Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa
- [ABSC 5.5.1] Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa
- [ABSC 5.7.2] Impedire che per le utenze amministrative vengano utilizzate credenziali deboli
- [ABSC 5.7.5] Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova
- [ABSC 5.7.6] Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi

Misure Tecniche – Cifratura dei dati

Il sistema Sicr@Web adotta misure di sicurezza a protezione dei dati sensibili con la "pseudonimizzazione" che prevede l'assenza di identificabilità diretta del soggetto interessato («trattamento dei dati personali in modo tale che i dati non possano essere più attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive»);

Gli Enti possono inoltre adottare sistemi di cifratura a protezione delle copie di sicurezza (backup) dei dati ed utilizzare certificati di sicurezza per garantire la cifratura della comunicazione Client-Server.

Misure Tecniche – Log

La soluzione Sicr@Web prevede una completa gestione dei log all'interno dell'RDBMS sia per tracciare e registrare le operazioni svolte dagli utenti che accedono all'applicazione tramite le credenziali attribuite), per tracciare e registrare le operazioni svolte dagli amministratori di sistema che accedono all'applicazione

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

tramite le credenziali attribuite. Il sistema gestisce la tracciabilità delle modifiche a livello infrastrutturale direttamente sui sistemi RDBMS utilizzati. Il logging avviene a livello transazionale offrendo il massimo livello di accuratezza e veridicità.
Il livello di dettaglio può essere configurato fino ad arrivare alla tracciatura delle letture e non solo delle modifiche. I log prodotti sono consultabili direttamente dall'ambiente applicativo, semplificando così notevolmente le attività degli amministratori di sistema.

Integrazione con componenti esterne
Per quanto riguarda l'utilizzo di componenti esterne quali Java e Libre Office, trattandosi di tecnologie e prodotti in continua evoluzione e non potendo avere certezza della retro-compatibilità delle versioni, al fine di garantire la stabilità e il corretto funzionamento dei nostri prodotti, vengono progressivamente certificate le nuove release, previo collaudo dell'intera piattaforma. Al momento le release certificate con Sicr@web sono Java JRE 1.8.0_151 e Libre Office 4.2.6.3

Diritti degli interessati (Capo III GDPR)
In relazione alla tipologia del servizio offerto dal modulo software installato, in accordo con l'ente si provvederà a fornire il supporto necessario, implementando misure per fornire assistenza alla committente.

Violazione dei dati (art. 33 e 34 del GDPR)
In ottemperanza con quanto previsto agli art. 33 e 34 Maggioli Spa rispetterà i tempi di comunicazione previsti dal GDPR.

Cancellazione dei dati (art. 17 "diritto all'oblio")
In relazione normative specifiche di ogni singolo settore supportato dal Software Sicr@Web Maggioli Spa fornirà il supporto per rispettare quanto previsto dall'art. 17 del GDPR.

Maggioli S.p.A.
Responsabile del Trattamento
Dott.ssa Cristina Maggioli

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

Maggioli Informatica

è un marchio **Maggioli Spa**

Santarcangelo di Romagna, 14/12/2020

DICHIARAZIONE DI CONFORMITA SERVIZI CLOUD MAGGIOLI IN TEMA DI MISURE MINIME DI SICUREZZA (Circ. Agid 2/2017)

Gentile Cliente,

con la presente si informa che i servizi Cloud di Maggioli S.p.a. erogati dai propri Datacenter sono conformi alle indicazioni della Circolare Agid n.2/2017 del 18 aprile 2017 in relazione alle «*Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015*)».
I nostri servizi Cloud Hosting/IaasS/PaaS sono sottoposti a specifiche e rigorose certificazioni e controlli inerenti la sicurezza dei dati quali ISO27001 (di cui riportiamo il certificato) e ne rispettano le direttive Agid sino a permettere a Maggioli Spa lo status di conservatore accreditato Agid (http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/elenco-conservatori-attivi)
Poiché per precisione la circolare n.2/2017 riporta punti di diversa competenza e dominio (postazioni e/o risorse locali, dominio di tipo applicativo ecc..) elenchiamo di seguito quelli correlati a servizi Cloud Hosting/IaasS/PaaS oggetto della presente dichiarazione di conformità.

Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ABSC 1.1.1
Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ABSC 1.1.3
Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ABSC 1.3.1
Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ABSC 2.3.1
Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	ABSC 2.3.3
Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	ABSC 3.1.1
Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	ABSC 3.2.1

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	ABSC 3.2.2
Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	ABSC 3.4.1
Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	ABSC 4.1.1
Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	ABSC 4.4.1
Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	ABSC 4.5.1
Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio	ABSC 4.7.1
Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	ABSC 4.7.2
Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	ABSC 4.8.1
Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	ABSC 4.8.2
Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	ABSC 5.1.1
Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	ABSC 5.1.2
Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	ABSC 5.2.1
Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	ABSC 5.5.1
Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	ABSC 5.7.3
Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	ABSC 5.7.3
Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le	ABSC 5.10.3

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	ABSC 5.11.1
Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	ABSC 8.1.3
Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	ABSC 10.1.1
Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	ABSC 10.1.2
Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	ABSC 10.1.3
Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	ABSC 10.2.1
Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	ABSC 10.3.1
Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	ABSC 10.4.1

Maggioli Informatica

è un marchio **Maggioli Spa**

AntiMalware, Data Retention e Manutenzione Programmata.

In aggiunta alla risoluzione delle specifiche AGID sopra indicate il sistema di gestione a norme ISO27001 applicato nella gestione dei DataCenter Maggioli definisce e garantisce i seguenti parametri tecnico/operativi:

- A livello perimetrale per i servizi contenuti è implementata una rete firewall di ultima generazione Fortinet che implementa funzionalità antimalware, antispam, DDOS con capacità di auto-aggiornamento delle firme malware in base oraria.
- Sempre a livello globale, tramite tecnologia di backup virtuale VMWare, è implementato il sistema di backup con una ciclicità che, in determinazione delle specificità applicative e progettuali del servizio, può variare da minimo di 30 giorni ad un massimo di 180 definendo così automaticamente su questi valori anche i parametri minimi e massimi di data-retention.
- Le procedure ISO27001 implementate definiscono infine le seguenti tipologie di attività di manutenzione programmata:
    - Controlli antimalware e backup -> Settimanali
    - Controlli estesi delle piattaforme HW e networking -> Mensili

Cordiali Saluti

Maggioli Informatica
Responsabile Sistemi
Oscar Bevoni

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it

Maggioli Informatica

è un marchio **Maggioli Spa**

DNV·GL

MANAGEMENT SYSTEM CERTIFICATE

Certificato No./Certificate No.:
276910-2018-AIS-ITA-ACCREDIA

Data prima emissione/Initial date:
09 marzo 2010
Data precedente OdC/
Previous CB date

Validità/Valid:
08 marzo 2019 - 08 marzo 2022

Si certifica che il sistema di gestione di/This is to certify that the management system of

MAGGIOLI S.p.A.

Sede Legale: Via del Carpino, 8 - 47822 Santarcangelo di Romagna (RN) – Italy
e i siti come elencati nell'Appendix che accompagna questo certificato /
and the sites as mentioned in the appendix accompanying this certificate

È conforme ai requisiti della norma per il Sistema di Gestione/
Has been found to conform to the Management System standard:

ISO/IEC 27001:2013

Questa certificazione è valida
per il seguente campo applicativo:

Analisi, progettazione, sviluppo, manutenzione e assistenza di software per la Pubblica Amministrazione e Aziende erogato anche in modalità SaaS. Erogazione di servizi applicativi in ambito IT come System integrator di prodotti propri e di terze parti. Erogazione di servizi di inserimento dati, anche presso la sede del cliente, stampa, rendicontazione, invio in multicanalità e supporto alla riscossione delle sanzioni amministrative degli atti elevati della Polizia Locale o da altri uffici della Pubblica Amministrazione. Erogazione di servizi di housing, hosting, IaaS, PaaS, Disaster Recovery e Cloud Computing in accordo alle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2014. Erogazione di servizi di conservazione a norma di documenti informatici

(EA: 35, 33)

In accordo alla Dichiarazione di Applicabilità del 28 giugno 2019, Rev. 5

This certificate is valid
for the following scope:

Analysis, design, development, maintenance and assistance of software for the Public Administration and Companies provided also in SaaS mode. Provision of IT application services as a System integrator of proprietary and third parties products. Provision of data entry services, even at customer sites, printing, reporting, multi-channel mailing and support for the collection of the administrative sanctions of the administrative acts of Local Police and other offices of the Public Administration. Provision of housing, hosting, IaaS, PaaS, Disaster Recovery and Cloud Computing according to ISO/IEC 27017:2015 and ISO/IEC 27018:2014 Guidelines. Provision of digital preservation services for IT documents

(EA: 35, 33)

In accordance with the Statement of Applicability of 28 june 2019, Rev. 5

Luogo e Data/Place and date:
Vimercate (MB), 02 agosto 2019

ACCREDIA

Per l'Organismo di Certificazione/
For the Certification Body

~~Zeno Beltrami~~
Management Representative

La validità del presente Certificato è subordinata al rispetto delle condizioni contenute nel Contratto di Certificazione/
Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
DNV GL Business Assurance Italia S.r.l. Via Energy Park, 14, 20871 Vimercate (MB), Italy. Tel: 039 68 99 905. www.dnvgl.it/assurance

Maggioli Informatica
via Bornaccino, 101
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 621153
informatica@maggioli.it
www.maggioli.it