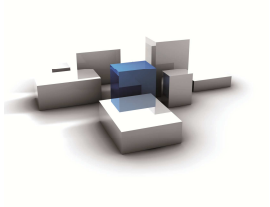
PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE

Urbi Smart

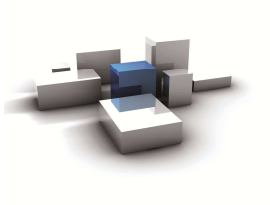
LA SICUREZZA DEI DATI

Urbi Smart e la gestione della sicurezza dei dati



PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE

Indice



1. Urbi Smart: cloud computing e licenza d'uso

Unico strumento di supporto per il governo del Comune e degli Enti, accessibile da qualsiasi dispositivo mobile (essendo web nativo, si "muove" agevolmente in Internet) e in qualsiasi momento e luogo (grazie alla modalità cloud computing), **Urbi Smart è il sistema informativo gestionale e direzionale integrato, web nativo, con un'unica base dati, che ha rivoluzionato la gestione delle informazioni nella Pubblica Amministrazione**.

Disponibile nella tradizionale forma in licenza d'uso, Urbi Smart può essere utilizzato anche nella modalità CLOUD COMPUTING, SAAS (Software as a service) o ASP (Application Service Providing).
L'architettura web nativa – con accesso mediante qualsiasi PC con browser collegato a Internet, anche attraverso i più moderni strumenti mobile come ipad (Apple, tablet con Android oltre che iPhone, smartphone, palmari ecc.) – consente, infatti, una naturale predisposizione verso il cloud computing.

Le applicazioni alloggiano nella "nuvola informatica", sono in rete, non risiedono presso i server dell'ente che ne fruisce ma in server dislocati presso un IDC esterno.

Oltre ad essere in linea con le direttive dell'Agenzia per l'Italia Digitale (ex Digit PA già CNIPA), tale modalità di erogazione consente di utilizzare soluzioni ad alto profilo tecnologico e costantemente aggiornate, protette ed in grado di facilitare notevolmente l'interazione con i cittadini o altri soggetti esterni, senza forti investimenti infrastrutturali e pesanti costi di gestione (ad es. acquisto di software, hardware e infrastrutture di rete, costi di personale altamente specializzato per la gestione di infrastrutture complesse necessarie per usufruire della rete ecc.).

L'ente si avvale così anche **di un servizio specializzato che consente il ripristino rapido e completo dei dati in caso di interruzioni impreviste dei servizi e, quindi, la continuità operativa dei propri utenti** (in linea con quanto disposto dall'art. 50 del D.L. 82/2005, Codice dell'Amministrazione Digitale).

Attualmente oltre 400 Enti utilizzano Urbi in modalità ASP/Cloud Computing.

La tecnologia web rende le applicazioni Urbi Smart estremamente efficaci, comunque, anche se acquisite in modalità licenza in quanto sono tecnologicamente predisposte per essere installate in un proprio CED o presso altra server farm ed essere aperte alla rete internet. In questo contesto Urbi Smart si presta ad essere l'unica soluzione per aggregazioni di Comuni, CST, Comunità Montane che vogliono erogare i servizi direttamente dalla loro server farm o CED.

2. Cloud computing: vantaggi

- Nessuna necessità di competenza informatica per la gestione di hardware, software e degli archivi.
- Nessun limite connesso alla necessità di dimensionamento del sistema: non occorre infatti stabilire a priori il dimensionamento dell'hardware, dato che, anche al crescere delle esigenze occorre esclusivamente aggiungere i posti di lavoro utente necessari.
- Nessun vincolo hardware e software.
- Totale eliminazione della responsabilità di archiviazione dei dati.
- Nessun vincolo contrattuale per l'eventuale cambio di fornitore.
- Estrema scalabilità.
- Aggiornamenti del software applicativo immediatamente disponibili.
- Supporto garantito con tempi di risposta velocizzati: il servizio help desk PA Digitale può intervenire tramite l'attivazione del servizio di assistenza da remoto che, sfruttando il collegamento Internet, può operare sul PC del cliente (previo consenso per l'accesso) ed effettuare la corretta diagnostica al fine di apportare le operazioni correttive direttamente "sulle" soluzioni applicative in uso dal cliente.

3. Sicurezza dei dati e continuità operativa

PA Digitale è sinonimo di sicurezza dei dati: all'interno del Datacenter posto in un ex caveau bancario blindato – posto sul territorio nazionale, di proprietà della nota software house Zucchetti spa (www.zucchetti.it), ubicato a Lodi e certificato in base agli standard internazionali ISO/IEC 27001:2005 - le apparecchiature per la trasmissione dei dati e le architetture hardware/software preposte all'erogazione dei servizi sono poste in condizioni di **massima sicurezza applicativa e fisica** (sistemi antincendio, controllo accessi, telesorveglianza ai piani, sorveglianza armata esterna; ridondanza dei sistemi elettrici e di refrigerazione, ecc.), **informatica e logica** (sistemi antintrusione). Inoltre, i sistemi di backup dei dati, il disaster recovery, la continuità dei servizi, offrono agli utenti i più elevati livelli di servizio, 24 ore su 24, 7 giorni su 7, 365 giorni all'anno.

Garanzie fondamentali e indispensabili per gli Enti, sia per rispondere agli obblighi di legge in materia di ***business continuità*** (già citato art. 50, D.L. 82/2005, CAD), sia per poter garantire il corretto e regolare svolgimento della vita di cittadini e imprese nel caso di servizi in modalità online.
A tal fine, PA Digitale garantisce un servizio di **Disaster Recovery** completamente automatizzato in tutti i suoi processi e monitorato 24x7x365. Vengono utilizzate risorse di elaborazione virtuali per i servizi web, dedicate per i servizi di elaborazione e gestione dati. Tutti i sistemi ed apparati di rete/strutturali sono in configurazione fault-tollerance per evitare single point of failure.
La capacità di elaborazione del sistema di Disaster Recovery permette, in caso di disastro, il ripristino dell'erogazione dei servizi con prestazioni equivalenti al sito asp.urbi.it, in tempi conformi al Tier 3.
Attività di verifica e test di funzionamento dei sistemi sono svolte regolarmente per la massima sicurezza di dati e sistemi.

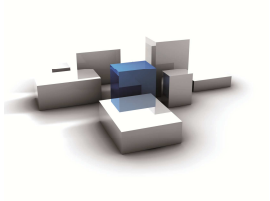
Il disaster recovery viene effettuato su cloud di ARUBA (http://www.cloud.it/en/infrastructures/italy-dc-it1.aspx)
L'ubicazione dell'IDC Zucchetti Spa è a Lodi, via Polenghi Lombardo 9; per ARUBA ad Arezzo - Via Gobetti 96.

3.1 Internet Data Center

L'IDC acquisisce risorse di banda da diversi carriers, per avere la massima affidabilità contando su linee completamente ridontate e carriers anch'esso ridondati.
Il Data Center dispone di una **connessione ad Internet** attraverso linee multiple per una capacità complessiva di alcuni Gbit/s e sono dotati di **sistemi di condizionamento, gruppi di continuità, generatori elettrici, sistemi antincendio e monitoraggio attivo 24/24 ore per 7/7 gg.** Il Data Center è connesso alla rete tramite linee ridondate ad elevata capacità, in grado di garantire la massima disponibilità ed affidabilità.

In particolare:
- il Data Center risiede in un caveaux blindato;
- è attivo un servizio di sorveglianza armata h24 dell'intero complesso;
- sono attivi sistemi di sorveglianza elettronica contro l'intrusione, l'incendio e anomalie ambientali critiche;
- ciascun piano è dotato di sistemi automatici di videocontrollo (ai sensi T.U. Sulla privacy);
- è previsto un sistema ridondante di controllo del clima delle sale macchine con allarmi locali e remoti su valori critici;
- è previsto un sistema di alimentazione ridondante per ogni fila di armadi con prese e spine di sicurezza antistrappo e antifuoco;
- l'impianto di sicurezza dell'alimentazione prevede un impianto di terra certificato conforme alla L. 626 e separazione galvanica delle sorgenti;
- i locali sono dotati di istema anticendio a gas con sensori a soffitto e a pavimento a saturazione ambientale; bombole dedicate per ogni piano, impianto ridondato e separato;
- ogni piano ha doppie porte antincendio con dispositivo automatico di chiusura;
- è previsto un condizionamento statico dell'alimentazione tramite gruppi di continuità statici online;
- il gruppo elettrogeno diesel consente l'erogazione continuata di elettricità in mancanza della rete.

E' assicurata la sorveglianza dei locali 365/7/24 con personale proprio o esterno autorizzato o con sistemi di monitoraggio remotizzato. Tutti gli accessi alle areee di datacenter sono sottoposti ad identificazione e registrazione accessi basato su badge e finger print.



3.2 Infrastruttura di sistema

L'**architettura del Data Center** è basata su componenti le cui principali caratteristiche sono:
- affidabilità delle singole componenti scelte;
- ridondanza fisica di tutti i componenti HW;
- ridondanza dei componenti SW di sistema e networking.

La disponibilità dell'infrastruttura presenta un uptime del 99.95%, garantita a diversi livelli sia grazie alle scelte architetturali che alle tecnologie utilizzate.

3.3 Sottosistema di virtualizzazione

L'infrastruttura si basa su **Cloud Server HA** configurati con le seguenti tecnologie di alta affidabilità:
- Vmotion: consente di migrare real time le VM tra host fisico ad un altro cluster;
- Storage Vmotion: rilocazione di VM fra datastore senza interruzione del servizio;
- High Availability: in caso di failure di un host virtualizzatore o della VM.

Inoltre l'**infrastruttura fisica** ha le seguenti caratteristiche di alta affidabilità:
- i server fisici sono raggruppati in cluster ridondati N+1;
- il fault di un server comporta la rilocazione delle risorse sugli altri due nodi del cluster;
- i server fisici utilizzati sono di classe Enterprise multiprocessore;
- le schede di rete e gli apparati di rete sono ridondati;
- switch e schede HBA FC sono ridontati e configurati in bilanciamento;
- gli storage box sono di livello enteprise ad alimentatori ridondati, controller ridondati, dischi in configurazione RAID, porte fc ridondate ed in bilanciamento vs gli switch della SAN;
- switch e pattern FC della SAN sono ridontati sia livello edge che core, con realizzazione dual fabric.

Le caratteristiche fisiche dei **server virtualizzatori** sono le seguenti:
- hardware di classe enterprise;
- processori multicore Intel Xeon E7/X7 o Amd;
- FC : 3 x dual port 4Gb
- ethernet 1Gb
- ethernet 10Gb
- HD interni SAS a 15K

3.4 Sottosistema storage

Per eliminare ogni rischio di interruzione del servizio dovuto a guasti HW, tutti i dischi delle VM e dei dati sono memorizzati esclusivamente su **SAN ad alte prestazioni dedicate al servizio**.
La configurazione della SAN garantisce assenza di Single Point of Failure, tutti i sistemi sono in costante monitoraggio che garantisce tempi di sostituzione componenti hw senza completo fermo del sistema.
Le garanzie:
- **alta affidabilità dei componenti fisici**, tutti i componenti sono ridontati, cioè disco in RAID5 + hot-spare, SAN dual-fabric ecc.
- **scalabilità verticale ed orizzontale dell'infrastruttura** che è in grado di supportare richieste di workload e di spazio addizionale evitando situazioni di overbooking.

3.5 Sottosistema di backup

Implementazioni di **backup** esistono **per tutti i layer dell'infrastruttura**, lato server come switch FC per la SAN ed apparati di networking.
Le risorse degli apparati di salvataggio e stoccaggio dati, quali tape library o storage dedicati al backup, sono implementate seguendo la crescita delle dimensioni dei dati da salvare.
Il sistema dispone di una procedura di disaster recovery con RPO di 1gg ed RTO minimo di 1gg e massimo di 3gg. (Tier 3)

3.6 Sottosistema di networking

L'infrastruttura di rete è basata su **scalabilità e flessibilità**, al fine dell'erogazione dei servizi applicativi.
Il modello architetturale verte su un impiego massivo della **virtualizzazione dei servizi di rete**, con una suddivisione logica a più livelli del contesto.

Dal punto di vista fisico la **rete** è:
- completamente ridondata;
- strutturata in blocchi con un livello di accesso separato per isolare i contesti applicativi e gestionali;
- utilizza reti ethernet ad 1Gb per gli host con backbone a 10Gb;
- banda internet ampliabile in base all'utilizzo, anche temporaneamente.

3.7 Sottosistemi firewall e componenti di sicurezza

L'architettura di sicurezza e firewall è implementata utilizzando **due cluster firewall in alta affidabilità**: per la gestione dell'accesso internet e per la gestione della rete interna (VLAN).
Ogni cluster FW è altresì composto da due unità fisiche di FW in alta affidabilità.
I server applicativi utilizzano **VLAN** per ottenere una separazione del livello database da quello applicativo, al fine di elevare la sicurezza di gestione dei documenti e di ridurre al minimo il rischio di compromissione dei sistemi in caso di attacco.
L'infrastruttura dispone di **sonde IPS** (Intrusion Prevention System) che garantiscono una protezione perimetrale da attacchi, per esempio di tipo DDOS (Distributed Denial of Service).
La sicurezza di accesso ai componenti del sistema è garantita attraverso l'uso di **password a criptazione forte**.
L'accesso da parte di PA Digitale Spa ai sistemi per scopi di amministrazione avviene attraverso connessioni autenticate attraverso username/password e certificati digitali.

3.8 Servizi di back up

Tutte le operazioni di backup dei sistemi e dei dati relativi a servizi ospitati nel Data Center si basano su 2 processi:
- **archiviazione su disco**
- **storicizzazione su nastro**.

Entrambi i processi sono implementati attraverso il software Simpana CommVault con una infrastruttura composta da 6 server, 1 storage e 3 tape library.
Il processo di archiviazione su disco sfrutta spazio disco (SATA) fornito da tre server collegati ad uno storage in FC (EMC² AX5).
Il processo di storicizzazione su nastro sfrutta 3 unità library con Tecnologia LTO4 collegate all'ambiente SAN in FC.
Le library sono delocalizzate in una Server Room esterna al DataCenter.
La tecnologia adottata per i processi sopracitati potrebbe essere soggetta a modifiche (*a titolo puramente esemplificativo: il numero di server potrebbe aumentare o diminuire oppure la versione software di backup potrebbe cambiare*).

3.9 Politiche di back up

Le politiche di backup adottate prevedono la gestione di tutti i dati relativi agli applicativi Urbi Smart: database, documenti ecc.

I **job di backup** prevedono la raccolta del dato giornaliera (processo di archiviazione) durante una "finestra" predefinita dalle ore 22.00 alle ore 06.00 al fine di garantire il successivo consolidamento su nastro (processo di storicizzazione).
L'orario di backup non è definibile a priori perché potrebbe variare in base alla durata dei singoli job che sono a loro volta variabili in base alle dimensioni del dato da backuppare.
La policy prevede un backup settimanale in modalità full ed un backup giornaliero in modalità differenziale.
In ogni caso indipendentemente dalle policy sopra citate, i dati vengono resi disponibili in una modalità specifica: retention di 30 giorni con una granularità giornaliera e per un anno con granularità mensile.

3.10 Rintracciabilità del dato, attività di restore e test ripristino

Sulla base di quanto sopra descritto, le attività di recupero dei dati archiviati si basano su informazioni fondamentali che costituiscono le "coordinate" del dato (posizione fisica, localizzazione temporale…).
In funzione di questi elementi sarà sempre possibile risalire alla versione più recente del dato o ad una sua precisa versione temporalmente identificabile con granularità a seconda della vetustà del dato richiesto.
Una volta alla settimana viene effettuato un test di ripristino in modalità random.
L'operazione di "**restore di test**" viene effettuata per verificare la consistenza del dato archiviato su nastro.
Il **processo di restore** dei dati avviene secondo le modalità e prestazioni definite dallo SLA del fornitore del servizio.

3.11 Messa in sicurezza dei nastri di backup

I nastri e le medesime library che effettuano il backup sono posizionati in **sito secondario e delocalizzato** rispetto al DataCenter.
E' previsto un apposito modulo che consente **di monitorare e tenere traccia sia della presa in carico dei nastri che della consegna presso il locale EXTRA CED – Cassaforte**.

4. La gestione della sicurezza e sistemi di security management per le procedure applicative

La gestione della sicurezza costituisce una tra le componenti più delicate nell'ambito, più generale, della gestione dei dati dei Clienti.

PA Digitale, dovendo implementare un IDC per l'erogazione dei servizi di amministrazione degli enti in modalità ASP, ha da tempo sviluppato e attuato una metodologia per l'analisi dei rischi legati alla sicurezza e alla sua gestione attraverso opportuni meccanismi e strumenti di controllo e di intervento.
Le scelte adottate, in linea con quanto enunciato dall'Agenzia per l'Italia Digitale in materia di sicurezza, portano a:

- **controllo e monitoraggio degli accessi in modo puntuale e nel tempo;**
- **identificazione di eventuali anomalie;**
- **intervento nel minor tempo possibile per ripristinare la situazione correttamente.**

4.1 Gestione della Sicurezza degli Accessi

Per soddisfare adeguati requisiti sicurezza la soluzione applicativa supporta una serie di servizi e di primitive di sicurezza atte ad implementare funzioni di autenticazione, autorizzazione e crittografia.

L'**autenticazione** indica il fatto che gli utenti si debbano identificare con una serie nota di credenziali, ad esempio nome utente e password. Per **autorizzazione**, invece, si intende l'assegnazione di determinati livelli di accesso al sistema che si riflettono in ben identificate capacità operative sul sistema da parte dell'utente correttamente identificato. La **sicurezza** dei dati, deve essere garantita sia durante la fase di trasporto a livello di link tra client e server, che tra sottosistemi applicativi che durante la fase di giacenza a livello di archiviazione nei Data Base.

In sintesi, sono inoltre previste le seguenti caratteristiche:

- controllo costante dell'erogazione e delle prestazioni del servizio mediante **strumenti di supervisione accessibili via web** dal personale abilitato;
- eventuale utilizzo di **sistemi di crittografia** di tipo SSL a 128 bit o superiore per lo scambio di dati sensibili;
- **sistema di validazione e profilazione** di tutti gli utenti;
- **identificazione** degli enti coinvolti nello scambio dei flussi informativi e degli utenti abilitati all'accesso ai servizi anche tramite l'utilizzo di certificati digitali.

4.2 Protezione delle applicazioni

La politica di protezione delle applicazioni si basa sui ruoli degli utenti, così come sono definiti nella pianta organica.
I soggetti dal punto di vista della protezione sono individui o ruoli definiti in pianta organica e storicizzati nel tempo.

4.3 Protezione dei dati

Anche per la protezione dell'accesso ai dati, il meccanismo si fonda su un sistema di permessi basato sui ruoli definiti in pianta organica.
L'accesso ai dati avviene solo attraverso l'applicazione; inoltre, i server di database sono protetti da un **doppio sistema di firewall e da regole di routing** che non ne consentono la visibilità dall'esterno della rete.
La gestione della base dati unica relativa al singolo ente è basata su database standard. Nel caso di utilizzo del sistema in modalità ASP con il collegamento al Data Center messo a disposizione da PA Digitale, il database adottato è MySQL. In tutti i casi il sistema ne rispecchia le caratteristiche in termini tecnico-funzionali.

I database dei singoli Enti **sono distinti** e ad ognuno di essi è stato associato un utente/schema.
Ad ogni schema **non vengono concessi privilegi** ulteriori **che comportino l'accesso, né tantomeno la gestione, di oggetti appartenenti ad altri schemi**.
Non esistono aree condivise tra i vari schemi.
La connessione dall'application server al database avviene attraverso un servizio di rete diverso per ognuno degli Enti.
Gli utenti di un ente al momento dell'accesso discriminano lo schema associato e l'autenticazione viene effettuata attraverso l'utente, lo schema e relativa password. Questi tre elementi sono indipendenti per ogni ente.

4.4 Autenticazione

La suite Urbi Smart utilizza un **sistema di autenticazione basato su sessione**. Ogni programma Urbi Smart, verifica la validità della sessione in corso prima di fornire la pagina richiesta. Allorchè la sessione sia scaduta o non sia attiva, qualsiasi richiesta viene ridirezionata al sistema di autenticazione. Il sistema di autenticazione NON è predeterminato ma è configurabile e varia quindi da cliente a cliente. Nella fattispecie, sono attualmente stati implementati come sistemi di autenticazione i seguenti:

- autenticazione basata su **Login e Password**;
- autenticazione basata su **recupero delle credenziali da firma digitale**;
- autenticazione basata su **CRS regione Lombardia**;
- autenticazione **CUSTOM** (specifica per cliente) che nel tempo ha annoverato:
  - **a.** autenticazione basata su sistema di SSO Yale CAS 2.0;
  - **b.** autenticazione basata su sistema di SSO con Active Directory basato su network protocol "Kerberos over http" [1];
  - **c.** autenticazione basata su LDAP.

4.5 Gestione delle password

Le password sono tutte crittografate con **algoritmo proprietario** che e' una implementazione dello standard AES (Advanced Encryption Standard) a 256bit.
(http://it.wikipedia.org/wiki/Advanced_Encryption_Standard)

1 Prerequisiti
Installazione in locale di Tomcat con JAVA 1.6 disponibile per l'installazione del Auth.System UrbiSPNEGO.
Checklist pre-flight di SPNEGO completata con successo dal server che ospiterà Tomcat e da almeno un client in rete con AD. http://spnego.sourceforge.net/pre_flight.html

Gestione dell'autenticazione basata su Login e Password

Urbi Smart permette la definizione di tre tipologie di utenti in funzione della loro visibilità ed accessibilità alle varie procedure, e quindi in funzione del tipo di menù assegnato. In particolare:

1. **Utente Standard**: l'utente può entrare nell'area delle procedure abilitate ed accedere di default a tutti i programmi accessibili in virtù del suo **Profilo** (Visione, Gestione, Supervisore). E' tuttavia possibile prevedere un ulteriore livello di autorizzazione, disabilitando l'accesso solo ad alcuni programmi.
2. **Utente Scrivania**: questo tipo di utente può accedere esclusivamente ai programmi che gli sono stati espressamente abilitati (situazione opposta rispetto alla precedente in cui l'utente, di default ha accesso a tutte le applicazioni: in questo caso invece, l'utente vede solo i programmi che gli sono stati assegnati).
   L'utente **Scrivania** può accedere ad Urbi Smart solamente per le procedure che gli sono state assegnate e la pagina di accesso proposta contiene solamente i programmi che gli sono stati assegnati (non ha la navigazione completa dell'utente **Standard**).
3. **Utente Misto**: è l'utente che è **Standard** per alcune procedure e **Scrivania** per altre. Ad esempio: un utente standard dell'anagrafe (che ha a disposizione tutte le scelte del menù anagrafico) al quale viene attivata la sola funzione di visualizzazione delle delibere o visualizzazione dei protocolli.

E' possibile prevedere **ulteriori autorizzazioni relative a specifiche applicazioni Urbi Smart**.

Sigla Registro Utente (*Vale solo per procedura **Inventario***)
Nella gestione dei beni mobili, qualora l'ente necessiti di una gestione multi-registro, l'utente dovrà obbligatoriamente dichiarare l'abilitazione di uno di questi. La sigla fornita determinerà gli interventi operativi nel registro dichiarato.

Responsabile Funzione (*Vale solo per procedura **Contabilità Finanziaria***)
L'istruzione di un capitolo è possibile solo previo verifica del responsabile competente. Un utente nel momento che accede alla procedura resta individuato come *subordinato* ad un certo *Responsabile di Funzione*. L'associazione di un utente al responsabile si costituisce con la dichiarazione di un codice soggetto individuato tra i Responsabili. Associato un utente ad un certo responsabile di funzione, l'utente potrà accedere alla variazione dei soli capitoli che gli competono.

Responsabile Procedimento (*Vale solo per procedura **Contabilità Finanziaria***)
La registrazioni di movimenti finanziari è possibile solo previo verifica del responsabile competente. Un utente nel momento che accede alla procedura resta individuato come *subordinato* ad un certo *Responsabile di Procedimento*. L'associazione di un utente al responsabile si costituisce con la dichiarazione di un codice soggetto individuato tra i Responsabili. Associato un utente ad un certo responsabile di procedimento, l'utente potrà accedere alla movimentazione dei soli capitoli che gli competono.

Abilitato alla gestione di tutti i capitoli (*Vale solo per procedura **Contabilità Finanziaria***)
Qualora non si intenda procedere alla gestione dei capitoli tramite responsabili, occorre richiedere per l'utente questo indicatore.
Questo equivale alla totale visibilità e gestione dei capitoli indipendentemente dalla loro natura.

Classe Articoli

Nell'ambito di Urbi Smart gli articoli di magazzino sono elementi che interagiscono con alcuni moduli (magazzino, contabilità, tributi) e particolare attenzione può essere posta ad un eventuale filtro.
È possibile restringere la visibilità e la successiva gestione per un utente a una determinata classe di articoli. La scelta di associare gruppi di articoli a specifici utenti è a completa discrezione del responsabile di servizio, mutuata dal Supervisore, e si realizza con le seguenti modalità.
In fase di registrazione utenti, il supervisore associa ad ogni utente una classe di articoli. L'utente a cui viene associata una classe, in fase di inserimento nuovi articoli e di movimentazione, inserirà i soli articoli corrispondenti alla classe a lui associata. In fase di registrazione dei movimenti le liste di articoli si limiteranno ai soli articoli con corrispondenza di classe.
Un utente a cui non è stata associata alcuna classe avrà la totale visibilità e gestione degli articoli.
La gestione non è, ovviamente obbligatoria, costituisce solo un utile strumento di controllo e di garanzia di legittimità di interventi in funzione dei vari contesti.

Ufficio (*Vale solo per procedure **Delibere e Protocollo***)

- **Delibere**: se dichiarato un ufficio diverso da **SEGRETERIA**, l'utente che accede alla procedura delibere vedrà associato alle proprie proposte l'ufficio dichiarato. Di contro la dichiarazione di appartenere all'ufficio **SEGRETERIA**, determina la presentazione di funzioni di supervisione e di maggiore operatività nell'ambito della procedura.
- **Protocollo**: se dichiarato un ufficio, l'utente che accede alla procedura protocollo, avrà visibilità dei soli documenti collegati all'ufficio dichiarato

E-mail Informazione utile per l'invio di posta elettronica, accetta l'indirizzo e-mail dell'utente

4.6 Abilitazione Procedure

Tutti i programmi Urbi Smart, al momento del rilascio, sono suddivisi per singole **Procedure** e ciascuno di essi viene rilasciato con un livello di accesso di défault scelto fra tre tipologie di **Programma**: **Programma di Visione**, **Programma di Gestione** o **Programma di Supervisore**.
Analogamente eventuali **Funzioni** associate ai programmi stessi sono rilasciate con un valore di default fra **Funzione Abilitata** o **Funzione Disabilitata**.

Urbi Smart prevede la gestione delle abilitazioni organizzata a livelli:

- a livello di **Procedura**, relative a tutti i programmi della procedura;
- a livello di **Programma**, con accesso al programma, inserimento di dati, annullamento di dati, variazione di dati;
- abilitazioni all'interno del programma di particolari **Funzioni**.

Di conseguenza, sono previsti tre livelli di intervento per la definizione dei privilegi utente:

1. associazione di uno dei **Profili di Base** previsti (a livello di procedura);
2. abilitazione o meno dello specifico programma;
3. abilitazione del programma con inibizione o meno di specifiche funzioni.

Nella tabella seguente sono evidenziate le abilitazioni di default sui programmi di una procedura in funzione dei **Profili di Base** di un utente:

Profilo Base	Abilitazione di défault dei programmi della procedura
Visione	Solo programmi definiti come Visione
Gestione	Programmi definiti come Visione e Gestione
Supervisore	Programmi definiti come Visione, Gestione e Supervisore
Scrivania	Solo programmi esplicitamente assegnati (**solo per utenti di tipo Misto**)

Controllo interventi sui soggetti
Il soggetto sia esso una persona fisica o un soggetto giuridico, acquisisce in Urbi Smart un'importanza elevata. Costituendo il punto centrale di indagini nell'ambito del sistema informativo ed essendo presente una sola volta come codice e relativo corredo anagrafico, necessita di una serie di controlli capillari sulla manipolazione delle sue informazioni.
Due sono le sezioni previste per il controllo degli interventi sui soggetti: **Variazione** e **Annullamento**.
Ogni variazione inerente a quello che è stato definito *corredo anagrafico* (fanno parte di questo per esempio cognome, nome, data nascita) di un soggetto, viene autorizzata esclusivamente se l'utente che vuole effettuare una delle due operazioni è autorizzato.

Gestione classi di utenti
La funzione è stata progettata per rendere più funzionale ed ottimizzata la gestione delle profilazioni degli utenti.
E' possibile identificare una serie di utenti di riferimento (*utenti di tipo **classe***) e permettere a tutti gli utenti collegati a una classe di **ereditare** le caratteristiche dell'utente capofila o di riferimento.
Grazie a tale impostazione, è possibile effettuare estrazioni od applicare filtri esclusivamente a determinate classi di utenti.
Gli utenti rispettano la Pianta organica impostata ed unica per tutte le aree applicative Urbi Smart utilizzate dall'ente.