Istituto Nazionale di Statistica

CENSIMENTO PERMANENTE DELLA POPOLAZIONE E DELLE ABITAZIONI
ALLEGATO B

Caratteristiche tecniche delle fasi di acquisizione dei dati

Il presente allegato descrive le caratteristiche tecniche delle fasi di acquisizione dei dati e di monitoraggio della raccolta dei dati nell'ambito delle rilevazioni censuarie.

1. Acquisizione degli Archivi Amministrativi

L'infrastruttura a supporto del censimento permanente (CP) prevede l'acquisizione di dati esclusivamente attraverso canali di comunicazione cifrati, nella fattispecie HTTPS per l'acquisizione da archivi amministrativi su applicativi web dedicati (come nel caso del sistema di acquisizione dati ARCAM) oppure FTP su canali cifrati (a seconda dei casi utilizzando SSL/TLS o una VPN).

Gli utenti possono accedere ad ARCAM con utenza e password da utilizzare tramite sito HTTPS. Le utenze, rilasciate dall'Istat, sono nominative e sono associate ai referenti formalmente incaricati del trasferimento dati presso le amministrazioni di appartenenza.

Le misure per il controllo della qualità degli archivi sono le seguenti: nel caso di acquisizione dei dati tramite applicativo web, il controllo è basato su meccanismi di hashing per permettere la ritrasmissioni dell'intero file o parte di esso in caso di err ori di trasmissione, nel caso di acquisizione tramite FTP su VPN i file degli archivi sono firmati digitalmente mentre nel caso di acquisizione di FTP sul SSL/TLS si utilizza un controllo di parità (checksum).

2. Acquisizione da Indagine censuaria

L'architettura di sicurezza per la rilevazione diretta sul campo avviene attraverso l'uso di dispositivi dotati di connessione a rete mobile (tablet).

La gestione dei dispositivi tablet è stata realizzata tenendo conto delle esigenze di controllo centralizzato e protezione dei dati raccolti. Essa è effettuata mediante l'uso combinato di un Setup Manager (SM) e di un Mobile Device Management (MDM). In particolare, il SM permette di configurare tramite rete i dispositivi mobili secondo specifiche esigenze: all'accensione del dispositivo mobile il SM provvede a un'identificazione dello stesso basata sul codice IMEI. In seguito, viene definito un primo set di specifiche che rendono il tablet pronto per la registrazione (enrollment) obbligatoria del dispositivo sulla piattaforma di MDM.

Tale piattaforma, sfruttando le primitive (API) fornite dal sistema operativo del tablet stesso, garantisce la gestione centralizzata e l'applicazione delle impostazioni ed effettua l'installazione delle applicazioni necessarie al corretto svolgimento del lavoro degli utenti.

La configurazione dei tablet è la seguente:

1. il tablet ha configurazioni e applicazioni definite centralmente e non modificabili dall'utente finale;
2. l'utente del dispositivo potrà accedere alle sole applicazioni e impostazioni che sono state consentite attraverso la piattaforma MDM;
3. non è possibile installare applicazioni mediante gli store di terze parti dal momento che la piattaforma MDM consente di installare esclusivamente le applicazioni certificate dall'Istat e distribuite tramite uno store "privato" dedicato alla sola rilevazione censuaria. Anche nel corso della raccolta dati sul campo, qualora si renda necessario, sarà possibile distribuire in maniera centralizzata e mediante lo store dedicato dell'Istat ulteriori applicazioni e/o patch di sicurezza delle applicazioni già presenti sui tablet;
4. la navigazione web è consentita solo verso i siti appartenenti al dominio Istat.it, verso il sito del Ministero dell'interno e verso i siti istituzionali dei comuni;
5. in caso di furto/smarrimento dei dispositivi o di riassegnazione dei tablet a comuni diversi è possibile effettuare un ripristino alle impostazioni di fabbrica del tablet in modalità remota (full wipe).

Si precisa che il tablet viene autenticato sulla piattaforma di SM tramite la registrazione iniziale basata sul codice IMEI dell'apparato.

La gestione dei dati sul tablet è delegata all'applicativo Sistema Gestione Indagine (SGI). Quando il rilevatore esegue un'intervista si collega a SGI tramite username e password definite. Se il tablet ha connessione di rete, i dati sono immediatamente trasmessi ad Istat e resi non modificabili sul dispositivo.

Al fine di garantire una maggiore qualità e sicurezza del dato, si sono utilizzati strumenti di analisi statica del codice nello sviluppo delle applicazioni e sono in fase di definizione misure di pseudonimizzazione, basate su tecniche di hash, su particolari variabili presenti nel questionario.

Per evitare accessi non autorizzati ai dati nel caso in cui il tablet venisse assegnato ad un altro rilevatore prima della sincronizzazione, l'applicativo fa in modo che ogni rilevatore abbia visibilità solo dei dati associati alla propria utenza di SGI, tramite un sistema di controllo degli accessi.

Le misure di sicurezza tecnico organizzative per le fasi di acquisizione dati e monitoraggio indagine (SGI) del trattamento prevedono:

- accesso ai dati relativi ai censimenti tramite gli applicativi web solo da parte del personale incaricato che accede con utenze nominative riconducibili a una sola persona (sia per gli utenti interni, sia per la rete di rilevazione) con registrazione degli accessi;
- accesso ai database del CP da parte del personale interno e degli applicativi con meccanismi di accesso che seguono le policy dell'Istituto;
- tracciamento delle singole operazioni effettuate sui database dei censimenti;
- test di vulnerabilità degli applicativi web eseguiti prima della messa in produzione;
- tracciamento degli accessi degli amministratori di sistema.

Per l'acquisizione dei dati attraverso la compilazione diretta del questionario da parte del rispondente (rilevazione L), l'Istat provvede a fornire all'interessato, tramite la lettera informativa, le credenziali di accesso.

In caso di necessità di modifica del PIN di accesso, il rispondente deve recarsi presso l'Ufficio Comunale di censimento o attendere il rilevatore che compilerà il questionario insieme all'interessato. In nessun caso, è previsto che le nuove credenziali siano comunicate dall'Istat tramite e-mail; tale misura è finalizzata a mitigare la possibilità di attacchi di 'phishing' sui rispondenti che possano compromettere la riservatezza e la qualità dei dati raccolti.

2. Acquisizione da Indagine censuaria in modalità offline

Se la connessione di rete è assente il lavoro del rilevatore può essere svolto in modalità "offline" tramite l'utilizzo dell' app denominata "Rilevo".

Questa consentirà di lavorare solo i dati presenti in locale che verranno sincronizzati "on demand" (su richiesta dell'utente) con quelli presenti sul server centrale, in presenza di collegamento di rete. Non è prevista la lavorazione online direttamente sui dati del server.

L'app è installata in automatico sui tablet degli utenti o, in ogni caso, è scaricabile dalla piattaforma protetta MDM. Eventuali aggiornamenti, segnalati direttamente dall'app, seguono lo stesso iter divulgativo fatto per la prima installazione.

L'app è accedibile con le medesime credenziali utilizzate per SGI on line. Al fine di verificare la username e la password inserite nella schermata di login dell'app, il primo accesso di un utente dovrà avvenire online, in presenza di collegamento di rete e dopo aver effettuato il cambio password, in modo che la validazione venga eseguita dall'Identity Provider di Istat (Shibboleth).

In caso di esito positivo dell'identificazione, l'app memorizzerà in locale un hash della password dell'utente che verrà utilizzato per verificare le credenziali nei successivi accessi in modalità offline. All'utente sarà richiesto di effettuare il login nei seguenti casi:

- all'apertura dell'app;
- al rientro nell'app già in esecuzione (ad esempio dopo lo swipe sulla schermata di blocco di Android);
- ogni volta che richiede la sincronizzazione dei dati con il server.

Per poter lavorare sull'app l'utente deve inoltre avere delle unità di rilevazione assegnate. Ogni utente che lavora in modalità offline ha quindi una visibilità dei dati limitata strettamente al lavoro che deve effettuare.

Qualora un utente venga disabilitato dal sistema, alla richiesta di sincronizzazione, tutti i dati vengono cancellati e non potrà più accedere alla rilevazione.

I dati lavorati in modalità offline vengono criptati con algoritmo 256-bit AES e memorizzati sul tablet in un database locale, SQLite, incorporato. Qualora più utenti utilizzassero lo stesso tablet viene creato un database per ogni utente.

La sincronizzazione è stata sviluppata nell'ottica di permanenza minima del dato sul tablet, ossia con l'obiettivo di lasciare sullo stesso solo le informazioni e i dati che devono essere ancora lavorati. I microdati dei questionari compilati quindi sono cancellati dal tablet e non vengono più inviati una volta che gli stessi sono stati salvati sul server.