



*Ministero dell' Interno*  
*Dipartimento Affari Interni e Territoriali*  
*Direzione Centrale per i Servizi Demografici*

**“La rete dei servizi demografici: i sistemi di sicurezza”**

15 Giugno 2006

Relazione del Direttore Centrale per i Servizi Demografici  
Prefetto Mario Ciclosi

EuroP.A. 2006 Rimini 14 – 17 Giugno 2006

## **SOMMARIO**

<b>1. Gli obiettivi .....</b>	<b>3</b>
<b>2. Definizione del contesto di applicazione delle politiche di sicurezza .....</b>	<b>5</b>
<b>3. La cultura della sicurezza: “Nuovo approccio mentale e comportamentale nell’uso di sistemi informativi e reti” .....</b>	<b>7</b>
<b>4. L’attuazione: la sicurezza di sistema e la sicurezza dei processi</b>	<b>7</b>
<b>5. Modello di sicurezza del CNSD.....</b>	<b>7</b>
<b>6. L’accesso in sicurezza ai servizi: la CIE.....</b>	<b>9</b>
<b>7. Il modello organizzativo di riferimento per la gestione della circolarità demografica degli Enti locali.....</b>	<b>11</b>
<b>8. La sensibilizzazione e formazione.....</b>	<b>19</b>

## 1. Gli obiettivi

Il Ministero dell'Interno, titolare sia dei compiti relativi all'**anagrafe** della popolazione residente in Italia e dei **cittadini residenti all'estero** sia di quelli attinenti gli archivi dello **stato civile**, sia infine dei processi relativi all'emissione ed uso della Carta di Identità Elettronica, è da tempo impegnato nella riorganizzazione dell'erogazione dei servizi demografici mediante sistemi informatizzati, che comportano la tenuta e la comunicazione di dati personali da parte delle Amministrazioni pubbliche centrali e locali coinvolte, con particolare attenzione al tema della sicurezza delle reti informatiche e dei flussi di dati concernenti i cittadini italiani e gli stranieri residenti nel territorio nazionale.

A tal fine con il decreto del Ministro dell'Interno in data 23 aprile 2002 è stato costituito, presso la Direzione Centrale per i Servizi Demografici, il Centro Nazionale Servizi Demografici (CNSD) con l'obiettivo di supportare e coordinare a livello tecnologico l'azione dei Comuni e del ministero stesso nel complesso istituto della circolarità anagrafica.

Il CNSD nasce come conseguenza logico-normativa degli interventi legislativi svolti negli ultimi anni in materia di AIRE – Anagrafe Italiani Residenti all'Estero, di CIE – Carta di Identità Elettronica, di INA – Indice Nazionale delle Anagrafi e, non ultimo, di Stato civile. Al CNSD è affidata la gestione unitaria delle attività e delle infrastrutture informatiche centrali relative al rilascio della Carta d'identità elettronica e alla sua utilizzazione per l'accesso ai servizi erogati dalle Amministrazioni Pubbliche centrali e locali. Al CNSD è affidata inoltre la gestione unitaria e coordinata dell'Indice nazionale delle anagrafi (INA), del Sistema di accesso e interscambio anagrafico (SAIA), delle Anagrafi degli italiani residenti all'estero (AIRE) e dello Stato civile e i processi di interscambio tra le diversi fonti anagrafiche primarie e con le Amministrazioni alle stesse interessate.

L'obiettivo è di gestire unitariamente e in sicurezza le attività di tutte le attuali infrastrutture informatiche centrali di interesse dei Servizi demografici, e di quelle in via di realizzazione, al fine di garantire la trasparenza e la sicurezza dei processi di autenticazione e di convalida dei dati anagrafici. Al Centro, in particolare, sono affidate:

- tutte le funzioni connesse alla gestione dei processi di autenticazione e convalida dei dati anagrafici;
- tutte le funzioni connesse alla gestione, all'aggiornamento e alla consultazione dell'Indice Nazionale delle Anagrafi (INA);
- tutte le funzioni connesse alla gestione del Sistema di Accesso e Interscambio Anagrafico dei dati (SAIA);
- tutte le funzioni connesse sia alla gestione tecnica delle componenti telematiche e informatiche che alla gestione logistica per la conservazione delle risorse informative derivanti dall'attuazione delle predette funzioni;
- tutte le funzioni di natura organizzativa connesse alle attività di assistenza ai comuni, ai cittadini, alle amministrazioni pubbliche durante l'espletamento delle funzioni sopraindicate.

Il Centro nazionale dei servizi demografici, pertanto, si avvale delle seguenti infrastrutture tecnologiche:

- Sistema di Sicurezza del Circuito di Emissione delle carte d'identità e dei documenti d'identità elettronici;
- Call Center per il blocco delle carte d'identità elettroniche smarrite o rubate;
- Help Desk per i comuni per la carta d'identità elettronica;
- Indice nazionale delle anagrafi;
- Centro Servizi Anagrafici del Sistema di Accesso e Interscambio Anagrafico;
- Anagrafe degli Italiani Residenti all'Estero;

È stato inoltre allocato presso il CNSD il Centro nazionale di raccolta dei supporti informatici contenenti i dati registrati negli archivi informatici comunali dello stato civile, da realizzare ai sensi

dell'art. 10, comma 2, lett. d) del D.P.R. n. 396/2000. In riferimento alle funzioni svolte dal CNSD e all'infrastruttura telematica necessaria per garantire la connettività del Centro Nazionale verso le strutture coinvolte, i servizi offerti dal CNSD costituiscono il punto di riferimento nazionale per il mantenimento della coerenza e dell'allineamento delle informazioni anagrafiche sintetiche dei cittadini e il punto di riferimento di tutto il sistema delle informazioni anagrafiche.

Il Centro Nazionale dei Servizi Demografici (CNSD) rappresenta quindi il sistema di gestione dei servizi demografici e fornisce i servizi di circolarità anagrafica e di supporto alle funzioni di vigilanza anagrafica di competenza del Ministero dell'Interno.

In tale contesto particolare rilevanza assumono gli aspetti organizzativi di ciascun ente e quelli relativi alle modalità di interazione tra i diversi enti per la gestione dei processi di circolarità anagrafica. È appena il caso di rilevare che, allo stato attuale, usufruiscono dei servizi del CNSD non solo i Comuni e il Ministero dell'Interno stesso ma anche un gran numero di altri enti quali Agenzia delle Entrate, ISTAT, INPS, Motorizzazione Civile, Consiglio del notariato e che molti altri si stanno connettendo, come, ad esempio, il sistema delle Regioni. Tramite il CNSD è infatti possibile recepire tutte le modifiche che si verificano all'interno dell'anagrafe comunale, convalidarle e notificarle alle altre amministrazioni autorizzate al fine di garantire omogeneità nei dati anagrafici gestiti tra i vari attori coinvolti nel sistema di circolarità anagrafica.

Il CNSD rappresenta quindi un esempio compiuto di Pubblica Amministrazione erogatrice di servizi verso cittadini ed altre Pubbliche Amministrazioni. I servizi del CNSD, che giova ricordarlo trattano, tra l'altro, dati sensibili e fondamentali per il funzionamento e la sicurezza del sistema Paese, devono essere altamente affidabili e dunque devono presentare caratteristiche di qualità e di sicurezza commisurate all'importanza del servizio.

Per tali motivi, nella definizione del modello organizzativo e di sicurezza del CNSD, non si è tenuto conto solo della normativa nazionale ed internazionale ma si è anche emanata una normativa specifica che tiene conto sia della complessità del processo di circolarità e vigilanza anagrafica sia del ruolo abilitante per l'accesso ai servizi di terzi del dato anagrafico e della CIE quale elemento di autenticazione certa in rete. Di tale normativa si riporta una breve sintesi:

### **Normativa internazionale e nazionale**

Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione (luglio 2002)

Direttiva "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali" (gennaio 2002)

Decreto del Ministro per l'innovazione e le tecnologie e del Ministro delle comunicazioni 17 febbraio 2005 - Linee guida provvisorie per l'applicazione dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione

Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali

Decreto Legislativo 28 febbraio 2005, n. 42 - Istituzione del sistema pubblico di connettività

Decreto Legislativo 7 Marzo 2005, n. 82 – Codice dell' amministrazione digitale

Decreto Legislativo 4 Aprile 2006, n. 159 – Disposizioni integrative e correttive al codice dell' amministrazione digitale

Linee guida per la sicurezza ICT delle pubbliche amministrazioni – i Quaderni CNIPA: n. 23, marzo 2006

Normativa specificamente emanata dal Ministero

D.M.I. 23 aprile 2002: costituzione Centro Nazionale Servizi Demografici (CNSD) – garante della sicurezza di tutti i servizi demografici nazionali (anagrafi, stato civile, AIRE, CIE)

D.M.I. 19/7/2000, 14/5/2003, 6/11/2003 e 2/8/2005: regole tecniche e di sicurezza CIE – definizione delle regole di sicurezza per i supporti e l'emissione della Carta di identità Elettronica

Legge 31 marzo 2005, n. 43 (articolo 7-vicies ter) – diffusione Carta di Identità Elettronica su tutto il territorio nazionale

D.M.I. 2/8/2005: regole tecniche e di sicurezza postazioni emissione CIE – definizione delle regole per la redazione dei piani di sicurezza comunali per la gestione delle postazioni di emissione CIE

D.M.I. 13/10/2005: Regolamento di gestione dell'Indice Nazionale delle Anagrafi (INA) – adozione piano di sicurezza secondo standard ISO 17799 e BS7799

Legge 26 del 28/2/2001 (Art. 2-quater)

Istituzione, presso il Ministero dell'interno, dell'Indice nazionale delle anagrafi (INA), per un migliore esercizio della funzione di vigilanza e di gestione dei dati anagrafici

Legge 43 del 31 Marzo 2005 (Art. 7 – Vicies ter)

Obbligo, entro il 31 Ottobre 2005, della predisposizione, da parte dei Comuni, dei necessari collegamenti all'INA presso il Centro Nazionale Servizi Demografici (CNSD)

Legge 88 del 31 Maggio 2005 (Art. 1- novies)

L'INA è alimentato e costantemente aggiornato, tramite collegamento informatico da tutti i Comuni.

L'INA promuove la circolarità delle informazioni anagrafiche essenziali al fine di consentire, alle amministrazioni pubbliche centrali e locali collegate le disponibilità, in tempo reale, dei dati relativi alle generalità delle persone residenti in Italia, certificati dai Comuni e, limitatamente al Codice Fiscale, dall'Agenzia delle Entrate.

## **2. Definizione del contesto di applicazione delle politiche di sicurezza**

Parlare di sicurezza informatica comporta inevitabilmente prendere in considerazione molti domini differenti, e dunque richiede un approccio a 360 gradi al problema. Presuppone l'abilità di osservare in maniera non convenzionale la propria organizzazione e le procedure di sicurezza adottate quotidianamente, con occhio critico, alla ricerca delle possibili aree oscure non coperte da alcuna procedura specifica, potenzialmente sfruttabili da un attaccante per eludere i controlli previsti e prendere il controllo del sistema informatico.

Le iniziative adottate sull' argomento sono abbondanti, sia per quanto attiene agli aspetti tecnici, sia per quanto concerne la normativa sulla tutela della privacy.

Pertanto, per una visione di insieme, che consideri unitariamente entrambi i profili, quello tecnico-informatico e quello giuridico, si rende indispensabile fornire agli operatori del settore i corretti riferimenti normativi e tecnici per poter valutare l' impatto sull' organizzazione e sulla gestione dei sistemi informatici.

La sicurezza, soprattutto la sicurezza nell'ambito di un sistema complesso, che vede anche l'interazione tra enti differenti, non è un concetto puramente tecnologico, ma è una priorità che investe molteplici e diversificati aspetti.

Tale aspetto è di assoluta rilevanza per i servizi anagrafici che, come già ricordato, presentano sia una grande rilevanza istituzionale (trattano informazioni primarie, fondamentali per l'esistenza stessa del cittadino e per lo Stato) sia una forte interazione tra diverse Amministrazioni: in particolare tra enti periferici, quali i Comuni, ed Enti Centrali, quali il Ministero dell'Interno ma anche gli altri Enti che vanno dall'Agenzia delle Entrate alla Motorizzazione, l'Inps e l'Istat.

È per tale motivo che, nell'ambito dei sistemi anagrafici del Ministero dell'Interno e del progetto della CIE, in considerazione della necessità di garantire la sicurezza e la tutela della privacy e dati anagrafici, il Ministero ha adottato ovviamente i maggiori livelli di sicurezza disponibili, andando a definire un modello di gestione della sicurezza che, per la complessità del problema e la forte componente innovativa delle soluzioni adottate, mira ad essere uno standard per grandi sistemi che vedono la cooperazione di un gran numero di enti differenti.

Questo modello si basa sui seguenti concetti fondamentali:

- l'individuazione certa dei soggetti e delle relative responsabilità, sia all'interno del CNSD che relativamente ai soggetti esterni che accedono ai servizi del CNSD;
- la garanzia del valore legale dei processi svolti in rete e dei documenti scambiati tra i diversi enti
- protezione della sicurezza e della privacy.

Mentre l'individuazione certa delle responsabilità all'interno del CNSD può essere risolta tramite l'adozione delle misure, di carattere organizzativo e tecnologico, previste da metodologie note, quali la BS7799, opportunamente formalizzate in un apposito Piano della Sicurezza, l'individuazione certa dei soggetti e delle responsabilità esterne presenta un livello di complessità superiore. Infatti ogni ente, sia esso un comune che trasmette informazioni anagrafiche al CNSD o un'altra Amministrazione autorizzata ad utilizzarle, deve essere precisamente individuato ed autorizzato allo scopo. A tal fine il Ministero dell'Interno mette a disposizione la Porta di Accesso ai domini applicativi del C.N.S.D. che identifica il punto di accesso autorizzato, presente presso la struttura di ciascun ente, che consente la fruizione in sicurezza dei servizi erogati dal C.N.S.D. stesso. La Porta di Accesso certifica il punto di origine delle comunicazioni, individuando univocamente l'ente che, tramite la Porta di Accesso stessa, si collega al C.N.S.D. La Porta di Accesso garantisce, inoltre, la protezione crittografica e il controllo dell'integrità e sicurezza delle comunicazioni tramite il canale di sicurezza Backbone. Infine la Porta di Accesso è anche un elemento di normalizzazione della comunicazione rispetto alle diverse tecnologie di rete (Internet, RUPA, Sistema Pubblico di Connettività) utilizzate dai diversi enti per comunicare con il CNSD.

In merito alla validità legale dei processi svolti in rete e dei documenti scambiati l'obiettivo principale è quello non solo di certificare il dato anagrafico scambiato ma anche di certificare la sua integrità, e le modalità e tempi di consegna. A tal proposito, oltre ai consueti meccanismi di protocollo, è stato adottato un sistema distribuito di documentazione dei processi in rete in grado di assicurare non solo l'avvenuta consegna di un documento integro ma anche di certificare l'esatta attuazione dell'intero processo svolto in rete e i relativi tempi di completamento. A titolo di esempio è possibile definire una periodicità di aggiornamento dell'INA da parte dei Comuni, verificarne capillarmente il rispetto e generare automaticamente allarmi in merito ai comuni che non rispettano la periodicità. In più è possibile vigilare in merito alla attuazione dei processi di intercambio da comune a comune o da comune a altro ente in merito, ad esempio, alle annotazioni o trascrizioni di Stato Civile.

La protezione della sicurezza e della privacy è garantita attraverso meccanismi di sicurezza statica (crittografia dei flussi, autenticazione forte...) ma soprattutto attraverso meccanismi di sicurezza dinamica che, come vedremo nel seguito, sono tesi soprattutto al controllo e vigilanza sul corretto funzionamento del sistema attuato tramite un sistema di monitoraggio e allarme in grado di individuare i tentativi di attacco ai sistemi e processi del CNSD fornendo l'esatta individuazione delle modalità di attacco, dell'origine dell'attacco (sia interna che esterna al sistema) e della sua gravità.

### **3. La cultura della sicurezza: “Nuovo approccio mentale e comportamentale nell’uso di sistemi informativi e reti”**

È comunque da sottolineare che per garantire adeguati livelli di sicurezza in un sistema di tale complessità e articolazione è necessario attuare adeguate politiche relative ai diversi aspetti che caratterizzano la sicurezza del sistema, aspetti che riguardano:

- ✚ La consapevolezza dei rischi: il rischio, infatti, è condiviso tra i diversi attori (fornitori-fruitori): a tal proposito è da ricordare che quasi la totalità dei Comuni ha già presentato la prima versione del Piano di Sicurezza comunale (DMI 2/8/2005), basato sulla metodologia messa a disposizione gratuitamente dal Ministero dell’Interno a tutti i comuni. I piani di sicurezza comunali vengono valutati dalle Prefetture e aggiornati periodicamente con cadenza almeno semestrale
- ✚ La collaborazione tra Amministrazioni Centrali, Amministrazioni Locali e cittadini: a tal riguardo il coinvolgimento delle diverse amministrazioni e il ruolo svolto dalle Prefetture sono garanzia di rapporti di collaborazione chiari e continuativi

### **4. L’attuazione: la sicurezza di sistema e la sicurezza dei processi**

Il primo passo per garantire la sicurezza del sistema è quello di avere un preciso controllo e una precisa vigilanza sui flussi di comunicazione e sui dati che vengono scambiati all’interno dei processi dei diversi enti in modo da poter intervenire immediatamente nel caso sia rilevato un attacco alla sicurezza. In particolare vigilanza e controllo garantiscono che i processi che rivestono un carattere istituzionale siano svolti correttamente e che gli enti, ovvero gli attori primari, abbiano la garanzia della correttezza dell’esito del processo. Il che equivale a garantire che:

1. il processo sia iniziato e finito correttamente
2. il dato finale ottenuto sia coerente con il dato atteso per il processo stesso.

Controllo e vigilanza rappresentano una garanzia anche per il cittadino in quanto consentono di tutelare la privacy e proteggere i dati sensibili di ogni cittadino, scambiati nell’ambito delle attività telematiche istituzionali.

## **5. Modello di sicurezza del CNSD**

Il modello di sicurezza del CNSD si basa sui seguenti concetti di base:

- Sicurezza organizzativa e fisica che trova attuazione nel Piano di sicurezza del CNSD
- Sicurezza logica che trova attuazione nei concetti di sicurezza statica e sicurezza dinamica

Il Piano di sicurezza del CNSD affronta e regola i seguenti aspetti:

1. Ricognizione e sensibilizzazione
2. Precisa individuazione di ruoli e responsabilità
3. Valutazione dei beni e dei rischi
4. Sicurezza fisica (protezione, controllo accessi)
5. Sicurezza logica
  - Interna (regole di accesso ai sistemi, protezione dai virus, controllo dati, recovery)
  - Esterna (identificazione univoca degli enti che accedono via rete geografica – Internet, Interdominio, SPC- identificazione postazione, protezione dati, crittografia...)
  - Tutela della Privacy

## 6. Monitoraggio

- Interno (controllo continuo degli indicatori di performance, sicurezza e rischio)
- Esterno (allarmi relativamente ai tentativi di intrusione, allarmi relativi a tentativi di manomissione logica/fisica dei punti unici abilitati all'accesso al CNSD, allarmi relativi a tentativi di accesso non autorizzato, allarmi relativi a tentativi di attacco "denial of service" o "man in the middle" ...)

## 7. Gestione degli incidenti e ripristino

Alcuni aspetti di sicurezza logica meritano, comunque, un approfondimento. In particolare i concetti di sicurezza statica, cioè della sicurezza atta a proteggere le reti, i dati e le altre componenti tecnologiche del sistema e di sicurezza dinamica che riguarda i sistemi e le azioni che vengono messi in atto per prevenire e individuare i tentativi di attacco al sistema o alle reti di comunicazione e le azioni correttive che devono essere intraprese a seguito di un allarme di sicurezza.

In particolare le misure di **sicurezza statica** adottate garantiscono la **Protezione** dei flussi di comunicazione, dei dati e delle componenti tecnologiche, centrali e periferiche, del sistema. Ad esempio, per quanto riguarda la protezione dei flussi di dati del sistema, vengono impiegate diverse tecnologie in grado di garantire la sicurezza di base, come la crittografia. Per la protezione dei servizi anagrafici del Centro Nazionale sistema il Ministero dell'Interno ha scelto i protocolli SSL e Backbone in grado di garantire la massima sicurezza dei dati anagrafici e dei servizi del CNSD.

Poiché si ritiene che la componente di sicurezza statica sia fondamentale ma che la reale sicurezza possa essere assicurata solo se accompagnata da adeguate politiche di gestione della **sicurezza dinamica** (in fondo anche le tecniche di attacco e difesa evolvono continuamente e l'individuazione di nuove strategie di attacco è ancora più importante della semplice protezione) si è data grande importanza alle azioni di **Contrasto** cioè al *controllo e vigilanza sul corretto funzionamento del sistema (sicurezza dinamica)* e alle conseguenti azioni di **Intervento** cioè alle *azioni correttive conseguenti ad un allarme di sicurezza, rilevato dalle componenti di controllo e vigilanza, teso a violare la protezione del sistema* (anch'esse afferenti al concetto di **sicurezza dinamica**).

In merito al contrasto assume un ruolo fondamentale il concetto di **controllo e vigilanza**. Il controllo e la vigilanza, infatti, non servono solo ad individuare tentativi di violazione della sicurezza provenienti dall'esterno ma anche a delimitare esattamente gli ambiti di responsabilità degli utilizzatori del sistema individuando eventuali utilizzi dello stesso non conformi alle reciproche competenze (a tal riguardo si ricordi il recente caso "Laziomatica"). Da qui la scelta del Ministero dell'Interno di garantire la sicurezza del circuito anagrafico del CNSD tramite specifici punti di accesso autorizzati, presenti presso ciascun ente ("porta di accesso") che certificano il punto di origine delle comunicazioni, individuando univocamente l'ente che accede al CNSD (DM 2 agosto 2005). L'infrastruttura di "Vigilanza informatica", realizzata dal Ministero, garantisce inoltre un controllo continuo relativo all'individuazione di tentativi di attacco ai sistemi e processi del CNSD fornendo l'esatta individuazione delle modalità di attacco, dell'origine dell'attacco e della sua gravità.

Nel caso si individui comunque un attacco intenzionale, proveniente dall'esterno o dall'interno, o un'altra violazione della sicurezza è necessario scoprire chi è che sta cercando perpetrare l'attacco e/o quali sono i motivi che hanno dato luogo al tentativo di violazione della sicurezza. A tal fine il Ministero dell'Interno utilizza le componenti del sistema di controllo, allarme e vigilanza che, rilevato l'allarme relativo al tentativo di attacco, consentono di intervenire con azioni correttive puntuali in quanto permettono di tracciare con esattezza la componente del sistema sotto attacco e l'origine dell'attacco stesso.

Il sistema di controllo, allarme e vigilanza, per le sue funzioni di sicurezza dinamica, si avvale di “Agenti di monitoraggio e allarme” distribuiti che:

- ✚ “Verificano” la correttezza dei flussi di comunicazione e dei servizi del CNSD
- ✚ “Verificano” la correttezza dei processi di emissione CIE
- ✚ In caso di anomalie allertano il Centro di Controllo
- ✚ Il centro di controllo valuta l’allarme ricevuto e reagisce in base alla sua classificazione:
  - Allarme di sicurezza
  - Allarme di sicurezza
  - Allarme Guasto

In particolare per svolgere le sue funzioni il Centro di controllo si avvale del Sistema di Monitoraggio e Controllo allarmi sicurezza che:

- ✚ Riceve le anomalie dagli Agenti di Monitoraggio e Controllo
- ✚ Compara le anomalie con le regole di sicurezza
- ✚ Valuta le anomalie e i malfunzionamenti
- ✚ Spedisce le rilevazioni agli agenti
- ✚ Genera report sul funzionamento del Sistema
- ✚ Attiva le contromisure di sicurezza e allerta la struttura di intervento per la loro gestione (**CERT del CNSD**)

## 6. L’accesso in sicurezza ai servizi: la CIE

Le componenti di sicurezza e garanzia descritte, che nel loro insieme vengono a costituire una vera e propria infrastruttura di sicurezza, sono fondamentali non solo in merito ai dati e sistemi anagrafici del CNSD ma anche per un progetto come quello della Carta di Identità Elettronica (CIE) che tocca un aspetto fondamentale per il cittadino, la sua identità. Non scordiamoci, infatti, che uno dei furti informatici più diffusi è proprio il furto di identità, qual modo migliore di rubare definitivamente sia l’identità fisica che elettronica che rubando la carta di identità elettronica? Per tali motivi il Ministero adotta le tecniche di vigilanza, protezione ed intervento descritte in precedenza anche ai processi e ai sistemi centrali e periferici del circuito di emissione della Carta di identità Elettronica e ha anche previsto che i Comuni adottino, sulla base delle linee guida fornite dal Ministero stesso, specifici Piani di Sicurezza relativi alla emissione della CIE.

Infatti una completa protezione e gestione in sicurezza dei sistemi di servizio della PP.AA. deve trovare il suo completamento nel garantire ai cittadini gli strumenti per accedere, in rete, in sicurezza ai servizi messi a disposizione dalla PP.AA.. Lo strumento per l’autenticazione del cittadino e l’erogazione dei servizi della PP.AA. in sicurezza e nel rispetto della tutela della privacy è la CIE, che sia da un punto di vista tecnologico e di sicurezza, sia dal punto di vista della maturità del circuito di emissione ed uso, sia infine dal punto di vista della completezza della normativa sottostante, è all’avanguardia in Europa e nel mondo.

La CIE, infatti, garantisce elevati standard di sicurezza per l’identificazione certa del titolare (anche a fini elettorali), contro la contraffazione del documento e per la tutela della privacy e dei dati personali e sensibili (con particolare riferimento a quelli biometrici).

La sua adozione su tutto il territorio nazionale, ormai in corso, garantisce uno strumento unitario a disposizione di tutti i cittadini per l’accesso in rete ai servizi, strumento che, nella sua fase di uso si basa sui seguenti aspetti fondamentali:

- ✚ Meccanismo standard di identificazione in rete mediante browser WEB
- ✚ Lettura del certificato dalla carta
- ✚ Verifica sulla black-list del Ministero dell’Interno che la CIE non sia revocata (Servizi distribuiti di validazione dei certificati delle CIE - OCSP distribuito)
- ✚ Acquisizione PIN per verifica della presenza fisica della CIE (challenge)
- ✚ Convalida anagrafica presso l’INA

- ✚ Acquisizione codice fiscale da Ministero dell' Interno (CNSD-INA) per eventuale recupero dati anagrafici
- ✚ Possibilità di verifica dati biometrici (in locale e senza trasmissione del dato biometrico in rete) per garantire la presenza fisica del titolare della CIE durante l'accesso ai servizi in rete
- ✚ Servizi di firma digitale a disposizione del titolare per tutti i servizi che richiedono l'apposizione di firma autografa (sia per i servizi in rete sia per i servizi di firma di documenti quale ad esempio la sottoscrizione di un atto o contratto)

Si viene quindi a definire un sistema completo, dalla disponibilità di informazione anagrafica certificata, elemento abilitante per la definizione di servizi certi da parte di tutte le PP.AA. alla disponibilità dello strumento di autenticazione per accedervi (la CIE) fino alla disponibilità del circuito di accesso e controllo per l'erogazione e l'accesso ai servizi stessi.

## **7. Il modello organizzativo di riferimento per la gestione della circolarità demografica degli Enti locali**

Per lo svolgimento delle funzionalità previste è necessario che le singole Amministrazioni si dotino di un'adeguata infrastruttura atta a rendere possibile una capillare implementazione della politica di sicurezza, unitamente ad un'equivalente e capillare verifica riguardo l'attuazione della stessa.

In tale ottica risulta indispensabile per il Comune provvedere alla definizione ed alla successiva istituzione, all'interno della propria struttura, di un'organizzazione che si occupi di sovrintendere e controllare i processi e le attività legate alla sicurezza.

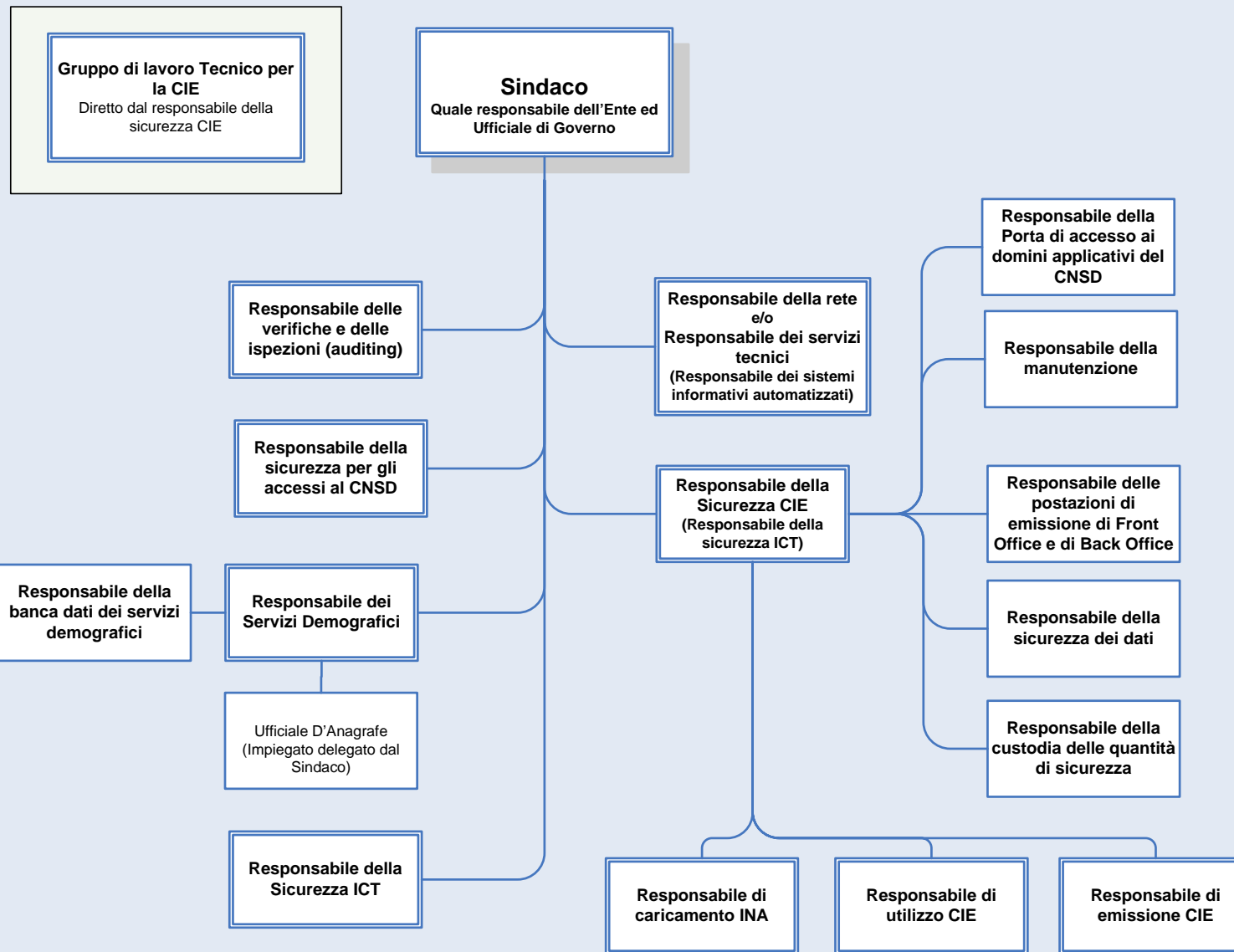
In particolar modo, in relazione al complessivo processo di emissione della CIE, sarà cura dell'Ente provvedere all'individuazione delle seguenti figure professionali:

- Responsabile comunale per la sicurezza degli accessi al CNSD;
- Responsabile della sicurezza CIE;
- Responsabile della custodia delle Quantità di Sicurezza;
- Responsabile di caricamento INA;
- Responsabile di emissione della CIE;
- Responsabile della sicurezza dei dati;
- Responsabile delle postazioni di emissione sia di front office che di back office;
- Responsabile della porta di accesso ai domini applicativi del CNSD;
- Responsabile della rete;
- Responsabile dei servizi tecnici;
- Responsabile delle verifiche e delle ispezioni (auditing);
- Responsabile della manutenzione;
- Responsabile di utilizzo della CIE;
- Responsabile della banca dati dei servizi demografici

ferma restando la possibilità che più ruoli siano ricoperti da una stessa persona a seconda della dimensione e della struttura organizzativa dell'Amministrazione Comunale considerata.

Di seguito viene presentato uno schema di modello organizzativo di riferimento per la gestione della circolarità demografica in sicurezza che soddisfa le vigenti direttive emanate in materia, sebbene resti a carico di ogni Amministrazione la progettazione e la realizzazione della security sulla base delle proprie esigenze individuali.

## Modello organizzativo di riferimento per la gestione della circolarità demografica



## **Definizione dei ruoli e delle responsabilità negli Enti locali**

Di seguito verranno definiti ed analizzati in dettagli tutti i ruoli previsti dal modello organizzativo di riferimento.

### **Sindaco**

Si tratta della figura al vertice della struttura, in quanto responsabile dell'Ente. Inoltre, per l'esercizio delle funzioni statali, assume anche la veste di Ufficiale di governo.

### **Gruppo di lavoro Tecnico per la CIE**

Questa struttura si configura come un organo collegiale, per l'elaborazione delle linee guida ed il coordinamento delle attività dei vari responsabili, che sebbene non esplicitamente richiesto dalla vigente normativa, risulta essere quasi indispensabile al fine di provvedere all'armonizzazione delle attività di esclusiva pertinenza e di completa responsabilità dei vari ruoli citati nel corso della precedente lezione (ed in gran parte definiti nel D.M.I. del 2/8/2005, sulle regole tecniche e di sicurezza per la realizzazione dei piani di sicurezza comunali per la gestione delle postazioni di emissione CIE).

A tale organismo viene demandata la politica di sicurezza delle infrastrutture tecnologiche e del patrimonio informativo utilizzato nell'ambito delle attività connesse alla carta d'identità elettronica.

Nel suo dimensionamento e collocamento all'interno della struttura (Modello organizzativo di riferimento per la gestione della circolarità demografica), il gruppo di lavoro Tecnico per la CIE viene effettivamente a configurarsi come una sorta di sottocomitato facente parte del più generale Comitato per la sicurezza ICT a cui viene demandata la politica di sicurezza delle infrastrutture tecnologiche e del patrimonio informativo prevalentemente gestito mediante soluzioni automatizzate. Ovviamente, qualora le dimensioni esigue dell'Ente non giustificano l'esistenza di due differenti organi collegiali sarà possibile procedere al loro accorpamento, nel senso che un unico comitato svolgerà interamente le funzioni previste da entrambi.

A questo punto è di fondamentale importanza sottolineare un aspetto centrale nella comprensione dei rapporti tra il summenzionato comitato ed i vari ruoli di responsabilità previsti dal D.M.I. del 2/8/2005 sulla redazione dei Piani di Sicurezza Comunali; infatti, sebbene tale organo collegiale svolga un'importante funzione di raccordo tra i vari responsabili va tenuto presente come questi e solamente questi siano in grado di assumere le decisioni strategiche connesse al loro mandato. In tal senso il Comitato si limita a consigliare una strada, da percorrere collegialmente, che poi ogni Responsabile di una data funzione può o meno, riprendere e perseguire nell'ambito degli atti e delle decisioni di sua esclusiva pertinenza.

Il Gruppo di Lavoro Tecnico per la CIE, diretto dal Responsabile della Sicurezza CIE, è composto da varie figure, tra le quali, a titolo di esempio, è possibile ricordare:

- il Direttore Generale (ove previsto) od il Segretario Comunale;
- il Responsabile dei Servizi Demografici;
- il Responsabile dei sistemi informativi;
- il Responsabile (eventuale) dell'Ufficio di Ragioneria;
- il Responsabile (eventuale) dell'Ufficio Segreteria;
- il Responsabile della sicurezza CIE;
- il Responsabile di caricamento INA;
- il Responsabile di emissione CIE;
- il Responsabile di utilizzo CIE;
- il Responsabile comunale per la sicurezza degli accessi al CNSD;
- il Responsabile delle verifiche e delle ispezioni (auditing).

Di seguito vengono elencate le molteplici funzioni in materia di sicurezza ICT che il comitato si trova a svolgere nell'ambito degli adempimenti previsti per la circolarità anagrafica e la CIE.

#### Elaborazione del piano di lavoro

Il Gruppo di lavoro tecnico ha il compito di provvedere alla definizione di un piano di lavoro di dettaglio. Al suo interno dovranno essere chiaramente indicate:

- le modalità ed i tempi di rilascio della CIE;
- la quantificazione dei supporti necessari a coprire il fabbisogno della popolazione residente.

#### Elaborazione del Documento di progetto

Il Gruppo di lavoro tecnico ha il compito di provvedere alla definizione di un idoneo Documento di progetto indicante:

- il piano di gestione del progetto;
- un documento atto a descrivere i servizi che si intende erogare;
- un documento atto alla definizione dei meccanismi di integrazione tecnica tra il sistema dei servizi comunali e l'infrastruttura del sistema CIE attestata in seno all'Ente (per quanto concerne l'emissione e l'autenticazione);
- i documenti contenenti il piano della sicurezza comunale di cui al D.M.I. del 2/8/2005. Tale piano dovrà essere preventivamente approvato dal Prefetto dell'Ufficio Territoriale del Governo (UTG) competente per il territorio, affinché possa aver luogo la consegna dei supporti bianchi inizializzati della CIE.

### Avvio delle procedure preliminari propedeutiche all'emissione della CIE

Il Gruppo di lavoro tecnico ha il compito di avviare tutte quelle attività ritenute preliminari, nonché propedeutiche alla successiva fase di emissione della CIE, quali:

- allineamento dei codici fiscali con l'Agenzia delle Entrate;
- caricamento dell'Indice Nazionale delle Anagrafi (INA);
- aggiornamento (costante) dell'Indice Nazionale delle Anagrafi (INA) tramite il Sistema di Accesso ed Interscambio Anagrafico (SAIA).

### Utilizzo del backbone applicativo

Il Gruppo di lavoro tecnico ha il compito di vigilare affinché sia garantito che l'autenticazione per l'accesso ai servizi nazionali, attraverso la CIE, avvenga esclusivamente tramite il modello del backbone applicativo e la porta comunale di accesso al CNSD.

### Sperimentazione dell'identificazione dell'elettore al seggio

Il Gruppo di lavoro tecnico ha il compito di vigilare affinché sia garantita l'attuazione della sperimentazione dell'identificazione dell'elettore al seggio in occasione delle consultazioni elettorali che si svolgeranno nel futuro.

### Realizzazione e gestione del Call Center

Il Gruppo di lavoro tecnico ha il compito di garantire l'eventuale realizzazione, nonché gestione di un call center comunale, in diretto collegamento con il CNSD, a disposizione dei cittadini. Qualora ne sia riscontrata la necessità, detta struttura potrà avere carattere intercomunale anziché comunale.

### Garantire la conformità degli apparati e delle attrezzature utilizzate

Il Gruppo di lavoro tecnico ha il compito di provvedere affinché sia garantita la conformità degli apparati, nonché delle attrezzature utilizzate nella fase di emissione della CIE, alle determinazioni adottate dal comitato tecnico permanente costituito in seno all'Istituto Poligrafico e Zecca dello Stato (IPSZ).

### Gestione delle richieste di ripristino dei flussi

Il Gruppo di lavoro tecnico ha il compito di vigilare affinché, in seguito al verificarsi di eventuali inconvenienti, la richiesta di ripristino dei flussi di emissione della CIE sia presentata al CNSD al più entro le dodici ore successive all'incidente accorso.

### Assistenza alle attività di monitoraggio e validazione

Il Gruppo di lavoro tecnico ha il compito di provvedere affinché sia garantita la più totale assistenza al Sindaco ed ai suoi incaricati nella redazione trimestrale delle schede di Monitoraggio e Validazione previste dal D.M.I. del 2/8/2005 sulla redazione del piano della sicurezza comunale per la gestione delle postazioni di emissione CIE.

### Assicurare la manutenzione e l'approvvigionamento delle stazioni d'emissione

Il Gruppo di lavoro tecnico ha il compito di provvedere affinché sia espletata l'attività di manutenzione delle postazioni di emissione, nonché sia garantito l'approvvigionamento dei materiali di consumo.

### Trasmissione al CNSD degli elenchi di rilascio, annullamento e revoca delle carte

Il Gruppo di lavoro tecnico ha il compito di provvedere affinché sia garantita la gestione delle carte valori a rigoroso rendiconto, provvedendo alla trasmissione al CNSD, secondo le direttive impartite dal Ministero dell'Interno, degli elenchi di rilascio, annullamento e revoca delle carte emesse dal Comune.

### **Responsabile della Sicurezza ICT**

A tale ruolo compete la definizione delle soluzioni tecniche, in attuazione delle direttive del Sindaco e/o su indicazione del Comitato per la sicurezza ICT oppure del Gruppo di Lavoro Tecnico per la CIE. La definizione delle soluzioni tecniche deve essere eseguita, da tale soggetto, sviluppando delle idonee politiche di sicurezza dei sistemi ICT inerenti sia le applicazioni che le informazioni utilizzate nell'ambito dell'Amministrazione.

Nello sviluppo di tali politiche, il Responsabile della sicurezza ICT dovrà avvalersi di una metodologia di analisi e gestione dei rischi da applicare a beneficio delle indicazioni contenute nella politica di sicurezza della P.A. e nell'eventuale politica di sicurezza dell'Amministrazione.

Ulteriore compito di tale ruolo consiste nell'obbligo di comunicare al Responsabile dei sistemi informativi automatizzati le definizioni relative alle soluzioni tecniche per la loro realizzazione e per il monitoraggio del loro corretto funzionamento.

Qualora la dimensione dell'Ente non sia elevata (ad esempio per i comuni con popolazione inferiore ai 15.000 abitanti) il ruolo di Responsabile per la Sicurezza ICT potrebbe essere ricoperto dal Responsabile della Sicurezza CIE.

### **Responsabile dei sistemi informativi automatizzati**

A tale ruolo compete la pianificazione degli interventi di automazione, della committenza delle attività da affidare all'esterno e dell'adozione delle cautele e delle misure di sicurezza. Sulla base della complessità organizzativa dell'Ente, al Responsabile dei sistemi informativi automatizzati può essere consentito di venire affiancato da assistenti, in numero proporzionato alla complessità dei sistemi informatici gestiti presso l'Amministrazione.

Qualora la dimensione dell'Ente non sia elevata (ad esempio per i comuni con popolazione inferiore ai 15.000 abitanti) il ruolo di Responsabile dei sistemi informativi automatizzati potrebbe essere ricoperto dal Responsabile della rete e/o dal Responsabile dei Servizi Tecnici.

### **Ufficiale d'Anagrafe**

A tale ruolo compete la tenuta e l'aggiornamento dell'Anagrafe comunale, nonché l'attuazione delle procedure di raccordo con l'INA e con il SAIA. Inoltre, quale delegato del Sindaco (titolare del dato anagrafico) è responsabile del trattamento dei dati ai sensi del D.Lgs. 196/2003.

### **Responsabile della custodia delle quantità di sicurezza**

A tale ruolo compete la custodia e gestione delle Quantità di Sicurezza (ovvero, nello specifico del progetto CIE, del supporto vergine inizializzato, dei pin, dei certificati di sicurezza e della relativa custodia). Il responsabile sarà tenuto a denunciare al responsabile della sicurezza CIE ogni tentativo di accesso non autorizzato. Esso dovrà verificare l'integrità del luogo di custodia e di tutte le relative credenziali di accesso consentendo l'accesso alle Quantità di Sicurezza al solo personale autorizzato. Inoltre dovrà provvedere alla registrazione di ogni accesso, avendo cura di riportare almeno le seguenti informazioni:

- Data ed ora della presa in consegna;
- Nominativo del personale a cui è stata consegnata la Quantità di Sicurezza;
- Data ed ora della restituzione.

In aggiunta a quanto detto è altresì responsabile della tenuta delle liste di carico e di scarico dei documenti a rigoroso rendiconto, nonché della contabilizzazione dell'avvenuto pagamento da parte dei cittadini.

### **Responsabile comunale per la sicurezza degli accessi al CNSD:**

Questo ruolo è direttamente responsabile dell'attivazione e della corretta gestione della Porta di Accesso ai Domini Applicativi del CNSD, nonché dell'attivazione dei sistemi comunali autorizzati all'accesso ai servizi applicativi del CNSD. Nell'ambito delle sue attività, al Responsabile comunale per la sicurezza degli accessi al CNSD è altresì affidata la responsabilità della custodia in sicurezza delle "Quantità di sicurezza, attivazione e certificazione"

### **Responsabile della sicurezza CIE**

A questo ruolo è affidato il compito di proporre e definire le regole di sicurezza del Comune. In particolar modo, qualora le dimensioni dell'Ente lo richiedano, questa figura potrà fungere da responsabile di riferimento per tutti e tre i macroprocessi CIE, ricoprendo anche gli altri ruoli di seguito definiti (Responsabile caricamento INA, Responsabile di emissione CIE e Responsabile di utilizzo CIE).

### **Responsabile caricamento INA**

A tale ruolo compete il compito di effettuare la gestione operativa dell'infrastruttura inerente al macroprocesso CIE di caricamento dell'INA.

### **Responsabile di emissione della CIE**

A tale ruolo compete il compito di effettuare la gestione operativa dell'infrastruttura inerente al macroprocesso di emissione CIE.

### **Responsabile della sicurezza dei dati**

A tale ruolo compete la responsabilità dei backup dei dati relativi ai tre macroprocessi CIE. Esso dovrà garantire l'integrità e la custodia di tutte le copie di sicurezza, consentendone l'accesso al solo personale autorizzato.

### **Responsabile delle postazioni di emissione sia di front office che di back office**

A tale ruolo competono la gestione ed il coordinamento delle attività di configurazione e/o aggiornamento che devono essere svolte sulle postazioni di front office e Back office CIE.

### **Responsabile della Porta di accesso ai domini applicativi del CNSD**

A tale ruolo competono la gestione ed il coordinamento delle attività di configurazione e/o aggiornamento che devono essere svolte sulla Porta di accesso ai domini applicativi del CNSD.

### **Responsabile della rete**

A tale ruolo competono la gestione ed il coordinamento delle attività di configurazione e/o aggiornamento che devono essere svoltesi tutti i sistemi inerenti la rete comunale (a titolo meramente esemplificativo: router, firewall, Proxy, etc...).

### **Responsabile dei servizi tecnici**

A tale ruolo competono la gestione ed il coordinamento delle attività di configurazione e/o aggiornamento che devono essere svolte in tutti gli altri sistemi informatici presenti nel Comune e comunque attinenti all'emissione ed all'uso della CIE.

### **Responsabile delle verifiche e delle ispezioni (auditing)**

A tale ruolo competono la pianificazione, la gestione ed il coordinamento di tutte le attività di controllo e di verifica della corretta attuazione del piano della sicurezza comunale.

### **Responsabile della manutenzione**

A tale ruolo competono la gestione ed il coordinamento di tutte le attività di manutenzione delle risorse tecnologiche impiegate nei processi di emissione ed uso della CIE.

### **Responsabile della banca dati dei servizi demografici**

A tale ruolo competono la gestione ed il coordinamento di tutte le attività di gestione e/o manutenzione delle risorse costituenti la banca dati dei servizi demografici.

### **Responsabile di utilizzo della CIE**

A tale ruolo compete il compito di effettuare la gestione operativa dell'infrastruttura inerente al macroprocesso di utilizzo della CIE.

## **7. La sensibilizzazione e formazione**

L'attività di formazione degli operatori dei servizi demografici comunali e dei funzionari e dirigenti delle Prefetture impegnati nel settore è stata oggetto di particolare attenzione nella politica generale dell'Amministrazione dell'Interno

Il Ministero dell'Interno sta promuovendo programmi di formazione nel settore informatico che potranno avvalersi sia dei metodi di formazione tradizionali, sia delle moderne tecniche di formazione a distanza (*e-learning*, Web-Based Training);

In particolare, per quanto attiene alla formazione degli operatori comunali, dopo aver validato la piattaforma del corso sperimentale realizzato in materia nella provincia di Macerata, l'Università degli Studi di Macerata ha provveduto a predisporre un corso e-learning che è stato sottoposto anch'esso alla validazione da parte del Comitato Tecnico Scientifico.

Il Corso avrà la durata di 36 ore e sarà strutturato in 3 unità, ognuna delle quali sarà suddivisa in Moduli. Il Corso sarà fruibile sia da utenti laureati, sia da diplomati. Alla fine di esso verrà rilasciato un Attestato di frequenza ai partecipanti che avranno effettuato almeno l'80% delle attività (attestate dal tracciamento informatico) e superato la prova finale.

Al riguardo, è stata stipulata un'apposita Convenzione fra il Ministero dell'Interno, l'ANCI e l'Università di Macerata per l'erogazione di tale corso ai piccoli Comuni.

In materia si sta avviando in collaborazione con l'Università di Tor Vergata un master Universitario di 1° e 2° livello in "*Sicurezza Informatica e tutela della privacy*" mirato all'alta qualificazione nel campo della formazione di figure professionali con le competenze necessarie alla gestione della sicurezza di sistemi informatici e di reti di comunicazione e alla tutela della privacy di dati sensibili (master di 1 livello) e al disegno, lo sviluppo e alla gestione di progetti nel settore della sicurezza informatica e gestione di dati sensibili (master di 2 livello), per l'industria e la pubblica amministrazione.

Inoltre considerato che solo l'attività di abilitazione riguarda circa 35000 unità e l'esiguità dei fondi disponibili, è necessario creare una sinergia di attività e di risorse tra le Amministrazioni Centrali e Locali, comunque coinvolte in quanto erogatrici di servizi ai cittadini, anche al fine di verificare la possibilità di un eventuale accesso ai fondi messi a disposizione dall'Unione Europea e della cui gestione le Regioni costituiscono il fulcro principale.

Sono pertanto in corso diversi tentativi di approfondimento a livello locale con tutti i rappresentanti dei settori interessati all'erogazione dei servizi comunali, al fine di approntare

una strategia comune per realizzare, nel migliore dei modi, le innovazioni previste dai programmi di e-government gestiti da questa Direzione Centrale anche al fine di migliorare i rapporti tra pubbliche amministrazioni e cittadini.