

Decreto 2 agosto 2005

“Regole tecniche e di sicurezza per la redazione dei piani di sicurezza comunali per la gestione delle postazioni di emissione CIE, in attuazione del comma 2 dell'articolo 7-vicies ter della legge 31 marzo 2005, n. 43.”

G.U. 19 settembre 2005, n. 218

IL MINISTRO DELL'INTERNO

- Visti il regio decreto 18 giugno 1931, n. 773 ed il regio decreto 6 maggio 1940, n. 635;
- Visto l'art. 2 della legge 15 maggio 1997, n. 127, come modificato dall'art. 2, comma 4, della legge 16 giugno 1998, n. 191;
- Visto il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437;
- Visto il decreto del Ministro dell'interno in data 19 luglio 2000 concernente regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici;
- Visto il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445;
- Visto il decreto-legge 23 gennaio 2000, n. 10;
- Visto il decreto legislativo 30 giugno 2003, n. 196;
- Visto il decreto-legge 7 marzo 2005, n. 82; Vista la legge 31 marzo 2005, n. 43;
- Vista la legge 31 maggio 2005, n. 88;
- Visto il comma 2, art. 7-vicies ter della legge 31 marzo 2005, n.43, che stabilisce che i comuni che non vi abbiano ancora ottemperato provvedano entro il 31 ottobre 2005 alla predisposizione dei necessari collegamenti all'Indice Nazionale delle Anagrafi (INA) presso il Centro Nazionale per i Servizi Demografici (C.N.S.D.) e dalla redazione del piano di sicurezza per la gestione delle postazioni di emissione secondo le regole tecniche fornite dal Ministero dell'Interno;
- Considerato che il Piano di sicurezza comunale per la carta d'identità elettronica «Piano di sicurezza comunale per la carta d'identità elettronica: linee guida e metodologia per la redazione del piano», è stato sperimentato sul campo presso 3 comuni rappresentativi delle tipologie di grande, di medio e di piccolo Comune;

DECRETA:

Capo I - Principi generali

Articolo 1 -Definizioni

Ai sensi del presente decreto si intende:

- a. per «D.P.C.M.»: il decreto del Presidente del Consiglio dei Ministri del 22 ottobre 1999, n. 437;
- b. per «documento»: la carta d'identità elettronica e/o il documento d'identità elettronico di cui all'art. 2 del decreto del Presidente del Consiglio dei Ministri costituito dall'insieme del supporto fisico e dei supporti informatici;
- c. per «dati»: i dati identificativi della persona di cui all'art. 1, comma 1, lettera d) e gli altri elementi di cui all'art. 3, comma 1, lettere da b) ad h), del decreto del Presidente del Consiglio dei Ministri;
- d. per «S.S.C.E.»: il Sistema di sicurezza del circuito di emissione dei documenti d'identità elettronica;
- e. per «C.N.S.D.»: il Centro Nazionale dei Servizi Demografici del Ministero dell'Interno costituito con il decreto del Ministro dell'interno del 23 aprile 2002;
- f. per «I.N.A.»: l'Indice Nazionale delle Anagrafi istituito con legge 28 febbraio 2001, n. 26, sostituita dalla legge 31 maggio 2005, n. 88, per la fornitura dei servizi di convalida anagrafica durante l'emissione e l'uso del documento;
- g. per Backbone C.N.S.D.: la dorsale di sicurezza e certificazione del C.N.S.D. per l'accesso ai servizi applicativi del C.N.S.D.;
- h. per «Porta di accesso ai domini applicativi del C.N.S.D.»: la Porta di accesso, attraverso il Backbone C.N.S.D., ai servizi del C.N.S.D. secondo standard «busta di e-gov» di SPC;
- i. per «Porta di accesso»: una «Porta di accesso ai domini applicativi del C.N.S.D.»;
- l. per «Porta di accesso del Comune»: la «Porta di accesso ai domini applicativi del C.N.S.D.» situata presso il comune;
- m. per «Porta di accesso della Prefettura-UTG»: la «Porta di accesso ai domini applicativi del C.N.S.D.» situata presso la prefettura-UTG;
- n. per «Porta di accesso del centro di allestimento periferico»: la «Porta di accesso ai domini applicativi del C.N.S.D.» situata presso un centro di allestimento periferico;
- o. per «Busta di e-gov»: il formato comune di interscambio tra porte di dominio di enti diversi;
- p. per «sito»: il sito Web della Direzione Centrale per i Servizi Demografici, accessibile all'indirizzo internet www.servizidemografici.interno.it;
- q. per «quantità di sicurezza, certificazione ed attivazione»: le credenziali digitali e i software di sicurezza, monitoraggio e allarmi forniti dal Ministero dell'interno;
- r. per SPC: il Sistema pubblico di connettività di cui al decreto legislativo n. 42 del 28 febbraio 2005;
- s. per «domini applicativi»: i domini applicativi del C.N.S.D. ovvero l'insieme dei servizi applicativi riferiti ad un'area (INA, AIRE, Stato civile ...);
- t. per «servizi applicativi»: i servizi applicativi dei singoli domini applicativi del C.N.S.D.;
- u. per «Protocollo XML-Soap»: il protocollo di trasporto della «busta di e-gov del C.N.S.D.» che uniforma i messaggi scambiati con la Porta di accesso;

- v. per busta di e-gov del C.N.S.D.: la busta di e-gov relativa ai domini applicativi del C.N.S.D.;
- aa. per «Protocollo post http XML»: la trasmissione di un evento in formato XML alla Porta di accesso;
- ab. per «C.I.E.»: Carta di identità elettronica;
- ac. per «AIRE»: Anagrafe italiani residenti all'estero;
- ad. per allegato A si intende il «Piano di sicurezza comunale per la carta d'identità elettronica: linee guida e metodologia per la redazione del piano». Per allegato B «Regole tecniche e di sicurezza per l'accesso ai domini applicativi del C.N.S.D.».

Articolo 2 - Adempimenti

1. I Comuni devono, entro il 31 ottobre 2005, provvedere a redigere il piano di sicurezza per la gestione delle postazioni di emissione secondo le regole tecniche fornite dal Ministero dell'Interno, in applicazione dell'art. 7-vicies ter, comma 2, della legge n. 43 del 31 marzo 2005.

Articolo 3 - Allegati

1. L'allegato A «Piano di sicurezza comunale per la carta di identità elettronica: linee guida e metodologia per la redazione del piano» e l'allegato B «Regole tecniche e di sicurezza per l'accesso ai domini applicativi del C.N.S.D.» formano parte integrante e sostanziale del presente decreto.

Articolo 4 - Funzioni dei comuni

1. I Comuni, nel rispetto delle regole tecniche e di sicurezza di cui all'allegato A, devono redigere il Piano di sicurezza comunale per la carta d'identità elettronica.
2. I Comuni, nel rispetto delle regole tecniche e di sicurezza di cui all'allegato B, devono predisporre i necessari collegamenti all'Indice Nazionale delle Anagrafi (INA) presso il Centro Nazionale per i Servizi Demografici tramite porta di accesso ai domini applicativi del C.N.S.D., entro il 31 ottobre 2005.

Articolo 5 - Redazione del piano di sicurezza comunale

1. I Comuni, ai fini della redazione del piano di sicurezza per la gestione delle postazioni di emissione della carta di identità elettronica, attuano la seguente procedura operativa:
 - a. nomina del responsabile comunale per la sicurezza degli accessi al C.N.S.D.;
 - b. redazione del Piano di sicurezza comunale per la C.I.E.;

- c. il Piano di sicurezza comunale per la C.I.E. deve essere sottoposto all'approvazione della Prefettura-UTG.

Articolo 6 - Collegamento al C.N.S.D.

1. Le amministrazioni e gli enti che, ai sensi della normativa vigente, esercitano funzioni e svolgono compiti nell'ambito delle procedure di produzione, trasmissione, formazione, rilascio, rinnovo, aggiornamento e relativa verifica della C.I.E. si connettono al Centro Nazionale per i Servizi Demografici tramite apposita porta di accesso, secondo le regole tecniche e di sicurezza di cui all'allegato B al presente decreto. Per l'attivazione del collegamento al C.N.S.D., le amministrazioni di cui al presente comma attuano la seguente procedura operativa:
 - a. attivazione e gestione delle «quantità di sicurezza, certificazione ed attivazione» fornite dal Ministero dell'Interno;
 - b. predisposizione ed attivazione della porta di accesso;
 - c. predisposizione ed attivazione dei sistemi comunali per l'accesso ai servizi applicativi del C.N.S.D.;
 - d. attivazione del collegamento all'INA tramite porta di accesso;
 - e. attivazione del collegamento tramite porta di accesso per l'emissione C.I.E.

Capo II - Norme procedurali

Articolo 7 - Nomina del responsabile comunale per la sicurezza degli accessi al C.N.S.D.

1. Il Sindaco è il Responsabile comunale per la sicurezza degli accessi al C.N.S.D. e può delegare formalmente tale incarico ad un funzionario comunale ritenuto idoneo ai sensi dell'art. 2 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223. L'atto di nomina è trasmesso al Ministero dell'Interno e alla Prefettura-UTG, secondo le modalità indicate sul sito, entro il 31 agosto 2005.
2. Per i comuni che hanno provveduto alla nomina del «responsabile del comune autorizzato all'attivazione del servizio di connessione al backbone applicativo Indice Nazionale Anagrafi» si intende che lo stesso assume anche il ruolo di responsabile comunale per la sicurezza degli accessi al C.N.S.D. a meno che non venga comunicato dal Sindaco un diverso nominativo entro il 31 agosto 2005.
3. All'atto della nomina il responsabile comunale per la sicurezza degli accessi al C.N.S.D. firma l'impegno alla riservatezza.
4. Il sindaco vigila sull'attività del delegato inviando semestralmente una relazione sull'operato del responsabile comunale per la sicurezza alla Prefettura-UTG.
5. Il Ministero dell'Interno provvede ad inviare al Sindaco le «quantità di sicurezza, certificazione ed attivazione» necessarie a:
 - a. abilitare la porta di accesso del Comune;

- b. predisporre ed attivare i sistemi comunali per l'accesso ai servizi applicativi del C.N.S.D.;
 - c. attivare il collegamento all'INA tramite porta di accesso del Comune;
 - d. attivare il collegamento per l'emissione C.I.E. tramite porta di accesso del Comune.
6. Il Sindaco consegna al responsabile comunale per la sicurezza degli accessi al C.N.S.D. le «quantità di sicurezza, certificazione ed attivazione» per gli adempimenti di competenza.
 7. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D., ricevute le «quantità di sicurezza, certificazione ed attivazione», è responsabile della corretta attivazione della porta di accesso del Comune e di tutti i sistemi comunali che accedono ai servizi applicativi del C.N.S.D. (sistemi per i servizi INA, sistemi per emissione C.I.E., etc.).

Articolo 8 - Redazione piano di sicurezza comunale

1. Il piano di sicurezza comunale deve essere redatto, in conformità alle regole tecniche e di sicurezza di cui all'allegato A, ed inviato, in formato digitale e cartaceo, ai fini della approvazione, alla Prefettura-UTG entro il 31 ottobre 2005. Successivamente il piano di sicurezza comunale deve essere aggiornato con cadenza semestrale.

Articolo 9 - Approvazione piano di sicurezza comunale

1. Il piano di sicurezza comunale è emanato dal Sindaco che è responsabile della sua applicazione e della sua custodia in sicurezza presso la propria «segreteria atti riservati». Il piano di sicurezza viene trasmesso alla Prefettura-UTG, tramite CD-ROM, recante la firma indelebile del Sindaco e creato secondo le modalità previste dalla «quantità di sicurezza, attivazione e certificazione», in busta sigillata tramite ceralacca del Comune e consegnato per mezzo di messo comunale.
2. La Prefettura-UTG valuta, entro trenta giorni dalla consegna, il Piano di sicurezza comunale per la C.I.E. secondo i criteri forniti dal Ministero, con apposita verifica, ed esprime un parere, che può essere:
 - a. di approvazione totale;
 - b. di approvazione parziale: la Prefettura-UTG indica le modifiche da apportare al piano della sicurezza;
 - c. di non approvazione.
3. In caso di approvazione parziale, il Comune è tenuto a rivedere il piano di sicurezza in base alle osservazioni effettuate dalla Prefettura-UTG. Il piano di sicurezza con le modifiche effettuate deve essere quindi nuovamente sottoposto alla Prefettura-UTG, con allegata la lista di verifica delle modifiche effettuate, per l'approvazione.
4. In caso di mancata approvazione il Comune è tenuto a rivedere il piano di sicurezza in base alle osservazioni effettuate dalla Prefettura-UTG e completare le eventuali parti mancanti. Il piano di sicurezza con le modifiche effettuate deve essere quindi nuovamente sottoposto alla Prefettura-UTG per l'approvazione.

5. Qualora il piano di sicurezza comunale non venga redatto nei termini stabiliti dal presente decreto o non sia riveduto in caso di approvazione parziale, il prefetto, previa diffida, esercita i poteri sostitutivi previsti dalla normativa vigente.
6. La Prefettura-UTG custodisce i piani di sicurezza comunali e ne trasmette una copia al C.N.S.D., in formato digitale, tramite la porta di accesso della prefettura-UTG.
7. la Prefettura-UTG svolge funzioni di vigilanza sulla corretta applicazione del piano di sicurezza. A tal fine devono essere pianificate apposite visite ispettive.
8. Il Comune, ai fini dell'emissione C.I.E., deve rendere operativo il Piano di sicurezza comunale per la carta di identità elettronica approvato dalla Prefettura-UTG entro e non oltre il 31 dicembre 2005.
9. Il Comune aggiorna, ogni sei mesi, il piano di sicurezza comunale e invia le variazioni alla Prefettura-UTG unitamente alla lista di verifica delle modifiche effettuate per l'approvazione. La Prefettura-UTG trasmette gli aggiornamenti al C.N.S.D. tramite la porta di accesso della Prefettura-UTG.
10. Al fine di verificare la piena corrispondenza con le dotazioni autorizzate dal Ministero dell'interno, prima della attivazione del piano di sicurezza il sindaco fa l'inventario delle «quantità di sicurezza, attivazione e certificazione», della porta di accesso comunale e delle postazioni C.I.E. con i relativi software, redigendo apposito verbale che, costituendo parte integrante del piano di sicurezza, verrà trasmesso unitamente allo stesso alla Prefettura-UTG.
11. Eventuali interventi modificativi o integrativi delle componenti software e hardware di cui al precedente comma, dovranno essere preventivamente autorizzati dal Ministero.
12. Le richieste di modifica o integrazione e le relative autorizzazioni devono essere conservate in originale secondo le modalità del successivo art. 10.

Articolo 10 - Quantità di sicurezza, attivazione e certificazione

1. Le «quantità di sicurezza, attivazione e certificazione» sono fornite dal Ministero dell'interno, protette da opportune credenziali, al Sindaco su supporto tecnologico-informatico di archiviazione che contiene i seguenti elementi:
 - a. credenziali digitali per l'identificazione univoca del Comune;
 - b. strumenti di sicurezza (agenti di controllo monitoraggio e allarme, certificati digitali, dotazioni di servizio) richiesti per l'attivazione della porta di accesso;
 - c. strumenti di sicurezza (certificati digitali, dotazioni di servizio) richiesti per l'attivazione delle postazioni comunali autorizzate all'accesso ai servizi applicativi del C.N.S.D. tramite porta di accesso;
 - d. strumenti di sicurezza (agenti di controllo monitoraggio e allarme, certificati digitali, dotazioni di servizio) richiesti per l'attivazione delle postazioni C.I.E.
2. Il Comune, prese in carico le «quantità di sicurezza, attivazione e certificazione», deve provvedere alla loro custodia in sicurezza, in coerenza con il Piano di sicurezza comunale per la C.I.E.

3. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D., dopo apposita denuncia alle competenti autorità di polizia, deve immediatamente comunicare alla Prefettura-UTG ed al Ministero dell'Interno qualsiasi avvenimento che comprometta la sicurezza delle «quantità di sicurezza, attivazione e certificazione», quali smarrimento, furto o manomissione del relativo supporto tecnologico-informatico di archiviazione, tramite immediata comunicazione al call center del C.N.S.D.

Articolo 11 - Attivazione della porta di accesso ai domini applicativi del C.N.S.D.

1. La porta di accesso del Comune ai domini applicativi del C.N.S.D. identifica il punto di accesso autorizzato, presente presso la struttura comunale, che consente la fruizione in sicurezza dei servizi erogati dal C.N.S.D. stesso. La porta di accesso certifica quindi il punto di origine delle comunicazioni, individuando univocamente il Comune che, tramite la porta di accesso, si collega al C.N.S.D. Nessuna altra modalità di comunicazione è quindi possibile tra Comune e C.N.S.D. Ciascun Comune deve dichiarare la porta di accesso che utilizza per le comunicazioni con il C.N.S.D., con modalità telematiche che saranno pubblicate sul sito del Ministero.
2. La procedura di attivazione di una porta di accesso deve essere effettuata dal responsabile comunale per la sicurezza degli accessi al C.N.S.D. utilizzando le credenziali e le «quantità di sicurezza, attivazione e certificazione» fornite dal Ministero dell'interno. La procedura operativa si articola nelle seguenti fasi:
 - messa a disposizione delle componenti hardware conformi alle regole tecniche e di sicurezza indicate dal Ministero, riportate nell'allegato B al presente decreto, e pubblicate nel sito;
 - configurazione dell'infrastruttura di rete comunale secondo le regole tecniche e di sicurezza indicate dal Ministero, riportate nell'allegato B al presente decreto, e pubblicate nel sito;
 - attivazione, a cura del responsabile della sicurezza, e nel rispetto delle regole di sicurezza del C.N.S.D., della porta di accesso. L'attivazione consta delle seguenti fasi:
 - a. abilitazione della porta di accesso tramite «quantità di sicurezza, attivazione e certificazione», attivazione del canale Backbone del C.N.S.D., attivazione degli agenti di controllo monitoraggio e allarme, predisposizione del certificato digitale server per il colloquio secondo standard SSL (Secure Socket Layer) con i sistemi comunali;
 - b. registrazione, presso il C.N.S.D., della porta di accesso tramite «quantità di sicurezza, attivazione e certificazione»;
 - c. verifica, sulla base della lista fornita con le «quantità di sicurezza, attivazione e certificazione», che sulla porta di accesso sia presente tutto il software autorizzato e necessario e che non sia presente software non necessario e non autorizzato. A seguito della verifica viene compilato il verbale di cui al comma 10 dell'art. 9. A garanzia del funzionamento in sicurezza della porta, il software autorizzato viene firmato tramite certificati digitali forniti con le «quantità di sicurezza, attivazione e certificazione» al fine di impedirne qualsiasi

manomissione. Una porta su cui sia presente software non autorizzato non viene considerata abilitata alle sue funzioni e quindi qualsiasi operazione effettuata tramite la stessa è da considerare a tutti gli effetti una violazione della sicurezza;

- d. prova di comunicazione, effettuata tramite dotazione di servizio fornita, della porta di accesso in termini di sicurezza e di dimensionamento dei flussi di comunicazione con il C.N.S.D.
3. Alla conclusione delle suddette fasi il Ministero dell'Interno - C.N.S.D. certifica la porta di accesso in funzione dei risultati della prova di cui al punto precedente. Farà seguito una comunicazione di certificazione che perverrà al Comune sulla medesima porta di accesso.
4. Alla corretta conclusione delle fasi sopra descritte, la porta di accesso si ritiene attivata e, quindi, è ritenuta un punto di accesso al C.N.S.D. riconosciuto ed autorizzato. La porta di accesso rappresenta il punto di presa in carico delle comunicazioni provenienti dal Comune relative ai flussi di aggiornamento INA e di emissione della C.I.E. e trasmissione al C.N.S.D., tramite Backbone, di tali comunicazioni in apposita «busta di e-gov» creata dalla porta stessa secondo le specifiche del Sistema Pubblico di Connettività.
5. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D. deve controllare la corretta attivazione della porta di accesso, secondo le regole tecniche e di sicurezza riportate nel presente decreto.
6. Presso ogni Comune, entro il 30 settembre 2005, deve essere attivata una porta di accesso del Comune. Per i piccoli comuni, se l'unica postazione presente è la postazione attualmente usata per l'invio dei dati AIRE su Backbone AIRE, la stessa deve essere utilizzata, previa attivazione secondo la procedura descritta nel presente articolo, come porta di accesso del Comune mantenendo anche le attuali funzioni svolte per l'AIRE.
7. La porta di accesso della Prefettura-UTG ai domini applicativi del C.N.S.D. identifica il punto di accesso autorizzato, presente presso la Prefettura-UTG, che consente l'accesso, in sicurezza, ai servizi erogati dal C.N.S.D. stesso. Presso ogni Prefettura-UTG, entro il 31 ottobre 2005, deve essere attivata una porta di accesso della Prefettura-UTG.

Articolo 12 - Abilitazione dei sistemi anagrafici comunali ai servizi applicativi del C.N.S.D.

1. I sistemi comunali devono accedere ai servizi del C.N.S.D. esclusivamente tramite la porta di accesso. La procedura per l'attivazione di un sistema anagrafico comunale è la seguente:
 - a. abilitazione e registrazione del sistema comunale alla porta di accesso per lo specifico servizio applicativo del C.N.S.D. tramite «quantità di sicurezza, attivazione e certificazione»: dal supporto tecnologico-informatico, di cui all'art. 8, fornito dal Ministero dell'interno vengono scaricati sul sistema comunale i certificati digitali client forniti per l'abilitazione alla comunicazione, secondo standard SSL, del sistema comunale stesso con la porta di accesso;
 - b. prova di comunicazione, effettuata tramite dotazione di servizio fornita, relativa alla corretta configurazione e funzionamento dei canali di comunicazione. Le relative regole tecniche e di sicurezza di dettaglio sono riportate nell'allegato B al presente decreto.

2. Al termine delle fasi sopra descritte, il sistema comunale si ritiene attivato e, quindi, è autorizzato ad inviare le informazioni (secondo protocollo XML SOAP o Post HTTP XML) alla porta di accesso che crea la busta di e-gov e la trasmette automaticamente, tramite Backbone, al servizio applicativo del C.N.S.D. per cui è stata effettuata l'attivazione.
3. I formati XML per la comunicazione tra sistema comunale e porta di accesso sono forniti dal Ministero dell'interno.
4. I sistemi comunali che accedono ai servizi del C.N.S.D. devono essere registrati presso la porta di accesso.
5. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D. ha il compito di controllare l'attivazione e la registrazione dei sistemi comunali, secondo le reali esigenze.
6. I livelli di sicurezza relativi ai sistemi e ai prodotti della porta di accesso sono certificati, sulla base degli standard internazionali, dal Ministero dell'interno.

Articolo 13 - Attivazione del collegamento all'INA

1. I sistemi comunali utilizzati per l'accesso all'INA, devono essere attivati per l'accesso al servizio INA del C.N.S.D., tramite porta di accesso, entro e non oltre il 31 ottobre 2005, coerentemente con il disposto dell'art. 7-vicies ter della legge n. 43 del 31 marzo 2005.
2. I formati XML che devono essere utilizzati per inviare le interrogazioni INA e gli aggiornamenti INA, sono forniti e pubblicati dal Ministero dell'Interno sul sito.

Articolo 14 -Emissione CIE

1. Le postazioni C.I.E. devono accedere ai servizi del C.N.S.D. e, attraverso questo, a SSCE esclusivamente tramite porta di accesso. Le postazioni C.I.E. possono essere:
 - a. postazioni C.I.E. di «Front office» deputate all'acquisizione dei dati anagrafici dei richiedenti e alla consegna e attivazione della C.I.E.;
 - b. postazioni C.I.E. di Back Office per l'allestimento della C.I.E. deputate alla predisposizione e stampa dei supporti C.I.E. sulla base dei dati anagrafici acquisiti al Front office;
 - c. postazioni C.I.E. di Back Office per l'elaborazione e le comunicazioni di informazioni con il C.N.S.D. e, attraverso questo, con il SSCE;
 - d. postazioni C.I.E. che integrino due o più delle tipologie precedenti.
2. Per qualsiasi tipologia di postazione C.I.E. deve essere seguita la seguente procedura di attivazione:
 - a. abilitazione della postazione C.I.E. tramite «quantità di sicurezza, attivazione e certificazione»;
 - b. registrazione, da effettuarsi prima della installazione del software di emissione C.I.E., della postazione C.I.E. sulla porta di accesso tramite «quantità di sicurezza, attivazione e certificazione»; a seguito di tale registrazione viene assegnato automaticamente un identificativo univoco alla postazione di emissione che la abilita

- all'emissione della C.I.E. e che viene utilizzato per tutte le comunicazioni con il Ministero dell'Interno ed il circuito di emissione della C.I.E.;
- c. attivazione degli agenti di controllo, monitoraggio e allarme forniti dal Ministero dell'Interno e del software di emissione C.I.E.;
 - d. installazione e attivazione del software di emissione C.I.E.;
 - e. verifica, sulla base della lista fornita con le «quantità di sicurezza, attivazione e certificazione», che sulla postazione C.I.E. sia presente tutto il software autorizzato e necessario e che non sia presente software non necessario e non autorizzato. A seguito della verifica viene compilato il verbale di cui al comma 10 dell'art. 9. A garanzia del funzionamento in sicurezza della postazione C.I.E., il software autorizzato viene firmato tramite certificati digitali forniti con le «quantità di sicurezza, attivazione e certificazione» al fine di impedirne qualsiasi manomissione. Una postazione C.I.E. su cui sia presente software non autorizzato non viene considerata abilitata alle sue funzioni e quindi qualsiasi operazione effettuata tramite la stessa è da considerare a tutti gli effetti una violazione della sicurezza;
 - f. prova, effettuata tramite dotazione di servizio fornita, della corretta configurazione dei canali di comunicazione.

Le relative regole tecniche e di sicurezza di dettaglio sono riportate nell'allegato B al presente decreto.

3. Al termine delle fasi sopra descritte, la postazione C.I.E. si ritiene attivata e, quindi, è autorizzata ad inviare i flussi relativi all'emissione C.I.E. alla porta di accesso. Tramite porta di accesso sono garantiti i servizi di sicurezza per l'accesso ai sistemi distribuiti di verifica dello stato dei certificati C.I.E.
4. Le regole tecniche e di sicurezza di cui agli allegati A e B al presente decreto devono essere rispettate anche dagli eventuali centri di allestimento periferici che potrebbero essere costituiti per la stampa della C.I.E.

I Sindaci dei Comuni presso i quali saranno costituiti i centri di allestimento dovranno nominare il responsabile del centro di allestimento per la sicurezza degli accessi al C.N.S.D.

5. Il Ministero dell'Interno controlla e verifica il rispetto dei vincoli di sicurezza relativi all'intero processo di emissione C.I.E. avvalendosi anche delle proprie infrastrutture tecnologiche di controllo, monitoraggio e allarme.
6. Il responsabile comunale per la sicurezza degli accessi al C.N.S.D., ha il compito di controllare l'attivazione e la registrazione delle postazioni C.I.E.
7. I livelli di sicurezza relativi ai sistemi e ai prodotti del circuito di emissione della C.I.E. sono certificati, sulla base degli standard internazionali, dal Ministero dell'interno.

Roma, 2 agosto 2005

Allegato A

LINEE GUIDA E METODOLOGIA PER LA REDAZIONE DEL PIANO

Scopo e campo di applicazione (Pagine 17-24)

INDICE

1. Scopo e campo di applicazione pag. 17
2. Riferimenti pag. 18
3. Definizioni e acronimi pag. 19
4. Introduzione pag. 20
5. Obiettivi pag. 21
6. Principi generali pag. 21
 - 6.1. Responsabilita pag. 22
 - 6.2. Revisione ed adeguamento del piano pag. 22
 - 6.3. Vincoli pag. 22
7. Uso degli allegati e risultati attesi pag. 22
8. La metodologia utilizzata per l'attuazione del piano della sicurezza pag. 23

Allegato 1

RIFERIMENTI NORMATIVI E REGOLAMENTARI (Pagine 27-32)

Pag. 25

Pag. 26 (Pagina bianca)

Pag. 27

pag. 28

pag. 29

pag. 30

pag. 31

pag. 32

INDICE

1. Descrizione delle norme relative alla «sicurezza» pag. 27
 - 1.1. Ambiti relativi alla sicurezza pag. 27
 - 1.2. La sicurezza nell'ITC (Tecnologie dell'Informazione e della Comunicazione) pag. 27

- 1.3. Il contesto internazionale pag. 28
 - 1.3.1. Applicare le BS7799 pag. 29
 - 1.3.2. Composizione delle norme BS7799 pag. 29
- 1.4. Il contesto nazionale pag. 30
- 1.5. Prospetto sintetico delle norme e degli standard di riferimento pag. 31

Allegato 2

POLITICHE DI SICUREZZA E METODOLOGIA DI ATTUAZIONE DEL PIANO DELLA SICUREZZA (Pagine 35-52)

- 1. Ambito di applicazione del piano della sicurezza comunale pag. 35
- 2. Attuazione del piano della sicurezza comunale pag. 35
 - 2.1. Definizione piano di sicurezza versione alfa pag. 35
- 3. Descrizione dei macroprocessi di emissione ed uso CIE pag. 37
 - 3.1. Macroprocesso di caricamento dell'INA pag. 39
 - 3.2. Macroprocesso di emissione della CIE pag. 40
 - 3.3. Macroprocesso di uso della CIE pag. 44
- 4. Politiche di sicurezza pag. 45
 - 4.1. Politica e standard di sicurezza (Security Policy) pag. 46
 - 4.2. Organizzazione per la sicurezza (Security Organization) pag. 47
 - 4.3. Classificazione e Controllo delle risorse (Asset Classification and Control) pag. 47
 - 4.3.1. Inventario delle risorse pag. 48
 - 4.4. Sicurezza del personale (Personnel Security) pag. 48
 - 4.5. Sicurezza materiale e ambientale (Physical and Environmental Security) pag. 48
 - 4.6. Gestione dei sistemi e delle reti (Computer and Network Management) pag. 48
 - 4.7. Controllo degli accessi (System Access Control) pag. 49
 - 4.8. Sviluppo e manutenzione dei sistemi (System Development and Maintenance) pag. 50
 - 4.9. Gestione della continuità del servizio (Business Continuity Management) pag. 50
 - 4.10. Conformità (Compliance) pag. 52

Allegato 3

REDAZIONE DEL PIANO DI SICUREZZA VERSIONE ALFA: DEFINIZIONE STRUTTURA DI RIFERIMENTO, ANALISI E CLASSIFICAZIONE DELLE PROCEDURE OPERATIVE (Pagine 55-112)

- 1. Introduzione pag. 55

2. Come si utilizza questo allegato pag. 55
 - 2.1. Descrizione della struttura organizzativa, logistica e tecnologica di riferimento per l'emissione e l'uso della CIE pag. 56
 - 2.2. Descrizione dei macroprocessi di emissione ed uso CIE pag. 56
3. Struttura generale, modalità organizzativa e struttura logistica di riferimento per l'emissione e l'uso della CIE pag. 57
 - 3.1. Presentazione del Comune pag. 57
 - 3.2. Descrizione dei Macroprocessi di emissione ed uso della CIE pag. 57
 - 3.3. Descrizione degli uffici e dei servizi pag. 57
 - 3.4. Ruoli e figure professionali per l'emissione e l'uso della CIE pag. 59
 - 3.5. Descrizione dei dispositivi installati pag. 61
 - 3.6. Altre Informazioni sensibili per la sicurezza pag. 62
 - 3.6.1. Ubicazione dei servizi e degli uffici CIE negli immobili pag. 62
 - 3.6.2. Descrizione dell'infrastruttura di sicurezza per ciascun immobile rilevante ai fini della sicurezza CIE pag. 63
 - 3.6.3. Elenco del personale e sua assegnazione agli uffici pag. 64
4. Macroprocessi e relativi flussi informativi di emissione ed uso CIE pag. 65
 - 4.1. Il macroprocesso di caricamento dell'INA pag. 65
 - 4.1.1. Acquisizione delle «quantità di sicurezza, attivazione e certificazione» pag. 65
 - 4.1.2. Predisposizione Porta di Accesso ai domini applicativi del CNSD pag. 70
 - 4.1.3. Predisposizione ed attivazione dei sistemi comunali per l'accesso ai servizi applicativi INA del CNSD pag. 75
 - 4.1.4. Allineamento dei codici fiscali con gli archivi dell'Anagrafe Tributaria pag. 78
 - 4.1.5. Primo caricamento dell'Indice Nazionale delle Anagrafi pag. 84
 - 4.1.6. Aggiornamento continuo dell'Indice Nazionale delle Anagrafi pag. 87
 - 4.2. Il macroprocesso di emissione CIE pag. 90
 - 4.2.1. Nomina del responsabile della sicurezza CIE pag. 91
 - 4.2.2. Predisposizione delle Postazioni di Emissione pag. 92
 - 4.2.3. Attivazione delle Postazioni di Emissione ai servizi applicativi di emissione CIE del CNSD pag. 93
 - 4.2.4. Acquisizione delle quantità di sicurezza pag. 95
 - 4.2.5. Acquisizione delle CIE inizializzate pag. 98
 - 4.2.6. Rilascio CIE ai cittadini pag. 100
 - 4.3. Il macroprocesso di uso della CIE pag. 109
 - 4.3.1. Abilitazione di una postazione di lavoro al riconoscimento in rete dei cittadini che accedono tramite CIE ai servizi comunali pag. 110

- 4.3.2. Abilitazione di un server comunale per l'identificazione in rete dei cittadini che accedono tramite CIE ai servizi in rete del Comune pag. 111

Allegato 4

SCHEDE DI ATTUAZIONE DELLA VERSIONE ALFA DEL PIANOSICUREZZA DEI COMUNI: CLASSIFICAZIONE MINACCE, VULNERABILITÀ E VALUTAZIONE DEL RISCHIO (Pagine 115-176)

Allegato 5

MONITORAGGIO E VALIDAZIONE DEL PIANO (176-181)

pag. 177

pag. 178 (Pagina bianca)

pag. 179

pag. 180

pag. 181

1. Introduzione pag. 115
2. Schede di classificazione delle minacce e delle vulnerabilità pag. 115
3. Minacce e vulnerabilità pag. 170
 - 3.1. Minacce pag. 170
 - 3.2. Vulnerabilità pag. 173
4. Valutazione del rischio pag. 176
 - 4.1. Modalità di compilazione ed uso della tabella di valutazione del rischio pag. 176
5. Trattamento del rischio pag. 178
6. Attuazione dei trattamenti pag. 180
7. Definizione delle procedure operative pag. 180
 - 7.1. Modulo di definizione e descrizione delle procedure operative pag. 181
 - 7.2. Procedure operative obbligatorie pag. 182

Allegato 6

MANUTENZIONE ED EVOLUZIONE DEL PIANO (183-190)

1. Descrizione delle attività pag. 193
 - 1.1. Variazioni della struttura organizzativa, logistica e tecnica pag. 193
 - 1.2. Analisi e classificazione dei processi interessati pag. 194

1.3. Classificazione minacce, vulnerabilità e valutazione del rischio pag. 195

1.4. Variazioni delle procedure operative pag. 197

Allegato 7

DOCUMENTO OPERATIVO PER I COMUNI AI FINI DELLA COMPILAZIONE DEL PIANO DI SICUREZZA (191-195)

pag. 191

pag. 192 (pagina vuota)

pag. 193

pag. 194

pag. 195

1. Introduzione pag. 201
2. Indice Piano di Sicurezza pag. 201

Allegato B (Pagine 201-212)

REGOLE TECNICHE E DI SICUREZZA PER L'ACCESSO AI DOMINI APPLICATIVI DEL CNSD

INDICE

1. Introduzione pag. 201
2. Attivazione Porta di accesso ai domini applicativi del CNSD pag. 202
 - 2.1. Requisiti hardware e software di base pag. 203
 - 2.2. Requisiti di connettività della Porta di accesso ai domini applicativi del CNSD pag. 204
3. Accesso al dominio applicativo INA del CNSD pag. 207
 - 3.1. Accesso al dominio applicativo INA del CNSD - Requisiti di connettività tra sistemi comunali e Porta di accesso ai domini applicativi del CNSD pag. 208
4. Accesso al dominio applicativo CIE del CNSD pag. 209
 - 4.1. Accesso al dominio applicativo CIE del CNSD - Requisiti di sicurezza e connettività tra sistemi CIE e Porta di accesso ai domini applicativi del CNSD pag. 211