Ministero dell'Interno

Dipartimento per gli Affari Interni e Territoriali
Direzione Centrale per i Servizi Demografici

UNIVERSITA' DEGLI STUDI DI ROMA TorVergata
LABORATORIO nestor

Implementazione della sicurezza

Linee guida per i Comuni

Indice

1. Introduzione

Questo documento fornisce un insieme di linee guida organizzative per i Comuni come supporto nella progettazione e realizzazione del proprio piano di sicurezza per l'attuazione della seconda fase del progetto CIE. Tali linee guida sono definite sulla base:

- dell'architettura di sicurezza del backbone INA_SAIA;
- dell'architettura di sicurezza del Sistema di Sicurezza del Circuito di Emissione;
- della direttiva (denominata direttiva Stanca) 16 gennaio 2002 del Dipartimento per l'innovazione e le tecnologie, sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni;
- dello standard BS 7799 (ISO 17799) – Code of Practice for Information Security Management;

Nell'ambito di ciò che si definisce sicurezza si è soliti comprendere quattro settori specifici:

1. Norme funzionali relative ai prodotti, aventi come scopo principale la ricerca della interoperabilità dei sistemi informatici
2. Criteri di valutazione dell'assurance, ossia della fiducia riponibile nella sicurezza realizzata da sistemi e prodotti informatici
   - TC SEC (Applicato in USA)
   - IT SEC (Applicato in Europa)
   - ISO/IEC 15408 (Common Criteria – evoluzione ed integrazione di entrambi)
3. Norme relative al sistema di gestione della sicurezza
   - ISO 9000 (solo di riflesso – Analisi del rischio)
   - ISO/IEC TR 13335 (parti 1, 2, 3, 4)
   - BS 7799 parte1 – Code of practice
   - BS 7799 parte2 – Verifica

- ISO/IEC 17799 (che recepisce la parte 1 delle BS7799

4. Norme legali

- Legge 675/96
- DPR 318/99
- Altre leggi e direttive nazionali ed europee.

2. Gli elementi dei piano di sicurezza

Sono definiti tre aspetti fondamentali relativi alla sicurezza delle informazioni:

1. **Confidenzialità:** solo gli utenti autorizzati possono accedere alle informazioni necessarie.
2. **Integrità:** protezione contro alterazioni o danneggiamenti; tutela dell'accuratezza e completezza dei dati.
3. **Disponibilità:** le informazioni vengono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

Si considerano primari i due concetti di **politica di sicurezza** e di **sistema di governo della sicurezza** (di cui la prima costituisce uno degli aspetti) nonché dalla specificazione dei controlli di sicurezza (logici, fisici, procedurali) necessari per farla rispettare e del modo in cui questi devono essere realizzati, secondo un approccio simile a quello degli standard della serie ISO9000 per la certificazione di qualità. I concetti di politica di qualità e di sistema di gestione della qualità sui quali tali serie si basa, sono sostituiti da quelli di politica di sicurezza dell'informazione e di sistema di governo della sicurezza dell'informazione o ISMS (Information Security Management System).

La politica di sicurezza è la specificazione ad alto livello degli obiettivi di sicurezza (espressi, come di consueto in termini di volontà di salvaguardare la riservatezza, l'integrità e la disponibilità dell'informazione in presenza di minacce) che l'organizzazione si propone di conseguire.

L'ISMS, invece, è il complesso di procedure per il governo della sicurezza attuato e mantenuto dall'organizzazione per garantire nel tempo il soddisfacimento della politica di sicurezza.

3. Controlli di sicurezza

Dallo standard BS7799 si ricavano un insieme di 127 controlli raggruppati nelle seguenti dieci categorie:

1. Politica di sicurezza
2. Organizzazione per la sicurezza
3. Controllo e classificazione delle risorse
4. Sicurezza del personale
5. Sicurezza materiale e ambientale
6. Gestione operativa e comunicazione
7. Controllo degli accessi
8. Sviluppo e manutenzione dei sistemi
9. Gestione della business continuità
10. Conformità

Nell'insieme dei 127 controlli previsti vanno selezionati, attraverso un processo di analisi del rischio, quelli che soddisfano le esigenze di protezione dell'organizzazione. I controlli prescelti costituiscono una sorta di regolamento di sicurezza che l'organizzazione si impone di rispettare. Tali controlli devono essere realizzati: attraverso meccanismi hardware o software (sistemi di autenticazione tramite password e/o smart-card, sistemi di autenticazione delle postazioni di accesso ai servizi, prodotti per la protezione crittografica dei dati, firewall, sistemi di controllo attacchi, ecc.), nel caso dei controlli attuati mediante misure di sicurezza di tipo tecnico; attraverso l'installazione di sistemi anti-intrusione, telecamere, casseforti, contenitori ignifughi, ecc. nel caso dei controlli che richiedono misure di sicurezza fisiche; attraverso la creazione di apposite strutture o cariche e la definizione di precise procedure per la messa in atto dei controlli di tipo procedurale (ad esempio l'istituzione del forum interorganizzativo per la gestione della sicurezza dell'informazione, l'affidamento dell'incarico di indottrinamento periodico del personale, le procedure per l'accettazione di visitatori all'interno della sede dell'organizzazione, ecc.).

Inoltre, in base al contenuto dell'art. 5 del DPR 318/99 risulta evidente come debbano essere individuati i "singoli elaboratori" tramite cui vengono effettuati trattamenti di dati personali (comma 2 art. 5 DPR 318/99) e risulta evidente la necessità di conoscere l'accoppiata elaboratore-codice identificativo per evitare che con lo stesso identificativo utente si possa accedere da più postazioni alla stessa fonte informativa (comma 6 art. 5 DPR 318/99).

L'unione di queste due esigenze (la conoscenza della postazione e il controllo dell'univocità dell'accoppiata postazione-identificativo personale) trova la sua risposta nel modello di funzionamento del Backbone in quanto quest'ultimo implementa il concetto di autenticazione "forte", tramite la soluzione della porta applicativa e del client backbone in grado di individuare univocamente sia la postazione di accesso, sia l'utente che richiede l'accesso in rete.

3.1. Politica di sicurezza (Security Policy)

Gli obiettivi sono: fornire le direttive di gestione e supporto per le informazioni di sicurezza

Il Comune deve definire quali sono i principi di massima e gli elementi portanti della sicurezza interna. Questo significa porre in una scala gerarchica gli elementi di maggior interesse e criticità circa la sicurezza.

In prima analisi questi elementi possono ricondursi ai dati che il comune raccoglie e gestisce, quali i dati anagrafici dei cittadini e i dati relativi alla fiscalità comunale in genere, la custodia dei supporti cartacei e quelli digitali anche in riferimento alla documentazione di base del comune come fogli filigranati, bolli, carte di identità in bianco, ecc.

Una particolare cura deve essere posta nel trattamento dei dati anagrafici necessari al primo caricamento dell'INA.

3.2. Organizzazione per la sicurezza (Security Organization)

Gli obiettivi sono:

- controllare la sicurezza delle informazioni in seno all'organizzazione
- gestire la sicurezza delle funzioni di elaborazione di informazioni organizzative e le informazioni disponibili accedute da terze parti
- gestire la sicurezza delle informazioni quando la responsabilità dell'elaborazione dell'informazione è stata richiesta esternamente ad un'altra organizzazione

Il Comune deve definire e istituire, all'interno della struttura, una organizzazione che si occupi di sovrintendere e controllare i processi e le attività legate alla sicurezza.

In particolare il Comune deve indicare il resposabile della postazione/i SSCE, il responsabile delle comunicazioni, il responsabile della Porta Applicativa di accesso al CNSD (in tal caso o l'ufficiale di anagrafe o un funzionario da lui delegato).

3.3. Controllo e classificazione delle risorse (Asset Classification and Control)

Gli obiettivi di questa sezione sono: gestire una appropriata protezione delle risorse e garantire che le risorse informative ricevano un livello adatto di protezione

Il Comune deve fornire informazioni su tali risorse, in particolare, in questo ambito le risorse possono essere:

- Sistemi informativi centrali
- Sistemi informativi periferici
- Sistemi di networking tra le varie sedi (intranet, internet)
- Postazioni di lavoro
- Punti accesso multimediali aperti al pubblico

3.4. Sicurezza del personale (Personnel Security)

Gli obiettivi sono:

- ridurre il rischio di errori umani, furto, frode o uso improprio delle strutture dell'organizzazione
- accertarsi che gli utenti interni siano informati sulle minacce alla sicurezza delle informazioni e siano formati a sostenere le politiche di sicurezza del Comune nel corso della propria attività lavorativa
- minimizzare il danno per incidenti e malfunzionamenti circa la sicurezza e mettere a frutto l'esperienza di avvenimenti precedenti.

Il Comune deve condurre un'analisi tesa ad individuare il personale direttamente coinvolto nelle attività legate alle informazioni da proteggere (i dati delle CIE, i certificati di sicurezza, …), siano esse in formato digitale che cartaceo. Deve essere resa evidenza di

politiche di accesso alle informazioni con la tracciatura delle richieste di accesso e delle operazioni effettuate.

Un'attività parallela è quella della formazione del personale sulle questioni della sicurezza mettendo in evidenza i fattori di garanzia per il personale stesso che la gestione della sicurezza consente di acquisire.

3.5. Sicurezza materiale e ambientale (Physical and Environmental Security)

Gli obiettivi sono:

- impedire l'accesso non autorizzato, il danneggiamento e l'interferenza all'interno del flusso delle informazioni del "business"
- impedire perdita, danni o i beni del sistema e la interruzione delle attività economiche
- impedire la manomissione o il furto delle informazioni

Il Comune deve rendere evidenza di aver adottato sistemi informatici in grado di garantire funzionamenti anche in caso di guasti improvvisi prevedendo ad esempio apparati "fault tolerant". Non di meno devono essere previsti ambienti adatti sia dal punto di vista dell'accesso che dal punto di vista di eventi gravi quali incendi, inondazioni ecc. per garantire la corretta conservazione delle informazioni.

In particolare, le postazioni SSCE e la Porta Applicativa, in quanto elementi di comunicazione di dati sensibili verso l'Amministrazione Centrale, devono essere posizionati in ambienti protetti.

3.6. Gestione operativa e comunicazione (Computer and Network Management)

Gli obiettivi sono:

- assicurare il corretto e sicuro funzionamento delle funzioni di elaborazione delle informazioni
- minimizzare il rischio di guasti dei sistemi
- proteggere l'integrità del software e delle informazioni
- gestire l'integrità e la disponibilità dei processi di elaborazione dell'informazione e della comunicazione

- garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture di supporto
- prevenire i danni ai servizi e le interruzioni alle attività economiche
- evitare la perdita, modifica o abuso delle informazioni scambiate tra le organizzazioni

La sicurezza in questo ambito può essere gestita da parte del Comune adottando politiche di separazione dei sistemi SSCE e Porta Applicativa dagli altri sistemi informativi comunali attraverso l'uso di soluzioni tecniche (firewall, router, …) che consentano il controllo delle comunicazioni.

3.7. Controllo degli accessi (System Access Control)

Gli obiettivi sezione sono:

- controllare l'accesso alle informazioni
- prevenire l'accesso non autorizzato ai sistemi di informazione
- assicurare la protezione dei servizi in rete
- prevenire l'accesso non autorizzato al calcolatore
- rilevare attività non autorizzate
- garantire la sicurezza delle informazioni quando sono utilizzate dalle postazioni mobili in servizi di rete e telematici

Il Comune deve definire tabelle gerarchiche dei permessi di accesso ai sistemi SSCE e Porta Applicativa, prevedendo certificazioni sia delle eventuali postazioni di lavoro usate per l'accesso automatico a tali sistemi (SIC – Sistema Informativo Comunale) sia del personale incaricato dell'attività.

In questo ambito sono da prevedere sistemi di documentazione degli accessi che consentano anche la segnalazione immediata di anomalie riscontrate.

Si ricorda di prestare una particolare attenzione alla protezione dei dati anagrafici nelle fasi del primo caricamento dell'INA, essendo queste ultime svolte in coordinamento con altre amministrazioni.

3.8. Sviluppo e manutenzione dei sistemi (System Development and Maintenance)

Gli obiettivi sono:

- garantire che la sicurezza è costruita in sistemi in funzione
- prevenire la perdita, modifica o cattivo utilizzo dei dati nei sistemi applicativi
- proteggere la riservatezza, autenticità e integrità dell'informazione
- assicurare che i progetti informatici e le attività di supporto siano condotte in modo sicuro
- gestire la sicurezza del software e dei dati di sistema

Il Comune, ai fini della corretta gestione di questa fase deve realizzare procedure organizzative che consentano di installare solo software autorizzati e con la metodica pulizia dei sistemi con gli ormai noti sistemi di prevenzione da virus, trojan ecc.. Inoltre deve essere impedito l'uso dei sistemi comunali da parte di operatori non autorizzati.

Questi accorgimenti vanno attuati su tutte le macchine che si trovano nella stessa rete della postazione SSCE e della Porta Applicativa di accesso al CNSD.

3.9. Gestione della business continuità (Business Continuità Planning)

Gli obiettivi sono di contrastare le interruzioni delle attività di servizio e dei processi sdi servizio critici, dagli effetti di malfunzionamenti o disastri principali

Per una corretta gestione del governo delle informazioni il Comune deve garantire la continuità dei servizi basati sull'uso della CIE erogati al cittadino sia nei casi diretti (fornitura di informazioni agli sportelli) che indiretti (informazioni date tramite altre amministrazioni, fornitura di servizi su rete Internet, …).

3.10. Conformità (Compliance)

Gli obiettivi sono:

- Garantire il rispetto delle leggi civili, penali, obblighi statutari, regolamentari o contrattuali e di qualsiasi requisito di sicurezza
- assicurare la conformità dei sistemi con criteri e standard di sicurezza organizzativi

- aumentare l'efficacia e minimizzare le interferenze verso e dal processo di controllo del sistema

La legislazione italiana a proposito è stringente soprattutto per tutto ciò che riguarda la gestione della privacy che in un ambito della pubblica amministrazione comunale è intesa sia come gestione della privacy per tutti i dati che riguardano i cittadini (dati anagrafici, dati sugli immobili, dati sulle controversie tra cittadini e la stessa pubblica amministrazione), con riguardo agli stessi dipendenti dell'amministrazione per tutto quello che concerne ad esempio le posizioni lavorative, l'accesso alle informazioni e le responsabilità sulle operazioni amministrative. Allo stesso modo è necessario garantire la privacy per quelle transazioni tra amministrazioni prevedendo la fornitura di dati strettamente necessari alle operazioni richieste e preservando l'accesso a quelle non utili nel singolo contesto.