Ministero dell'Interno

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

Vademecum per il

Modello di Monitoraggio della sicurezza

Sezione 1

1. Introduzione

Questo documento fornisce un insieme di linee guida organizzative per i Comuni 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

   - Decreto legislativo 30 Giugno 2003 n. 196 (Codice in Materia di Protezione dei dati Personali)

   - Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni: "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione", marzo 2004.

   - Legge 43/2005

   - Decreto legge 31 marzo 2005 n. 44 convertito nella legge 31 maggio 2005 n. 88

   - Regole tecniche e di sicurezza per l'accesso ai domini applicativi del CNSD

   - 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 alla vigente normativa devono essere individuati i "singoli elaboratori" tramite cui vengono effettuati trattamenti di dati personali e conosciuta l'accoppiata elaboratore-codice identificativo per evitare che con lo stesso identificativo utente si possa accedere da più postazioni alla stessa fonte informativa.

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.

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.

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

Gli obiettivi di questa sezione sono: gestire un'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, 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 di accesso ai domini applicativi del CNSD, 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

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

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

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.

3.9. Gestione della business continuità (Business Continuity Planning)

Gli obiettivi sono di contrastare le interruzioni delle attività di servizio e dei processi di 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

Sezione 1
Definizione del Piano di Sicurezza

Domanda 6
Verificare se il trattamento dei dati personali è conforme a quanto previsto dall'*Art. 35, lett. b, c, del Dlgs196_2003 (*accessi alle stanze con documenti riservati*).*

Domanda 8 – 9 - 12
Verificare la conformità con quanto prescritto dalla Direttiva del 16 gennaio 2002 del Ministro per l'Innovazione e le Tecnologie.

Domanda 12
Verificare se il trattamento dei dati personali è conforme a quanto previsto dall'*Art. 34, lett. f, g del Dlgs196_2003 (*trattamenti con strumenti elettronici).

Domanda 13
Verificare se il trattamento dei dati personali è conforme a quanto previsto dall'*Art. 34, lett. d, e, g del Dlgs196_2003 (*accessi alle stanze con documenti riservati*).*

Domanda 14
Verificare se il trattamento dei dati personali è conforme a quanto previsto dall'*Art. 34, lett. d, e, f, g del Dlgs196_2003 (*accessi alle stanze con documenti riservati*).*

Domanda 16
Verificare se il trattamento dei dati personali è conforme a quanto previsto dall'*Art. 34, lett. f, g del Dlgs196_2003 (*trattamenti con strumenti elettronici).
Domanda 19
Verificare se il trattamento dei dati personali è conforme a quanto previsto dall'*Art. 34, lett. f, g del Dlgs196_2003 (*trattamenti con strumenti elettronici).

Sezione 2
Operatività Piano di Sicurezza

SICUREZZA ORGANIZZATIVA

Domanda1

Per apparecchiature informatiche si intendono qualsiasi apparecchiatura hardware (server, postazione di lavoro, stampante) in dotazione al comune.

Domanda 4
Gli eventi che incidono sulla sicurezza vanno registrati in modo contestuale. Verificare l'esistenza di documenti di rendicontazione periodica e l'effettiva registrazione di tali eventi.

Domanda 5
Verificare se il trattamento dei dati personali è conforme a quanto previsto dall' *Art. 34, lett. b,c, g del Dlgs196_2003 (*trattamenti con strumenti elettronici*).*

SICUREZZA FISICA

Domande 1—2-3-4-5-6-7-8
Verificare se le misure di sicurezza fisica sono conformi a quanto prescritto dall'Allegato 2 alla Direttiva del 16 gennaio 2002 del Ministro per l'Innovazione e le Tecnologie.

Domande 8
Verificare se il trattamento dei dati personali è conforme a quanto previsto dall'*Art. 35, lett. b,c Dlgs196_2003* (trattamento senza l'ausilio di strumenti elettronici*)*