PIANO OPERATIVO PER LE MISURE DI SICUREZZA MINIME IN ORDINE AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI

Adottato con deliberazione di G.C. n.1006 del 29/12/2000
Pubblicato all'Albo Pretorio il giorno 8/11/2001
Divenuto esecutivo il 18/01/2001

_____

Premessa

Per *Sistema Informativo Automatizzato* si intende il sistema costituito da risorse tecnologiche, dati applicazioni, risorse umane, regole organizzative e dalle procedure deputate all'acquisizione, memorizzazione, elaborazione, scambio, ritrovamento e trasmissione delle informazioni.

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dalla Pubblica Amministrazione per lo snellimento comporta una serie di nuovi rischi che, non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi dovuti all'affidabilità, cioè la non garanzia di corretto funzionamento sia nelle componenti hardware sia in quelle software, e all'esposizione alle intrusioni informatiche.

Occorre inoltre precisare che la sicurezza del Sistema Informativo Automatizzato non dipende solo da aspetti tecnici, ma anche, se non principalmente, da quelli organizzativi, sociali e legali.

Questo documento definisce il piano per la sicurezza dei sistemi informativi automatizzati che il Comune di Manfredonia ha adottato e intende adottare in base a quanto previsto dall'art. 15 della legge 31 dicembre 1996 n. 675; tale processo dovrà essere approfondito in considerazione della rapidità e della complessità dell'evoluzione tecnologica sopra indicata.

Con decreto del Sindaco n. 10 del 28/03/2000, protocollo n. 12707 è stata avviata la procedura per l'adozione delle misure minime di sicurezza con la quale i dirigenti del Comune di Manfredonia sono stati nominati "Responsabili del trattamento dei dati" .

Con provvedimento del Sindaco prot. n. 19487 del 19/05/2000 i Responsabili del trattamento dei dati sono stati invitati a nominare gli incaricati del trattamento dei dati, in base al modello dell'*allegato A.*

Con provvedimento del Segretario generale n.27504 i Dirigenti sono stati invitati ad individuare per il proprio settore di competenza un referente interno, che, coordinato dal CED, assicuri le operazioni connesse alla gestione informatizzata delle procedure.

La legislazione italiana relativa alla sicurezza informatica si basa sulle seguenti leggi fondamentali:

- Dlgs n° 518 del 1992 che modifica il regio decreto n° 633 del 1941, relativo al diritto d'autore, integrandolo con norme relative alla tutela giuridica dei programmi per elaboratore.
- Legge n° 547 del 1993 che modifica il codice penale italiano in tema di criminalità informatica introducendo i cosiddetti "computers crimes".
- Legge n° 675 del 31/12/1996 e successive modificazioni, che disciplina il trattamento dei dati personali.
- D.Lgs. 135/99, contenente le disposizioni integrative della Legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici.
- DPR 318/99 relativo all'adozione delle misure minime di sicurezza per il trattamento dei dati personali.
- Provvedimenti del Garante per la protezione dei dati personali
- Autorizzazioni del Garante per il trattamento dei dati sensibili

Lo sviluppo dei sistemi informatici e informativi espone l'Amministrazione, i suoi utenti e i propri responsabili a rischi di coinvolgimento sia penale che patrimoniale. Occorre, pertanto, adeguare le politiche di sicurezza cercando di limitare tali rischi, predisponendo, in ossequio alle norme vigenti, adeguate contromisure di carattere tecnico, organizzativo e normativo, anche tenendo presente la normativa in materia di semplificazione e trasparenza delle procedure d'accesso ai dati delle P.A. così come articolate nelle leggi:

- Legge 7 Agosto 1990 n° 241 – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Legge 15 Marzo 1997 n° 59 – Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa;

- Legge 15 Maggio 1997 n° 127 – Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e controllo;
- Legge 16 Giugno 1998 n° 191 – Modifiche ed integrazioni alle leggi n° 59 del 15/03/1997 e n° 127 del 15/05/1997, nonché norme in materia di formazione del personale dipendente e di lavoro a distanza nelle pubbliche amministrazioni.

Un Sistema Informativo Automatizzato viene definito sicuro se soddisfa le seguenti proprietà:

- *Disponbilità*: l'informazione ed i servizi che eroga devono essere a disposizione degli utenti del sistema compatibilmente con i livelli di servizio.
- *Integrità:* l'informazione ed i servizi erogati possono essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tale operazione.
- *Autenticità:* garanzia e certificazione della provenienza dei dati.
- *Confidenzialità o Riservatezza:* l'informazione che contiene può essere fruita solo dalle persone autorizzate a compiere tale operazione.

L'approccio globale alla sicurezza richiede di considerare gli aspetti tecnici (sicurezza fisica e logica), strategici (obiettivi e budget), organizzativi (definizione di ruoli, procedure, formazione), economici (analisi dei costi) ed infine legali (leggi e decreti, provvedimenti Garante Privacy).

In particolare si ritiene necessario verificare preliminarmente, ogni qual volta si debba trattare di sistemi sicuri, la validità, a livello generale, dei seguenti assunti:

tutti i componenti, hardware e software, devono garantire che ogni loro mal funzionamento o messa fuori operazione non comporti una diminuzione della sicurezza di esercizio, eventualmente anche attraverso una messa fuori uso della particolare stazione interessata;

le responsabilità dell'esercizio e dei controlli interni di sicurezza sono affidate a persone distinte e collocate nella struttura organizzativa in modo tale che in alcun modo il responsabile del personale possa influire sulla carriera/retribuzione del responsabile dei controlli interni di sicurezza;

sono adeguate le procedure per l'accertamento della qualità delle verifiche effettuate;

è sempre possibile individuare, inequivocabilmente, in un apposito "activity log file", l'autore di una qualsiasi operazione;

è garantita, al di là di ogni dubbio, l'integrità di questo log file e la sua disponibilità nel tempo per il periodo concordato;

è sempre possibile ripristinare il sistema di fronte a guasti od eventi, naturali o dolosi, allo stato in cui si trovava, prima del verificarsi dell'evento stesso, di un certo tempo concordato a priori tra le parti;

è garantita l'integrità del software, ad ogni livello, dal sistema operativo alle applicazioni, e dei relativi file di configurazione;

è convincente il programma dei test di penetrazione, sia interna che esterna, effettuati periodicamente, secondo la frequenza concordata;

sono adeguate le procedure per l'effettuazione delle varie operazioni di manutenzione e per il trattamento dei supporti di memorizzazione di massa obsoleti;

è conveniente il programma di accertamento della qualità dei controlli sull'aggiornamento continuo dell'hardware e del software, dal controllo della completa sincronizzazione delle versioni, aggiornate tempestivamente, dello stesso software all'aggiornamento delle varie "patches" distribuite dai fornitori per chiudere i vari "buchi", man mano che vengono scoperti.

Una struttura come quella del Comune di Manfredonia, si trova a dover risolvere il problema di trovare un equilibrio tra il livello di sicurezza accettabile e le disponibilità economiche dell'ente.

Va inoltre ricordato che una serie di leggi emanate in questi ultimi anni obbligano i fornitori e gli utenti di servizi informatizzati al rispetto di alcune regole e alla messa in opera di una serie di contromisure atte a prevenire o minimizzare i rischi di un incidente informatico. L'adozione di tali contromisure non è più lasciata alla discrezione delle singole Amministrazioni ma in alcuni casi è un obbligo di legge.

Obiettivi del presente documento

La sicurezza dei Sistemi Informativi Automatizzati è un requisito fondamentale per il corretto sviluppo dei programmi di automazione del Comune di Manfredonia ed è necessario che si realizzino le migliori condizioni di sicurezza al fine di garantire l'affidabilità delle informazioni trattate e l'efficacia ed efficienza dei servizi erogati.

Il presente documento programmatico in materia di sicurezza dei Sistemi Informativi Automatizzati ha l'obiettivo di:

incrementare la consapevolezza di rischi ed insidie che possono coinvolgere la gestione e l'utilizzo dei sistemi informativi automatizzati;

indicare possibili percorsi tecnici ed organizzativi di salvaguardia per prevenire situazioni di pericolo per le risorse e per chi se ne avvale, nonché affrontare e risolvere eventuali problemi insorgenti al verificarsi di eventi lesivi del patrimonio informativo;

stimolare lo sviluppo di strutture in grado di disegnare, pianificare, implementare e gestire misure di protezione corrispondenti alle esigenze degli specifici contesti di competenza;

incrementare l'utilizzo delle risorse informative disponibili su supporto informatico ed accessibili per via telematica con le imprescindibili garanzie di sicurezza.

Le soluzioni di sicurezza adottate e da adottare a tutela dei sistemi informativi automatizzati hanno l'obiettivo di:

assicurare la protezione degli interessi dei soggetti, pubblici e privati, che fanno affidamento sui sistemi informativi del Comune di Manfredonia;

evitare eventi pregiudizievoli che possano danneggiare disponibilità, riservatezza, e integrità del patrimonio informativo disponibile su sistemi di elaborazione e tramite reti di connessione telematica.

Il Processo della Sicurezza del Sistema Informativo Automatizzato

L'articolazione progettuale del Piano di Sicurezza prevede l'esecuzione delle seguenti attività:

- Analisi del Rischio
- Definizione delle Politiche di Sicurezza
- Gestione del Rischio
- Il Piano Operativo
- Formazione
- Organizzazione

L'esecuzione di tali attività consente da un lato di realizzare il sistema di sicurezza del Sistema Informativo Automatizzato e dall'altro di avviare un processo di gestione del sistema stesso caratterizzato dalla ciclicità

necessaria per il controllo e il mantenimento dei livelli di sicurezza nel tempo.

Il primo passo da compiere nella definizione di un piano di sicurezza è l'individuazione degli elementi del sistema informativo automatizzato che necessitano protezione e delle minacce a cui gli stessi possono essere sottoposti. Nello svolgimento di tale fase devono essere presi in considerazione tutti gli aspetti possibili senza trascurare il benché minimo dettaglio; ossia bisogna tenere sotto controllo ogni fattore, sia tecnologico che umano.

Anche se alcune cose sembrano ovvie è opportuno procedere ad una elencazione di tutte le possibili componenti che hanno un impatto con il problema sicurezza. Occorre analizzare inoltre anche le relazioni che le singole componenti hanno fra loro e, più in generale, con il resto dell'ambiente.

E' necessario, cioè, rappresentare e classificare non solo le componenti, ma come queste sono relazionate tra loro, sia fisicamente che logicamente, e definire un disegno completo del Sistema Informatico.

Portando avanti un processo di classificazione dei beni in funzione degli elementi di integrità, riservatezza e disponibilità, è possibile attribuire ai diversi beni un valore dipendente da una serie di scenari di impatto significativi ai fini della sicurezza.

La valutazione dei beni è indispensabile per capire la strategicità degli stessi all'interno del Sistema Informativo e per poter quindi successivamente valutare il livello di esposizione al rischio.

I criteri per la valorizzazione in linea di massima dovranno tener conto, pertanto, in ordine decrescente, di parametri quali:

- rischio per la sicurezza dell'Ente e/o dei cittadini
- interruzione di pubblico servizio
- alterazione di pubblico servizio
- sottrazione ed alienazione di patrimonio pubblico
- danneggiamento di patrimonio pubblico

Si procederà, quindi, ad una operazione di analisi del patrimonio informativo del Comune di Manfredonia in termini di dati e risorse elaborative.

I Dati

Iniziamo l'analisi specificando cosa si intende per "dati" e indicando quali sono le potenziali minacce a cui essi vengono esposti. Nel termine "dati" vengono convenzionalmente inclusi i seguenti elementi:

- il contenuto di archivi;
- il contenuto delle Basi di dati;
- i dati di transito;
- le copie storiche;
- i file di log.

Le minacce a cui i dati sono esposti sono legate alle debolezze dei sistemi operativi e delle applicazioni che operano sulle macchine su cui risiedono, e sono riconducibili a due categorie:

- l'accesso non autorizzato, cioè la possibilità per utenti esterni o interni di visualizzare informazioni riservate a particolari categorie di utenti;
- modifiche deliberate o accidentali, cioè da una parte la possibilità per utenti non autorizzati di modificare o cancellare dati a loro "non appartenenti", dall'altra errori commessi da utenti autorizzati che inavvertitamente procedono alla modifica o cancellazione di informazioni significative.

Ai fini delle politiche di sicurezza da adottare, si possono classificare tutte le tipologie di dati, che il Comune di Manfredonia può trovarsi a dover trattare, secondo le seguenti categorie:

- **Dati personali** (definizioni a livelli di sicurezza minimi riferiti alla legge n.675 sulla privacy) e dati esclusi all'accesso, come stabilito dalla legge e dal regolamento di accesso agli atti.
- **Dati sensibili** (definizioni e livelli di sicurezza minimi riferiti alla legge n.675 sulla privacy).
- Oltre a questa classificazione, si è deciso anche di distinguere gli archivi dati in due classi:
- **Archivi strutturati.** Tale tipologia possiede una precisa definizione dei dati in essa contenuti. Tali dati sono organizzati in record, tabelle, data base, secondo precise definizioni di campi (es.: nome, saldo, ecc.) e attributi (es.: campo chiave unica, campo non modificabile, ecc.).

I sistemi di accesso agli archivi strutturati sono costituiti da programmi specializzati (detti anche "procedure") che permettono di inserire, modificare, leggere e stampare le informazioni in essi contenute.

La proprietà dei dati è del titolare proprietario degli archivi, la responsabilità è del dirigente e del funzionario incaricato del loro trattamento, (livello apicale nell'ufficio).

L'amministrazione dei dati è dell'incaricato sotto il coordinamento del gestore informatico (CED) che detiene il sistema di sicurezza e i programmi di accesso previa autorizzazione del proprietario.

Il coordinamento è operato d'intesa con il soggetto esterno per i casi di esternalizzazione del servizio.

Le politiche di sicurezza di accesso e di conservazione dei supporti di salvataggio devono essere concordate tra proprietario e amministratori in base alla riservatezza e criticità dei dati.

Archivi non strutturati. Sono di fatto dei contenitori in cui è possibile caricare informazioni diversificate di cui a priori non è possibile predefinire un contenuto. Non sono strutturati, ad esempio, le cartelle di Windows, le caselle di posta elettronica, gli archivi di testo di un word processor.

La proprietà e la responsabilità dei dati è dell'utente; è dell'utente anche la responsabilità di amministrare i dati e applicare le necessarie politiche di sicurezza, non essendo possibile esercitare alcun controllo sulla criticità dei medesimi.

Le politiche di sicurezza sono stabilite dall'amministratore. Eventuali usi impropri degli archivi sono responsabilità dell'utente.

In virtù di questa premessa, la sicurezza dei dati può essere fatta derivare dalla corretta e accurata gestione delle seguenti quattro tipologie di risorse:

- Risorse hardware (dispositivi, documentazione cartacea, supporti di memorizzazione)
- Risorse software (sistemi operativi, software applicativo)
- Risorse logistiche (locali, linee di comunicazione)
- Risorse professionali (dipendenti, professionisti esterni, collaboratori)

Il CED del Comune di Manfredonia, con lo scopo di:

- classificare e valutare i beni gestiti
- valutare le minacce e la vulnerabilità di tali beni
- individuare l'esposizione al rischio

- analizzare il livello di sicurezza con cui gestisce i propri archivi di dati, ha deciso di avviare il censimento di tutte le postazioni di lavoro presenti nell'ente utilizzando un modello descrittivo in cui si analizzano tutte le caratteristiche principali delle diverse procedure relative all'erogazione dei servizi informatici del Comune.

Risorse Hardware

Rientrano in questa categoria i personal computer, le stampanti, i disk drive, le linee di comunicazione, la rete interna, i server, dispositivi di *back-up* dei dati.

La manutenzione sulle singole stazioni di lavoro viene garantita per un periodo di tre anni dal momento dell'acquisto ed è intenzione dell'Amministrazione garantire assistenza oltre tale periodo mediante un contratto con ditte specializzate.

Il *back-up* dei dati è una procedura attraverso la quale viene periodicamente effettuata una copia di tutti i dati presenti nel sistema su dispositivi opportuni. In caso di guasto hardware dei dischi è quindi possibile "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo *back-up*. Il *back-up* viene effettuato periodicamente, in base alle necessità e la gestione dei supporti è tale da scongiurare i disastri derivanti da cause fisiche (incendi, distruzione di locali, ecc.): le copie sono conservate in luoghi differenti dal PC dal quale i dati vengono copiati, ed è nelle intenzioni dell'amministrazione la volontà di utilizzare una apposita cassaforte ignifuga in locali diversi da quelli in cui sono collocate le macchine.

Le principali minacce a cui i dispositivi hardware sono sottoposti sono:

mal funzionamenti dovuti a guasti o sabotaggi

mal funzionamenti dovuti a eventi naturali quali allagamenti e incendi

furti e intercettazione (tale minaccia riguarda gli apparati di rete, cioè le linee di comunicazione, i router e i server; è infatti possibile effettuare il monitoraggio indebito o l'alterazione della trasmissione di dati effettuata da questi apparati, sia che questa avvenga tra terminali, tra computer, tra stazioni di lavoro periferiche e sistemi centrali di elaborazione).

deterioramento nel tempo;

inaffidabilità del mezzo fisico che in alcuni casi può presentare difetti di costruzione che ne compromettono il buon funzionamento nel tempo;

evoluzione tecnologica e del mercato;

mancata documentazione sulla serie storica dei supporti di memorizzazione;

modalità e i luoghi di conservazione delle copie storiche.

Sicurezza delle apparecchiature hardware

La sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione e di condizionamento. Anche la manutenzione dell'hardware rientra in questa area, come anche la protezione da manomissioni e furti.

Un'iniziativa potrebbe essere quella di decidere di collocare tutti i server in uno o più ambienti aventi le caratteristiche già menzionate nella stesura di questo documento.

Allo stato attuale, si ritiene utile richiamare l'attenzione sui locali in cui sono collocati i server affinché:

siano impartite disposizioni atte a garantire il rispetto delle condizioni minime (es.: chiusura degli ingressi al locale del server, e, più in generale, maggiore attenzione alla chiusura degli accessi all'edificio).

responsabilizzazione del personale sui rischi legati alla presenza di uno o più server all'interno dei propri uffici.

Nell'eventualità in cui tali aspetti minimi non fossero rispettati, dovrà essere presa in considerazione la possibilità di far controllare i locali da soggetti esterni addetti al controllo degli accessi.

L'architettura di rete del Comune di Manfredonia

Esistono diverse reti locali che mettono in collegamento i dipendenti appartenenti a ogni singolo settore o servizio consentendo loro di accedere ad archivi e procedure informatizzate indispensabili per il loro lavoro.

Per dare attuazione alle misure di sicurezza è in atto un programma per la realizzazione di una rete unica attraverso un cablaggio strutturato fonia/dati, per consentire la completa integrazione dei servizi comunali.

Buona parte dei servizi comunali è attualmente collegata in rete, tramite piccole LAN per consentire la condivisione degli archivi. Le principali reti locali sono le seguenti:

- *rete dei servizi demografici:* è costituita da circa 20 nodi e permette la condivisione degli archivi per la gestione dei servizi demografici.
- *rete del protocollo:* è costituita da circa 15 nodi e permette la condivisione degli archivio del protocollo, per consentire agli uffici del I settore la protocollazione e la visualizzazione degli atti dell'ufficio protocollo.
- *rete ufficio tributi*: è costituita da circa 8 nodi e permette la condivisione degli archivi per la gestione di tutti i tributi comunali
- *rete contabilità*: è costituita da circa 8 nodi e permette la condivisione degli archivi per la gestione della contabilità
- *rete rilevazione presenze:* è costituita da 5 nodi e permette la condivisione degli archivi per la gestione degli archivi del personale dipendente.

Gli accessi provenienti dall'esterno sono permessi solo per i casi di assistenza ai software gestionali da parte di ditte specializzate, nei confronti delle quali sono state adottate misure di sicurezza in base a quanto previsto dalla legge, nominando *Incaricati al trattamento dei dati* i tecnici a cui viene permesso l'accesso alle banche dati.

La maggior parte delle postazione è dotata di password di avvio, inoltre per quanto riguarda i software di rete è prevista una singola password per ogni utente per l'accesso agli archivi in rete.

La gestione delle password, dove è possibile, viene delegata all'utente; in caso contrario, il CED assegna all'utente un codice individuale di accesso al servizio non modificabile senza previa richiesta di autorizzazione. L'orientamento è comunque quello di tendere ad una completa autonomia dell'utente in merito a possibili variazioni delle password, il tutto a tutela della propria privacy nell'ambiente di lavoro.

La sicurezza delle reti di telecomunicazione

La sicurezza della rete deve principalmente garantire da un lato l'utilizzo della risorsa trasmissiva ai soli utenti autorizzati e nelle specifiche modalità abilitate, e, dall'altro, che i dati contenuti in una comunicazione non possano essere:

- divulgati o alterati nel momento appena precedente al loro invio ad un destinatario

- intercettati (attivamente o passivamente) quando sono trasmessi sui mezzi trasmissivi, compromettendo la loro integrità e/o riservatezza
- conosciuti da utenti non autorizzati quando giungono a destinazione.

Controllo del traffico di rete

Il controllo degli accessi alla rete deve avere l'obiettivo di garantire che la rete sia utilizzata esclusivamente dall'utenza autorizzata e nelle modalità definite dai profili di abilitazione (ovvero quali servizi di rete è possibile abilitare e come).

Risorse Software

Rientrano in questa categoria i Sistemi Operativi e Software di Base (utility, diagnostici), Software Applicativi, Gestori di basi di dati, Software di rete, i programmi in formato sorgente e oggetto.

L'elenco di tutte le risorse software, ridefinito e aggiornato ai fini dell'adempimento di quanto previsto dal DPR 318/99, è conservato presso il CED.

Le minacce principali legate all'uso di questi prodotti sono:

- la presenza di errori involontari commessi in fase di progettazione e/o implementazione che consentono ad utenti non autorizzati l'esecuzione di operazioni e programmi riservati a particolari categorie di utenti;
- la presenza di codice insidioso inserito volontariamente dai programmatori dell'applicazione stessa, al fine di poter svolgere operazioni non autorizzate sul sistema o per danneggiare lo stesso. Rientrano in questa categoria di minacce i virus, i trojan horse, le bombe logiche, le backdoor;
- attacchi sulla rete facilmente estendibili a un qualunque servizio. Si tratta di attacchi non distruttivi il cui obiettivo è saturare la capacità di risposta di un servizio con l'obiettivo ultimo di renderlo inutilizzabile agli altri utenti del sistema.

Particolare importanza ricoprono anche i formati sorgente delle applicazioni, che possono essere oggetto di furto per un'eventuale rivendita ad altre organizzazioni o di modifica per l'inserimento di codice insidioso.

Da quanto desumibile dall'elenco degli applicativi conservato al CED, i software in uso nelle stazioni di lavoro degli uffici del Comune di Manfredonia sono riconducibili a due categorie:

- software proprietario, cioè sviluppato dai tecnici del CED
- software acquistato sul mercato

I software proprietari sono procedure sviluppate con i prodotti di Microsoft Office, utilizzate solo su alcune postazioni di lavoro, come ad esempio il software di gestione del protocollo, gestione determinazioni, delibere e ordinanze.

Per quanto riguarda il software acquistato sul mercato il Comune di Manfredonia acquista i propri applicativi da ditte fornitrici di livello nazionale in grado di assicurare e garantire la buona qualità dei propri prodotti.

Un aspetto critico, collegato all'acquisto degli applicativi sul mercato, riguarda la disponibilità di avere dati in un formato fisico, non leggibile da altri sistemi, e logico senza l'esplicitazione delle relazioni tra i dati specialmente se codificati, ma comunque esportabili in formato standard solo da personale autorizzato.

Sicurezza Logica

La sicurezza logica è un componente particolarmente critico della sicurezza del sistema informativo.

Il campo di applicazione della sicurezza logica riguarda principalmente la protezione dell'informazione, e di conseguenza applicazioni, dati, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Le contromisure di sicurezza logica sono quindi da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.

Meccanismi di sicurezza: rappresentano le modalità tecniche attraverso le quali è possibile realizzare i servizi di sicurezza. ISO individua i seguenti meccanismi di sicurezza:

- cifratura
- firma digitale
- meccanismi per il controllo degli accessi
- integrità dei dati

- meccanismi per l'autenticazione
- saturazione del traffico in rete
- controllo instradamento
- notarizzazione

La definizione dell'architettura di sicurezza logica deve rispondere ai seguenti punti:

- Quali funzioni di sicurezza devono essere garantite e per quali beni?
- Con quali meccanismi di sicurezza è conveniente realizzare tali funzioni?
- In quali livelli dell'architettura del sistema informatico devono essere collocati i diversi meccanismi?

Il controllo degli accessi ai sistemi di elaborazione

Il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informativo avvengano esclusivamente secondo modalità prestabilite. Il controllo accessi può essere visto come un sistema caratterizzato da soggetti (utenti, processi) che accedono a oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione). Funzionalmente è costituito da:

Un insieme di politiche e di regole di accesso che stabiliscono le modalità (lettura, aggiornamento, ecc.) secondo le quali i vari soggetti possono accedere agli oggetti;

Un insieme di procedure di controllo (meccanismi di sicurezza) che controllano se la richiesta di accesso è consentita o negata, in base alle suddette regole (validazione della richiesta).

Per garantire quanto sopra esposto, è indispensabile prevedere un meccanismo che costringa ogni utente ad autenticarsi (cioè dimostrare la propria identità) prima di poter accedere ad un calcolatore; il meccanismo sinora più usato a tale scopo è quello delle password. Si concede all'utente una coppia user-id e password al livello del sistema operativo e/o per ogni applicazione (di solito in numero limitato) al cui accesso quell'utente è abilitato. Si arriva molto presto alla constatazione che il meccanismo delle password non è però sufficientemente adeguato a garantire il livello di sicurezza richiesto nella fase di autenticazione. I problemi principali legati all'uso delle password sono: la scelta di password estremamente facili da indovinare da parte degli utenti e la possibilità di intercettarle quando transitano in rete.

Per far fronte a questi problemi sono stati individuati dei meccanismi di autenticazione forte, che consentono di rendere molto più sicura una qualunque fase di autenticazione. Tali meccanismi sono basati sul riconoscimento di un attributo posseduto dall'utente. Tale attributo può essere:

- una caratteristica fisica quale l'impronta digitale, la forma della mano, l'iride, la retina, o una caratteristica comportamentale quale la firma, la voce; in questo caso parliamo di dispositivi di autenticazione biometrici;
- una password generata dinamicamente da un apposito dispositivo personalizzato per ogni utente;
- un certificato digitale che attesta l'identità dell'utente, solitamente memorizzato su smart card.

Considerati i costi che tali sistemi comportano e l'assenza di una tecnologia già affermata, si ritiene adeguato il controllo degli accessi effettuato secondo le modalità già descritte. Si ritiene comunque che, quando tali prodotti avranno raggiunto un rapporto costi/benefici favorevole, sarà utile prenderli in considerazione.

Antivirus

I computer virus sono i rappresentanti più noti di una categoria di programmi scritti per generare intenzionalmente una qualche forma di danneggiamento a un computer o ad una rete. Considerato che un virus informatico può dar luogo a:

- danni all'hardware
- danni al software
- danneggiamento ai dati (integrità)
- perdita di tempo impiegato a ripristinare le funzioni del sistema
- infezione di altri sistemi
- è necessario che le Amministrazioni attribuiscano la debita priorità all'adozione di iniziative a difesa attivando una protezione sistematica dei propri sistemi informatici e dei dati in essi custoditi e gestiti contro la minaccia rappresentata da virus.

Tali "programmi" sono in grado, senza alcun intervento dell'utente, di:

"infettare" altri programmi, cioè creare copie di sé stessi su altri programmi presenti nel sistema

insediarsi nella tabella di partizione e nel settore di boot del disco rigido, dove attende il verificarsi di un determinato evento per poter assumere il

controllo di alcune funzioni del sistema operativo, con il fine di svolgere azioni dannose per cui è stato programmato.

Inserire operazioni automatizzate (c.d. macroistruzioni) in documenti di testo, di archivio o di calcolo degli effetti indesiderati e nocivi.

Autoreplicarsi all'interno del sistema al fine di saturarlo.

Le azioni di danneggiamento possono andare dalla modifica del contenuto di alcuni file residenti sull'hard disk, alla completa cancellazione dello stesso; così come all'alterazione del contenuto del video o alla impostazione hardware della tastiera.

La miglior difesa contro i virus informatici consiste nel definire una architettura antivirus composta da regole comportamentali e da procedure operative, a protezione dell'intero sistema informatico.

Tutti gli utenti del sistema sono tenuti a conoscere e rispettare le regole emesse dall'Amministrazione e l'amministratore di sistema è tenuto a mantenere costantemente operative e aggiornate le procedure software predisposte.

Gli utenti, con frequenza mensile, aggiornano il proprio antivirus; dato l'elevato numero di utenti, diventa impensabile eseguire l'aggiornamento in modo centralizzato, così, ogni utente diventa responsabile di questo compito per la propria stazione di lavoro.

Controllo del software

Tra i principali punti di debolezza di un sistema informatico vanno sicuramente annoverati il sistema operativo e le applicazioni. Spesso, attraverso lo sfruttamento di errori presenti in questi programmi, un estraneo riesce a guadagnare un accesso al sistema. Le contromisure da adottare in questo caso sono essenzialmente di due tipi:

- l'aggiornamento costante dei prodotti non appena viene scoperto un bug che compromette la sicurezza del sistema; tale procedura è nota con il nome di patch;
- la verifica periodica dell'installazione e della configurazione dei prodotti software; un errore anche minimo in questa fase può trasformare un prodotto che dovrebbe contribuire a migliorare la sicurezza del sistema, come ad esempio un firewall, nel prodotto che compromette ogni misura.

Per il controllo del software applicativo ci si affida ai fornitori: si demanda a loro il monitoraggio e l'aggiornamento. Per i sistemi operativi

ci si affida al supporto di ditte specialistiche in quanto internamente non si dispone di professionalità adeguate da assegnare specificatamente al presidio di questo problema.

Strumenti per la disponibilità dei dati

I dati di un sistema sono sottoposti ad una serie di rischi che ne minacciano continuamente la disponibilità. Questi rischi vanno dai mal funzionamenti hardware agli atti di vandalismo perpetrati da intrusori informatici. E' possibile ridurre al minimo gli effetti, spesso disastrosi, di tali eventi, predisponendo meccanismi di back-up. Si tratta di una serie di procedure attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema su dispositivi opportuni. In caso di guasto hardware dei dischi è quindi possibile "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo back-up. Il problema principale in questo caso è legato al fatto che anche i dispositivi di back-up possono guastarsi.

La regola attualmente in uso è quella di fare copie giornaliere ruotando i nastri nell'arco di una settimana con archiviazione definitiva di una copia a fine mese. Per ogni server si intende predisporre un registro in cui l'addetto alle copie attesta l'effettuazione della copia segnalando eventuali anomalie.

Le Risorse Professionali

In questa categoria rientrano gli amministratori di sistema, i sistemisti, i programmatori, gli operatori, gli utenti finali, i manutentori hardware e software, i consulenti ecc.

Il Comune di Manfredonia deve necessariamente rivolgersi a personale specializzato esterno per assolvere ad alcune funzioni sistemistiche collegate alla gestione del software applicativo e di sistema.

Per quanto riguarda l'assistenza dei software acquistati all'esterno, ci si rivolge alle ditte fornitrici del software stesso, in quanto nella maggior parte dei casi si tratta di software proprietari.

Al personale degli uffici è affidata la procedura di backup dei dati.

Si avverte comunque la necessità di interventi da parte di personale specializzato affinché aumentino i vincoli e le garanzie in termini di sicurezza del sistema informativo.

Le Risorse logistiche

Appartengono a questa categoria i locali in cui sono conservati gli archivi dati e in cui sono collocati i macchinari e tutto il cablaggio che permette alla rete di funzionare.

È intenzione dell'Amministrazione inserire tra le risorse logistiche una cassaforte ignifuga, utilizzata per la conservazione delle copie di back up dei diversi archivi informatizzati; tale cassaforte potrà essere utilizzata anche da altri uffici comunali che hanno esigenza di conservare delle copie dati su supporti informatici.

Le principali minacce che possono interessare questo tipo di risorse sono:

- accessi fisici non autorizzati ai locali del Comune e delle sedi periferiche
- eventi naturali
- possibili danneggiamenti fisici ai cablaggi.

Valutazione delle Minacce e delle Vulnerabilità dei beni e definizione delle Politiche di Sicurezza

La situazione presente nel Comune di Manfredonia può essere riassunta nelle seguenti osservazioni:

- si sta svolgendo un'opera di continua sensibilizzazione dei dipendenti relativamente ad un corretto uso dei PC, affinché, per esempio, spengano la macchina quando si allontanano dalla postazione di lavoro, e scelgano password adeguate per l'accesso ai diversi servizi loro attivati.

Per i PC portatili esiste il pericolo del furto. A questo proposito, attraverso appositi apparati di controllo degli accessi si è in grado di disattivare immediatamente le password di abilitazione una volta sporta la denuncia di furto. Inoltre, con una mirata politica di sensibilizzazione, si sta cercando di istruire i dipendenti sui potenziali danni che possono inconsapevolmente arrecare alla rete comunale attraverso un incauto uso dei PC portatili.

Di fronte all'eventualità di guasti tecnici, il Comune si tutela stipulando dei contratti di manutenzione sia per i server che per il software;

Sulla possibilità che si manifestino errori umani si cerca di tutelarsi attraverso un'adeguata politica di formazione del personale e mediante il sistema di copie dei dati quotidiane.

La sicurezza deve essere considerata, inoltre, da tutti i dipendenti, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione.

Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

Le politiche di sicurezza si basano sul principio che le risorse informatiche (dati, risorse hardware, software, ecc.) sono un patrimonio che deve essere protetto dal momento in cui viene creato/installato, durante il suo utilizzo, fino al momento in cui viene distrutto. Inoltre devono essere portate a conoscenza (per le parti di pertinenza) delle società esterne (es. software house, consulenti, ecc.) che interagiscono con l'Amministrazione, le quali devono accettarne i contenuti ed impegnarsi a rispettarle.

Le politiche devono essere periodicamente aggiornate per riflettere eventuali nuovi indirizzi e/o evoluzioni e normative in materia di sicurezza.

Le politiche dovrebbero almeno considerare i seguenti aspetti:

- Classificazione delle informazioni: le informazioni, in qualsiasi forma esse si presentano (posta elettronica, archivi informatici, programmi, ecc.), devono essere protette con normative e misure tecniche commisurate all'importanza che esse rappresentano per l'Amministrazione (riservatezza, criticità, ecc.). Le politiche dovrebbero stabilire i criteri generali secondo i quali le informazioni dovrebbero essere classificate (es.: informazioni riservate o informazioni vitali per l'attività dell'Amministrazione, informazioni ad uso interno, dati personali o altri dati critici, informazioni non classificate). La stesura del presente documento programmatico ha favorito il censimento delle banche dati, effettuato tramite le schede procedura.

Protezione fisica delle risorse: l'obiettivo è la definizione di misure di sicurezza per la predisposizione e il mantenimento d un ambiente di lavoro protetto che impedisca perdite di informazioni e di patrimonio intellettuale di proprietà, promuova la protezione delle risorse informatiche presenti e la riduzione dei rischi di interruzione dei servizi informatici. Tale obiettivo viene raggiunto attraverso misure di controllo

crescenti, correlate ai rischi e al valore dei beni e delle informazioni presenti nell'ambiente. Ne fanno parte le seguenti componenti:

- La classificazione dei settori (es.: aree riservate, aree interne, aree pubbliche)
- L'accesso controllato alle aree considerate critiche
- La sicurezza fisica (impianti) e la sorveglianza di queste aree
- La tempestiva rilevazione di eventuali incidenti di sicurezza.

In definitiva per tutti i diversi casi occorre lavorare molto sulla formazione del personale; a ciò, per quanto riguarda gli ultimi due punti, va aggiunta la necessità di innalzare le barriere di protezione fisica acquistando i nuovi prodotti disponibili sul mercato.

Protezione logica delle informazioni: anche le misure di sicurezza logica dovranno essere commisurate al livello di classificazione delle informazioni. Ne fanno parte i seguenti aspetti:

- Il controllo degli accessi alle informazioni
- Il mantenimento della loro integrità e riservatezza
- La sicurezza nella trasmissione e nelle comunicazioni all'interno dell'Amministrazione e con l'esterno (Internet, altre Amministrazioni, ecc.).
- La sicurezza delle stazioni di lavoro e dei personal computer
- La sicurezza nel processo di sviluppo delle applicazioni informatiche
- La sicurezza nella gestione operativa delle installazioni informatiche
- La tempestiva rilevazione di eventuali incidenti di sicurezza

Nell'ambito del Comune di Manfredonia sono stati ben individuati i punti di accesso alla rete che, come già descritto, si possono sintetizzare in tre tipologie:

Utenti collegati fisicamente alla rete telematica tramite cablaggio interno di proprietà del Comune; per questa tipologia di utenti il livello fisico di protezione è adeguato.

Collegamento verso il mondo Internet; si tratta sicuramente di una situazione critica per la quale sono state individuate quelle soluzioni adeguate, riuscendo ad isolare in parte la rete interna dal mondo Internet.

Per le applicazioni sviluppate direttamente da alcuni dipendenti al di fuori del CED, questi dovranno attenersi alle politiche e alle indicazioni esposte nel presente documento programmatico

Norme per il personale: tutti i dipendenti concorrono alla realizzazione della Sicurezza, pertanto dovranno proteggere le informazioni assegnate loro per lo svolgimento dell'attività lavorativa nel rispetto di quanto stabilito dalle politiche almeno in termini di:

- Utilizzo delle risorse informatiche
- Accesso ai sistemi di dati
- Uso della password

Piano di continuità operativa: l'obiettivo è quello di garantire la continuità del servizio informatico e la disponibilità delle informazioni (aggiornate), evitando o limitando i danni al patrimonio informativo a fronte di una emergenza. A tale scopo dovrebbe essere previsto da ogni Amministrazione un Piano di Ripristino delle informazioni e delle operazioni che contenga gli aspetti organizzativi e normativi, le modalità e le risorse di back up necessarie (centro di calcolo, risorse hardware, software, personale, ecc.) alla ripresa delle attività a seguito di una emergenza che impedisca la normale erogazione del servizio informatico.

Gestione degli incidenti: i rischi informatici devono essere sempre costantemente controllati e monitorati. Devono essere definite le responsabilità e le modalità con cui gestire eventuali incidenti di sicurezza.

Sviluppo e manutenzione dei sistemi hardware e software utilizzati nel realizzare il piano di sicurezza. Occorre regolare le procedure con cui il software dovrà essere aggiornato e/o modificato e gli apparati sostituiti o riparati.

Gestione e formalizzazione delle procedure di raccolta e analisi delle transazioni e/o trasmissioni effettuate utilizzando il Sistema Informativo Automatizzato, nel caso in cui la normativa vigente preveda la possibilità di dispute legali che abbiano come oggetto di contesa queste operazioni.

L'applicazione delle Politiche di Sicurezza all'interno dell'Amministrazione richiede la definizione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, da divulgare all'interno dell'ente mediante una appropriata attività di formazione intena.

La sicurezza deve essere quindi vista in termini relativi come il "giusto" compromesso tra i "costi della sicurezza" ed i "costi della non sicurezza", frutto della ponderazione degli elementi precedentemente indicati.

Una volta definito il livello di sicurezza da raggiungere, e quindi il rischi residuo ritenuto accettabile, è possibile procedere all'individuazione della strategia di gestione del rischio.

Tale strategia dovrà contemplare le opportune indicazioni in relazione alle ipotesi di:

- Trasferimento del Rischio
- Abbattimento del Rischio

Per "trasferimento del rischio" si intende generalmente la sottoscrizione di polizze assicurative che possono coprire alcuni rischi generalmente legati alla distruzione fisica di sistemi. Tali polizze garantiscono una copertura finanziaria per i danni fisici ed i costi di riacquisto dei sistemi, ma non rappresentano certamente una copertura rispetto ai rischi di perdita di integrità, riservatezza e disponibilità del patrimonio informativo nel suo complesso.

Per "abbattimento del rischio" si intende l'adozione di un insieme di contromisure di natura fisica, logica ed organizzativa che possono fornire protezione in differenti maniere:

- Ridurre la minaccia
- Ridurre la vulnerabilità
- Ridurre l'impatto di eventi accidentali
- Rilevare un evento accidentale
- Aiutare nel ripristino di un evento accidentale

Il Piano Operativo

Definite quali sono le risorse da proteggere, le strategie di abbattimento del rischio ed il livello di rischio ritenuto accettabile si procede con la stesura del piano operativo

Questo piano operativo consente di determinare, tra l'insieme delle contromisure (funzioni di sicurezza) di natura fisica, logica ed organizzativa individuate, quali siano le più idonee, verificarne la fattibilità, stabilirne le priorità di attuazione valorizzandone le mutue interdipendenze per una copertura dei rischi sulla base degli obiettivi posti dalle politiche.

L'output sarà costituito da un piano operativo la cui esecuzione sarà regolata dalle priorità espresse dall'amministrazione e dai tempi relativi dell'evoluzione complessiva del sistema informativo.

Il piano conterrà l'individuazione dell'insieme delle attività di sviluppo della sicurezza.

Piano di Continuità Operativa

Il piano di continuità operativa rappresenta l'aspetto della sicurezza principalmente orientata a garantire la continuità e la disponibilità dei sistemi informativi automatizzati rispetto a danneggiamenti causati da eventi accidentali, sabotaggi, disastri naturali.

L'obiettivo del piano di continuità operativa è quello di ripristinare i servizi informatici entro un tempo prestabilito, in funzione dei livelli di servizio attesi, e di rendere minime le perdite causate dall'interruzione dell'attività.

Ciò vuol dire che il piano di continuità operativa non deve essere inteso come misura alternativa a quelle di prevenzione, ma a completamento di queste ultime, al fine di:

- garantire la continuità dei principali processi assicurando l'erogazione dei servizi essenziali
- limitare gli impatti degli eventi a carattere distruttivo sulla posizione finanziaria.

Il piano di continuità operativa si occupa del controllo delle interruzioni di operatività al fine di prevenirne e minimizzare l'impatto, individuando un insieme specifico di contromisure di sicurezza in grado di sostenere le operazioni critiche di missione istituzionale anche attraverso infrastrutture alternative.

Lo scopo è quello di raggiungere e mantenere un sistema di operazioni che risponda alle politiche della continuità, che quindi prevenga i rischi e, in caso di accadimento dell'evento distruttivo, ne limiti l'impatto sulla continuità dei servizi.

A tal fine sarebbe opportuno attivare un processo di sviluppo e mantenimento di specifici piani che includano misure di identificazione e riduzione del rischio orientate a limitare le conseguenze di un impatto dannoso e ad assicurare un rapido ripristino delle operazioni essenziali.

Il processo di pianificazione della continuità operativa dovrebbe essere visto come un quadro di riferimento per la gestione di più procedure di ripristino orientate a coprire scenari di impatto differenziati in relazione ai diversi eventi dannosi: dalla semplice caduta di alimentazione fino agli eventi catastrofici che richiedono un vero e proprio piano di disaster recovery.

La realizzazione del piano di continuità operativa si basa su contromisure di carattere sia tecnologico che organizzativo che indicano cosa fare, con

quali risorse e quali procedure seguire in condizioni di emergenza che rendano i sistemi informativi automatizzati parzialmente o totalmente indisponibili.

I principali aspetti tecnologici riguardano:

il sistema di continuità per l'alimentazione elettrica.

I server vengono alimentati con una batteria di continuità (UPS) che garantisce l'erogazione di energia elettrica per un tempo limitato, generalmente intorno ai quindici minuti, ma comunque sufficiente per l'effettuazione della chiusura automatica del sistema. Per quello che riguarda le singole stazioni di lavoro, esse non vengono protette da gruppi di continuità.

Il recupero dei supporti di back-up.

Su tutti i server è prevista un'unità di back-up per il salvataggio dei database e, dove occorre, anche della configurazione dei sistemi operativi. Presso il CED prossimamente sarà istituito ed attivato un registro delle copie, mentre, per tutti le postazioni collocate in posti differenti dal CED, sono state date indicazioni ai singoli responsabili dei relativi settori.

Verifica della sicurezza dei sistemi informativi automatizzati

La verifica dell'efficacia e della validità nel tempo delle misure di sicurezza adottate è un punto fondamentale per tutto il processo per la sicurezza dei sistemi informatici automatizzati.

Infatti in un contesto tecnologico in rapidissima evoluzione è necessario avere le massime garanzie circa l'adeguatezza delle misure di sicurezza adottate nei confronti del sempre più vasto, articolato ed aggiornato panorama delle possibili minacce.

Per quanto sopra, le attività di verifica dovranno consistere in due attività distinte, sia per compiti, che per organizzazione.

La prima – monitoraggio – è l'attività di verifica continua dell'efficacia delle misure di sicurezza realizzate, ed è effettuata, sotto la responsabilità della struttura che progetta e realizza le misure di sicurezza, durante la progettazione, implementazione ed esercizio delle misure stesse.

La seconda – audit di sicurezza – è un'attività di verifica effettuata da una struttura esterna alla struttura che ha implementato le misure di sicurezza, è potrà avvenire in modo estemporaneo e non prevedibile.

Si riporta, nel seguito, una breve descrizione dei contenuti delle attività sopra indicate.

Monitoraggio delle misure di sicurezza

E' necessario prevedere un controllo continuo delle misure di sicurezza. Tutto ciò per poter intercettare il più presto possibile eventuali attacchi ai danni del sistema, non previsti in fase di definizione delle contromisure o resi possibili da errori presenti o commessi in fase di installazione delle misure di sicurezza e degli apparati software e hardware ad esse collegati. Questa fase viene solitamente definita monitoraggio.

Il metodo principale per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei file di LOG, cioè quei file in cui i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono tutte le principali operazioni svolte dagli utenti per loro tramite.

Attraverso questa analisi, che nelle organizzazioni complesse deve essere necessariamente effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi di accesso al sistema riusciti, o meno, e l'esecuzione di operazioni sospette.

Audit delle misure di sicurezza

Definito il piano di sicurezza, ultimato il piano operativo ed emanate le norme comportamentali, è necessario verificare con periodicità fissa, ed inoltre con verifiche casuali non annunciate, che tutte le misure implementate, sia quelle tecnologiche che quelle organizzative, siano consistenti con gli indirizzi definiti nel piano operativo. Più precisamente si deve verificare che le misure tecnologiche implementate ed il loro effettivo dispiegamento svolgano correttamente le funzionalità per cui sono state adottata.

I test specifici di verifica delle misure tecnologiche possono essere effettuati con l'ausilio dei moderni sistemi automatizzati.

E' particolarmente importante affiancare a queste attività una serie di attacchi di tipo intrusivo (test di penetrabilità), che prevedono ad esempio tentativi esaustivi di individuazione delle password. E' utile per questi test l'impiego di professionalità che abbiano un'esperienza consolidata di penetrazione dei sistemi informatici, e che possano

operare sia dall'interno che dall'esterno del sistema informativo oggetto della verifica.

Per completare il quadro della sicurezza, non vi è dubbio circa l'importanza di attivare un sistema di monitoraggio e verifica adeguato. Questo comporta un consistente impegno economico e delle professionalità adeguate. Attualmente il Comune di Manfredonia non dispone delle risorse necessarie per poter attivare e gestire questo tipo di attività, e quindi ci si limita a dei controlli di tipo generico.

Introduzione e diffusione della cultura della sicurezza informatica nella Pubblica Amministrazione

Assicurare la miglior sicurezza dei sistemi informativi automatizzati presenta particolari problematiche d'ordine culturale, sociale ed organizzativo oltre che legale e tecnico, per questo è anche necessario elaborare ed attuare specifici processi di formazione, sensibilizzazione e corresponsabilizzazione.

La sensibilizzazione alle tematiche della sicurezza informatica ed a costanti comportamenti coerenti con le politiche e le disposizioni date in merito, deve interessare tutte le risorse umane dell'Amministrazione, anche quelle non direttamente interessate dalla formazione predetta, ad ogni livello di responsabilità ed attività.

Ciò al fine di diffondere una cultura generalizzata della sicurezza, che consenta tra l'altro di favorire la miglior efficacia ed efficienza delle misure prese oltre che di sopperire ad eventuali mancanze delle stesse.

Presentazioni, opuscoli, seminari, riunioni dei dirigenti e con i propri collaboratori, a solo titolo di esempio, possono rappresentare opportunità per raggiungere questo obiettivo.

Per la corresponsabilizzazione, si deve prevedere di:

- Coinvolgere i dirigenti e rappresentanze degli addetti in tutte le fasi di definizione del piano per la sicurezza (analisi e gestione dei rischi, politiche, piano operativo e audit);
- Effettuare interventi di richiamo e, se necessario, adottare gli adeguati provvedimenti disciplinari in caso di inadempienze e/o superficialità in tema di sicurezza informatica.
- Analoghi processi devono essere previsti con eventuali partner e collaboratori esterni, privati e pubblici, persone fisiche e giuridiche, che interagiscono in modo significativo con l'Amministrazione.

Formazione

L'introduzione di un sistema di sicurezza, come di qualunque altro elemento che modifichi le modalità lavorative all'interno di una qualsiasi realtà, ha sicuramente un forte impatto sull'organizzazione.

La formazione interviene in due momenti ben precisi del processo di introduzione di un sistema di sicurezza:

- Sensibilizzazione sulle problematiche della sicurezza e sulla loro importanza (vedi punto precedente)
- Conoscenza delle misure di sicurezza da adottare e da gestire ai diversi livelli di responsabilità
- Anche i fruitori della formazione saranno di diversa tipologia: è fondamentale riuscire a sensibilizzare i vertici dell'Amministrazione affinché si riesca a trasmettere i principi fondamentali del sistema all'interno delle loro realtà.
- Occorre quindi progettare tipologie distinte di sensibilizzazione a seconda dei destinatari: il primo, indirizzato alla direzione, deve prevedere cenni sulla normativa, indicazioni sulle politiche di sicurezza, analisi dei rischi; l'altro, indirizzato al personale operativo, deve fornire indicazioni precise sui comportamenti da adottare sia nelle operazioni quotidiane che nelle situazioni di emergenza.

Occorre progettare interventi in base alle diverse esigenze ed ai diversi sistemi di sicurezza sviluppati, in funzione del diverso patrimonio informativo da proteggere e dal diverso grado di informatizzazione raggiunto; in generale non potranno mancare riferimenti a:

- Normativa vigente
- Definizione delle responsabilità

Elenco delle vulnerabilità: spesso non c'è la consapevolezza dei rischi che si possono correre; vale quindi la pena individuare i punti di vulnerabilità del sistema, sia nell'ottica della prevenzione che nell'individuazione di possibili incidenti.

Regole comportamentali che comprendono:

- Gestione degli accessi (password,…)
- I possibili rischi: virus, intercettazioni, intrusioni,…
- Firma digitale

Audit dei sistemi di sicurezza: su questo argomento è necessario sensibilizzare il personale che dovrà affrontare le verifiche da parte di personale specializzato.

DESCRIZIONE GENERALE DELLE MISURE ADOTTATE PER LA SICUREZZA DEI DATI PER IL TRATTAMENTO NON AUTOMATIZZATO

Il Comune di Manfredonia, con lo scopo di classificare e valutare i beni gestiti, valutare le minacce a tali beni, individuare l'esposizione al rischio e analizzare il livello di sicurezza con cui gestisce i propri archivi, ha avviato il censimento di tutte le postazioni di lavoro presenti nell'Ente, utilizzando un modello descrittivo in cui si analizzano le procedure relative alla gestione degli archivi informatizzati e cartacei.

Dal procedimento, attualmente in corso di svolgimento, risulta che gli archivi cartacei contenenti dati sensibili vengono custoditi osservando le misure di sicurezza riportate nella seguente tabella:

Settore/servizio	Dati sensibili	Luogo di custodia
Servizi demografici	**Origine razziale ed etnica** **Opinioni politiche** **Abitudini sessuali** **Stato di salute**	**Armadi chiusi con chiave in possesso dell'incaricato.**
Servizi sociali	**Stato di salute** **Abitudini sessuali**	**Armadi e altri supporti chiusi con chiave in possesso dell'incaricato.**
Polizia locale	**Stato di salute**	**Armadi e classificatori chiusi con chiave in possesso dell'incaricato.**
Personale	**Stato di salute**	**Armadi e classificatori chiusi con chiave in possesso dell'incaricato.**
Trattamento sanitari obbligatorio	**Stato di salute**	**Armadi chiusi con chiave in possesso dell'incaricato.**
Archivio generale	**Vari**	**- Armadi chiusi con chiave in possesso dell'incaricato** **- Porta blindata**

Anche per quanto riguarda la conservazione dei dati personali si evince che la maggior parte degli incaricati utilizza supporti fisici che

garantiscono le misure minime di sicurezza per la riservatezza delle informazioni.

L'Amministrazione intende completare entro breve tempo l'attività di censimento per effettuare un'analisi completa sui criteri di custodia degli archivi e garantire interventi per fare in modo che siano osservate le norme corrette.

Inoltre, al fine di garantire il massimo interesse, i Responsabili del trattamento dati procederanno ad effettuare la formazione dei dipendenti incaricati del trattamento, e renderli edotti sui rischi possibili e sulle modalità per prevenire ogni danno.