COMUNE DI QUARRATA

Provincia di Pistoia

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

- anno 2009 -

Articoli 33-36 D.Lgs. 196 del 30/06/2003 («Codice della Privacy»)

SOMMARIO

Indice generale

1 GENERALITA'

Il D.Lgs. n. 196/2003, denominato «Codice della Privacy» (di seguito, "Codice"), sostituisce dal 1° gennaio 2004 la Legge n. 675/1996 in materia di **trattamento** dei dati personali. L'articolo 2050 del Codice Civile qualifica il trattamento dei dati come attività pericolosa.

Il Codice (Art. 2) garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità degli interessati, con particolare riferimento alla riservatezza, alla identità personale ed al diritto di protezione dei dati personali. Viene ribadito di verificare che le finalità del trattamento siano realizzate tramite l'utilizzo di dati anonimi o adeguate modalità che consentano di identificare l'interessato solo se indispensabili per il raggiungimento delle finalità consentite.

Il Codice detta una serie di regole e principi, che costituiscono una sorta di statuto di protezione della privacy. I dati personali devono essere:

- trattati in modo lecito e corretto;
- trattati per scopi chiari e leciti
- esatti e tenuti aggiornati;
- pertinenti e non eccedenti rispetto agli scopi per i quali sono stati raccolti (Art. 22, comma 5);
- trattati temporaneamente, cioè non oltre il periodo di tempo necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati.

Devono essere adottate **obbligatoriamente** opportune **misure di sicurezza** attraverso mezzi e strumenti di protezione, al fine di garantire l'integrità dei dati ed escludere gli accessi non autorizzati.

Il Codice prevede l'obbligo – sanzionato – di adozione di misure di sicurezza da parte del titolare del trattamento; in particolare:

- gli articoli 33-36 attengono alle **misure minime** di sicurezza
- l'articolo 31 fa invece riferimento all'adozione di **misure di sicurezza idonee**.

Tale differenza non è solo terminologica, ma anche di ordine sostanziale:

- le misure minime sono individuate dal disciplinare tecnico (allegato B al Codice) e devono essere adottate obbligatoriamente, pena la sanzione penale (art. 169);
- le misure idonee invece sono quelle che devono essere valutate ***in process*** e adattate continuamente anche in relazione alle conoscenze acquisite in base al progresso tecnologico, alla natura dei dati e alle specifiche caratteristiche del trattamento: esse devono fare in modo che siano ridotti al minimo i rischi di distruzione o perdita dei dati, nonché l'accesso non autorizzato o il trattamento non consentito o non conforme alle finalità.

1.1 TERMINI E DEFINIZIONI

Di seguito vengono riportate alcune definizioni che verranno utilizzate nel presente documento:

1. **Codice**: si intende il «Codice della Privacy», cioè il D.Lgs n. 196 del 30/06/2003, in materia di protezione dei dati personali.
2. **Trattamento**: (Art. 4) è una qualunque operazione o insieme di operazioni svolte sui dati, con o senza l'ausilio di un elaboratore elettronico; tali operazioni possono consistere in: raccolta, registrazione, organizzazione, conservazione, elaborazione, blocco, modifica, utilizzo, interconnessione, comunicazione, diffusione, cancellazione, selezione, estrazione, raffronto.
3. **Dati personali**: (Art. 4) una qualunque informazione su persone fisiche, giuridiche, enti o associazioni, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, incluso un numero di identificazione personale. Il Garante ha precisato che per "dato personale" non deve intendersi il solo dato oggettivo (per es. nome e cognome), ma ogni altro dato personale contenuto in valutazioni soggettive, giudizi e analisi di dipendenti, ispezioni o relazioni posseduti dall'ente.[1]
4. **Dati sensibili**: sono quei dati personali che riguardano la razza, la religione, le convinzioni filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, a sindacati, ad associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale di una persona.[2]

1 Sono esempi di dati personali: una login e una password; il nome, il cognome, l'indirizzo, il numero di telefono, il codice fiscale, la partita IVA, i dati bancari; le informazioni circa la composizione del nucleo familiare, la professione esercitata da un determinato soggetto (sia fisico che giuridico), la sua formazione; fotografie, radiografie, video, suoni, impronte; informazioni relative al profilo creditizio, alla retribuzione; informazioni relative alla salute di un soggetto, alla vita sessuale, alla partecipazione ad associazioni di categoria, a partiti, trattenute sindacali, cartelle cliniche, rilevazioni di presenze.

2 Sono esempi di dati sensibili le trattenute sindacali, i dati relativi ad infortuni o malattie, i dati delle cartelle cliniche, le radiografie.

5. **Titolare**: la persona fisica o giuridica, la pubblica amministrazione o qualsiasi altro ente cui competono le decisioni circa le finalità e le modalità del trattamento dei dati personali, ivi compreso il profilo della sicurezza;
6. **Responsabile**: la persona fisica o giuridica, la pubblica amministrazione e qualsiasi altro ente preposto dal Titolare al trattamento dei dati personali;
7. **Incaricato**: la persona fisica che compie le operazioni del trattamento di dati personali, attenendosi alle istruzioni impartite dal Titolare o dal Responsabile;
8. **Sicurezza fisica**: protezione delle persone che operano sui sistemi, le aree e le componenti del sistema informativo; può essere ricondotta alla sicurezza di area e sicurezza delle apparecchiature:
   - **sicurezza di area**: ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi informatici;
   - **sicurezza delle apparecchiature**: riconducibile da un lato alla protezione da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione e di condizionamento;
9. **Sicurezza logica**: protezione dell'informazione e di conseguenza dei dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo; sono da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa;
10. **Servizi di sicurezza**: sono le funzioni di sicurezza che il sistema dovrà garantire su tutte le piattaforme ed a tutti i livelli di elaborazione (ne sono alcuni esempi l'autenticazione, il controllo accessi, la confidenzialità, l'integrità ed il non ripudio);
11. **Meccanismi di sicurezza**: rappresentano le modalità tecniche attraverso le quali è possibile realizzare i servizi di sicurezza, come ad esempio la cifratura, la firma digitale, meccanismi per il controllo degli accessi; l'integrità dei dati, i meccanismi per l'autenticazione, il *traffic padding* ovvero la saturazione traffico in rete ed il controllo dell'instradamento);
12. **Monitoraggio**: attività di verifica continua della efficacia delle misure di sicurezza realizzate, effettuata sotto la responsabilità della struttura che progetta e realizza le misure di sicurezza, durante la progettazione, implementazione ed esercizio delle misure stesse;
13. **Audit di sicurezza**: attività di verifica effettuata da una struttura esterna alla struttura che ha implementato le misure di sicurezza; potrà avvenire in modo estemporaneo ed imprevedibile.

1.2 OGGETTO E FINALITA'

Il Codice nasce per conformare le innumerevoli disposizioni relative, anche indirettamente, alla privacy. In molte parti esso recepisce e codifica le numerose pronunce emanate e i pareri forniti dal Garante negli ultimi anni. Tra le novità più significative va sottolineato il "**Principio di necessità**" (Art. 3) nel trattamento dei dati personali: in base a tale principio i sistemi informativi ed i programmi informatici devono essere, dal momento della loro configurazione, predisposti in modo da ridurre al minimo l'utilizzo di dati personali e di dati identificativi. Il **trattamento** di dati sensibili da parte di enti pubblici è consentito solo se autorizzato da espressa disposizione di legge che specifica i tipi di dati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Altrimenti (Art. 20, comma 2) il trattamento è consentito solo se l'ente approva regolamenti, solo con parere conforme del Garante.

Il presente elaborato costituisce quindi il «DOCUMENTO PROGRAMMATICO SULLA SICUREZZA» (D.P.S.) previsto dagli articoli 33-36 e dall'allegato B del Codice, da aggiornarsi con cadenza almeno annuale.

Nel presente documento vengono definiti i compiti e le responsabilità in materia di sicurezza del trattamento e in particolare vengono descritti i criteri utilizzati per lo svolgimento delle attività di analisi e di valutazione dei rischi al fine di adottare un piano di interventi per la tutela e la protezione:

a) delle aree e dei locali;
b) dell'integrità dei dati;
c) delle trasmissioni dei dati.

Lo scopo è di elaborare criteri e procedure per il trattamento dei **rischi** cosiddetti **residuali**: procedere non solo all'eliminazione dei rischi monitorati, ma anche alla loro riduzione o in alternativa al trasferimento degli stessi (ove possibile) a terzi.

I rischi in generale sono imputabili a due fattori caratteristici delle tecnologie dell'informazione:

- l'**inaffidabilità**: cioè la non garanzia di corretto funzionamento, sia nelle componenti hardware, sia in quelle software;
- l'**esposizione alle intrusioni informatiche**.

In termini più operativi è bene intendere la sicurezza del sistema informativo automatizzato non solo come *protezione del patrimonio informativo da rilevazione, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali* ma anche come *limitazione degli effetti causati dall'eventuale occorrenza di tali cause*.

Inoltre la sicurezza del sistema informatico non dipende solo da aspetti tecnici, ma anche da quelli organizzativi, sociali e legali. La sicurezza delle informazioni si ottiene implementando una serie di contromisure che potrebbero consistere in politiche, prassi, procedure, strutture organizzative e funzioni software; la selezione di tali misure dipende dagli specifici obiettivi di sicurezza che l'organizzazione si è data.

Un sistema informatico viene definito *sicuro* quando consente la *riservatezza*, l'*integrità* e la *disponibilità* delle informazioni:

- **riservatezza**: garantire che le informazioni siano accessibili solo alle persone autorizzate;
- **integrità**: salvaguardare l'esattezza e la completezza delle informazioni e dei metodi per la loro elaborazione;
- **disponibilità**: garantire che gli utenti autorizzati abbiano accesso alle informazioni ed ai beni associati nel momento in cui lo richiedono.

1.3 APPLICABILITÀ

Il presente documento si applica a tutte le funzioni svolte all'interno dell'Amministrazione Comunale di Quarrata in merito alle attività di trattamento dei dati personali.

2 INDIVIDUAZIONE E VALUTAZIONE DEI BENI E DEI RISCHI

2.1 OGGETTO E FINALITÀ

La presente sezione definisce i criteri e le modalità operative adottate per individuare e valutare i beni da proteggere e i rischi per la sicurezza delle aree, dei dati e delle trasmissioni. In particolare la fase della valutazione costituisce un momento importante e fondamentale nel processo di gestione del rischio residuo: è dalla completezza o meno di questa operazione e dalle sue risultanze, che dipendono la predisposizione di un programma idoneo di misure di prevenzione e di protezione.

2.2 APPLICABILITÀ

Le indicazioni e le prescrizioni contenute nella presente sezione sono applicabili a tutte le attività connesse all'uso dei sistemi informativi automatizzati.

2.3 RESPONSABILITÀ

2.3.1 TITOLARE DEL TRATTAMENTO

Il titolare è il responsabile dell'analisi e della valutazione dei rischi, azioni strumentali all'adozione del documento programmatico sulla sicurezza. In questa sezione vengono descritte le modalità per lo svolgimento di tali operazioni.

2.4 CRITERI PER L'INDIVIDUAZIONE DEI BENI E DEI RISCHI

Occorre procedere all'individuazione dei beni da tutelare, al fine dell'adozione delle misure di sicurezza e per disegnare un quadro completo del sistema informativo automatizzato utilizzato.

2.4.1 IDENTIFICAZIONE DEI BENI DA PROTEGGERE

Il primo passo da compiere nella definizione di un piano di sicurezza è l'individuazione degli elementi del sistema informativo automatizzato che necessitano di 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.

Occorre, cioè, rappresentare e classificare non solo le componenti, ma anche come queste sono relazionate tra di loro, sia fisicamente che logicamente, definendo un disegno completo del sistema informatico.

Si tratta di specificare quale è il patrimonio informativo in termini di dati e risorse elaborative che sarà oggetto del piano della sicurezza.

2.4.1.1 Risorse hardware

Rientrano in questa categoria: workstation, personal computer, stampanti, linee di comunicazione, switch, hub, server, router.

Le principali minacce a cui questi dispositivi sono sottoposti sono: malfunzionamenti dovuti a guasti o sabotaggi, malfunzionamenti dovuti a eventi naturali, quali allagamenti e incendi, furti e intercettazione; quest'ultima minaccia interessa gli apparati di rete, cioè le linee di comunicazione, i router, i server, gli switch e gli hub. È infatti possibile eseguire 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.

2.4.1.2 Risorse software

Rientrano in questa categoria i sistemi operativi e software di base *(utilities*, diagnostici), software applicativi, gestori di basi di dati, software di rete, programmi in formato sorgente e oggetto, ecc.

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 malizioso 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 *backdoor*;
- attacchi di tipo *denial of service* vengono generalmente portati a servizi di rete, ma sono 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.

2.4.1.3 Dati

Intendiamo con ciò il contenuto degli archivi, delle basi di dati, dati di transito, copie storiche, *file di log*, ecc.

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

- 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 la possibilità per utenti non autorizzati di modificare o cancellare dati a loro "non appartenenti", oppure errori commessi da utenti autorizzati che inavvertitamente procedono alla modifica o cancellazione di informazioni significative.

2.4.1.4 Le risorse professionali

Si intendono appartenenti a questa categoria gli amministratori di sistema, i sistemisti, i programmatori, gli operatori, gli utenti finali, i manutentori hardware e software, i consulenti, ecc. È questa una categoria alquanto particolare in quanto può essere invitata in merito a minacce che compromettono la sicurezza del sistema, ma può a sua volta costituire una minaccia per la sicurezza del sistema.

Nel primo caso il personale può essere oggetto di attacchi così detti di *social engineering* in cui estranei cercano attraverso varie strategie di ottenere informazioni utili ad attaccare il sistema quali le password degli utenti, il contenuto dei file di configurazione, gli indirizzi IP delle macchine e così via.

Il personale, per contro, diventa una minaccia quando matura motivi di rivalsa nei confronti dell'amministrazione e quando ha una scarsa consapevolezza del problema sicurezza.

2.4.1.5 Documentazioni cartacee

Si intende appartenente a questa categoria la documentazione relativa ai programmi, all'hardware, ai sistemi, alle procedure di gestione, ecc.

Le principali minacce a cui tali elementi sono sottoposti sono la distruzione e/o l'alterazione ad opera di eventi naturali, di azioni accidentali e di comportamenti intenzionali.

2.4.1.6 Supporti di memorizzazione

Si tratta dei supporti su cui vengono tenute le copie dei software installati, le copie dei file di log e dei backup.

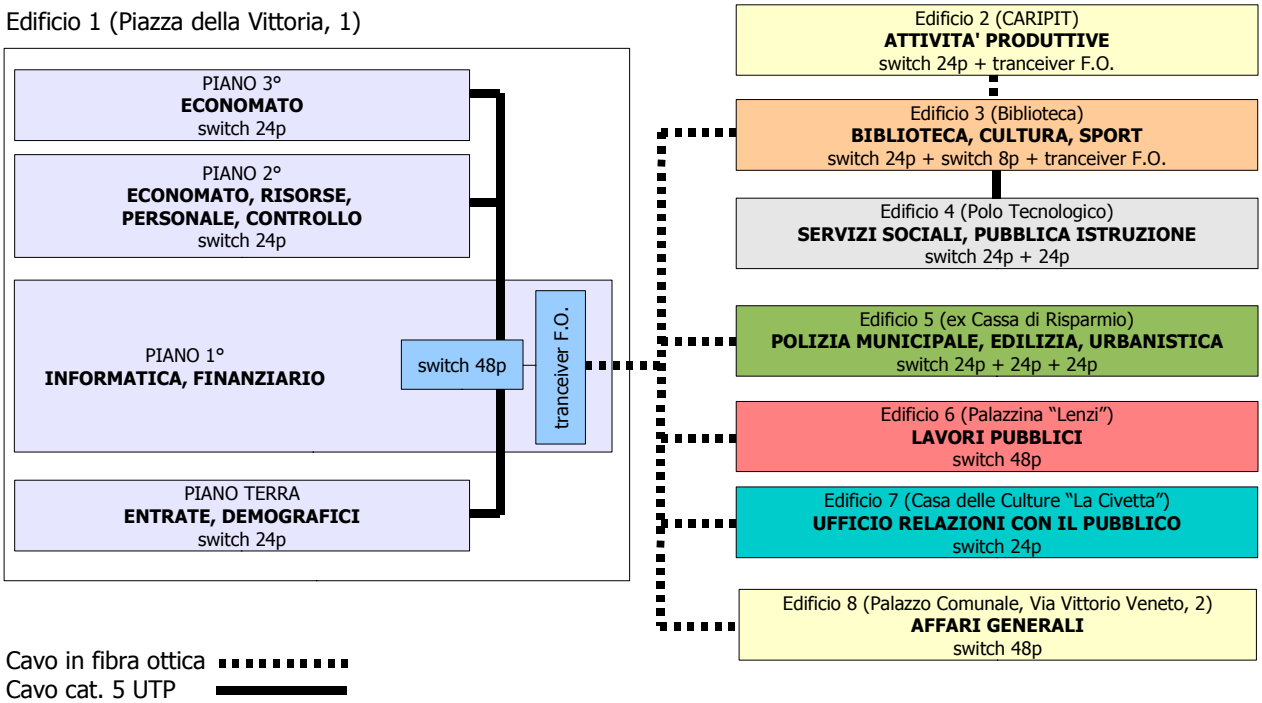
Le principali minacce a tali dispositivi, oltre a quelle già menzionate per i dispositivi cartacei, sono:

- il deterioramento nel tempo;
- l'inaffidabilità del mezzo fisico che in alcuni casi può presentare difetti di costruzione che ne compromettono il buon funzionamento nel tempo;
- l'evoluzione tecnologica del mercato.

2.4.2 ANALISI DELLA SITUAZIONE ATTUALE

2.4.2.1 L'infrastruttura informatica

Gli uffici sono attualmente distribuiti in 8 edifici ed il collegamento tra gli edifici è realizzato con cavi in fibra ottica in canalizzazioni di proprietà dell'Ente.



Complessivamente il numero di computer collegati alla rete sono 140; tra cui 4 notebook e 12 server di rete collocati in 2 edifici; alcuni server sono condivisi tra più Servizi, mentre gli altri sono ad uso esclusivo di un ufficio.

L'accesso ad INTERNET avviene tramite ADSL; la rete è protetta tramite da firewall installati in ambiente Linux.

Nella tabella seguente sono riportate alcune caratteristiche dei server, le applicazioni installate e le loro collocazioni fisiche.

I server COMPAQ, HP e DELL sono dotati di una configurazione RAID dei dischi e sono montati in armadio rack.

La rete è sotto dominio Windows 2003 Active Directory, quindi consente di avere una struttura di archiviazione centralizzata dei documenti, attraverso aree ad accesso controllato e con diversi profili di autorizzazioni (privato, di gruppo e pubblico).

Edificio	Server	Sistema Operativo	Applicazioni
1	COMPAQ Proliant 1600	SCO Open Server Enterprise v.5.0.5	Edilizia, determine, finanziaria, tributi
1	COMPAQ Proliant 1600	Microsoft Windows NT Server 4.0	Posta elettronica interna, file server
1	HP ProLiant DL380	UnixWare 7.1.3	Anagrafe, Delibere, Pubblica Istruzione, Servizi Sociali, Stato Civile
1	PC Smart	Linux	Proxy server, firewall
1	PC Smart	SmoothWall (Linux)	Proxy server, firewall
1	IomegaNAS	Microsoft Windows XP Embedded	File server, copie di salvataggio
1	Dell PowerEdge 2580	Microsoft Windows 2000 Server	ICI, SUAP, file server, copie di salvataggio
1	Dell PowerEdge 860	Microsoft Windows 2003 Server	Domain controller, file server, copie di salvataggio
1	HP Server TC3100	Microsoft Windows 2000 Server	Personale, Paghe, Presenze
1	Dell PowerEdge 1950	Linux Ubuntu server	Database Postgresql/PostGIS
1	Dell PowerEdge 2950	Linux Red Hat Enterprise server 5.0	Affari generali
5	Dell	Microsoft Windows 2000 Server	Cartografie, Sistema Informativo Territoriale

2.4.2.2 I locali

Allo stato attuale esiste una sala macchine, ovvero un locale adibito esclusivamente alla salvaguardia di tutti i server: i server COMPAQ, HP e DELL, montati in configurazione rack, ed i server per il collegamento a Internet, sono raggruppati in un unico locale al primo piano dell'Edificio 1 (Piazza della Vittoria, 1); la sicurezza fisica del locale è garantita da una porta blindata.

La protezione dei locali da intrusione è da considerarsi soddisfacente; in più le finestre del piano terreno dell'Edificio 1 e sono dotate di tapparelle blindate. Le porte di accesso agli edifici 1 e 6 sono dotate di un sistema di apertura tramite scheda magnetica.

Le attrezzature principali (server ed armadi di rete) così come i singoli personal computer, sono collegati alla rete elettrica tramite gruppi di continuità (con funzioni anche di stabilizzatore) di sufficiente potenza per garantire un corretto spegnimento delle macchine in caso di interruzione prolungata dell'alimentazione.

Gli armadi principali e l'impianto interno agli uffici sono dotati di interruttori magnetotermici e di salvavita.

2.4.2.3 La sicurezza dei dati

2.4.2.3.1 Le copie di riserva

Per i server montati in armadio rack il backup viene effettuato automaticamente ogni notte, mentre per gli altri il salvataggio dei dati viene effettuato con una cadenza temporale stabilita dagli uffici che ospitano i server di rete; i nastri di salvataggio vengono custoditi in un armadio blindato collocato nell'Edificio 7.

2.4.2.3.2 L'accesso ai dati

Le reti locali Microsoft (nell'ambito del dominio gestito dal server con Windows 2003 Server) e UNIX prevedono l'identificazione dell'utente al momento del collegamento tramite un profilo di dominio pubblico ed una parola chiave che dovrebbe essere conosciuta solamente dal singolo operatore. Questo escluderebbe accessi indesiderati e garantirebbe che ogni utente abbia a disposizione esclusivamente i dati e le funzioni che gli sono stati assegnati.

Nell'ambito della rete UNIX, è inoltre disponibile la funzione che vieta l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

Viene inoltre fornita la possibilità di modificare autonomamente, sia su UNIX che in Windows, la propria password.

Le chiavi di accesso e le parole riservate relative ai profili tecnici di gestione dei server di rete (che quindi hanno autorizzazioni diverse e superiori a quelle dei normali utenti) sono conosciute solo dal personale del Servizio Informatica.

Per quanto riguarda invece le varie stazioni di lavoro, queste hanno sistemi operativi diversi: Microsoft Windows XP professional e Microsoft Windows 2000 professional. L'accesso alle risorse della macchina e di conseguenza anche a quelle di rete, è subordinato all'immissione di una parola chiave che solamente l'utente finale dovrebbe conoscere.

Uno degli elementi centrali dell'architettura di tali sistemi operativi è la sicurezza integrata: infatti la sequenza di accesso (utilizzando i tasti CTRL+ALT+CANC) previene la possibilità d'intercettazione del nome utente e della password.

La caratteristica di blocco dell'account permette di specificare il numero massimo di tentativi di accesso. Se non viene fornita la password corretta entro questo numero di tentativi, l'account non potrà essere utilizzato fino a quando gli addetti al Servizio Informatica non eseguiranno lo sblocco oppure fino a quando non sarà passato un determinato periodo di tempo. Questo impedisce l'accesso illegale al sistema da parte degli utenti che tentano di indovinare la password.

I sistemi operativi citati assicurano la protezione dei dati e del sistema attraverso la definizione del livello di controllo discrezionale che gli utenti possono avere sul sistema stesso.

Il modello di sicurezza di Microsoft Windows XP professional e Microsoft Windows 2000 professional permette agli addetti al Servizio Informatica di applicare la sicurezza alla rete ed a tutti gli oggetti di sistema, intervenendo sul sistema affinché gli utenti non danneggino i file vitali o cambino la configurazione.

Il file system nativo di tali sistemi operativi (NTFS) fornisce questo livello di sicurezza anche al file system.

I sistemi operativi citati forniscono inoltre il supporto all'accesso multiutente: più utenti possono condividere un singolo computer mantenendo comunque il controllo sui loro file individuali. Utilizzando le funzioni di controllo disponibili, l'accesso al dominio Windows 2003 Active Directory è consentito solo dai client impostati dal Servizio Informatica, indipendentemente dal loro sistema operativo, ed in determinate ore del giorno, cioè durante il periodo lavorativo: questo consente di evitare accessi non autorizzati da postazioni diverse da quelle previste ed in ore del giorno non autorizzate.

Per quanto riguarda la rete UNIX, esiste una procedura che permette l'autonoma sostituzione della password da parte dell'utente finale entro un periodo di validità prestabilito, nonché di eseguire controlli sul periodo temporale entro il quale l'accesso è consentito.

2.4.2.3.3 La sicurezza logica

Per "sicurezza logica" viene intesa quella serie di attività che hanno come obbiettivo quello di garantire la riservatezza dei dati e la disponibilità esclusivamente per quegli utenti che ne hanno l'autorizzazione.

In effetti quando si parla di "accesso ai dati" viene coinvolta sia la "sicurezza fisica", cioè la possibilità materiale di poter disporre di una stazione di lavoro connessa alla banca dati voluta, sia la "sicurezza logica", cioè il controllo che, una volta attivata la stazione di lavoro e collegata alle banche dati necessarie, vengano resi disponibili esclusivamente i dati previsti e che questi siano esatti e congruenti.

È indispensabile poter controllare non solo chi accede alle attrezzature informatiche ma anche a quali tipi di informazioni l'utente accede e per fare che cosa.

Si possono individuare alcune tipologie di utenti:

1. utenti operativi con funzioni di controllo (i responsabili dei servizi) i quali devono avere la massima visibilità sui dati ma solamente per quanto attinente al proprio servizio e su questi devono avere anche l'operatività, anche se per loro non si tratta della funzione

principale; devono inoltre aver accesso e poter modificare eventuali parametri di funzionamento delle procedure (ad esempio inizializzare determinati contatori, ecc.);

2. utenti operativi standard (gli impiegati) i quali devono avere accesso a tutte e sole le informazioni utili per lo svolgimento del proprio lavoro, indipendentemente dal servizio che le gestisce, ma devono poter operare esclusivamente sui dati che hanno direttamente a che fare con la loro attività, con l'esclusione dei parametri delle procedure (ad esempio un impiegato del Servizio Tributi deve poter consultare le informazioni anagrafiche di un cittadino ma senza poterle modificare, mentre può evidentemente intervenire sui dati relativi alle posizioni ICI);
3. utenti addetti alla sicurezza ed alla manutenzione dei dati (personale del Servizio Informatica, specificatamente individuato) i quali devono poter accedere a qualunque informazione, comprese quelle operative di sistema, ed avere su queste tutte le autorità gestionali.

Per tutti questi utenti l'assegnazione di una particolare chiave di identificazione diventa di primaria importanza in quanto solo così il sistema è in grado di individuare esattamente l'utente collegato e mettergli a disposizione tutte e solo le risorse necessarie.

Sempre in adeguamento con quanto previsto dalle misure minime di sicurezza è necessario garantire che:

- lo stesso profilo utente non venga assegnato a persone diverse, neppure in tempi diversi;
- lo stesso utente non possa collegarsi contemporaneamente alla stessa applicazione da stazioni di lavoro diverse.

Nell'ambito della parole chiave di accesso diventa fondamentale il raggiungimento di alcuni obbiettivi e precisamente:

- ogni utente deve avere un'unica parola chiave con la quale accedere a tutte le risorse e le informazioni che gli sono necessarie;
- le parole chiave devono essere memorizzate dall'utente e mai scritte da qualche parte; come conseguenza ne deriva che devono essere scelte direttamente dall'utilizzatore perché quelle definite da terzi spesso sono di difficile memorizzazione ed inevitabilmente vengono registrate in luoghi facilmente accessibili dal posto di lavoro con grave danno alla sicurezza;
- le parole chiave devono essere significative per l'utente ma non facilmente scopribili da terzi; sarà quindi necessario evitare l'uso dei nomi dei figli, delle date di nascita, ecc... che invece sono tipici e individuabili con estrema facilità;
- per diminuire il rischio che le parole chiave siano conosciute anche da altri si impone una limitazione alla durata di validità delle stesse ad alcuni mesi impedendo, via software, il riutilizzo della stessa password per un sufficiente periodo di tempo; l'adozione di questo genere di misure presuppone una consapevolezza da parte degli utenti delle problematiche legate alla sicurezza e l'adozione di specifiche disposizioni regolamentari;
- le parole chiave dovranno essere segrete e strettamente individuali; dato che non è possibile attivare dei controlli automatici che impediscano la diffusione e la comunicazione ad altre persone della propria chiave di accesso, è necessario sensibilizzare adeguatamente il personale al problema della sicurezza.

2.4.2.3.4 I virus

I "virus" informatici sono una particolare classe di programmi che hanno la principale caratteristica di essere capaci di duplicarsi e di nascondersi in mezzo alle altre informazioni.
Fondamentalmente possiamo individuare queste categorie di virus:

virus non distruttivi: possono impedire assolutamente di lavorare ma non danneggiano i dati presenti sul computer (ad esempio i virus che ogni volta che viene eseguito un programma

aumentano l'indicazione dello spazio occupato sul disco determinando dopo un po' di tempo il blocco totale delle operazioni a causa del disco virtualmente pieno);

virus distruttivi: modificano e/o distruggono le informazioni registrate, soprattutto i programmi eseguibili ma anche i dati, con danni normalmente non recuperabili, fino ad arrivare a rendere totalmente inutilizzabile l'intero sistema. Possono anche attaccare il settore di "boot" del disco, cioè quella parte di disco che i sistemi operativi leggono non appena iniziano ad operare e nella quale sono registrate in modo non utilizzabile dalle normali applicazioni le informazioni basilari necessarie al sistema operativo stesso. In questi casi il virus assume totalmente il controllo del computer ed in genere opera delle modifiche tali a tutta la struttura per cui il sistema operativo può continuare a funzionare (apparentemente in modo del tutto regolare) solo con l'intermediazione del virus stesso e la sua eliminazione provoca l'impossibilità per il sistema operativo di riconoscere le componenti corrette e quindi di funzionare.

È evidente che in una situazione nella quale vengono prodotti alcune centinaia di nuovi virus ogni mese e nella quale esistono banche dati disponibili a chiunque, nelle quali trovare le istruzioni per creare un virus e pezzi di codice già pronti da mettere insieme per fare un nuovo virus, il problema è diventato assolutamente prioritario ed obbliga a predisporre contromisure indubbiamente onerose sia dal punto di vista finanziario che da quello gestionale.

Un antivirus richiede un continuo aggiornamento per essere continuamente efficace, in modo da riconoscere i nuovi virus e le nuove varianti che si diffondono giorno per giorno per scambio di file, per scarico di informazioni da Internet e tramite la posta elettronica.

È stato installato un sistema di protezione virale con aggiornamento centralizzato delle definizioni dei virus e gestione centralizzata delle postazioni client; pertanto su ciascun personal computer e su ciascun server con sistema operativo Microsoft Windows l'antivirus viene automaticamente aggiornato, all'accensione della macchina, ogni qual volta sono disponibili nuove "impronte virali".

Sui server UNIX e LINUX, utilizzati esclusivamente come server per applicazioni gestionali, i dati sono tutti filtrati dalle applicazioni, per cui il rischio di infezione è da considerarsi pressoché nullo.

2.4.2.4 Elenco dei dati personali trattati dai singoli Servizi

Servizi Sociali	Archivio cittadini richiedenti prestazioni socio economiche (es. contributi affitti, assegni di maternità e nucleo familiare, per abbattimenti barriere architettoniche, prestiti d'onore, etc.) Archivio denunce infortuni sul lavoro per il Servizio Anagrafica partecipanti a gare d'appalto bandite dal Servizio Archivio richiedenti assegnazione alloggi Archivio ricoveri in RSA e centri diurni Archivio associazioni di volontariato e cooperative sociali svolgenti funzioni sociali Archivio richieste per soggiorni estivi (bambini e anziani) Archivio richieste assistenza domiciliare e scolastica Archivio richieste trasporti sociali (anziani e diversamente abili) Archivio richieste per servizio di telesoccorso Archivio utenti centri socio educativi Archivio utenti alloggi comunali e ERP Archivio utenti sportello immigrati Archivio denunce infortuni sul lavoro per il Servizio
Servizi Statistici e Demografici	Anagrafe della popolazione residente e AIRE Archivio di Stato civile Liste elettorali Archivio denunce infortuni sul lavoro per il Servizio
Servizio Affari Generali	Archivio Amministratori Archivio raccolta firme per referendum e leggi di iniziativa popolare Archivio denunce infortuni sul lavoro per il Servizio Archivio sinistri Archivio determinazioni, deliberazioni ed atti in genere dell'amministrazione

	Soggetti coinvolti nella cooperazione internazionale Protocollo Archivio relate di notifica (attività dei messi comunali)
Servizio Attività Negoziali	Contratti Anagrafica partecipanti a gare d'appalto Archivio cause legali in cui la PA è parte Archivio pareri legali Dati dei professionisti (progettisti, avvocati etc) Anagrafe delle prestazioni Archivio denunce infortuni sul lavoro per il Servizio
Servizio Attività Produttive	Elenco operatori economici; Denunce di Inizio Attività (DIA); Autorizzazioni; Beneficiari contributi economici; Certificati medici ambulanti (su carta); Elenco pratiche SUAP Archivio denunce infortuni sul lavoro per il Servizio
Servizio Cultura e Comunicazione	Archivio denunce infortuni sul lavoro per il Servizio Anagrafica partecipanti a gare d'appalto bandite dal Servizio Archivio utenti fruitori dei servizi bibliotecari Segnalazioni e reclami URP Raccolta istanze rivolte al Difensore Civico Richieste per l'uso degli impianti sportivi
Servizio Edilizia	Pratiche edilizie (concessioni, autorizzazioni, permessi a costruire) DIA (denuncia di inizio attività) Condoni edilizi Abusi edilizi Archivio denunce infortuni sul lavoro per il Servizio
Servizio Finanziario ed Economato	Anagrafica clienti e fornitori Archivio denunce infortuni sul lavoro per il Servizio
Servizio Informatica	Albo fornitori Anagrafica partecipanti a gare d'appalto bandite dal Servizio SIT (dati estratti dalla banca dati dell'anagrafe e dal catasto) Archivio denunce infortuni sul lavoro per il Servizio
Servizio Lavori Pubblici	Archivio fornitori e imprese esecutrici di lavori Dati progettisti esterni Anagrafica partecipanti a gare d'appalto bandite dal Servizio Dati necessari per il servizio di protezione civile Dati relativi a procedimenti espropriativi Archivio relativo ai progetti di bonifica ambientale Richieste autorizzazioni scarichi civili fuori fognatura Archivio denunce infortuni sul lavoro per tutti i Servizi Presentazione di piani attuativi (dati anagrafici dei proprietari dei terreni; dati catastali riferiti alla proprietà di immobili con, eventualmente, copia degli atti attestanti la proprietà; dati anagrafici dei tecnici liberi professionisti che firmano i piani)
Servizio Personale e Organizzazione	Archivio fascicoli personali dipendenti ed ex dipendenti (per la gestione giuridica ed economica del personale) Archivio collaborazioni esterne, stage, tirocini formativi Dati relativi a professionisti e/o imprese che svolgono attività di formazione per gli enti pubblici Archivio amministratori Archivio concorrenti concorsi e selezioni Archivio denunce infortuni sul lavoro per il Servizio
Servizio Polizia Municipale	Accertamenti edilizi; Video sorveglianza; Accertamenti sulle attività commerciali e ricettive; Rilievo di sinistri stradali a seguito dei quali vengono trattati anche dati sensibili (referti); Accertamenti e contestazioni di violazioni al CDS;

	Accertamenti di Polizia Giudiziaria, accertamenti di residenza, accertamenti relativi all'idoneità degli alloggi; Accertamenti per iscrizione all'albo artigiani, accertamenti patrimoniali, morali e quant'altro richiesti da altri Enti; Autorizzazioni di occupazione di suolo pubblico; Tesserini per portatori di handicap; Autorizzazioni al parcheggio in deroga per i residenti; Rilascio e ritiro di tesserini venatori, pass di accesso in zone interdette al traffico per particolari motivi Archivio notizie di reato Archivio elenco giudici popolari Archivio trattamenti sanitari obbligatori Archivio denunce infortuni sul lavoro per il Servizio
Servizio Pubblica Istruzione	Richiedenti e fruitori del servizio di mensa scolastica Richiedenti e fruitori del servizio di trasporto scolastico (compreso dichiarazioni ISEE per avere tariffe agevolate) Richiedenti e fruitori servizi post scuola (bambini della scuola materna) Richiedenti e fruitori servizi complementari per l'infanzia Buoni libro per utenti della scuola Buoni studio per il biennio scuole superiori del comune Richiedenti e fruitori dei corsi di lingua italiana rivolti a stranieri Richiedenti e fruitori dell'asilo nido Richiedenti e fruitori dei centri estivi Richiedenti e fruitori di esoneri dal pagamento di servizi scolastici Richiedenti diete speciali (per ragioni di salute, e/o religiose) Archivio denunce infortuni sul lavoro per il Servizio Anagrafiche partecipanti a gare d'appalto bandite dal Servizio
Servizio Entrate	Anagrafe e posizioni contributive dei contribuenti ICI, TIA, COSAP e pubblicità; Archivio denunce infortuni sul lavoro per il Servizio
Servizio Urbanistica	Presentazione di piani attuativi (dati anagrafici dei proprietari dei terreni; dati catastali riferiti alla proprietà di immobili con, eventualmente. copia degli atti attestanti la proprietà; dati anagrafici dei tecnici liberi professionisti che firmano i piani) Archivio denunce infortuni sul lavoro per il Servizio

2.4.3 DEFINIZIONE DEI RISCHI

Per una struttura pubblica come il Comune di Quarrata i danni che una persona, autorizzata o meno, può apportare, volutamente o inconsciamente, agli archivi comunque gestiti che contengano informazioni personali, sensibili e/o riservate si possono raggruppare in:

- accesso ad informazioni non autorizzate;
- modifica non controllata del contenuto delle banche dati con conseguente perdita delle caratteristiche di correttezza, completezza e congruità logica;
- distruzione delle banche dati;
- copia non autorizzata dei dati contenuti nelle banche dati;
- malfunzionamento del servizio;
- interruzione del servizio;
- utilizzo di macchine e indirizzi telematici del Comune di Quarrata per compiere azioni illecite nei confronti di altri soggetti.

Esistono però anche altri tipi di rischio non legati alle attività umane ma derivanti da eventi naturali, incidenti, guasti meccanici, ecc. che possono comunque provocare malfunzionamenti o interruzioni dei servizi, di cui è necessario tenere conto.

2.4.3.1 Elementi da valutare per l'esame del rischio:

Risorse umane	Hardware	Software	Dati	Collegamenti	Sistemi di sicurezza	Eventi naturali	Incidenti
insufficiente conoscenza del sistema e/o dell'applicazione	obsolescenza	malfunzionamento	accesso non autorizzato	malfunzionamento	incompletezza	terremoto	incendio
insufficiente conoscenza dei rischi e delle misure di sicurezza	avaria	virus	modifica non autorizzata	interruzione	mancata verifica	alluvione	allagamento
distrazione	distruzione hardware	distruzione software	distruzione dati	intercettazione	illeggibilità copie di backup		cedimento strutturale
negligenza	furto	duplicazione non autorizzata	esportazione illegittima				campi elettromagnetici
incidente	manomissione	obsolescenza					
atto doloso		modifica non controllata					

2.4.3.2 Schede di dettaglio

2.4.3.2.1 Risorse umane

2.4.3.2.1.1 Insufficiente conoscenza del sistema e/o dell'applicazione

A volte l'operatore può involontariamente compiere azioni che comportano un danno semplicemente perché non è perfettamente a conoscenza delle conseguenza del suo operato.

Il danno che può essere provocato varia da:

- blocco momentaneo della stazione di lavoro;
- blocco di una o più transazioni che possono coinvolgere anche altri utenti;
- permettere la visione di dati riservati o sensibili a persone non autorizzate;
- inserimento, modifica o cancellazione di informazioni.

Nessun intervento può completamente eliminare questo fattore di rischio; è però possibile ridurne drasticamente la pericolosità attraverso misure organizzative, quali interventi di formazione nel tempo degli utenti, per una sempre migliore padronanza dell'informatica di base, degli strumenti di produttività individuale e delle specifiche applicazioni necessarie al servizio.

2.4.3.2.1.2 Insufficiente conoscenza dei rischi e delle misure di sicurezza

È determinato da utenti aventi una certa superficialità di comportamento in merito alla sicurezza, dovuta in genere, ad una non comprensione dei rischi che ne possono derivare.

I casi più tipici ed evidenti sono:

- diffusione nell'ambito dell'ufficio della password personale;
- comunicazione a qualche collaboratore della password di chi ha autorizzazioni più elevate;
- lasciare la stazione di lavoro accesa e collegata mentre ci si assenta;
- lasciare stampe e tabulati contenenti dati personali, sensibili o riservati, in luoghi non sicuri;
- non effettuare copie di riserva dei propri documenti ed archivi.

È evidente che nessun sistema di password può essere efficace se manca la collaborazione cosciente da parte dell'utenza, per cui si tratta di un fattore di rischio non completamente eliminabile ma che può essere ridotto tramite:

misure organizzative:

- intervento di formazione nel tempo degli utenti, per una sempre migliore sensibilizzazione alle problematiche della sicurezza ed ai possibili rischi derivanti dall'osservanza delle norme;
- emanazione di indicazioni (anche verbali), disposizioni e/o regolamenti che disciplinino il comportamento dell'utente, a qualsiasi livello;

- controllo periodico da parte di un gruppo appositamente costituito che verifichi la corretta applicazione delle norme;

misure fisiche:

- distruzione di tutti i supporti cartacei non più necessari che contengano dati personali, sensibili o riservati; si tratta quindi di diffondere maggiormente e incentivare l'uso di trita documenti (come per es. accade presso il Servizio Informatica ed i Servizi Demografici);

misure logiche:

- utilizzo di *screen saver* dotati di password da attivare a tempo ma anche tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro;
- spostamento di tutti i documenti o archivi che contengono dati personali, sensibili o riservati su supporti di rete ad accesso controllato in modo da garantirne le copie di sicurezza.

2.4.3.2.1.3 Distrazione

La distrazione si può classificare in tipo "fisico" o "logico":

- nel primo caso determina in genere danni alle attrezzature ed a volte, come conseguenza, danni anche ai dati; ne sono alcuni esempio il rovesciamento di una tazzina di caffè sulla tastiera oppure, molto più grave, una bottiglia d'acqua sull'unità centrale oppure urtare un'attrezzatura facendola cadere e danneggiandola;
- la distrazione "logica" invece genere provoca esclusivamente danni ai dati; ne sono esempi la distrazione dovuta ad una telefonata che distoglie l'attenzione dall'attività in corso di svolgimento, con pressione inavvertita di tasti che possono provocare l'esecuzione di operazioni non volute.

Anche in questo caso non è pensabile poter eliminare questo fattore di rischio ma solo di limitarlo tramite:

misure organizzative:

- intervento di formazione degli utenti per una sensibilizzazione ai possibili rischi derivanti da certi comportamenti;
- tenuta di un registro con l'esatta configurazione di ogni stazione di lavoro per permettere di ripristinare la situazione originale;

misure fisiche:

- mantenere a disposizione un numero minimo di parti di ricambio per ridurre i tempi di fermo dell'attrezzatura;

misure logiche:

- copia di riserva di tutti i dati dell'utente.

2.4.3.2.1.4 Negligenza

Per certi versi appare analoga alla distrazione ma presuppone un comportamento "colposo" da parte dell'utente.

A titolo di esempio potremmo ipotizzare il caso di un'attrezzatura posizionata accanto ad una finestra che viene lasciata aperta durante un temporale, consentendo così alla pioggia di bagnare la macchina, danneggiandola. Le misure di prevenzione sono:

misure organizzative:

- intervento di formazione degli utenti per una sensibilizzazione ai possibili rischi derivanti da certi comportamenti;
- emanazione di indicazioni, anche verbali, disposizioni o regolamenti che disciplinino certi comportamenti;
- tenuta di un registro con l'esatta configurazione di ogni stazione di lavoro per permettere di ripristinare la situazione originale;

misure fisiche:

- mantenere a disposizione un numero minimo di parti di ricambio per ridurre i tempi di fermo dell'attrezzatura;

misure logiche:

- copia di riserva di tutti i dati dell'utente.

2.4.3.2.1.5 Incidente

Si tratta di un avvenimento non imputabile, se non in maniera molto indiretta, all'utente ma ad una "fatalità".

Il danno può essere conseguenza di un corto circuito, di un incendio, di un allagamento dovuto alla rottura di un tubo, ecc... Le misure di prevenzione sono:

misure organizzative:

- emanazione di disposizioni che individuino i comportamenti da tenere in queste particolari situazioni ed addestramento specifico del personale;
- tenuta di un registro con l'esatta configurazione di ogni stazione di lavoro per permettere di ripristinare la situazione originale;

misure fisiche:

- verifica periodica dell'impiantistica, eliminazione delle situazioni ad alto rischio (gruppi di spine multiple, raccordi elettrici non a norma, sovraccarico degli impianti, ecc.);
- attivazione di rilevatori di fumo;

misure logiche:

- copia di riserva di tutti i dati.

2.4.3.2.1.6 Atto doloso

È il più grave e pericoloso dei fattori di rischio legati al fattore umano in quanto presuppone una precisa volontà di manomettere o distruggere le attrezzature o i dati. Proprio perché si tratta di un disegno criminoso, spesso pensato e realizzato da persone esperte, la prevenzione risulta particolarmente difficile e consiste in:

misure organizzative:

- emanazione di disposizioni o regolamenti che disciplinino l'accesso ai locali e/o alle apparecchiature, soprattutto in fasce orarie diverse da quelle abituali;

misure fisiche:

- protezione fisica dei locali in cui si trovano le apparecchiature più importanti e dove sono conservati i dati personali, sensibili e riservati;

misure logiche:

- controllo degli accessi alle apparecchiature ed ai dati con registrazione su file di log delle operazioni che vengono eseguite.

2.4.3.2.2 Hardware

2.4.3.2.2.1 Obsolescenza

Più che un fattore attivo di rischio, l'obsolescenza delle attrezzature - che nel campo informatico è particolarmente rapida - può impedire l'attivazione di misure di sicurezza fisiche o logiche che si rendano opportune per eliminare o ridurre alcuni rischi: ne sono alcuni esempi l'uscita dal mercato di un determinato modello di supporto per l'archiviazione dei dati, rendendo così impossibile le future operazioni di backup su nuovi supporti oppure l'impossibilità di reperire parti di ricambio.

L'eliminazione totale di questo fattore di rischio è possibile ma piuttosto onerosa; il rischio può essere comunque ridotto con misure fisiche come il potenziamento, nei limiti dell'economicità dell'intervento, delle attrezzature obsolete per metterle comunque in condizione di soddisfare degli standard minimi di sicurezza.

2.4.3.2.2.2 AVARIA

Come tutte le macchine, anche le attrezzature informatiche sono soggette a guasti che possono renderle inutilizzabili per periodi più o meno lunghi. A seconda del tipo di guasto si può avere solo un blocco dell'attività della stazione di lavoro oppure anche danneggiamento o perdita di dati (per esempio nel caso di guasto dell'hard disk).

L'eliminazione di questo fattore di rischio non è possibile; si può comunque ridurlo con:

misure organizzative:

- contratti di assistenza e manutenzione che prevedano tempi predefiniti per l'intervento di riparazione o la sostituzione temporanea della parte guasta nel caso di tempi di riparazione più lunghi;

misure fisiche:

- duplicare, sulle macchine più delicate (tipicamente i serve di rete) le componenti a maggior rischio quali l'alimentatore ed i dischi;

misure logiche:

- effettuare periodiche copie di riserva dei dati.

2.4.3.2.2.3 DISTRUZIONE HARDWARE

La distruzione, volontaria o fortuita, determina una totale perdita della funzionalità della stazione di lavoro e dei dati contenuti. Si può quindi assimilare ad una forma particolarmente grave di avaria. Ne consegue che anche l'eliminazione di questo fattore di rischio non è possibile; si può comunque ridurlo con:

misure organizzative:

- contratti di assistenza e manutenzione che prevedano tempi predefiniti per l'intervento di riparazione o la sostituzione temporanea della parte guasta nel caso di tempi di riparazione più lunghi;
- regolamentazione degli accessi ai locali ed alle attrezzature più importanti;
- allestimento di architetture per il backup automatico dotate di funzionalità di *disaster recovery*;

misure fisiche:

- duplicare, sulle macchine più delicate (tipicamente i serve di rete) le componenti a maggior rischio quali l'alimentatore ed i dischi;
- proteggere i locali e le attrezzature più importanti con un controllo degli accessi;

misure logiche:

- effettuare periodiche copie di riserva dei dati.

2.4.3.2.2.4 FURTO

Il furto equivale ad una distruzione totale del bene e quindi la perdita dei dati contenuti. L'eliminazione di questo fattore di rischio non è possibile; si può comunque ridurlo con:

misure organizzative:

- controllo degli accessi ai locali, soprattutto al di fuori dell'orario di apertura degli uffici;
- emanazione di indicazioni, anche verbali, o disposizioni regolamentari che disciplinino alcuni comportamenti (tipo chiudere a chiave la porta della stanza che rimane abbandonata, non lasciare aperte le finestre facilmente accessibili dall'esterno, ecc.);
- mantenimento di un registro delle configurazioni di ogni stazione di lavoro;

misure fisiche:

- proteggere i locali in cui sono posizionate le apparecchiature più importanti e quelle che contengono dati personali, sensibili e riservati;

- bloccare con strumentazione apposita (catene, lucchetti, blocca cavi, ecc.) le apparecchiature più esposte;

misure logiche:

- copia di sicurezza dei dati.

2.4.3.2.2.5 Manomissione

Trattandosi di apparecchiature hardware, anche la manomissione diventa rapidamente avvertibile dal momento che provoca comunque dei malfunzionamenti.

Si tratta comunque quasi sempre di un intervento doloso, generalmente attuato da persona esperta, tendente ad impedire il corretto funzionamento della stazione di lavoro, ad esempio mettendo fuori uso le testine di lettura/scrittura dei dischi o alterando la formattazione degli stessi per rendere non più rintracciabili le informazioni.

C'è anche la possibilità che la manomissione sia la causa di una manovra sbagliata compiuta dall'operatore, magari involontariamente, per imperizia o distrazione.

In molti casi la manomissione dell'hardware è conseguenza di un'infezione da virus. L'eliminazione di questo fattore di rischio non è possibile; si può comunque ridurlo con:

misure organizzative:

- interventi costanti di formazione degli utenti con lo scopo di dotarli delle conoscenze informatiche necessarie ad evitare operazioni che possono rivelarsi dannose, coscienti degli effetti che possono avere i vari tipi di virus ed informati sui comportamenti di sicurezza da mantenere per evitare le infezioni;
- limitare le possibilità di accesso ai locali ed alle attrezzature in cui vi siano dati personali, sensibili o riservati;

misure logiche:

- copia di sicurezza dei dati.

2.4.3.2.3 Software

2.4.3.2.3.1 Malfunzionamento

Partendo dalla constatazione di fatto che il software perfetto non esiste, si possono individuare alcune categorie di danno che il malfunzionamento del software può provocare:

- danno di immagine per l'amministrazione che utilizza o pubblica dati non corretti;
- danno economico quando l'errato funzionamento di un programma provoca errori nell'adempimento di operazioni obbligatorie e soggette a sanzione;
- danno gestionale quando questo malfunzionamento provochi un rallentamento o un blocco delle normali attività operative;
- danno organizzativo (oltre che nuovamente economico) in quanto è necessario destinare risorse umane e finanziarie alla ricerca e soluzione del malfunzionamento verificatosi.

Per ridurre il rischio, che non è evidentemente eliminabile, occorre adottare:

misure organizzative:

- per tutto il nuovo software che viene installato, che sia prodotto internamente oppure acquistato, dovrebbe essere sviluppato un ciclo completo di test teso ad individuare immediatamente eventuali comportamenti non previsti o voluti.

2.4.3.2.3.2 Virus

Oltre a danneggiare i dati (eventualità che verrà trattata nell'apposita sezione) i virus possono attaccare e danneggiare più o meno profondamente anche il software installato sulle macchine. Per ridurre il rischio, che non è eliminabile, occorre adottare:

misure organizzative:

- formazione di tutti gli utenti sui pericoli derivanti dai virus, sulle nuove forme che assumono, sulle fonti di contagio;
- emanazione di direttive o regolamenti che disciplinino i comportamenti degli utenti in merito al problema;

misure logiche:

- installazione di programmi antivirus in grado di prevenire anche forme di attacco attualmente non note;
- impedire l'avvio da disco floppy, evitando così l'infezione del settore di boot delle macchine.

2.4.3.2.3.3 Distruzione software

Un programma, o parte di esso, può essere distrutta intenzionalmente o accidentalmente, ad esempio per una errata operazione dell'utente, per uno sbalzo elettrico, per un malfunzionamento dell'hardware, ecc. A parte il danno derivante dal blocco temporaneo di tutta l'attività basata sul software distrutto c'è da considerare l'eventualità che non ne sia possibile la ricostruzione. Questa seconda eventualità può verificarsi, ad esempio, per:

- mancanza di copie di riserva del software;
- software installato su un'unica macchina e quindi non replicabile da altre stazioni di lavoro;
- software sviluppato esternamente da società che non esistono più;
- software sviluppato internamente e non documentato o del quale si è persa la documentazione;
- software particolarmente "vecchio" per il quale non c'è più manutenzione.

Per ridurre il rischio occorre adottare:

misure organizzative:

- tenuta di un registro di tutto il software installato;
- disposizioni interne che obblighino alla documentazione del software sviluppato;
- inserimento, nei contratti di acquisto delle licenze d'uso del software sviluppato esternamente, di una clausola di salvaguardia che obblighi la società fornitrice a documentare i propri prodotti;

misure fisiche:

- copia di riserva di tutto il software installato;

misure logiche:

- abilitare le funzioni di sicurezza che rendano non modificabili gli eseguibili a chi non è espressamente autorizzato.

2.4.3.2.3.4 Duplicazione non autorizzata

Il danno, in questo caso, consiste nella violazione delle norme vigenti che individuano questo evento come reato di tipo penale.

La diffusione non arrestabile della posta elettronica, la presenza di masterizzatori a prezzi sempre più bassi, ecc. rendono praticamente impossibile un controllo totale su questa tipologia di eventi. Per ridurre il rischio occorre adottare:

misure organizzative:

- formazione di tutti gli utenti sulle normative di legge al riguardo e sui principi fondamentali della sicurezza;
- emanazione di direttive o regolamenti che disciplinino i comportamenti degli utenti in merito al problema;

misure fisiche:

- blocco dei supporti magnetici rimovibili sulle stazioni di lavoro più a rischio (come quelle facilmente accessibili al pubblico);

misure logiche:

- installazione di programmi di log che registrino le duplicazioni effettuate.
- abilitare le funzioni di sicurezza che rendano non modificabili gli eseguibili a chi non è espressamente autorizzato;

2.4.3.2.3.5 Obsolescenza

Il rischio derivante dall'obsolescenza dei programmi consiste nell'incapacità degli stessi di rispondere correttamente alle mutate esigenze operative e/o normative. Per ridurre il rischio occorre adottare:

misure organizzative:

- stipula di contratti di assistenza e manutenzione con le società fornitrici del software acquistato esternamente;
- coinvolgimento di tutti i servizi interessati per conoscere prima possibile le nuove normative e le nuove esigenze operative per poter effettuare per tempo i test necessari e provvedere a far fare le modifiche necessarie.

2.4.3.2.3.6 Modifica non controllata

Si tratta dell'effetto tipico di una infezione da virus; in alcuni casi però può avvenire a seguito di una modifica volontaria di un programma, realizzata in fretta o da personale che non conosce esattamente la procedura, che porta in cascata modifiche impreviste. Per ridurre il rischio occorre adottare:

misure organizzative:

- formazione di tutti gli utenti sui pericoli derivanti dai virus, sulle nuove forme che assumono, sulle fonti di contagio;
- emanazione di direttive o regolamenti che disciplinino i comportamenti degli utenti in merito al problema;

misure fisiche:

- copia di sicurezza di tutto il software installato;

misure logiche:

- installazione di programmi antivirus;
- abilitare le funzioni di sicurezza che rendano non modificabili gli eseguibili a chi non è espressamente autorizzato;
- assegnazione ai tecnici della manutenzione di una password che abiliti l'accesso solo alle applicazioni di loro competenza.

2.4.3.2.4 Dati

2.4.3.2.4.1 Accesso non autorizzato

Secondo la normativa vigente, ogni operatore deve poter accedere a tutte e sole le informazioni che gli sono necessarie per svolgere correttamente il proprio lavoro. Occorre quindi fare in modo che l'accesso ai dati personali, sensibili o riservati sia rigidamente controllato. Le possibilità di accesso non autorizzato a dati gestiti in modalità informatica sono la conseguenza di:

- distrazione o negligenza di un utente, che ad esempio lascia la propria stazione di lavoro collegata e si allontana;
- conoscenza della password di un altro utente;
- varchi nel sistema di attribuzione del sistema di sicurezza e di assegnazione delle autorizzazioni.

Una ulteriore possibilità di accesso ai dati deriva dal non corretto utilizzo delle stampe che contengano informazioni personali, sensibili o riservate. Ne sono esempi le stampe prodotte come

supporto al lavoro di un ufficio, che vengano lasciate sulle scrivanie anche nei momenti in cui il posto di lavoro non è presidiato e, quando non servono più, vengano gettate nella carta da buttare; altro caso quello in cui le stampe prodotte per l'invio all'esterno o ad altri servizi vengano messe in contenitori non chiusi o addirittura, specie per trasmissioni interne all'amministrazione, inviate senza alcun contenitore.

Per ridurre il rischio determinato da divari nel sistema di assegnazione delle autorizzazioni, occorre adottare:

misure organizzative:

- mantenere un registro con l'elenco di tutte le tipologie di dati personali, sensibili o riservati che è necessario proteggere nonché l'elenco di tutti i profili utenti che hanno diritto di accesso e delle corrispondenti autorizzazioni accordate;
- cercare la collaborazione di tutti gli utenti perché segnalino immediatamente tutte le anomalie che riscontrano in merito (sospetto di conoscenza da parte di terzi della propria password, scoperta di possibili debolezze del sistema di autorizzazioni, ecc.);

misure logiche:

- verifica periodica da parte dei tecnici della sicurezza o di personale esterno appositamente incaricato della validità delle misure adottate;
- attivazione di procedure per impedire l'accesso al di fuori dell'orario di lavoro e comunque attivazione dei file di log per registrare l'accesso ai dati.

Quando i dati sono gestiti in modalità cartacea, invece, occorre:

misure organizzative:

- identificazione di un responsabile e/o incaricato per ogni archivio nel quale siano custoditi i dati;
- tenuta di un registro dei prelievi del materiale;
- tenuta di un registro degli accessi ad archivi di dati sensibili effettuati fuori dell'orario di servizio;

misure fisiche:

- utilizzo di contenitori dotati di serrature le cui chiavi devono essere custodite dagli addetti e una copia di sicurezza in apposito armadietto ugualmente dotato di serratura;
- presenza di un addetto in orario di servizio nei locali contenenti archivi di dati personali; al di fuori dell'orario di servizio, chiusura dei locali con chiavi custodite dagli addetti e con copia di sicurezza conservato in altro contenitore pure dotato di serratura.

Per quanto riguarda la gestione delle stampe, dei fax e del protocollo occorre adottare:

misure organizzative:

- formazione del personale sulle normative connesse alla gestione dei dati personali, sensibili e riservati;
- emanazione di disposizioni regolamentari che disciplinino la tenuta delle stampe contenenti dati personali, sensibili o riservati prevedendo la loro custodia in contenitori chiusi a chiave quando non vengano utilizzate e la loro distruzione quando non servano più, nonché le modalità di trasmissione delle stesse all'interno della struttura comunale o all'esterno;
- nomina degli addetti alla ricezione dei fax, degli addetti alla protocollazione e degli addetti allo smistamento dei fax e della posta come incaricati del trattamento dei dati, emanando specifiche disposizioni che ne regolamentino l'attività specifica;
- stipula con le società fornitrici del software di contratti che prevedano esplicitamente la fornitura di programmi di controllo sulle stampe contenenti dati personali, sensibili o riservati;

misure fisiche:

- installazione di ulteriori e più efficienti apparecchiature per la distruzione delle stampe;
- separazione del fax addetto alla ricezione da quello addetto alla spedizione e spostamento del primo in un locale protetto (per esempio la stanza dell'ufficio protocollo), con nomina di un responsabile;

misure logiche:

- attivazione di programmi di controllo che registrino chi, quando e da dove richiede le stampe contenenti dati personali, sensibili o riservati.

2.4.3.2.4.2 Modifica non autorizzata

La modifica non autorizzata dei dati può essere la conseguenza di una operazione, volontaria o involontaria, dell'utente oppure la conseguenza di un virus. Non è possibile ipotizzare di impedire agli utenti la modifica dei dati in quanto questo impedirebbe lo svolgimento del normale lavoro operativo, per cui è necessario operare sul sistema delle autorizzazioni. Se la modifica è dovuta ad un virus la prevenzione risulta la stessa già indicata nell'analisi dei rischi legati al fattore software e cioè:

misure organizzative:

- formazione di tutti gli utenti sui pericoli derivanti dai virus, sulle nuove forme che assumono, sulle fonti di contagio;
- emanazione di direttive o regolamenti che disciplinino i comportamenti degli utenti in merito al problema;

misure logiche:

- installazione di programmi antivirus.

Se la modifica è opera di un utente occorre distinguere tra volontarietà ed involontarietà: nel primo caso ci si trova di fronte ad un atto doloso, quindi più grave e presumibilmente più difficile da scoprire. Si possono ridurre i danni con:

misure organizzative:

- tenuta di un elenco di tutte le autorizzazioni concesse per la manipolazione dei dati personali, sensibili o riservati (facoltà connesse ad ogni specifico profilo utente);
- verifica periodica da parte del personale addetto alla sicurezza della validità e completezza di queste autorizzazioni;

misure fisiche:

- copie di riserva aggiornate dei dati;

misure logiche:

- attivazione di programmi che prevedano la registrazione su un file di log dell'autore della modifica, della stazione di lavoro dalla quale viene effettuato il collegamento e la data/ora;
- attivazione di procedure per consentire l'accesso solo da una postazione di lavoro alla volta ed in orari predefiniti.

Nel caso di modifica involontaria questa può derivare dal cattivo funzionamento di un programma (l'analisi di questo tipo di rischio è stata fatta nella sezione dedicata al software), oppure da un difetto delle misure di sicurezza relative all'assegnazione delle autorizzazioni. Si può comunque ipotizzare che una modifica involontaria, per quanto non autorizzata, venga immediatamente rilevata dall'operatore il quale deve avvisare subito chi di dovere.

2.4.3.2.4.3 Distruzione dati

ltre che come forma aggravata della modifica non autorizzata, di cui ci siamo già occupati, la distruzione dei dati può essere conseguenza di un guasto hardware (anche questo già esaminato). Le misure di riduzione del rischio sono quindi già state esaminate.

2.4.3.2.4.4 Esportazione illegittima

'esportazione illegittima dei dati, oltre al danno patrimoniale che può provocare ed al danno di immagine derivante dalla "fuga di notizie", si può configurare come una forma indiretta di accesso non autorizzato alle informazioni. È infatti evidente che questa esportazione, proprio perché illegittima, permette la conoscenza dei dati a persone fisiche o giuridiche che non ne avrebbero la possibilità. Oltre alle misure già esaminate in precedenza occorre adottare:
misure organizzative:

- obbligo del visto del responsabile dei dati personali, sensibili o riservati su tutte le esportazioni esterne di dati personali, sensibili o riservati;
- tenuta, presso ogni responsabile, di un registro delle esportazioni esterne effettuate che contenga tutte le informazioni necessarie per un controllo (destinatario, data, tipo di informazioni esportate, motivazione, ecc.).

2.4.3.2.5 Collegamenti

2.4.3.2.5.1 Malfunzionamento

I collegamenti possono essere di diverso tipo: quelli che riguardano il funzionamento delle apparecchiature (tipicamente la rete elettrica) e quelli che riguardano il flusso dei dati (rete telefonica, rete locale, ecc.). Il malfunzionamento delle rete elettrica (ad esempio sbalzi di tensione) possono provocare momentanei blocchi delle apparecchiature oppure, nei casi più gravi, rotture di alcune componenti con possibile danneggiamento o perdita dei dati registrati. Per ridurre il rischio occorre adottare (e tali soluzioni sono già state utilizzate):
misure fisiche:

- proteggere le macchine più importanti (soprattutto i server) e gli apparati di rete con stabilizzatori di tensione e gruppi di continuità;
- alimentare queste apparecchiature con linee elettriche separate da quelle degli altri uffici in modo da renderle non sensibili ad eventuali sovraccarichi delle linee "normali";
- installare server dotati di alimentatori multipli e sovradimensionati.

Per ridurre i rischi di malfunzionamento della rete locale occorre invece adottare:
misure fisiche:

- installazione di *switch* intelligenti in grado di isolare il ramo della rete in cui si è verificato il problema senza permettere che questo influisca sull'intera rete;

misure logiche:

- installazione di programmi centralizzati di monitoraggio della rete in grado di segnalare tempestivamente tutte le situazioni che possono provocare un malfunzionamento (ad esempio una porta che effettua troppi tentativi prima di riuscire a connettersi) in modo da permettere interventi di manutenzione preventiva.

2.4.3.2.5.2 Interruzione

L'interruzione è a tutti gli effetti una forme grave di malfunzionamento che, oltre ad eventuali danni fisici alle apparecchiature e conseguenti danni ai dati, comporta inevitabilmente il fermo di tutte o parte delle attività. Le misure da adottare per la riduzione del rischio sono le stesse già viste per i malfunzionamenti.

2.4.3.2.5.3 Intercettazione

L'intercettazione è equivalente ad un accesso non autorizzato ai dati tramite collegamento alle linee di trasmissione dati. Può essere involontaria (malfunzionamento della linea di comunicazione o dei commutatori per cui tutti o parte dei dati "passano" anche su una linea adiacente), ma più spesso si tratta di azioni dolose effettuate da esperti. Per ridurre i rischi occorre adottare:

misure fisiche:

- utilizzo esclusivamente di linee dedicate sulle quali vengano effettuati costanti controlli sulla qualità del segnale (la comunicazione interna all'ente avviene già utilizzando linee dedicate e di proprietà dello stesso);

misure logiche:

- adozione della firma elettronica per certificare non solo chi spedisce e chi riceve i dati ma anche che questi non sono stati manomessi durante la trasmissione.

2.4.3.2.6 Sistemi di sicurezza

2.4.3.2.6.1 INCOMPLETEZZA

Per quanti sforzi vengano fatti per la messa a punto di un sistema di sicurezza è sempre possibile che rimangano dei varchi aperti o per una incompleta analisi o per qualche errore nell'implementazione oppure, ancora, per l'avvento di nuove tecniche di intrusione non conosciute inizialmente. È quindi necessario adottare:

misure organizzative:

- monitoraggio dei vari log di sistema per accertare comportamenti anomali che possano presupporre violazione dei criteri di sicurezza stabiliti;
- revisione periodica dell'analisi dei rischi che tenga conto dell'esperienza accumulata e delle nuove tecnologie e metodologie che si rendono disponibili.

2.4.3.2.6.2 MANCATA VERIFICA

Accade che una procedura di sicurezza, perfettamente studiata a tavolino, si riveli poi inefficace per una errata o incompleta implementazione. E' quindi necessario adottare delle misure organizzative, quali il coinvolgimento di tutti i servizi per la segnalazione di eventuali anomalie nella sicurezza riscontrate durante le normali attività d'ufficio.

2.4.3.2.7 Illeggibilità copie di backup

Tutti i supporti magnetici, per loro natura, tendono ad un degrado, con conseguente possibilità di rendere impossibile la lettura totale o parziale dei dati memorizzati. Naturalmente più un supporto è economico (floppy disk) più è soggetto a deterioramento, ma persino sui CD/DVD-ROM non si hanno garanzie sulla effettiva durata della registrazione. Diventa però estremamente pericoloso accorgersi che non è possibile ripristinare una copia fatta, sulla quale evidentemente si faceva affidamento. Può inoltre accadere che, per un errore materiale, la copia di riserva venga effettuata su un supporto sbagliato, già utilizzato per altre copie, con l'effetto di cancellare quelle precedenti che vengono perse. E' quindi necessario adottare:

misure organizzative:

- obbligo di effettuare copie periodiche di tutti i dati richiedendo anche la copia doppia per tutte le informazioni ritenute importanti o non facilmente ricostruibili;
- rigenerazione periodica delle copie di salvataggio a lunga scadenza;

misure fisiche:

- conservazione dei supporti magnetici contenenti le copie di riserva in idonei contenitori che garantiscano una sufficiente protezione dai campi elettromagnetici e dagli eventi naturali (fuoco, acqua, ecc...) nonché dalle intrusioni;
- conservazione della seconda copia in ulteriori idonei contenitori posizionati in ambienti fisicamente separati e distanti prevedendo normative specifiche per lo spostamento dei supporti da e per questi contenitori.

2.4.3.2.8 Eventi naturali

2.4.3.2.8.1 Terremoto

Il territorio comunale di Quarrata, dove sono situati gli edifici comunali, è classificato come zona a rischio sismico. Si ritiene pertanto di poter valutare questa tipologia di rischio come significativa, in quanto la data di costruzione di tali edifici è anteriore alle norme relative alle costruzioni in zone soggette a rischio sismico.

2.4.3.2.8.2 Alluvioni

Gli edifici comunali sono collocati in zone a basso rischio di alluvione; in ogni caso i server di rete (ad esclusione di quelli presenti nell'edificio 5) sono collocati in piani superiori e quindi non a rischio.

2.4.3.2.9 Incidenti

2.4.3.2.9.1 Incendio

Negli uffici comunali sono presenti in misura più o meno maggiore materiali infiammabili, come carta e mobili, pertanto il rischio di incendi non è eliminabile; si può tentare di ridurlo facendo opera di formazione degli operatori sulle misure di prevenzione da adottare ed emanando disposizioni che regolamentino l'attività dei fumatori. Sono stati posizionati all'interno degli edifici, in punti prestabiliti, degli estintori di tipo a polvere e quindi adatti per le apparecchiature elettriche.

2.4.3.2.9.2 Allagamento

Le possibilità di allagamento sono limitate ad infiltrazioni dalle oppure per infiltrazioni dai piani superiori. L'unica difesa da questo tipo di rischio consiste nell'adozione di disposizione che regolino certi comportamenti e nell'effettuazione delle copie di riserva dei dati in modo da poter sostituire le apparecchiature danneggiate senza avere perdita di dati.

2.4.3.2.9.3 Cedimento strutturale

Per gli edifici comunali, di costruzione relativamente recente, si può ipotizzare che non sia possibile un improvviso collasso strutturale ma che eventuali cedimenti sarebbero preceduti da segni evidenti (crepe, rigonfiamenti, ecc.) facilmente diagnosticabili dai tecnici che operano nello stesso palazzo. Questo fattore di rischio può quindi essere considerato non significativo.

2.4.3.2.9.4 Campi elettromagnetici

I campi elettromagnetici possono danneggiare i supporti informatici alterando le informazioni registrate; inoltre, se la potenza del campo è sufficiente, si possono avere anche blocchi o malfunzionamenti delle apparecchiature elettromeccaniche, elettriche ed elettroniche. Non vi sono però nelle vicinanze del palazzo comunale e delle altre sedi dei servizi comunali fonti di emissione di potenza tale da creare problemi di questo genere; inoltre la loro eventuale presenza creerebbe gravi disagi anche alle persone che lavorano nella zona per cui il rischio assumerebbe anche caratteristiche diverse e più gravi. Danneggiamenti ai supporti informatici ed alle apparecchiature si possono verificare se queste sono posizionate vicino ad apparecchi non schermati che generano tali radiazioni abbastanza potenti (condizionatori, stufe elettriche, pompe, ascensori, archivi rotanti, ecc.). La contromisura da adottare si riduce pertanto in una oculato posizionamento delle apparecchiature informatiche lontano da tali fonti di radiazione.

2.4.4 CRITERI PER LA VALUTAZIONE DEI RISCHI

Una volta individuati i rischi, connessi alle risorse ed ai beni individuati, occorre procedere alla valutazione degli stessi, attraverso una indicizzazione del tipo di danno o di lesione possibili.

In particolare, nel processo di valutazione, si tiene conto di due indici fondamentali:

1. la **probabilità** (P): riguarda la frequenza riscontrata o riscontrabile (è importante l'anamnesi);
2. il **danno** (D) è da valutarsi in termini sia quantitativi (ad esempio valore del bene, costi di riparazione, tempi fermo macchina), sia qualitativi (danno all'immagine, interruzione di servizio pubblico, ecc.)

Il **rischio** (R) quindi non è altro che il prodotto tra la probabilità di un evento o di un atto e il danno che questo evento può causare. Secondo i criteri adottati, dando a P un valore fra 1 e 4 ed a D ugualmente fra 1 e 4 si otterrà il valore di R compreso fra 1 e 16.

Probabilità (P)		**Danno (D)**	
1	Improbabile	1	Lieve
2	Poco probabile	2	Medio
3	Probabile	3	Grave
4	Estremamente probabile	4	Gravissimo

Il numero, indicato arbitrariamente con la lettera R (Rischio), dato dal prodotto dei fattori arbitrari P x D, è per l'Ente un indice della gravità dello specifico rischio residuo associato alla specifica mansione presente.

Il valore di R può quindi essere compreso, in maniera discontinua, tra 1 e 16. La tabella riporta l'indicazione degli specifici valori attribuiti ai diversi elementi di rischio.

Tipologia di rischio	P	D	R
accesso non autorizzato	3	4	12
atto doloso	3	4	12
distrazione	3	4	12
manomissione	3	4	12
negligenza	3	4	12
avaria	3	3	9
insufficiente conoscenza dei rischi e delle misure di sicurezza	3	3	9
virus	3	3	9
esportazione illegittima	2	4	8
furto	2	4	8
illeggibilità copie di backup	2	4	8
incendio	2	4	8
incidente	2	4	8
incompletezza	2	4	8
insufficiente conoscenza del sistema e/o dell'applicazione	2	4	8
intercettazione	2	4	8
mancata verifica	2	4	8
duplicazione non autorizzata	3	2	6
malfunzionamento	2	3	6
modifica non autorizzata	2	3	6
modifica non controllata	2	3	6
obsolescenza	2	3	6
malfunzionamento	2	2	4
allagamento	1	4	4

alluvione	1	4	4
cedimento strutturale	1	4	4
distruzione dati	1	4	4
distruzione hardware	1	4	4
distruzione sofware	1	4	4
terremoto	1	4	4
campi elettromagnetici	1	3	3
interruzione	1	2	2

3 TRATTAMENTO DEI RISCHI E PROGRAMMA OPERATIVO

3.1 IL PIANO OPERATIVO

Una volta 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 passo 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'esecuzione del piano operativo sarà regolata dalle priorità espresse dall'Amministrazione e dai tempi relativi all'evoluzione complessiva del sistema informativo.

Le attività di sviluppo sono raggruppabili all'interno delle seguenti aree:

- sicurezza fisica;
- sicurezza logica;
- sicurezza organizzativa;
- piano di continuità operativa.

Di seguito sono riportate, per ogni area di intervento, le principali contromisure attuabili. Gli aspetti della sicurezza organizzativa sono essenziali sia per la sicurezza fisica sia per la sicurezza logica.

3.1.1 SICUREZZA FISICA

Il ruolo della sicurezza fisica è quello di proteggere le persone che operano sui sistemi, le aree e le componenti del sistema informativo.
Le contromisure di sicurezza fisica possono essere ricondotte alle seguenti:

3.1.1.1 Sicurezza di area

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi IT (*Information Tecnology*). Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle *computer room* rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

3.1.1.2 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 pure la protezione da manomissione o furti.

3.1.2 SICUREZZA LOGICA

La sicurezza logica è una componente particolarmente critica della sicurezza del sistema informativo.

Il campo di applicazione della sicurezza logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, 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 (*Information and Communication Technology*) e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.

Nell'ambito della definizione di un'architettura di sicurezza vengono in generale prese in considerazione alternative diverse per l'implementazione di una stessa funzionalità: la scelta dell'opzione da rendere esecutiva viene fatta solo dopo un'analisi costi/benefici.

Le categorie di strumenti tecnologici più utilizzati per far fronte ai principali rischi legati alla sicurezza logica sono i seguenti:

3.1.2.1 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 degli 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 verificano 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 personal computer: il meccanismo più usato a tale scopo è quello delle password, ovvero 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.

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, che può essere:

- una caratteristica fisica, quale l'impronta digitale;
- un certificato digitale che attesta l'identità dell'utente, solitamente memorizzato su *smart card*.

La loro importanza è legata anche al fatto che lo stesso meccanismo può essere utilizzato per realizzare la firma digitale di documenti.

3.1.2.2 Antivirus

I 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, indicati con il termine generico di "codice maligno".

Considerato che un virus informatico può dar luogo a:

a) danni all'hardware;
b) danni al software;
c) danneggiamento di dati (integrità);
d) perdita di tempo impiegato a ripristinare le funzioni del sistema;
e) infezione di altri sistemi;

è necessario attribuire la debita priorità all'adozione di iniziative a difesa attivando una protezione sistematica del sistema informatico e dei dati in essi custoditi e gestiti contro la minaccia rappresentata da virus e macro-virus.

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

a) "infettare" altri programmi, cioè creare copie di se stessi su altri programmi presenti nel sistema;

b) insediarsi nella tabella di partizione e nel settore di *boot* del disco rigido, dove attendono 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 sono stati programmati;
c) inserire operazioni automatizzate (c.d. macro-istruzioni) in documenti di testo, di archivio o di calcolo, dagli effetti indesiderati e nocivi;
d) 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 un'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 gli incaricati dei Servizio Informatica sono tenuti a mantenere operative e aggiornate le procedure software predisposte.

3.1.2.3 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 (*bugs*) 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 dei prodotti non appena viene scoperto un *bug* che compromette la sicurezza del sistema. Tale procedura è nota come installazione 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 di un sistema, come ad esempio un *firewall*, nel prodotto che compromette ogni misura.

3.1.2.4 Strumenti per la riservatezza ed autenticità dei dati

I dati conservati in un sistema informatico devono essere protetti da letture e/o modifiche da parte di utenti non autorizzati. Due sono i momenti principali in cui tali dati devono essere difesi: l'accesso in locale e la trasmissione in rete.

Nel caso in cui i dati da proteggere risiedono su basi di dati è necessario ricorrere a prodotti che implementino politiche di autorizzazione per l'accesso, ai dati possibilmente legati a meccanismi di autenticazione forte degli utenti.

Se l'Amministrazione dispone anche di una infrastruttura per la firma elettronica, è possibile utilizzare tali strumenti anche per apporre firme digitali ad interi file, garantendo in questo modo l'autenticità e l'integrità degli stessi, o in fase di trasmissione si può utilizzare uno schema unico basato sulla cifratura dei dati stessi.

3.1.2.5 Strumenti per la disponibilità dei dati

I dati di un sistema sono sottoposti a una serie di rischi che ne minacciano continuamente la disponibilità. Questi rischi vanno dai mal funzionamenti hardware agli atti di vandalismo perpetrati da intrusi informatici. È possibile ridurre al minimo gli effetti, spesso disastrosi, di tali eventi, predisponendo una serie di accorgimenti tecnologici, come:

- sistemi RAID (*Redundant Array of Inexpensive Disks*): si tratta di hard disk multipli, visti però dal sistema operativo come un singolo disco. La principale proprietà di questi dispositivi è quella di garantire la disponibilità e l'integrità dei dati anche nel caso di guasto hardware di uno dei dischi che compongono il sistema;

- *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*.

È importante quindi predisporre armadi a isolamento termico e/o magnetico, nonché copie multiple dei *back-up* da tenersi in luoghi differenti e distanti tra loro.

3.1.2.6 Sicurezza organizzativa

Il processo della sicurezza dei sistemi informativi automatizzati richiede che, accanto all'adozione di misure tecnologiche precedentemente illustrate, vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo medesimo.

Gli aspetti organizzativi della sicurezza dei sistemi informativi automatizzati riguardano principalmente:

- la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo sicurezza;
- l'adozione di specifiche procedure che vanno a completare e rafforzare le contromisure tecnologiche adottate.

Una serie di aspetti che devono essere regolamentati dalle procedure di sicurezza sono:

- Documenti: accesso ai documenti, conservazione dei documenti, consegna documenti, distruzione;
- Utilizzo del software: installazione, licenze d'uso, modalità d'uso;
- Password: modalità di assegnazione, gestione ed utilizzo, validità nel tempo;
- Virus informatici: misure preventive, regole operative, norme sull'utilizzo dei programmi antivirus;
- Posta elettronica: norme generali, utilizzo corretto, attivazione del servizio;
- Risorse informatiche: generalità, diritto d'uso, autorizzazioni, dismissione, installazione delle postazioni, ergonomia e salute del lavoratore, sicurezza ambientale, protezione da furti, blocco fisico dell'apparato, blocco dell'avvio da disco floppy, protezioni logiche della risorsa;
- Supporti rimovibili, magnetici e ottici: supporto di memorizzazione fisso o rimovibile, distruzione dei supporti magnetici e ottici;
- Rete: gli utenti di rete, directory condivise, monitoraggio e gestione, backup centralizzato di rete, utilizzo della rete;
- Sicurezza dei personal computer portatili;
- Comportamenti illegali;
- Norme disciplinari;
- Riferimenti normativi.

Un ulteriore aspetto inerente alla sicurezza organizzativa è quello concernente i controlli sulla consistenza e sulla affidabilità degli apparati.

È necessario prendere tutte le precauzioni affinché i computer e tutti gli apparati utilizzati per l'erogazione dei servizi non siano un punto di criticità del sistema. Al di là di tutti quelli che sono i controlli sul materiale che va acquistato, è importante creare una banca dati di tutte le dotazioni hardware e software.

È importante che questo archivio venga tenuto aggiornato con le sostituzioni, riparazioni e con i consumi delle apparecchiature.

Questa banca dati dei sistemi informativi, se correttamente gestita, permette di avere una visione storica e precisa del patrimonio arricchita di informazioni estremamente utili e statistiche sul grado di affidabilità e uso dei sistemi; sarebbe di conseguenza di grande aiuto nei processi di acquisto ed in quelli di pianificazione degli investimenti e delle scorte e materiali di consumo.

Nell'acquisto delle apparecchiature più importanti (server, apparati di rete) occorre prevedere sistemi di protezione elettrica delle stesse, quali stabilizzatori di corrente e apparecchiature UPS.

Per l'hardware impiegato in attività di fondamentale importanza, ai fini del conseguimento degli obiettivi istituzionali (*server*), è importante prevedere la necessità di utilizzare apparati che si avvicinino ad un concetto di garantire la massima ridondanza ed affidabilità (*Fault Tolerance*).

Oltre a regolamentare il comportamento dei propri utenti è necessario anche regolamentare quello di utenti esterni (ad esempio consulenti e fornitori) che operano con il sistema informativo automatizzato o comunque che sono abilitati a connettersi con esso.

3.2 OGGETTO E FINALITÀ

Scopo della presente sezione è definire quali misure adottare, e determinare un piano per l'attuazione delle stesse. In particolare le azioni necessarie per l'adozione di idonee misure di sicurezza riguardano:

- **prevenzione**: attività che permette di impedire gli accadimenti negativi, agendo direttamente sulla diminuzione delle probabilità di manifestazione reale di tali accadimenti;
- **protezione**: attività che permette di diminuire la gravità degli effetti nocivi, frutto della manifestazione dell'accadimento negativo.

L'Ente dovrà programmare attività di prevenzione e protezione per ognuno degli agenti di rischio identificati.

3.3 APPLICABILITÀ

Le indicazioni e le prescrizioni contenute nella presente sezione sono applicabili a tutte le attività svolte nell'Ente, aventi influenza sul livello di sicurezza dei lavoratori addetti.

3.4 RESPONSABILITÀ

3.4.1 TITOLARE DEL TRATTAMENTO

È il primo responsabile dell'adozione delle misure di sicurezza nella migliore versione possibile, ai sensi degli articoli 4 e 28 del codice: l'omessa adozione di misure di sicurezza è sanzionata penalmente ai sensi dell'articolo 169.

Inoltre non solo occorre adottare le misure minime, ma anche le misure ritenute idonee alla salvaguardia dell'integrità dei dati e delle trasmissioni (articolo 31).

In questo secondo caso, pur non essendoci una sanzione penale in caso di omissione, tuttavia il titolare può essere chiamato a risarcire i danni causati a terzi, ai sensi dell'articolo 15 del codice.

3.4.2 RESPONSABILE DEL TRATTAMENTO

È nominato, ai sensi dell'articolo 29 del codice, tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento dati, compreso il profilo della sicurezza.

In particolare quindi:

- gestisce e coordina l'opera, sia dei dipendenti interni, sia degli eventuali consulenti esterni, in base alle istruzioni ricevute dal titolare;
- indica le misure preventive e protettive atte alla eliminazione/diminuzione dei rischi identificati in precedenza;
- sottopone al titolare l'elenco delle misure preventive e protettive e predispone, in base alle sue indicazioni, il programma di attuazione particolareggiato di tali misure.

3.5 MISURE DI PREVENZIONE E PROTEZIONE

Dopo aver individuato i fattori di rischio connessi alle risorse e ai beni da proteggere a seguito della valutazione, vengono individuate le misure di prevenzione e protezione più idonee a ridurre o eliminare il rischio stesso.

L'insieme delle misure preventive e protettive costituisce un programma di fondamentale importanza nell'ambito della politica per la sicurezza, poiché fornisce una guida operativa, che permette di gestire la sicurezza con organicità e sistematicità.

Gli interventi correttivi indicati nell'analisi dei rischi possono essere raggruppati in:

misure organizzative:

- O1 - interventi di formazione degli utenti sull'informatica di base, sulle applicazioni gestionali che devono usare, sulle normative relative al trattamento dei dati personali, sulle problematiche della sicurezza, sui virus e le modalità di contagio, ecc...;
- O2 - emanazione di direttive e/o regolamenti che diano istruzioni di comportamento e modalità operative da tenere, sufficientemente elastiche per adattarsi alla maggior parte delle situazioni ma altrettanto rigide e stringenti per le situazioni giudicate ad alto rischio;
- O3 - tenuta di registri, cartacei o informatici, che permettano di avere sotto controllo la configurazione delle macchine, il software installato, la tipologia di contenuto delle diverse banche dati ed il responsabile dei dati, l'elenco degli utenti autorizzati con le specifiche autorizzazioni, ecc...;
- O4 - revisione dei contratti di fornitura del software, di assistenza e manutenzione hardware e software, della fornitura di servizi, ecc...;
- O5 - monitoraggio delle attività connesse a situazioni a rischio;
- O6 - massimo coinvolgimento dei servizi e degli utenti per la messa a punto e la manutenzione di misure di sicurezza efficaci ed efficienti.

misure fisiche:

- F1 - adozione della strumentazione hardware e software più adatta per il raggiungimento degli obiettivi di sicurezza definiti;
- F2 - distruzione dei supporti, cartacei o magnetici, contenenti dati personali, sensibili o riservati non più necessari;
- F3 - attivare la protezione fisica dei locali e dei contenitori dove siano tenuti dati personali, sensibili o riservati;
- F4 - effettuare regolari copie di salvataggio del software e dei dati;
- F5 - verifica periodica della validità dei supporti di salvataggio e delle procedure di recovery.

misure logiche:

- L1 - registrare tutte le modifiche apportate ai dati personali, sensibili o riservati;
- L2 - verifica periodica della "solidità" del sistema di sicurezza adottato;
- L3 - installazione di software di protezione da virus e da accessi ed attività non consentite;
- L4 - installazione di software che renda sufficientemente semplice il monitoraggio dei file di "log";
- L5 - installazione di software di monitoraggio centralizzato della rete e delle comunicazioni.

Intervento	Tempo di avvio	Persone esterne	Costo	Difficoltà	Valutazione Complessiva
O1	Basso	Si	Medio	Bassa	4,8
O2	Medio	No	Basso	Media	5
O3	Medio	No	Basso	Media	5
O4	Medio	Si	Alto	Alta	9,6
O5	Alto	No	Alto	Alta	9
O6	Basso	No	Basso	Media	4
F1	Medio	No	Alto	Alta	8
F2	Basso	No	Basso	Bassa	3
F3	Alto	Si (+)	Alto	Media	12
F4	Basso	No	Basso	Bassa	3
F5	Medio	No	Basso	Media	5
L1	Medio	Si (+)	Alto	Alta	12
L2	Alto	Si (+)	Medio	Alta	12
L3	Basso	Si	Medio	Media	6
L4	Medio	Si (+)	Alto	Alta	12
L5	Alto	Si (+)	Alto	Media	12

Nella tabella precedente si è cercato di dare un peso a questi interventi utilizzando i parametri:

- tempo necessario per rendere operativo l'intervento
- necessità di coinvolgimento di persone o società esterne
- costo dell'intervento
- difficoltà di realizzazione.

Per i fattori *tempo*, *costo* e *difficoltà* è stata usata una scala su tre livelli (basso, medio, alto) corrispondenti ai valori 1, 2, 3; per le persone esterne è stato utilizzato il fattore di correzione 1 se non sono previste, 1,2 se l'intervento è previsto per la fornitura di software o servizi abbastanza standard, 1,5 se si prevede lo sviluppo di soluzioni personalizzate.

Il valore della valutazione complessiva è pertanto dato dalla somma dei tre valori moltiplicato per il fattore di correzione.

Questo dato può quindi assumere valori compresi tra 3 e 13,5.

Dal confronto dei valori riportati nelle tabelle è quindi possibile determinare un piano di intervento che tenga conto della gravità del rischio, della complessità dell'intervento, delle disponibilità finanziarie.

Dato che in attuazione delle misure minime di sicurezza, sono già adottati:

1. il controllo degli accessi via terminale, attraverso l'uso di identificativo utente e password (successivamente potranno essere utilizzate tecnologie più evolute di accesso e di riconoscimento);
2. gli antivirus, che sono già installati su tutti i personal computer dell'Ente;
3. i gruppi di continuità per la protezione degli apparati di rete e dei server (in particolare i server sono già dotati di alimentatori ridondati);
4. aumentata la protezione fisica dei server, con soluzione ridondata dei dischi RAID e configurazione in rack;
5. aumento dell'efficacia dei sistemi antivirus con soluzioni centralizzate degli aggiornamenti;
6. tutte le postazioni sono state dotate di un proprio gruppo di continuità, al fine di ridurre il rischio di interruzioni improvvise dell'attività con rischio di perdita dei dati.
7. è stata resa obbligatoria l'immissione della password nella fase di login;

Saranno intraprese misure di controllo per aumentare l'efficienza delle soluzioni già adottate, mantenendo così aggiornati i sistemi di protezione.

Ulteriori misure previste nell'allegato C) alla delibera G.C. n. 57 del 24/3/98, di seguito riassunte:

misure fisiche:

- il sistema hardware nonché gli archivi cartacei devono essere situati in locali idonei, anche dal punto di vista antincendio, in cui sia sempre presente almeno un addetto in orario di ufficio, chiusi a chiave (con chiavi custodite dagli addetti e chiave di sicurezza in apposito armadietto) fuori dal suddetto orario;
- è disposto l'impiego di armadi e schedari adatti e dotati di congegni di chiusura a chiave per la conservazione dei fascicoli, raccoglitori, cartelle, registri ecc...;
- i supporti magnetici su cui sono stati effettuati i salvataggi di sicurezza degli archivi devono essere custoditi in armadi o cassetti chiusi a chiave;

misure logiche:

- identificazione del destinatario delle comunicazioni;
- si dovranno effettuare salvataggi con periodicità adeguata alla natura della banca dati e del suo aggiornamento, su almeno due supporti alternati;

misure organizzative comuni ai trattamenti automatizzati (banche dati) e ai trattamenti non automatizzati (archivi cartacei):

- Prescrizione di linee guida per la sicurezza con atto giuntale;
- Abilitazione, professionalità e responsabilità del manipolatore;
- Formazione professionale dell'utente tramite istruzione sulla portata del Codice, con particolare riferimento a obblighi e sanzioni.

4 PIANO DI FORMAZIONE DEL PERSONALE

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.

4.1 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.

Le opportunità per raggiungere quest'obiettivo sono ad esempio presentazioni, opuscoli, seminari, riunioni dei Responsabili dei Servizi con i propri collaboratori.

Per la corresponsabilizzazione, si deve prevedere di:

- coinvolgere i Responsabili dei Servizi 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 per i collaboratori esterni, privati e pubblici, persone fisiche e giuridiche, che interagiscono in modo significativo con l'Amministrazione.

4.2 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;
- conoscenza delle misure di sicurezza da adottare e da gestire ai diversi livelli di responsabilità.

Dunque anche i fruitori della formazione saranno di diversa tipologia: è fondamentale riuscire a sensibilizzare i manager delle Amministrazioni affinché questi riescano a trasmettere i principi fondamentali del sistema all'interno delle loro realtà.

Per raggiungere i suoi obiettivi il programma di formazione deve essere concepito in modo tale da:

- rendere consapevoli i partecipanti sull'importanza delle scelte compiute dall'Ente;
- coinvolgere i partecipanti sulle problematiche inerenti alla sicurezza;
- responsabilizzare i partecipanti sulle attività da eseguire per garantire il mantenimento di un livello di sicurezza accettabile.

Occorre quindi progettare due tipologie di corsi, distinte secondo i 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.

I corsi dovranno essere progettati in base alle esigenze ed al sistema di sicurezza sviluppato, in funzione del patrimonio informativo da proteggere e del 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 la gestione degli accessi (password, ecc…);
- i possibili rischi: virus, intercettazioni, intrusioni, ecc..

È necessario tenere presente che le attività relative alla sicurezza non rappresentano un appesantimento del lavoro quotidiano, ma una volta che entrano nel ciclo standard delle operazioni da compiere, contribuiscono a garantire il personale dal rischio di perdere o comunque compromettere parte del lavoro fatto.

4.3 NORME DI COMPORTAMENTO

Come è già stato anticipato nelle sezioni precedenti, il comportamento tenuto dal personale dell'ente al momento che interviene ed opera con il sistema informatico costituisce una componente fondamentale per il corretto funzionamento di un sistema di sicurezza. È opportuno che vi sia la consapevolezza da parte di ciascuno che gli effetti determinati dalle proprie azioni possono dare luogo ad una serie imprevedibile ed inaspettata di eventi con risultati, a volte, anche di estrema gravità.

4.3.1 FATTORI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE

I seguenti comportamenti, comportano un incremento dei livelli di rischio informatico:

a) uso di software (soprattutto giochi, sfondi, suonerie, screen saver, ecc…) prelevato da siti Internet o in allegato a riviste o libri;
b) allontanarsi dalla propria postazione di lavoro, per un determinato e significativo periodo, senza tornare alla finestra di blocco iniziale ma rimanendo con il programma aperto;
c) ricezione di applicazioni e dati dall'esterno, Amministrazioni, fornitori, ecc.;
d) utilizzo dello stesso computer da parte di più persone;
e) collegamento a Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
f) collegamento a Internet e attivazione degli applets di Java o altri contenuti attivi;
g) non prestare attenzione ai file allegati ai messaggi di posta elettronica;
h) riutilizzo di dischetti già adoperati in precedenza o preformattati;

4.3.2 NORME BASILARI DI COMPORTAMENTO

Al fine di evitare problemi correlati ad infezioni informatiche, dovranno essere rispettate almeno le seguenti prescrizioni:

a) i floppy disk/chiavi USB, sia quando vengono forniti sia quando vengono ricevuti, devono essere sottoposti a scansione da parte del programma antivirus;
b) è obbligatorio sottoporre a controllo antivirus tutti i floppy disk/chiavi USB o CD/DVD ROM di provenienza incerta prima di eseguire o caricare uno qualsiasi dei file in esso contenuti;
c) proteggere in scrittura tutti i propri floppy disk di sistema o contenenti programmi eseguibili;
d) non trasmettere mai in rete file eseguibili (.COM, .EXE) e di sistema (.SYS);
e) non utilizzare i server di rete come stazioni di lavoro;

f) tornare alla schermata di blocco iniziale del sistema o lanciare lo *screen saver* con attivata la password di protezione, ogni qualvolta ci si allontana dalla propria postazione di lavoro, per un determinato e significativo periodo di tempo;
g) limitare l'uso di floppy disk come supporto di scambio di dati all'interno dell'Ente, privilegiando l'uso della posta elettronica;
h) utilizzare le cartelle condivise pubbliche solo per le finalità per cui sono state predisposte, ovvero come aree temporanee di scambio per le informazioni, rimuovendo i dati al momento che non sono più necessari;
i) non modificare la configurazione hardware e software del personal computer, così come consegnata dal personale del Servizio Informatica;
j) l'installazione di un qualsiasi programma deve sempre essere autorizzata dal relativo Responsabile del Servizio e dal Servizio informatica sia per motivi di ordine di sicurezza e stabilità delle apparecchiature che per motivi legali;
k) non aggiungere mai dati o file ai floppy disk contenenti programmi originali.

4.3.3 REGOLE OPERATIVE

1. Tutti i computer dell'Amministrazione devono essere dotati di programmi antivirus.
2. L'Amministrazione deve assicurarsi che i computer delle società esterne, qualora interagiscano con proprio sistema informatico, siano dotati di adeguate misure di protezione antivirus.
3. Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo dischetti preventivamente controllati e certificati singolarmente ogni volta.
4. Ogni personal computer deve essere sottoposto a controllo antivirus.
5. I dischetti provenienti dall'esterno devono essere sottoposti a verifica da attuare con un personal computer non collegato in rete (macchina da quarantena), ed inoltre devono essere individuate le aree dell'Amministrazione che, in relazione alla loro particolare attività, sono da considerare a più alto rischio nei riguardi dell'infezione da virus.
6. All'atto della individuazione di una infezione, il virus deve essere immediatamente rimosso.
7. Tutti gli utenti del sistema informatico devono sapere a chi rivolgersi per la disinfezione e l'informazione dell'infezione deve essere mantenuta riservata.
8. Il personale deve essere a conoscenza che la diffusione dei virus è punita dall'art. 615-quinquies del Codice Penale, che qui si riporta:

Art. 615-quinquies. Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico:

"Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo e per effetto il danneggiamento di un sistema informatico o telematico, dei dati e dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, del suo funzionamento, è punito con la reclusione sino a due anni e con multa sino a lire venti milioni".

9. Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.
10. In base al Decreto Legge n. 518/1992 ciascun dipendente è diffidato dall'installazione di software non acquistato ufficialmente dall'Ente, ed in caso contrario ne sarà pienamente responsabile secondo quanto stabilito dal Decreto Legge menzionato, esonerando il Servizio Informatica da ogni conseguenza civile e penale.

4.3.3.1 Modulistica per la sicurezza organizzativa

La sicurezza organizzativa si realizza adottando opportune disposizioni per:

a) sistema di selezione e gestione del personale;

b) codici etici di comportamento;
c) suddivisione degli incarichi;
d) formazione/sensibilizzazione;
e) procedure interne.

A questo scopo è stata prevista una serie di moduli atti a definire le procedure interne per l'assegnazione e presa in carico da parte del personale delle risorse hardware e software.

Modello 1

Accettazione di responsabilità per l'utilizzo dei programmi

Cognome e nome dipendente _____
Servizio _____

Con la presente dichiaro:

a) Di assumermi le normali responsabilità circa la tutela del software (operativo, applicativo e comunicativo) che mi è stato assegnato nell'ambito delle mie competenze per lo svolgimento delle mie mansioni.
b) Di non manomettere e/o modificare in alcun modo la configurazione software come mi è consegnata, elencata e notificata nella "Accettazione di responsabilità per l'utilizzo della stazione di lavoro".
c) Di attenermi al rispetto delle norme contemplate dal Decreto Legislativo n. 518/1992, che recepisce la direttiva CEE 91/250 (di cui ho avuto copia conforme) e del regolamento interno.
d) Di non divulgare ad altri e a qualunque titolo, qualsiasi tipo di informazione di natura informatica, sia essa rappresentata da procedure, programmi, archivi, dati od altro, di proprietà dell'Ente, senza l'autorizzazione del mio Responsabile di Servizio.

_____ _____

Il responsabile del Servizio Il dichiarante

Modello 2

Accettazione di responsabilità per l'utilizzo della stazione di lavoro

Cognome e nome dipendente _____
Servizio _____

Con la presenta dichiaro di prendere in carico il personal computer, l'hardware collegato e l'elenco del software (operativo, applicativo e comunicativo) che l'Ente mi ha assegnato e che potrò utilizzare nell'ambito delle mie competenze, nello svolgimento delle mie mansioni, impegnandomi a non installare software aggiuntivo non regolarmente acquisito.

Personal Computer

Costruttore				**Matricola**		
				Modello		
CPU	**Clock**	**RAM**	**H.D.**	**CDROM**	**Scheda Audio**	**Monitor**
Scheda Video	**RAM Video**	**Scheda Rete**	**Altro**			

Hardware associato

Tipo	**Modello**	**Matricola**

Software

Marca	**Modello**	**Versione**	**Matricola**

Inoltre con la presente dichiaro:

- Di assumermi le normali responsabilità per la tutela delle attrezzature informatiche che mi sono state assegnate nell'ambito delle mie competenze per lo svolgimento delle mie mansioni.
- Di non manomettere e/o modificare in alcun modo la configurazione hardware che mi è stata assegnata, elencata in precedenza.

_____ _____

Il responsabile del Servizio Il dichiarante

Normativa di comportamento per l'installazione di programmi per personal computer

1. Questa specifica attività è permessa dalle leggi vigenti dello Stato e dalle procedure e/o norme e/o regolamenti ufficializzati ed attuati dall'Ente, nell'ambito dei suoi diritti e delle sue possibilità.
2. Per quanto riguarda la **tipologia**, viene inteso "**software per PC**" qualunque tipo di informazione (programmi, dati, archivi, documentazione, circolari, ecc.) che può essere installata, utilizzata e gestita sui personal computer e/o altre attrezzature informatiche di natura decentrata affidata all'utente e di proprietà dell'Ente.
3. Per quanto riguarda la **provenienza**, viene inteso "**software per PC**" qualunque tipo di informazione che giunge e/o è stata prodotta da fonti esterne all'Ente (ad esempio riviste specializzate, collaborazioni esterne, demo di software house, iniziative pubblicitarie, ecc.) che non sono previste, autorizzate dal Servizio Informatica.
4. L'operazione di installazione dovrà essere autorizzata, in forma scritta, dal Responsabile di Servizio e dal Responsabile del Servizio Informatica.
5. Prima di eseguire qualunque attività di installazione e di utilizzo del software sulla sua postazione di lavoro, il personale incaricato dai sistemi informativi dell'Ente, dovrà porre in funzione tutte le precauzioni, metodologie ed ogni operazione di diagnostica "antivirus" in suo possesso, atte a prevenire e precludere ogni forma di infezione.

Normativa di comportamento per la gestione delle attrezzature informatiche

1. Questa specifica attività è permessa dalle leggi vigenti dello Stato e dalle procedure e/o norme e/o regolamenti ufficializzati ed attuati dall'Ente, nell'ambito dei suoi diritti e delle sue possibilità.
2. Sono intese "**attrezzature informatiche**" i personal computer e ogni altro tipo di periferica hardware collegata ai PC come monitor, stampanti, scanner, unità di controllo e comunque ogni tipologia di attrezzature informatica o telematica utilizzata dagli utenti e di proprietà dell'Ente.
3. Se si opera utilizzando un collegamento con archivio di dati, tornare alla schermata di blocco iniziale del sistema operativo (tipicamente Microsoft Windows 200 professional o Microsoft Windows XP), ogni qualvolta ci si allontana dalla propria postazione di lavoro per un determinato e significativo periodo di tempo.