



Ufficio Sistemi Informativi

Documento programmatico sulla sicurezza

Ing. Paolo Bertamini

Indice

1 PREMESSE.....	5
1.1 RICHIAMI NORMATIVI.....	5
1.2 DEFINIZIONI.....	6
1.2.1 DEFINIZIONI GENERALI.....	6
1.2.2 TERMINI TECNICI	7
1.2.3 ABBREVIAZIONI.....	7
1.3 ASPETTI DELLA SICUREZZA NEL TRATTAMENTO DI DATI	7
2 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ	9
2.1 GENERALITÀ.....	9
2.2 DISTRIBUZIONE TERRITORIALE DELLE SEDI DELL'ENTE.....	9
3 SITUAZIONE ATTUALE E LINEE DI INTERVENTO.....	10
3.1 SICUREZZA RISPETTO ALLA POSSIBILITÀ DI DANNI AI LOCALI, AGLI ARCHIVI E/O PERDITA DEI DATI.....	10
3.1.1 ASPETTI GENERALI.....	10
3.1.2 SITUAZIONE ATTUALE.....	10
3.1.3 LINEE DI INTERVENTO.....	11
3.1.4 MISURE MINIME DI SICUREZZA	12
3.2 SICUREZZA RISPETTO ALLA POSSIBILITÀ DI INTERRUZIONE DEL FUNZIONAMENTO DELLE APPARECCHIATURE.....	12
3.2.1 ASPETTI GENERALI.....	12
3.2.2 SITUAZIONE ATTUALE.....	12
3.2.3 LINEE DI INTERVENTO.....	13
3.2.4 MISURE MINIME DI SICUREZZA	13
3.3 SICUREZZA RISPETTO ALLA POSSIBILITÀ DI ACCESSO FISICO AI LOCALI, AI SISTEMI ED AGLI APPARATI DI RETE....	14
3.3.1 ASPETTI GENERALI.....	14
3.3.2 SITUAZIONE ATTUALE.....	14
3.3.3 LINEE DI INTERVENTO.....	15
3.3.4 MISURE MINIME DI SICUREZZA	15
3.4 SICUREZZA RISPETTO AGLI ACCESSI NON AUTORIZZATI AI SISTEMI ED ALLE INFORMAZIONI.....	15
3.4.1 ASPETTI GENERALI.....	15
3.4.2 SITUAZIONE ATTUALE.....	16
3.4.3 LINEE DI INTERVENTO.....	16
3.4.4 MISURE MINIME DI SICUREZZA	17
3.5 SICUREZZA RISPETTO ALLA POSSIBILITÀ DI ACCESSO ALLA RETE ED AI SISTEMI PER VIA TELEMATICA.....	17
3.5.1 ASPETTI GENERALI.....	17
3.5.2 SITUAZIONE ATTUALE.....	17
3.5.3 LINEE DI INTERVENTO.....	18
3.5.4 MISURE MINIME DI SICUREZZA	18

3.6 SICUREZZA RISPETTO ALLA DIFFUSIONE DI VIRUS INFORMATICI ED AGGIORNAMENTI DEI PROGRAMMI APPLICATIVI E DEI SISTEMI OPERATIVI.....	18
3.6.1 ASPETTI GENERALI.....	18
3.6.2 SITUAZIONE ATTUALE.....	19
3.6.3 LINEE DI INTERVENTO.....	19
3.6.4 MISURE MINIME DI SICUREZZA	19
3.7 SICUREZZA RISPETTO ALL'INTERCETTAZIONE DELLE INFORMAZIONI TRASMESSE ATTRAVERSO RETI TELEMATICHE	19
3.7.1 ASPETTI GENERALI.....	19
3.7.2 MISURE MINIME DI SICUREZZA	20
3.8 SICUREZZA RISPETTO AL TRATTAMENTO DEI DATI CON STRUMENTI CARTACEI O COMUNQUE NON AUTOMATIZZATI	20
3.8.1 ASPETTI GENERALI.....	20
3.8.2 MISURE MINIME DI SICUREZZA	20

1 Premesse.

1.1 Richiami normativi

Il D.Lgs 196 del 30/06/2003 che sostituisce la legge 675/96 ed il relativo corollario normativo (in particolare il dlgs 135 del 11/5/99 ed il dpr 318/99), pone con forza l'attenzione sui vincoli e gli obblighi di sicurezza dei patrimoni informativi. In particolare vengono normati i trattamenti dei diversi tipi di informazione ovvero dati personali, dati identificativi, dati sensibili e dati giudiziari. I concetti espressi riguardano genericamente l'informazione, comprendendo articoli relativi sia al trattamento dei dati tramite l'ausilio di supporti di conservazione ed elaborazione elettronici sia per il trattamento degli archivi cartacei.

Il DPR n.318/99, regolamento emanato a norma dell'art.15, c.2 della L.675/96, individuava il complesso di misure tecnico-informatiche, organizzative, logistiche e procedurali di sicurezza che prefiguravano il livello minimo di protezione richiesta in relazione ai rischi di distruzione o perdita anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. In relazione al DPR n.318/99 la Provincia di Lucca, con delibera G.P. n°501 del 22/12/2000 ha approvato il primo **Documento Programmatico sulla Sicurezza** che prendeva in considerazione le diverse tipologie di rischio relative al trattamento dei dati sia in forma elettronica che in forma cartacea e per ciascuna di queste proponeva le norme minime da adottare per il corretto e sicuro trattamento delle informazioni.

L'art.34, comma g) del DLgs 196/03 prevede la stesura di un nuovo ed aggiornato Documento Programmatico sulla Sicurezza redatto secondo le specifiche indicate nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" della legge stessa, che tenga conto degli aggiornamenti normativi e delle evoluzioni tecnologiche degli ultimi anni. Queste informazioni, unitamente agli aggiornamenti dei Sistemi Informativi della Provincia di Lucca impongono un'articolazione del Documento Programmatico sulla Sicurezza che tenga conto delle mutate valutazioni di esposizione al rischio.

Con Deliberazione del Consiglio Provinciale n°139/A del 21/12/2006 si è provveduto all'aggiornamento degli elenchi dei dati sensibili e giudiziari trattati all'interno dell'ente a cui si fa ancora riferimento non essendo intervenute modificazioni nel frattempo.

Con provvedimento del Garante per la Privacy del 27 novembre 2008 pubblicato in G.U. n.300 del 24/12/2008 avente ad oggetto "*Misure ed accorgimenti prescritti ai titolari di trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" viene colmata una lacuna nelle definizioni del Codice sulla Privacy. Le funzioni tipiche dell'amministratore di sistema venivano richiamate in ogni caso nell'Allegato B dove si prevedeva l'obbligo per i titolari dei trattamenti di assicurare la custodia delle credenziali di autenticazione. Nel loro complesso le norme predette mettono in evidenza la particolare capacità di azione propria degli amministratori di sistema per le quali è previsto il possesso di requisiti tecnico-organizzativi, di onorabilità, professionali, morali e di condotta ma tali figure non erano ancora esplicitamente contemplate nelle definizioni. Con il provvedimento del Garante viene quindi introdotto l'obbligo da parte del titolare di trattamenti, di individuare la figura di "Amministratore di sistema". Il Segretario Generale, Direttore Generale, titolare dei trattamenti per la Provincia di Lucca, con nota prot. n° 67544 del 18/03/2009 ha individuato nella persona dell'Ing.Paolo Bertamini, Responsabile della U.O.C.Sistemi Informativi, l'**Amministratore di Sistema** per l'ente.

Ferme restando quindi le regole minime imposte dall'Allegato B del D.Lgs. 196/03 e successive modificazioni, le linee di intervento proposte in questo documento vanno nella direzione

dell'applicazione delle norme previste nella Legge, ma soprattutto in quella di garantire un adeguato livello di sicurezza al Sistema Informativo dell'ente.

1.2 Definizioni

1.2.1 Definizioni generali

Ai fini del presente documento si intende per:

a) **«trattamento»**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) **«dato personale»**, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) **«dati identificativi»**, i dati personali che permettono l'identificazione diretta dell'interessato;

d) **«dati sensibili»**, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) **«dati giudiziari»**, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del [D.P.R. 14 novembre 2002, n. 313](#), in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) **«titolare»**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) **«responsabile»**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) **«incaricati»**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) **«interessato»**, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) **«comunicazione»**, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) **«diffusione»**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) **«dato anonimo»**, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) «**blocco**», la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) «**banca dati**», qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

1.2.2 Termini Tecnici

Ai fini del presente documento si intende, inoltre, per:

a) «**misure minime**», il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

b) «**strumenti elettronici**», gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) «**autenticazione informatica**», l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) «**credenziali di autenticazione**», i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

e) «**parola chiave**», componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) «**profilo di autorizzazione**», l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

g) «**sistema di autorizzazione**», l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

h) «**Intranet**», il sito interno dell'ente raggiungibile solo attraverso la rete dati interna o attraverso accessi controllati dall'esterno gestiti dal firewall, attraverso il quale vengono forniti servizi alle strutture dell'ente.

1.2.3 Abbreviazioni

Ai fini del presente documento se non diversamente esplicitato, si intenderà per;

a) «**dati**», dati personali, identificativi, sensibili o giudiziari

1.3 Aspetti della Sicurezza nel trattamento di dati

Il termine "Sicurezza" fa in realtà riferimento a diversi tipi di rischio a cui un sistema informativo è sottoposto. Alcuni aspetti riguardano le garanzie della conservazione dei dati e del ripristino delle

funzionalità dei sistemi a fronte di guasti od eventi fortuiti che possono verificarsi. A fianco di questi aspetti, i più tradizionali, altri hanno assunto sempre maggiore importanza e peso: i rischi di intromissione, appropriazione o manomissione di dati per azioni premeditate di dolo o danneggiamento. Il seguente elenco riepiloga la casistica dei fattori di rischio:

1. Guasti od eventi fortuiti che causino danni agli archivi e/o perdita di dati;
2. Guasti od eventi fortuiti che rendano non utilizzabili i sistemi preposti ad una data funzione;
3. Accesso fisico non autorizzato ai sistemi ed agli apparati di rete.
4. Accesso non autorizzato alle informazioni gestite all'interno di un sistema informatico;
5. Accesso alla rete ed ai sistemi informatici attraverso strumenti telematici;
6. Danni provocati da Virus.
7. Intercettazione delle informazioni trasmesse attraverso reti telematiche.
8. Accesso ai dati personali contenuti in archivi cartacei o comunque non automatizzati.

Nel seguito i diversi aspetti saranno esaminati, partendo dalla situazione attuale, con la definizione delle misure di sicurezza attuali e le linee di intervento previste.

È importante tenere conto che per innalzare il livello di sicurezza (sia informatica che non) è necessario un impegno di risorse sia professionali che tecnologiche, proporzionale al risultato atteso. Impegno di risorse che viene ormai considerato strategico e fondamentale, da tempo nell'azienda privata e più recentemente anche nell'ambito della Pubblica Amministrazione.

2 Distribuzione dei compiti e delle responsabilità

2.1 Generalità

Con deliberazione di Consiglio Provinciale n° 69 del 21/03/2001 l'ente ha individuato nei Dirigenti delle strutture preposte al trattamento dei dati, i responsabili degli stessi.

Con Determinazione Presidenziale n° 9 del 2/2/2009 è stata affidata al Segretario Generale, Direttore Generale, Dr. Antonio Le Donne, la titolarità delle banche dati gestite dall'ente ai sensi del D.Lgs.196/03.

I Dirigenti delle strutture preposte al trattamento dei dati hanno individuato le U.O. o strutture a cui afferiscono per competenza gli ambiti del trattamento dei dati attribuiti.

I Dirigenti provvedono, ad ogni cambiamento organizzativo, all'individuazione dell'unità e degli addetti alla stessa.

Gli incaricati ai trattamenti svolgono la loro attività secondo le istruzioni impartite dai rispettivi Dirigenti.

L'ente dovrà prevedere nel proprio piano di formazione interna, specifici corsi destinati ai responsabili ed agli incaricati dei trattamenti.

2.2 Distribuzione territoriale delle sedi dell'ente

La Provincia di Lucca è dotata di molte sedi sparse sul territorio provinciale. Oltre alla sede principale di Palazzo Ducale nel centro di Lucca, che ospita molti servizi e uffici, vi sono la sede di via Barsanti e Matteucci che ospita i Servizi Agricoltura, Caccia e Pesca, Sviluppo Economico, Turismo, la sede di San Vito che ospita il Servizio Mercato del Lavoro, il Centro per l'Impiego di Lucca, il Servizio Formazione Professionale, la sede di via della Quarquonia che ospita il Servizio Difesa del Suolo, la Stazione Ferroviaria di Ponte a Moriano che ospita gli uffici della Polizia Provinciale, i Centri per l'Impiego di Viareggio, Fornaci di Barga e Castelnuovo, la sede territoriale della Formazione Professionale a Viareggio oltre a uffici di diversi servizi collocati presso la Stazione di Castelnuovo di Garfagnana.

Presso ciascuna di queste sedi vengono quindi trattati dati di tipo diverso e devono essere individuati, se del caso, i relativi responsabili della sicurezza fisica degli uffici.

Tutte queste sedi sono collegate con una rete privata virtuale alla sede principale. Alcune di queste sono dotate di server decentrati che effettuano backup locali dei dati trattati. Per quanto i server possano essere gestiti centralmente ed i backup monitorati dalla sede centrale, per ciascuna situazione deve essere individuato un responsabile per la sostituzione dei nastri di backup la dove non si sia già passati alla tecnologia di dischi esterni USB o di rete.

3 Situazione attuale e linee di Intervento

3.1 Sicurezza rispetto alla possibilità di danni ai locali, agli archivi e/o perdita dei dati

3.1.1 Aspetti generali

La sicurezza, nella sua accezione più generale, deve comprendere anche la sicurezza dei locali all'interno dei quali sono conservati i dati e gli archivi.

Si tratta quindi di prendere in considerazione possibili rischi collegati a calamità naturali, agli incendi, ai danni provocati da comportamenti dolosi, per capire quali potrebbero essere le migliori politiche di sicurezza per la protezione verso questa tipologia di rischi.

In particolare, sia per quanto riguarda i sistemi informatici che per gli archivi cartacei, deve essere presa in considerazione la sicurezza dei locali che li ospitano verso i rischi collegati ad esempio ad incendi o inondazioni.

Nel caso di dati conservati in formato elettronico, è necessario provvedere al loro salvataggio con politiche di backup che dipendono dalla tipologia e dall'importanza del dato.

3.1.2 Situazione attuale.

L'ente è dotato di dispositivi antincendio ai sensi del D.Lgs 626/94 e di un sistema di rilevazione dei fumi all'interno degli uffici posti a Palazzo Ducale.

Gli archivi cartacei si trovano all'interno di locali non soggetti a rischio inondazione in quanto posti al di sopra del piano stradale.

Esiste un sistema di video-sorveglianza all'interno di Palazzo Ducale che allo stato attuale non registra le immagini e non può quindi essere utilizzato per individuare accessi illeciti a posteriori.

La distribuzione degli applicativi e delle banche dati su diversi sistemi ha portato ad una frammentazione dei criteri di salvataggio delle applicazioni.

Per quanto riguarda le applicazioni su sistemi server, esistono già soluzioni differenziate:

- per i sistemi gestiti direttamente dalla U.O.C. Sistemi Informativi, i salvataggi vengono effettuati dal personale interno, con politiche di backup giornaliera, settimanali e/o mensili prestabilite a seconda dei dati trattati;
- per i server installati in sedi diverse o presso altri dipartimenti, i salvataggi vengono di norma gestiti dal personale del settore che utilizza il sistema, secondo criteri concordati tra il personale dell'Ufficio Sistemi Informativi, gli utenti ed eventualmente il fornitore del software. I server delle sedi periferiche dei Centri per l'Impiego e quello della sede di Lucca che condivide le risorse hardware con il servizio Formazione Professionale, ed il server presente nella sede di via Barsanti & Matteucci sono stati dotati di sistema di backup a disco invece del tradizionale nastro (hard disk esterni) che offre costi di gestione e velocità di ripristino decisamente migliori. Per aumentare ulteriormente la velocità nel recupero dei dati sono state abilitate su tutti i server Windows le cosiddette *shadow copy* che consentono 'fotografare' tutti i file che hanno subito una modifica rispetto alla fotografia precedente, in un arco temporale. Le shadow copy vengono eseguite due volte al giorno. Questo sistema consente di recuperare una copia di un file erroneamente modificato o addirittura cancellato senza fare ricorso ai nastri di backup

rendendo l'operazione molto più veloce e delegando ai nastri solo la gestione del *disaster recovery*.

- Per quanto riguarda i dati degli utenti che si collegano ad un 'dominio' interno, i dati risiedono in realtà sui server e vengono quindi salvati secondo le politiche sopra indicate.

Per le applicazioni ed i dati presenti sui diversi personal computer, i salvataggi sono demandati agli utenti.

Considerata la complessità dei diversi sistemi gestiti dall'U.O.C. Sistemi Informativi, si è ritenuto necessario definire un quadro complessivo esatto delle modalità di salvataggio e di conservazione delle copie, tenendo conto che la normativa oltre ai criteri di sicurezza impone ormai di riportare questi aspetti ad una gestione organizzata e documentata. Per questo motivo è stato preparato il documento "*Politiche di backup della Provincia di Lucca*" che costituisce l'**Allegato 1** al presente documento e che viene mantenuto aggiornato ad ogni cambiamento dei sistemi interni.

3.1.3 Linee di intervento.

L'alluvione del dicembre 2009 ha messo in risalto la pericolosità connessa allo stoccaggio di documenti e/o archivi in siti non idonei o soggetti ad esondazioni. Sarà pertanto opportuno verificare puntualmente che tutti gli archivi di deposito contenenti i documenti dell'ente, si trovino in zone non soggette a tali pericoli.

Il percorso verso questo obiettivo passa sicuramente attraverso una fase di ricognizione e verifica puntuale della situazione, partendo dall'elenco dei dati trattati dall'ente per poi individuare le zone eventualmente scoperte e/o migliorabili e procedere alla realizzazione della soluzione adeguata.

L'utilizzo dell'informatica personale ha poi posto un nuovo aspetto, quello del salvataggio dei dati prodotti direttamente dall'utente con strumenti di automazione d'ufficio (per la maggior parte documenti, ma talvolta anche veri e propri archivi) e della sua posta elettronica. Questo aspetto appare oggi inevitabilmente affidato all'utilizzatore del posto di lavoro. Se il problema del salvataggio dei documenti di office è risolvibile con l'utilizzo di File Server dipartimentali, il problema del salvataggio della posta elettronica non è altrettanto semplice. Nel corso dell'anno dovranno essere pertanto valutate diverse soluzioni per porre rimedio a questo problema che sta diventando sempre più strategico.

L'aspetto deve essere migliorato attraverso diverse attività in parte già attuate o avviate, che possono essere percorse parallelamente:

1. Integrazione della gestione dei documenti in applicazioni basate su database (deliberazioni, determinazioni, pratiche, cedolini, cartellini, etc.), che consentono l'archiviazione "organizzata" di una gamma di documenti importante per quantità e qualità;
2. Utilizzo di server dipartimentali per il controllo dell'accesso degli utenti alla rete interna dell'ente, per il salvataggio dei dati degli utenti e per l'organizzazione dei gruppi di lavoro. L'utilizzo di questi file server è utile anche per semplificare la manutenzione dei Personal Computer rendendo molto più semplice la loro sostituzione;
3. Utilizzo di un servizio di posta elettronica con protocollo IMAP e con caratteristiche adeguate a mantenere tutta la posta elettronica dell'ente in linea consultabile via web in modo da eliminare anche l'ultima banca dati importante ancora sicuramente collegata alla postazione di lavoro.

Nel corso del 2007 l'ente si è dotato di una cassaforte ignifuga che contiene i nastri dei server ospitati in sala macchine con l'esclusione di quelli delle due unità di backup multinastro che non possono essere sostituiti quotidianamente. La cassaforte è posizionata in una stanza diversa

rispetto alla sala macchine così da avere maggiori probabilità di resistere ad un eventuale danno che la dovesse colpire. La chiave della cassaforte è conservata presso i locali dell'Ufficio Sistemi Informativi. Le password dei sistemi server, di rete, delle banche dati e delle applicazioni, sono conservate in un'apposita banca dati protetta da password, su un server dell'ente e salvata quotidianamente.

3.1.4 Misure minime di sicurezza

Tutte le banche dati informatizzate ed i documenti elettronici contenenti dati personali, sensibili o giudiziari riportate nei trattamenti segnalati nell'allegato alla Delibera C.P. 139/A del 21/12/2006, devono essere salvati su sistemi server. Per garantire la conservazione dei dati l'addetto al trattamento delle informazioni ovvero l'Amministratore di Sistema o suo incaricato, procederà all'effettuazione periodica di copie di sicurezza al fine di evitare perdite anche involontarie per guasti o manovre errate. Le copie di sicurezza effettuate su supporti rimovibili dovranno essere conservate con cura all'interno di contenitori muniti di serratura ed i supporti utilizzati, dischetti, nastri, CD, DVD, ecc. dovranno essere rinnovati periodicamente per garantirne l'affidabilità. I supporti utilizzati per la memorizzazione di dati sensibili potranno essere riutilizzati a patto che il contenuto possa essere definitivamente cancellato, altrimenti dovranno essere distrutti.

3.2 Sicurezza rispetto alla possibilità di interruzione del funzionamento delle apparecchiature

3.2.1 Aspetti generali

L'aspetto è, per quanto possa suonare inconsueto, il meno critico rispetto a quelli elencati. Non si tratta infatti di perdita di informazione, ma di interruzione della sua fruibilità. Questo può comportare disservizi e rallentamento dell'operatività degli uffici, ma almeno nel breve periodo non prefigura situazioni di crisi.

È comunque opportuna, anche in questo caso, un'analisi della situazione nel suo complesso radicalmente modificata negli ultimi anni soprattutto da quando la Provincia di Lucca eroga servizi di sportello ai cittadini come quelli forniti attraverso i Centri per l'Impiego.

3.2.2 Situazione Attuale

Tutti i sistemi server e le parti attive dell'infrastruttura di rete dati, sono protetti da gruppi di continuità. È da evidenziare comunque che il gruppo di continuità protegge i dispositivi collegati e consente uno spegnimento controllato delle apparecchiature ed un rapido riavvio delle attività al ripristino dell'alimentazione elettrica, ma non consente comunque l'erogazione dei servizi, salvo che i singoli posti di lavoro non siano a loro volta attrezzati con gruppi di continuità (ipotesi attualmente percorsa per servizi di sportello particolarmente critici come il protocollo ed i Centri per l'Impiego) che comunque possono risolvere il problema per un periodo limitato di tempo. Tutti i server attualmente in funzione dispongono di una funzione di mirroring dei dischi gestita via software o via hardware (RAID), che consente di non interrompere il lavoro anche nel caso di rottura di uno degli hard disk.

Nel corso del 2005 l'ente si è dotato di un generatore elettrico in grado di fornire corrente alle sale della Protezione Civile. La linea elettrica che alimenta la Sala Macchine è collegata a quella proveniente dal generatore elettrogeno. In caso di mancanza di corrente quindi, i gruppi di continuità forniscono l'alimentazione alle attrezzature informatiche per il periodo necessario all'avvio del generatore.

Al fine di garantire continuità di servizio per i principali Sistemi Informativi dell'ente, i dati dei due DB server presenti, vengono incrociati in fase notturna in modo che, in caso di indisponibilità di uno dei due server, l'altro lo può sostituire operativamente in poco tempo con i dati aggiornati però alla sera precedente.

Nel corso del 2009 l'ente si è dotato di una coppia di server, di una Storage Area Network (SAN) e di una infrastruttura software per la virtualizzazione. Con questo sistema le due macchine fisiche ospitano diversi server virtuali che gestiscono i principali sistemi informativi dell'ente. Le immagini delle macchine virtuali sono ospitate sulla SAN collegata con sistemi in fibra ottica ridondata ai server. In caso di fermo di una delle macchine fisiche, le macchine virtuali ivi ospitate ripartirebbero automaticamente sull'altro server fisico riducendo moltissimo il fermo macchina ed i relativi disservizi.

3.2.3 Linee di intervento.

I passi operativi sono:

1. Analisi del livello di criticità delle diverse attrezzature per le attività dell'Ente;
2. Verifica/individuazione degli accorgimenti atti a garantire la continuità del servizio, anche in caso di problemi tecnici. Gli accorgimenti tecnici da prendere in considerazione sono:
 - a. Gruppo di continuità (livello base);
 - b. Ridondanza di componenti/funzioni (mirroring; hot swap, ridondanza fisica, ...)
 - c. Disponibilità di sistemi "di backup", in grado di sostituire le funzioni di quelli eventualmente guasti.
 - d. Virtualizzazione dei server critici e separazione fisica tra server applicativi e dati, al fine di ottenere un sistema in grado di garantire l'alta affidabilità.

Già tutti i sistemi server sono dotati di sistemi di sicurezza di livello base ed in buona parte anche di funzioni e componenti ridondanti. Soluzioni di livello superiore possono essere pianificate, eventualmente, in occasione di upgrade di sistemi, salvo diverse esigenze specifiche che dovessero emergere dall'analisi.

Un anello debole delle infrastrutture tecnologiche è rappresentato dalle infrastrutture di rete locale LAN e WAN (switch, router, canali di collegamento etc.). Con l'aumento dei servizi erogati in modo telematico e centralizzato, l'infrastruttura di comunicazione sta diventando sempre più una funzione realmente "*mission critical*" per l'Ente. In particolare per i Centri per l'Impiego è stato realizzato un sistema di backup basato su linee ADSL in modo da garantire la connettività anche quando le linee principali HDSL non dovessero funzionare. Per gli uffici di Lucca è stata inoltre realizzata una rete WiFi Mesh che collega i 4 edifici della città di Lucca, creando un ulteriore canale di distribuzione dati.

3.2.4 Misure minime di sicurezza

Tutti i sistemi informatici di tipo server dedicati al trattamento di dati personali, sensibili o giudiziari riportati nei trattamenti segnalati nell'allegato alla Delibera C.P. 139/A del 21/12/2006, dovranno prevedere sistemi di alimentazione, disco e rete ridondanti, oltre a gruppi di continuità che consentano quantomeno uno spegnimento corretto del sistema.

3.3 Sicurezza rispetto alla possibilità di accesso fisico ai locali, ai sistemi ed agli apparati di rete.

3.3.1 Aspetti generali

La sicurezza, nella sua accezione più generale, deve comprendere anche la sicurezza rispetto all'accesso ai locali all'interno dei quali vengono svolte le attività lavorative e dove vengono conservati archivi e documenti.

Si tratta quindi di prendere in considerazione possibili rischi collegati ad accessi non autorizzati agli uffici, per capire quali potrebbero essere le migliori politiche di sicurezza verso questa tipologia di rischi.

In particolare, per quanto riguarda i sistemi informatici, deve essere presa in considerazione la sicurezza dei locali che ospitano gli elaboratori centrali dell'ente oltre alle risorse distribuite, come gli armadi di rete e le postazioni di lavoro attraverso le quali è possibile accedere a banche dati contenenti dati personali, sensibili o giudiziari.

3.3.2 Situazione attuale.

Esiste un sistema di video-sorveglianza all'interno di Palazzo Ducale che allo stato attuale non registra le immagini e non può quindi essere utilizzato per individuare accessi illeciti a posteriori.

Per quanto riguarda la sicurezza rispetto alla possibilità di accesso non autorizzato ai dispositivi informatici è meglio distinguere 4 aree diverse.

3.3.2.1 Sala Macchine;

La stanza definita "Sala Macchine" contiene tutti i server presenti a Palazzo Ducale oltre ai sistemi di collegamento verso Internet e verso le sedi periferiche. Si trova attualmente in una stanza situata al primo piano mezzanino, dotata di chiave, accessibile solo dai locali dell'Ufficio Sistemi Informativi, ed appositamente condizionata. Le chiavi sono conservate nei locali dell'ufficio a disposizione dei dipendenti per le eventuali necessità.

3.3.2.2 Server;

La maggior parte dei server dell'ente si trovano all'interno della Sala Macchine e per loro valgono quindi le considerazioni già fatte. Per gli altri server la criticità sta nel fatto che questi sistemi, distribuiti in alcuni Servizi dell'Ente, sono spesso collocati in base a criteri logistici più che di sicurezza. Tuttavia nella maggior parte dei casi, è garantita la soglia minima di sicurezza.

3.3.2.3 Personal Computer / Posti di lavoro;

Le misure di sicurezza possono solo essere quelle definite per l'accesso all'ufficio. L'analisi del rischio e le conseguenti misure di sicurezza, in relazione alla tipologia delle informazioni trattate e conservate sui P.C. di un ufficio, dovrà essere curata dal responsabile dell'ufficio stesso: l'analogia tra quanto conservato in un armadio (eventualmente protetto da serratura) e quanto conservato in un P.C. (eventualmente protetto da password) è abbastanza evidente. Così come non devono essere lasciati fascicoli riservati sulla scrivania quando ci si allontana, analogamente è necessario bloccare il PC in modo che per qualsiasi operazione vengano richieste le credenziali.

3.3.2.4 Armadi di distribuzione dati

Gli armadi di distribuzione dati disposti presso i vari uffici dell'ente, si trovano in alcuni casi in locali accessibili al pubblico ma sono comunque tutti dotati di serratura. Copie delle chiavi sono conservate presso l'Ufficio Sistemi Informativi.

3.3.3 Linee di intervento.

Per quanto riguarda i Server, una linea di intervento a medio termine è quella di limitare la crescita del numero dei server distribuiti nelle diverse sedi, concentrandone le funzioni in un insieme ristretto di sistemi, adeguati per potenza e capacità, posizionandoli in una collocazione sicura. Tale attività, già iniziata nel 2007 con la virtualizzazione di 4 server, è proseguita poi nel corso del 2008 e nel 2009 con il raddoppio dei server virtualizzati, con ottimi risultati anche in termini di performance.

Per quanto riguarda il controllo degli accessi va portato a termine il progetto di videosorveglianza di Palazzo Ducale, con la messa in opera delle diverse telecamere installate che offrono sicuramente anche una funzione deterrente verso furti e/o accessi indebiti.

3.3.4 Misure minime di sicurezza

I server dovranno essere posizionati in locali non accessibili al pubblico e dovranno essere lasciati attivi sulla maschera di Login quando non utilizzati per attività sistemistiche.

Per quanto riguarda i server e le attrezzature site nella Sala Macchine o negli uffici dei Sistemi Informativi, le password relative agli utenti di amministrazione di tali macchine, saranno memorizzate in un apposito programma di gestione delle password.

Gli archivi cartacei contenenti dati personali, sensibili o giudiziari, dovranno essere collocati all'interno degli uffici utilizzati per le attività lavorative e chiusi a chiave al di fuori del normale orario di lavoro oppure in appositi locali chiusi a chiave. Le chiavi saranno custodite dal responsabile o dagli incaricati dei trattamenti.

3.4 Sicurezza rispetto agli accessi non autorizzati ai sistemi ed alle informazioni

3.4.1 Aspetti generali

Il problema dell'accesso non autorizzato ai sistemi informatici è collegato alle *credenziali di autenticazione* ed ai *profili di autorizzazione*. Attraverso le *credenziali di autenticazione* si individua chi si sta collegando al sistema. I *profili di autorizzazione* definiscono invece le diverse autorizzazioni associate agli utenti. Ciascun utente dovrebbe essere collegato ad un'unica credenziale di autenticazione alla quale vengono collegati i diversi profili di autorizzazione.

In realtà ogni Sistema Informativo definisce delle proprie *credenziali di autenticazione* ed al suo interno i *profili di autenticazione*.

Per semplificare la trattazione dell'argomento ed anche per maggiore chiarezza, è necessario distinguere tra controllo a livello sistemistico e controllo a livello applicativo:

- il livello sistemistico riguarda le autorizzazioni per l'accesso al Personal Computer (nome utente e password) o al dominio di autenticazione (utente, password e dominio) e conseguentemente alle risorse condivise sulla rete locale;
- il livello applicativo è invece un controllo che ciascuna applicazione o sistema informativo realizza per verificare chi accede all'applicazione.

In entrambi i casi si tratta comunque di un controllo che associa ad una credenziale di autenticazione uno o più profili di autorizzazione.

Le credenziali possono essere relativamente banali come nome utente e password ovvero più difficili da 'forzare' come quelle costituite da certificati digitali o sistemi biometrici.

La sicurezza in questo ambito è quindi collegata da un lato alla protezione delle credenziali di autenticazione in possesso dei singoli utenti e dall'altro alla corretta gestione dei profili di autorizzazione dei diversi Sistemi Informativi.

3.4.2 Situazione attuale

La quasi totalità dei sistemi informativi utilizzati nell'ente sfrutta come credenziali di autenticazione un nome utente e password.

Gli standard interni utilizzati per la lunghezza della password già tengono in conto in generale della lunghezza minima della password pari ad 8 caratteri ma non sempre questo controllo è possibile a livello sistemistico o applicativo.

Per tutti gli utenti che si collegano al dominio interno dell'ente sono state definite delle verifiche sulle credenziali di autenticazione che impongono determinati livelli minimi sulla lunghezza del nome utente e password e di complessità della password stessa (caratteri speciali o numerici obbligatori). La password di dominio ha una validità massima di 3 mesi. Quasi tutti gli utenti dell'ente sono ormai collegati al dominio 'INTRANET' e pertanto i relativi accessi rispettano le specifiche richieste a livello di misure minime di sicurezza.

Per la maggior parte dei Sistemi Informativi che non riescono ad utilizzare l'autenticazione basata sul protocollo LDAP ovvero il sistema di credenziali utilizzato per l'accesso al dominio interno, è necessario prevedere apposite istruzioni affinché gli operatori agiscano in modo autonomo per rispettare gli eventuali vincoli di legge riportati nella sezione 'Misure minime di sicurezza'.

L'ente si è inoltre dotato ormai da diversi anni di una Intranet attraverso la quale è possibile accedere direttamente ad alcuni sistemi informativi o comunque a informazioni private dei singoli dipendenti. Anche nel caso dell'accesso al '*Portale del dipendente*' la password scade ogni 3 mesi e la sua lunghezza minima è pari ad 8 caratteri.

3.4.3 Linee di intervento.

Risulta opportuna un'opera di istruzione e sensibilizzazione relativamente alla gestione delle proprie credenziali di autenticazione per i diversi sistemi di autenticazione.

Per l'identificazione degli utenti e la loro abilitazione, il miglioramento qualitativo può discendere dall'utilizzo di un sistema centralizzato che, a seguito di una identificazione dell'utente, consenta l'accesso a tutti i servizi e le funzioni a cui tale utente è abilitato.

La Provincia di Lucca ha scelto di affidare la gestione dei propri utenti a livello informatico all'infrastruttura di servizi denominata Microsoft Active Directory. Tale infrastruttura è compatibile con il protocollo LDAP (Lightweight Directory Access Protocol) utilizzato da altri sistemi ed applicazioni per effettuare il controllo delle credenziali. Tale compatibilità dovrà pertanto essere tenuta in considerazione nella scelta di nuovi sistemi informativi o nell'evoluzione di quelli esistenti, nell'ottica di accentrare ad una unica credenziale il controllo dell'accesso degli utenti, così come è stato fatto ad esempio per il software di Gestione degli Obiettivi e nel nuovo software di Gestione Documentale, di recente acquisizione.

Un ulteriore campo di intervento riguarda il collegamento del '*Portale del dipendente*' sviluppato internamente con il protocollo di autenticazione LDAP così da concentrare in un unico servizio la verifica delle credenziali per l'accesso ai diversi servizi.

3.4.4 Misure minime di sicurezza

Le credenziali di autenticazione (utente e password) sia sistemiche che applicative devono essere composte da almeno 8 caratteri oppure, nel caso in cui lo strumento elettronico non lo consenta, dal numero massimo di caratteri consentito dal sistema. La password non deve contenere riferimenti agevolmente riconducibili all'utente e deve essere modificata ogni 3 mesi.

3.5 Sicurezza rispetto alla possibilità di accesso alla rete ed ai sistemi per via telematica.

3.5.1 Aspetti generali

Il problema è, dagli anni ottanta, di rilevanza generale per i sistemi informativi complessi. Questi sono infatti costituiti da sistemi collegati in rete tra loro, e come tali necessariamente predisposti alla comunicazione ed alla interazione. Con l'apertura delle reti informatiche interne verso le reti geografiche ed in particolare alla rete Internet, questa predisposizione si è rivelata un punto debole per la sicurezza. Infatti soggetti esterni possono utilizzare le funzioni di comunicazione dei sistemi in rete per collegarsi ai server interni utilizzando eventuali falle dei sistemi operativi, e da qui procedere ad accessi ai dati, manomissione delle informazioni od anche atti di "vandalismo informatico".

In realtà quello che a cose normali rappresenta un pericolo, in altri casi si tratta di una importante opportunità da sfruttare per accelerare gli interventi di assistenza. Esistono infatti software che consentono di prendere il controllo di una macchina da remoto, appositamente realizzati per effettuare teleassistenza o telecontrollo.

3.5.2 Situazione attuale

Nel corso degli ultimi anni, l'ente si è dotato di una Rete Privata Virtuale (nel seguito per brevità VPN) che collega quasi tutte le sedi periferiche dell'ente con la sede principale di Palazzo Ducale. La navigazione su Internet avviene attraverso un unico collegamento centralizzato utilizzato da tutti gli uffici dell'ente e protetto da un firewall che isola la rete interna e la relativa VPN dal mondo Internet e da una zona, definita DMZ (DeMilitarized Zone), che ospita alcuni servizi Web accessibili anche dall'esterno. I server presenti sulla rete interna non sono accessibili direttamente dall'esterno e solo in pochi casi e con regole ben precise, viene dato l'accesso ad un PC interno per servizi di teleassistenza da parte di specifici fornitori e comunque limitatamente a specifici indirizzi IP di provenienza. Il Firewall consente di controllare i protocolli e le porte utilizzati dagli utenti per la navigazione. Allo stato attuale sono state lasciate aperte sostanzialmente le porte collegate alla navigazione delle pagine WEB e all'utilizzo della posta.

La navigazione verso Internet può essere mediata da un proxy che accelera la navigazione stessa e la rende più sicura, bloccando siti e protocolli considerati non sicuri.

Per l'accesso dall'esterno verso la rete interna, è stato predisposto nel corso del 2007 un server OpenVPN, ovvero un PC con sistema operativo Linux, virtualizzato nel corso del 2008, sul quale è stato installato un software Open Source che consente di instaurare un canale di comunicazione sicuro e criptato tra le postazioni esterne sulla rete Internet e la rete interna.

Su tutte le postazioni dell'ente è installato un software Open Source denominato VNC che consente, se lanciato sul PC che richiede assistenza, di prendere il controllo di quel PC da una postazione remota in ogni caso dopo la digitazione di una password nota ai dipendenti dell'Ufficio Sistemi Informativi. Questa possibilità se da un lato risulta estremamente utile per gli interventi di teleassistenza, dall'altra pone problemi di privacy e riservatezza. Per questo motivo il software per

la teleassistenza non parte in modo automatico all'avvio del PC ma deve essere lanciato manualmente dall'utente.

3.5.3 Linee di intervento

Vista la sempre crescente necessità di Banda per il collegamento sia delle sedi periferiche verso quella centrale, sia verso Internet, è probabile che si modificheranno i contratti per l'adeguamento delle VPN in essere. Restano comunque imprescindibili le questioni legate alla sicurezza ed in particolare alle intercettazioni. Per questo motivo, soluzioni di questo tipo dovranno comunque prevedere la possibilità di criptare i dati trasmessi per evitare intercettazioni.

Nel corso dell'anno dovrà essere estesa anche alle postazioni di Palazzo Ducale l'obbligatorietà all'utilizzo del server proxy, già in essere presso le sedi decentrate, per la navigazione su Internet, al fine di aumentare il livello di sicurezza interno.

3.5.4 Misure minime di sicurezza

È vietato l'uso di modem per il collegamento ad Internet da parte di postazioni collegate alla rete locale della Provincia di Lucca. La rete interna dell'ente e quella esterna devono sempre essere separate da un firewall. Sulla DMZ possono essere ospitati siti e front-end applicativi ma le banche dati, se ospitano dati sensibili o giudiziari, devono trovarsi nella rete interna dell'ente.

Al termine di una sessione di teleassistenza realizzata mediante l'apposito software VNC, l'utente richiedente deve terminare l'applicazione server in modo da evitare che altri utenti possano collegarsi al suo PC senza autorizzazione.

3.6 Sicurezza rispetto alla diffusione di virus informatici ed aggiornamenti dei programmi applicativi e dei sistemi operativi.

3.6.1 Aspetti generali

Per "virus" si intende, in ambito informatico, un programma software, o comunque un insieme di istruzioni eseguibili da un elaboratore, che introdotto in un sistema (associato ad un supporto magnetico, ad un programma o anche ad un documento in formato elettronico) viene eseguito all'insaputa dell'utilizzatore. I possibili effetti sono molteplici dalla semplice propagazione, manifestazione, fino alla cancellazione di dati. I virus sono in realtà una categoria di "malware" ovvero software creati con il solo scopo di causare danni più o meno gravi al computer su cui vengono eseguiti. Tra le varie categorie di malware, vanno citati in particolare gli **spyware** (software creati per raccogliere informazioni sul sistema su cui sono installati), **adware** (esecuzioni di comandi lanciati da PC 'offuscati'), Trojan horse (cavalli di troia per recuperare password al fine di entrare in sistemi protetti), keylogger (che catturano quanto digitato dall'utente sulla tastiera e quindi anche password).

Altri problemi di sicurezza sono invece intrinsecamente collegati a debolezze del sistema operativo utilizzato ovvero agli specifici software applicativi. Ad esempio Microsoft rilascia pacchetti cumulativi di aggiornamento per i propri sistemi operativi e per le proprie applicazioni. Anche le diverse distribuzioni del sistema operativo Linux prevedono la disponibilità degli aggiornamenti software sui siti dei rispettivi fornitori.

3.6.2 Situazione attuale.

Negli ultimi anni l'ente si è dotato di un sistema di gestione degli antivirus per PC e Server di tipo centralizzato. Da una consolle centrale è possibile monitorare lo stato di aggiornamento delle impronte virali installate sui PC dell'ente e le infezioni presenti sui PC verificando l'efficacia delle contromisure software. Il sistema centrale scarica ogni poche ore gli aggiornamenti delle impronte virali dal sito del fornitore. Le impronte ed i software aggiornati vengono automaticamente distribuiti sulla rete interna senza che venga richiesto alcun intervento da parte dell'utente. Come ulteriore politica di controllo, settimanalmente l'antivirus parte automaticamente su tutti i computer dell'ente per una scansione completa dei sistemi.

Presso l'U.O. Sistemi Informativi è stato installato un server SUS (Software Update Services) che scarica gli aggiornamenti per i diversi sistemi informativi della Microsoft. Questi aggiornamenti sono poi resi disponibili agli utenti della rete interna in modo automatico per gli utenti che accedono al dominio interno ovvero a seguito dell'installazione di un apposito programma nel caso degli altri PC.

Dalla Intranet dell'ente è possibile scaricare un software denominato "Spyboot Search and destroy" in grado di individuare alcuni tipi di spyware non intercettati dal sistema antivirus.

3.6.3 Linee di intervento.

A livello di Antivirus, la soluzione adottata si è dimostrata sufficientemente efficace. Per il futuro potrebbe essere interessante valutare l'estensione del software rendendolo in grado di controllare oltre ai virus, anche gli spyware ed in generale tutti i malaware.

3.6.4 Misure minime di sicurezza

Tutti i computer dell'ente devono essere dotati di software antivirus con gestione centralizzata o, nei pochi casi in cui ciò non è tecnicamente possibile, l'antivirus deve essere mantenuto costantemente aggiornato da parte degli utenti. I sistemi operativi Windows, devono essere mantenuti aggiornati attraverso il SUS interno ovvero avvalendosi del medesimo strumento offerto dalla Microsoft attraverso il suo sito.

3.7 Sicurezza rispetto all'intercettazione delle informazioni trasmesse attraverso reti telematiche

3.7.1 Aspetti generali

Per quanto il fattore di rischio rispetto alle intercettazioni delle informazioni trasmesse attraverso reti telematiche sia per ora estremamente limitato, si è ritenuto opportuno citare comunque questo fattore di rischio, tenendo conto della prospettiva di un sempre maggiore utilizzo delle reti telematiche per lo scambio di informazioni.

Il rischio di "intercettazioni telematiche" è peraltro ben considerato nelle tecnologie della sicurezza informatica. In considerazione di quanto sopra, ed in particolare degli sviluppi previsti per l'interconnessione delle sedi periferiche, si terrà conto nei relativi progetti delle problematiche legate alla sicurezza.

3.7.2 Misure minime di sicurezza

I dati sensibili potranno essere trasmessi per via telematica su rete pubblica solo se criptati. Anche eventuali reti private virtuali costituite con la tecnologia dei ponti radio, dovranno prevedere sistemi di criptazione per evitare che una eventuale intercettazione consenta di leggere i messaggi scambiati sulla rete.

3.8 Sicurezza rispetto al trattamento dei dati con strumenti cartacei o comunque non automatizzati

3.8.1 Aspetti generali

Il trattamento dei dati personali, sensibili o giudiziari avviene nella maggior parte dei casi tramite documenti cartacei e si riduce in generale alla gestione dei relativi archivi storici o degli atti connessi con la tenuta di archivi imposti dalle normative vigenti. Il concetto di sicurezza si esplica quindi nelle politiche di accesso agli archivi e nelle politiche di riservatezza della gestione dei flussi documentali. Le differenze sostanziali rispetto al trattamento dei dati con strumenti informatici sono due:

- ✓ il controllo sull'accesso ai dati;
- ✓ il controllo sulle operazioni effettuate sui dati.

Nel caso di archivio cartaceo l'accesso ai dati è legato all'accesso al locale, contenitore, mobile o cassaforte che contiene l'archivio stesso. Non vi è la possibilità di controllare le operazioni che un soggetto può compiere una volta che è entrato in possesso dei dati (solo visione, istruttoria di una pratica, etc.). Per questo motivo è importante che gli archivi contenenti dati personali, sensibili o giudiziari vengano custoditi sotto chiave e che gli accessi siano consentiti ai soli incaricati al trattamento dei dati.

3.8.2 Misure minime di sicurezza

Come nel caso del trattamento dei dati sensibili con strumenti automatizzati, anche le operazioni di trattamento dei dati cartacei e dei relativi flussi, devono essere gestite da soggetti esplicitamente incaricati a queste operazioni secondo quanto previsto dagli artt. 26, 27 e 28 dell'Allegato B al D.Lgs. 196/03.

Gli addetti al trattamento sono tenuti a conservare gli atti o i documenti in contenitori muniti di serratura durante il trattamento degli stessi.

L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato. Le persone ammesse alla consultazione di detti archivi dopo l'orario di chiusura dell'ufficio, sono identificate e registrate. Il controllo sugli accessi agli archivi è demandato al responsabile o, in mancanza di questo, al titolare dell'archivio stesso.



Politiche di backup della Provincia di Lucca

Ufficio Sistemi Informativi

1. PREFAZIONE.....	5
2. SCHEMI DI BACKUP.....	6
2.1 SALVATAGGIO SU NASTRI DAT DEL SERVER SIT (IN DISMISSIONE).....	6
2.2 SALVATAGGIO SU NASTRI DAT SERVER BARSANTI E MATTEUCCI.....	7
2.3 SALVATAGGIO DATI DAI SERVER WINDOWS DEI CENTRI PER L'IMPIEGO SU DISCO FISSO ESTERNO.....	8
2.3.1 Centro Impiego di Fornaci di Barga.....	8
2.3.2 Centro per l'impiego di Castelnuovo di Garfagnana.....	8
2.3.3 Centro per l'impiego di Viareggio.....	9
2.3.4 Centro per l'impiego di Lucca.....	9
2.4 SALVATAGGIO DATI DEL SISTEMA IBM AS400.....	9
2.5 SALVATAGGIO DATI DAI SERVER LINUX E DALLE PRINCIPALI BANCHE DATI.....	10
2.5.1 DataServer ORACLE principale.....	11
2.5.2 DataServer ORACLE secondario.....	12
2.5.3 DataServer Postgres su Intranet.....	12
2.5.4 DataServer MySQL (su rete Intranet).....	13
2.5.5 DataServer MySQL (su rete DMZ).....	13
2.5.6 DataServer PostGreSQL (su rete DMZ).....	13
2.5.7 Web Server OpenGis.....	14
2.5.8 WebServer IDOL.....	14

1. Prefazione

In questo documento vengono illustrati gli schemi di salvataggio dei dati della Provincia di Lucca e le politiche adottate per recuperare file modificati o cancellati per errore dagli utenti. La prima metodologia è necessaria per organizzare un sistema di disaster recovery che a fronte di un problema bloccante su un server, consenta di ripristinare su una macchina diversa le medesime funzionalità ed i relativi dati. La seconda metodologia consente invece, per alcuni sistemi, di ripristinare vecchie versioni dei file modificati o cancellati per errore, senza fare ricorso ai salvataggi effettuati su nastro, con dei tempi di ripristino estremamente rapidi.

Attualmente esistono, diversi processi di backup ed in particolare:

- Salvataggio su DAT del server SIT (servizio Urbanistica) e del server di via Barsanti e Matteucci;
- Salvataggio Centro per l'impiego Fornaci di Barga su disco fisso esterno;
- Salvataggio Centro per l'impiego Castelnuovo su disco fisso esterno;
- Salvataggio Centro per l'impiego Viareggio su disco fisso esterno;
- Salvataggio Centro per l'impiego di Lucca su disco fisso esterno;
- Salvataggio nastri AS400;
- Salvataggi incrociati di dati tra diversi server;
- Salvataggi su supporti non riscrivibili per i dati del protocollo.

Tra le politiche di backup citiamo essenzialmente le cosiddette '**shadow copy**' ovvero delle *copie automatiche* che vengono effettuate due volte al giorno dal server, solo dei file modificati rispetto all'ultimo salvataggio. Tali salvataggi risiedono direttamente sul file system (dischi del server) ma possono essere rapidamente ripristinati attraverso un'apposita consolle amministrativa. La finestra temporale che viene mantenuta in linea per recuperare file cancellati o modificati diversi giorni prima, è di due settimane, compatibilmente con lo spazio disco a disposizione sul server stesso.

I supporti magnetici vengono conservati in cassaforte ignifuga presso il CED.

Il salvataggio in "generale" si occupa semplicemente del backup delle cartelle principali sugli specifici server a intervalli determinati e schedulati.

2. Schemi di backup

Nei seguenti paragrafi verranno elencati gli schemi di backup dei diversi server e dispositivi di backup presenti nell'ente.

2.1 Salvataggio su nastri DAT del server SIT (in dismissione)

Mediante questo tipo di backup, si salvano i files presenti sui server del Sistema Informativo Territoriale. Questo tipo di salvataggio, viene effettuato con una serie di nastri settimanale sostituendo ogni mattina il nastro nell'unità di backup. Questo sistema consente quindi di avere una finestra temporale di recupero dei dati dal nastro di una settimana. Il sistema è attualmente in dismissione.

Specifiche generali di backup

Software utilizzato: NTBACKUP (Sit Server)

Tipo di backup: file system

Schedulazione: giornaliero

Modalità: Normale (completo)

Verifica dei dati: No

Compressione: Sì, a livello hardware

Generazione LOG: Sì

Struttura

Dove possibile sono state implementate delle configurazioni standard di salvataggio, uniformando gli scripts e i metodi. In "Operazioni Pianificate" di ogni server sono presenti i seguenti processi che vengono eseguiti nei giorni in cui è previsto il backup (dal lunedì al venerdì):

- Backup
- Invio del log
- Espulsione del nastro

La qualità del servizio di backup è di livello mediocre, in quanto il software in uso non permette operazioni sofisticate. Inoltre il LOG deve essere soggetto ad un controllo continuo in quanto non sono previste forme di allarme automatico.

I files che vengono salvati per i due server sono i seguenti:

SIT_SERVER

Orario giornaliero di backup: 22.30

Espulsione nastro ore: 13.00 il LUN, MER, VEN e 16.00 ore MAR, GIO

Mail LOG ore: 7.00

Del server vengono salvate le seguenti cartelle:

E:\ARCHIVI_GEOGRAFICI\archiviGIS\

E:\ARCHIVI_GEOGRAFICI\datiRADEX\

E:\ARCHIVI_GEOGRAFICI\datiSHARC\

E:\ARCHIVI_GEOGRAFICI\datiTNWEB\

2.2 Salvataggio su nastri DAT Server Barsanti e Matteucci

Mediante questo tipo di backup, si salvano i files presenti sui server presso Barsanti & Matteucci. Questo tipo di salvataggio, viene effettuato con una serie di nastri settimanale sostituendo ogni mattina il nastro nell'unità di backup, presso la sede. Questo sistema consente quindi di avere una finestra temporale di recupero dei dati dal nastro di una settimana.

Il sistema è attualmente in dismissione e sostituzione con backup tramite disco esterno.

Specifiche generali di backup

Software utilizzato: TAPEWARE

Tipo di backup: file system

Schedulazione: giornaliero

Modalità: Normale (completo)

Verifica dei dati: No

Compressione: Sì, a livello hardware

Generazione LOG: Sì

SERVER di via Barsanti e Matteucci

Orario giornaliero di backup: 23.00

Espulsione nastro ore: manuale, è stato delegato un dipendente nella sede il quale ha il compito di sostituire i nastri.

Mail LOG ore: nessuna

Del server vengono salvate le seguenti cartelle:

D:\Home\

D:\MySql\

Considerazioni

Non vi è nessuna procedura per il ripristino del sistema in caso di rottura dei dischi di sistema o ad esempio di un esito negativo all'installazione di una procedura software o un aggiornamento del sistema operativo

2.3 Salvataggio dati dai server Windows dei Centri per l'Impiego su disco fisso esterno

Mediante questo tipo di backup, già in corso e attivo, si salvano i files presenti sui server locali dei diversi Centri per l'Impiego. Nel caso dei Centri di Viareggio, Fornaci di Barga e Castelnuovo, l'unità esterna è un disco USB da almeno 500Gb. Nel caso del Centro per l'Impiego di Lucca, si tratta invece di un disco esterno di rete da 1Tb, in considerazione della maggiore quantità di dati che è necessario backuppare..

2.3.1 Centro Impiego di Fornaci di Barga

Specifiche generali di backup

Software:	Cobian backup
Tipo di backup:	file system
Schedulazione:	Giornaliero
Verifica dei dati:	Si
Compressione:	Si, a livello software
Generazione LOG:	Si

Considerazioni

Nessuna in particolare.

2.3.2 Centro per l'impiego di Castelnuovo di Garfagnana

Mediante questo tipo di backup, si salvano i files presenti sul server locale del Centro per l'Impiego di Castelnuovo di Garfagnana utilizzando un disco esterno USB 2.0.

Specifiche generali di backup

Software:	Cobian backup
Tipo di backup:	file system
Schedulazione:	Giornaliero
Verifica dei dati:	Si
Compressione:	Si, a livello software
Generazione LOG:	Si

Considerazioni

Nessuna in particolare.

2.3.3 Centro per l'impiego di Viareggio

Mediante questo tipo di backup, già in corso e attivo, si salvano i files presenti sul server locale di Viareggio utilizzando un disco esterno USB 2.0.

Specifiche generali di backup

Software:	Cobian backup
Tipo di backup:	file system
Schedulazione:	Giornaliero
Verifica dei dati:	Si
Compressione:	Si, a livello software
Generazione LOG:	Si

Considerazioni

Nessuna in particolare.

2.3.4 Centro per l'impiego di Lucca

Mediante questo tipo di backup, già in corso e attivo, si salvano i files presenti sul server locale di Lucca utilizzando un disco esterno di rete da 1Tb. Oltre ai dati del Centro per l'Impiego, vengono salvati anche i documenti del Servizio Formazione Professionale che è collocato nel medesimo edificio e con il quale vengono condivise le risorse hardware.

Specifiche generali di backup

Software:	Cobian backup
Tipo di backup:	file system
Schedulazione:	Settimanale completo + giornaliero incrementale
Verifica dei dati:	Si
Compressione:	Si, a livello software
Generazione LOG:	Si

Considerazioni

Nessuna in particolare.

2.4 Salvataggio dati del sistema IBM AS400

Su questo tipo di backup, attivo e funzionante, vengono salvate tutte le informazioni relative alle librerie utente presenti sul sistema IBM AS400.

Specifiche generali di backup

Il tipo di backup prevede un set di nastri settimanale. I salvataggi vengono effettuati dal lunedì al venerdì. Alle ore 12:00 viene effettuato un test per verificare se il nastro inserito è quello corretto. Il backup viene eseguito tutte le sere prima dello spegnimento. Come tutte le operazioni eseguite dal sistema AS400, viene generato un log del processo di backup.

Nel corso del 2008 il software principale funzionante su sistema AS400, ovvero quello della finanziaria dell'ente, è stato spostato su un'altra piattaforma. Allo stato attuale l'unica banca dati che viene aggiornata è quella del Servizio Caccia e Pesca. Nel corso del 2010 anche questo software dovrebbe essere migrato su una piattaforma WEB. Quando anche questa migrazione sarà completata, dato che il sistema rimarrà in funzione per la consultazione dei dati degli anni precedenti, sarà pensabile creare un backup completo del sistema, interrompendo poi l'attività schedualta di backup

Considerazioni

Nessuna in particolare

2.5 Salvataggio dati dai server Linux e dalle principali banche dati

L'ente è dotato di alcuni server Linux che gestiscono i dati utilizzando tipologie diverse di DBMS. Inoltre la nostra realtà prevede un insieme di servizi sia per l'utenza interna (intranet-side) che per l'utenza esterna (internet-side).

Seguendo quelle che sono le linee guida per una corretta suddivisione logica e fisica della rete, atta a garantire la sicurezza delle varie risorse, i server sono stati suddivisi in due gruppi:

1. quelli che forniscono dati all'interno,
2. quelli utilizzati per esporre dati all'esterno dell'ente.

In questa ottica ritroviamo quindi una situazione come quella raffigurata in Fig 1.

Chi fornisce dati di competenza interna all'ente sono:

- server ORACLE, che interessa i Sistemi Informativi del Protocollo (Protocollo), del Mercato del Lavoro (IDOL, DataWare house, CVWEB), del Personale (gestione Cedolini), della Ragioneria (JobTime, Gestione Obiettivi, Cassa Economale, Bilancio) e del servizio Viabilità e Fabbricati (contabilità dei cantieri)
- server MySQL, che gestisce dati legati al CED, al Sistema Informativo del Provveditorato (Utenze Telefoniche e Gestione Autoparco), al Sistema Informativo del Protocollo (programma Arianna)
- server PostGreSQL, contiene dati relativi al Sistema Informativo del servizio Tributi (Prelievi Idrici e Passi Carrai)

I server che forniscono dati anche per l'utenza esterna sono invece:

- server MySQL che gestisce i dati per il sistemi Informativo dell'Urbanistica (Servizio Pianificazione Territoriale) ed Egroupware, programma utilizzato in maniera trasversale da vari servizi dell'ente.
- Server PostGreSQL, contiene dati relativi all'URP (programma denominato Urptool) e (Conform).

Per questi server sono state previste politiche di backup che, durante le ore notturne, generano copie dei dati e li inviano ad una apposita macchina utilizzata prevalentemente per il salvataggio dei dati (nas server).

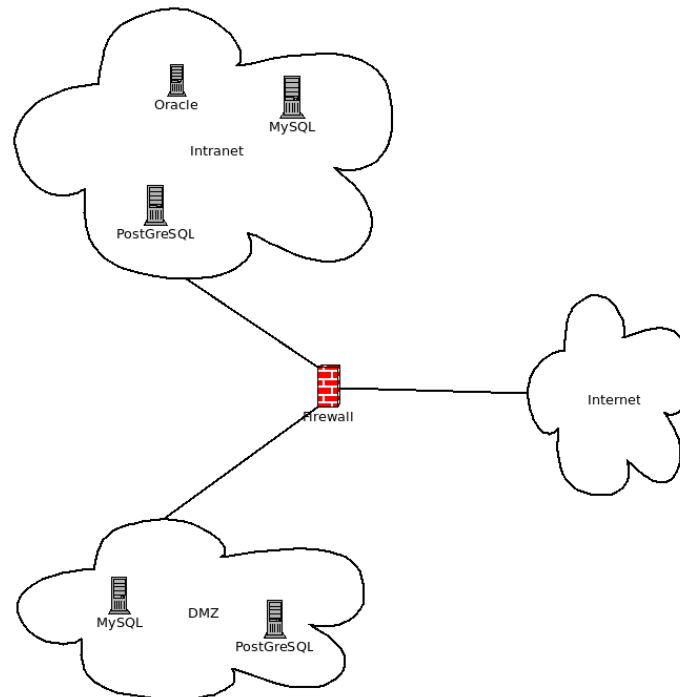


Fig 1: Disposizione server su rete

2.5.1 DataServer ORACLE principale

Vengono utilizzati i privilegi legati all'utente ORACLE per eseguire tutte le operazioni di backup dei dati gestiti dal DBMS ORACLE.

L'operazione viene avviata ogni giorno alle ore 22 e avviene mediante i seguenti passi:

1. tramite il programma exp avviene l'esportazione completa nella directory /home/oracle/oradata/backup dei dati legati agli utenti del database coinvolti nelle operazioni di salvataggio,
2. ogni file esportato viene successivamente compresso mediante il programma bzip2 ottenendo un file di salvataggio il cui nome è così costituito: *nomeutenteanno-mese-giorno.dmp.bz2*,
3. ogni file viene successivamente **spostato**, tramite trasferimento scp, sul server naslinux.intranet.provincia.lucca, nella directory /home/oracle, nella opportuna sottocartella,
4. alla fine delle operazioni di salvataggio, viene inviata una e-mail agli amministratori del server affinché possano verificare il risultato delle operazioni.

Considerazione a parte va fatta per i dati delle statistiche legati al mercato del lavoro che, per le loro caratteristiche di "staticità" (i dati vengono infatti aggiornati mensilmente) sono salvato solamente una volta al mese.

Gli utenti ORACLE dei quali sono salvati i dati sono:

- IDOL e SICUR_IDOL per i dati utilizzati dal servizio Lavoro per espletare gli obblighi di legge legati al mercato del Lavoro

- DMIDOL e DOFA per dati statistici del mercato del lavoro,
- CVWEB: gestione dei curriculum lavorativi ed utilizzato dal servizio Lavoro,
- PLUSTR: gestione della contabilità dei cantieri, utilizzato dal servizio Viabilità e Fabbricati,
- DOCPERSONALE: cedolini,
- SAGADOC: dati di protocollo.

2.5.2 DataServer ORACLE secondario

Vengono utilizzati i privilegi legati all'utente ORACLE per eseguire tutte le operazioni di backup dei dati gestiti dal DBMS ORACLE.

L'operazione viene avviata ogni giorno alle ore 22 e avviene mediante i seguenti passi:

1. tramite il programma exp avviene l'esportazione completa nella directory /home/oracle/oradata/backup dei dati legati agli utenti del database coinvolti nelle operazioni di salvataggio,
2. ogni file esportato viene successivamente compresso mediante il programma bzip2 ottenendo un file di salvataggio il cui nome è così costituito: nomeutenteanno-mese-giorno.dmp.bz2;
3. ogni file viene successivamente **spostato**, tramite trasferimento scp, sul server naslinux.intranet.provincia.lucca, nella directory /home/oracle, nella opportuna sottocartella.
4. alla fine delle operazioni di salvataggio, viene inviata una e-mail agli amministratori del server, contenente il risultato delle operazioni, affinché possano verificarne il risultato

Gli utenti coinvolti nel salvataggio dei dati sono quelli legati a:

- INFOR, JENTE, JENTE03 e JENTE05 per i dati utilizzati dal servizio Ragioneria per la gestione economico-finanziaria dell'ente
- TABELLE_PR_LU, ANAGRA_PR_LU, RETRIB_PR_LU, MASTER, JOBTIME, ILPROVLU, ILLOGON, PAGPROLU per i dati utilizzati dal servizio Personale per la gestione giuridico-economica del personale.

2.5.3 DataServer Postgres su Intranet

Vengono utilizzati i privilegi legati all'utente Postgres per eseguire tutte le operazioni di backup dei dati gestiti dal DBMS PostGreSQL.

L'operazione viene avviata ogni giorno alle ore 23 e consiste nei seguenti passi:

1. tramite il programma pg_dump avviene l'esportazione completa dei database idraeprlu e viae,
2. i dati, una volta esportati, vengono successivamente compressi mediante il programma bzip2 ottenendo un file di salvataggio il cui nome è così costituito: database-anno-mese-giorno.dmp.bz2,

3. ogni file viene successivamente **spostato**, tramite trasferimento scp, sul server naslinux.intranet.provincia.lucca, nella directory /home/postgres, nella opportuna sottocartella,
4. alla fine delle operazioni di salvataggio, viene inviata una e-mail agli amministratori del server, contenente il risultato delle operazioni, affinché possano verificarne il risultato.

2.5.4 DataServer MySQL (su rete Intranet)

Vengono utilizzati i privilegi legati all'utente root per eseguire tutte le operazioni di backup dei dati gestiti dal DBMS MySQL.

L'operazione viene avviata ogni giorno alle ore 22 e consiste nei seguenti passi:

1. tramite il programma mysqldump avviene l'esportazione completa dei database nag2web, arianna, autoparcprovlucca, autoparcoutenti, cacti, nagios, ocsweb, joomla, ntop, reclami, utenze, ARCSTO, nag2webNG
2. i dati, una volta esportati, vengono successivamente compressi mediante il programma bzip2 ottenendo un file di salvataggio il cui nome è così costituito: database-anno-mese-giorno.dmp.bz2,
3. ogni file viene successivamente **spostato**, tramite trasferimento scp, sul server naslinux.intranet.provincia.lucca, nella directory /home/mysql, nella opportuna sottocartella,
4. alla fine delle operazioni di salvataggio, viene inviata una e-mail agli amministratori del server, contenente il risultato delle operazioni, affinché possano verificarne il risultato.

2.5.5 DataServer MySQL (su rete DMZ)

Vengono utilizzati i privilegi legati all'utente mysql per eseguire tutte le operazioni di backup dei dati gestiti dal DBMS MySQL.

L'operazione viene avviata ogni giorno alle ore 22 e consiste nei seguenti passi:

1. tramite il programma mysqldump avviene l'esportazione completa del database eGroupWare e Joomla;
2. i dati, una volta esportati, vengono successivamente compressi mediante il programma bzip2 ottenendo un file di salvataggio il cui nome è così costituito: database-mysqldMZ-anno-mese-giorno.sql.bz2;
3. ogni file viene successivamente **spostato** nella directory, ~/scp; sarà il nas server che provvederà, giornalmente, a prelevare il backup dal server,
4. alla fine delle operazioni di salvataggio, viene inviata una e-mail agli amministratori del server, contenente il risultato delle operazioni, affinché possano verificarne il risultato.

2.5.6 DataServer PostGreSQL (su rete DMZ)

Vengono utilizzati i privilegi legati all'utente postgres per eseguire tutte le operazioni di backup dei dati gestiti dal DBMS PostGreSQL.

L'operazione viene avviata ogni giorno alle ore 22 e consiste nei seguenti passi:

1. tramite il programma `pg_dump` avviene l'esportazione completa dei seguenti databases:
 - `srty`
 - `urpbase`
 - `conform`
2. i dati, una volta esportati, vengono successivamente compressi mediante il programma `bzip2` ottenendo un file di salvataggio il cui nome è così costituito: `database-psql-anno-mese-giorno.sql.bz2`,
3. ogni file viene successivamente **spostato** nella directory, `~/scp`; sarà il nas server che provvederà, giornalmente, a prelevare il backup dal server,
4. alla fine delle operazioni di salvataggio, viene inviata una e-mail agli amministratori del server, contenente il risultato delle operazioni, affinché possano verificarne il risultato

2.5.7 Web Server OpenGis

Vengono utilizzati i privilegi legati all'utente `postgres` per eseguire tutte le operazioni di backup dei dati gestiti dal DBMS PostgreSQL.

L'operazione viene avviata ogni giorno alle ore 22 e consiste nei seguenti passi:

- tramite il programma `pg_dump` avviene l'esportazione completa dell'archivio `wgpaes`:
- i dati, una volta esportati, vengono successivamente compressi mediante il programma `bzip2` ottenendo un file di salvataggio il cui nome è così costituito: `database-psql-anno-mese-giorno.sql.bz2`,
- ogni file viene successivamente **spostato** nella directory, `~/scp`; sarà il nas server che provvederà, giornalmente, a prelevare il backup dal server,
- alla fine delle operazioni di salvataggio, viene inviata una e-mail agli amministratori del server, contenente il risultato delle operazioni, affinché possano verificarne il risultato

2.5.8 WebServer IDOL

Il server in esame contiene gli originali digitali del protocollo informatico. Tali documenti sono memorizzati nella directory `/home/jboss/repository/sagadoc/protocollo`.

Settimanalmente ne viene fatta una copia completa mentre giornalmente vengono salvati i nuovi documenti.

L'operazione viene avviata ogni giorno alle ore 23 e consiste nei seguenti passi:

1. tramite il programma di sistema `tar` avviene il backup (completo o incrementale) e la compressione dei dati contenuti nella directory precedentemente indicata,
2. i dati vengono memorizzati all'interno della directory `/home/jboss/temp/backup` con il nome così costruito: `/home/jboss/temp/backup/protocollo-aaaa-mm-gg.tgz`,
3. ogni file viene successivamente **spostato**, tramite trasferimento `scp`, sul server `naslinux.intranet.provincia.lucca`, nella directory `/home/saga`,

Osservazioni: I dati presenti sulla macchina naslinux.intranet.provincia.lucca, vengono mantenuti sulla macchina con una finestra temporale di 30 giorni.