



Piano per la sicurezza informatica

1. Introduzione

Il piano di sicurezza informatica garantisce che le informazioni siano disponibili, integre, riservate e che siano assicurate l'autenticità, la non ripudiabilità, la validità temporale dei documenti informatici.

I dati, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento, vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

1. le politiche generali e particolari di sicurezza da adottare all'interno del comune;
2. le modalità di accesso al servizio di gestione documentale e protocollo;
3. gli interventi operativi da adottare sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 *"Codice in materia di protezione dei dati personali"*.

Il servizio informatico dell'ente ha adottato le misure tecniche e organizzative di seguito specificate, al fine di garantire la sicurezza dell'impianto tecnologico dell'ente, la riservatezza delle informazioni registrate nelle banche dati e l'univoca identificazione degli utenti, in dettaglio:

1. utilizzo di sistemi operativi e hardware di qualità, aggiornati con le versioni più idonee in relazione ai prodotti in commercio;
2. predisposizione di idonei locali per la dislocazione dei server e relative attrezzature informatiche, dotati di sistemi di antintrusione, antincendio e gruppi di continuità per l'alimentazione elettrica;
3. protezione della rete con l'utilizzo software e hardware vari che insieme alle regole di comunicazioni tra apparati garantiscono l'accesso ai dati ai soli soggetti autorizzati;
4. assegnazione ad ogni utente del sistema di gestione documentale di una credenziale di identificazione (user ID) formata da un nome ed una password associate ad un profilo di autorizzazione operativo;
5. obbligo di cambio delle password con frequenza trimestrale durante la fase di esercizio;
6. esecuzione delle copie di riserva dei dati e documenti con frequenza giornaliera;
7. capacità di ripristino del sistema informativo in caso di disastro nel più breve tempo possibile;
8. conservazione, a cura del servizio informatico dell'ente, delle copie di riserva dei dati e dei documenti, in locali diversi e lontani il più possibile da quelli in



- cui è installato il sistema di elaborazione di esercizio (server principale);
9. gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne ed esterne qualificate;
 10. impiego e manutenzione di un adeguato sistema antivirus aggiornato in modo automatico (patch e service pack gestiti direttamente dai server);
 11. archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo;
 12. registrazione in appositi log delle attività di inserimento/modifica effettuate sui documenti memorizzati da ciascun utente.

2. Formazione dei documenti: aspetti di sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

1. l'identificabilità del soggetto che ha formato il documento;
2. la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
3. l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
4. l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
5. la leggibilità dei documenti nel tempo;
6. l'interscambiabilità dei documenti all'interno dello stesso ente e con enti diversi.

I documenti dell'ente sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Per il formato finale del documento si adottano preferibilmente i formati PDF, XML, JPG e TIFF, in accordo con le regole tecniche individuate dal CAD (D. lgs. 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale*").

I documenti informatici prodotti dall'ente su formati modificabili, quali doc, odt, xls, ods, ecc., sono convertiti, prima della loro sottoscrizione con firma digitale, nel formato standard PDF/A come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità con altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità e l'integrità del documento, lo stesso potrà essere sottoscritto con firma digitale.



3. Descrizione della struttura informatica comunale

3.1. Struttura del sistema e protezioni

3.1.1. Architettura della rete

Gli uffici dell'ente sono concentrati in un'unica sede all'interno del territorio comunale. Tutti le postazioni di lavoro sono dotate di personal computer collegati alla rete locale (intranet), dai quali si accede alle applicazioni dell'Ente, alle risorse condivise e ad Internet.

3.1.2. Sicurezza della rete

La rete del comune (intranet) è collegata all'esterno (internet) attraverso canali di trasmissione (gateway) filtrati dai sistemi di firewall aziendali connessi a provider privati.

I collegamenti dall'esterno verso la intranet possono essere realizzati con sistemi di VPN che consentano l'accesso tramite autenticazione con nome utente e password.

Tutti i sistemi elencati afferiscono a un sistema di firewall, che controlla il traffico dati in base alle politiche di sicurezza prestabilite.

3.1.3. Architettura del Sistema Informatico

Banche dati

I dati strutturati delle applicazioni gestionali sono memorizzati in banche dati centralizzate per le applicazioni utilizzate da più utenti; più raramente, su stazione di lavoro per applicazioni mono-utente.

Oltre alle banche dati delle applicazioni gestionali esistono archivi documentali non strutturati, residenti sui server centrali. Questi archivi sono copie di comodo per il lavoro da svolgere nei vari uffici, ma non contengono e non devono contenere documenti soggetti a conservazione digitale.

Anche per queste cartelle di lavoro è garantito il backup ed il ripristino dei dati.

Posta elettronica

La posta elettronica viene gestita internamente; ad ogni dipendente è assegnata una casella individuale. Esistono caselle non nominali corrispondenti a gruppi di lavoro, servizi, uffici o figure istituzionali.

Sistemi di autenticazione

Gli utenti accedono con credenziali per l'accesso alle procedure applicative formata da nome utente e password.



3.1.4. Sicurezza dei dati

Banche dati centralizzate

L'accesso ai dati avviene tramite le procedure gestionali che li trattano, all'utente viene richiesta la digitazione di username e password. Queste credenziali sono verificate dalla procedura stessa che attribuisce in modo contestuale il livello di operatività a cui è autorizzato il soggetto.

Archivi documentali centralizzati

I server contenenti archivi documentali richiedono l'autenticazione e l'autorizzazione dell'utente.

Banche dati ed archivi documentali residenti sulle memorie locali dei PC

Non sono autorizzate memorizzazioni di archivi documentali o dati personali sugli hard disk dei singoli personal computer, perché non è possibile garantire la copia e il ripristino degli stessi. E' lasciata alla discrezionalità del singolo la possibilità di utilizzare l'hard disk locale per copie di comodo, ma con l'obbligo di provvedere alla cancellazione delle stesse se non più utili e con la consapevolezza che delle stesse non viene fatta copia di sicurezza e non è garantito il ripristino.

3.2. Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni

3.2.1. Incaricati del trattamento informatico

Incaricato del trattamento è il Responsabile dei sistemi informatici.

3.2.2 Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica

Preposto alla gestione delle credenziali per l'accesso alle banche dati centralizzate che utilizzano i sistemi è il Responsabile del servizio sistemi informatici a cui compete la gestione del sistema informatico/telematico del comune.

Il preposto alla gestione delle credenziali può variare la password degli incaricati, in caso che si renda indispensabile ed indifferibile, per esclusiva necessità di operatività e sicurezza del sistema, dandone pronta comunicazione agli stessi in modo riservato.

Il preposto alla gestione delle credenziali attribuirà i diversi livelli di accesso alle risorse di rete e agli applicativi comunali in base alle specifiche e dettagliate disposizioni dei singoli dirigenti.

Le modifiche, revoche o cancellazioni delle credenziali dovranno essere comunicate tempestivamente al preposto alla gestione delle credenziali dai singoli Dirigenti.



3.2.3 Trattamento dei dati personali affidati ai lavoratori

Assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione consistono in un codice per l'autenticazione dell'incaricato (userid) associato ad una parola chiave riservata(password). In caso di assunzione di un nuovo lavoratore, quest'ultimo, il responsabile del settore competente o il responsabile del trattamento dei dati da lui delegato richiede al preposto alla gestione, attraverso l'apposita procedura informatica , l'assegnazione della casella di posta elettronica e delle credenziali di autenticazione. Il preposto alla gestione provvede all'assegnazione della posta elettronica, di userid e della password provvisoria inserendo le credenziali in [TIPO DOMINIO] e comunica le credenziali all'utente in modo riservato. E' a cura del lavoratore sostituire la password provvisoria con quella definitiva.

Può accadere che, per esigenze di servizio, esistano credenziali d'accesso non legate ad un singolo lavoratore e che possono essere condivise da tutto un gruppo di operatori. Queste credenziali non possono consentire l'accesso a banche dati o documenti contenenti dati personali e verranno assegnate unicamente a dipendenti del comune individuati quali responsabili della gestione della password.

Assegnazione delle autorizzazioni

Per poter accedere, a qualsiasi titolo, alle applicazioni ed alle banche dati del comune occorre essere autorizzati.

L'autorizzazione del singolo lavoratore ad accedere alle banche dati del Comune deve essere sempre preceduta dal conferimento dell'incarico al trattamento dei dati da parte del responsabile del trattamento dei dati d'intesa con il titolare del trattamento , vale a dire il responsabile dell'unità organizzativa.

La competenza alla richiesta, revoca, modifica delle autorizzazioni è della figura responsabile dell'unità organizzativa di appartenenza del lavoratore, che può delegarla per iscritto al responsabile al trattamento dei dati.

Accesso ad applicazioni e banche dati del settore di appartenenza

Il responsabile della UO di appartenenza/ responsabile delegato sulla base dell'incarico conferito al lavoratore, comunica al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, a quali banche dati il lavoratore è autorizzato ad accedere. Il preposto alla gestione delle credenziali abilita il lavoratore alle banche dati di sua competenza.

Cessazione del rapporto di lavoro

Dopo 30 giorni dalla data di cessazione del rapporto lavorativo, il preposto alla gestione delle credenziali, attraverso una procedura automatica, ricava dalla Banca dati centralizzata del Settore a cui compete la gestione del personale, il nominativo del lavoratore cessato, ne revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica, e ne informa, attraverso l'apposita procedura informatica, il responsabile informatico dell'applicazione.

Nel caso di rapporto di collaborazione coordinata e continuativa, di prestazione occasionale, di tirocinio formativo ed in genere in tutti i casi in cui non è possibile



ricavare l'informazione dell'avvenuta cessazione in modo automatico dalla Banca dati centralizzata del Settore a cui compete la gestione del personale, spetta al Dirigente del Settore competente/ responsabile delegato comunicare tempestivamente al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, l'avvenuta cessazione del rapporto di lavoro e chiedere la revoca delle relative credenziali e autorizzazioni. Il preposto alla gestione delle credenziali revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica e ne informa, attraverso l'apposita procedura informatica, il Dirigente del Settore competente e il responsabile informatico dell'applicazione.

Prima della cessazione del rapporto di lavoro, il lavoratore deve eliminare dal suo PC i documenti e le e-mail che non siano di interesse del Settore, autorizzando attraverso l'apposita procedura informatica, il Dirigente ad accedere ai documenti ed alle e-mail rimanenti. Il Dirigente di Settore/responsabile delegato deve prontamente avvisare il soggetto preposto alla pulizia o recupero delle banche dati di cui al punto 3.1 concordando con lui le modalità di gestione della stazione di lavoro e dei dati in essa contenuti.

Nel caso in cui, per esigenze contingenti, non sia stata rilasciata la liberatoria, il Dirigente di Settore/ responsabile delegato richiede ed autorizza l'intervento del tecnico dell'Ufficio Sistema e Reti. Questo intervento verrà documentato mediante apposito verbale redatto a cura del Dirigente di Settore/ responsabile delegato. Nel caso in cui si provveda al ritiro della stazione di lavoro, i dati legati al profilo del lavoratore verranno resi indisponibili dopo averne trattenuto una copia. Entro un mese il Dirigente di Settore/ responsabile delegato può richiedere il recupero delle banche dati e delle e.mail giacenti nella casella di posta disabilitata, esibendo la relativa autorizzazione del lavoratore. Trascorso tale periodo il preposto provvederà alla eliminazione definitiva dei suddetti dati.

Trasferimento del lavoratore

Nel caso di trasferimento presso un altro Settore di un lavoratore, il preposto alla gestione delle credenziali, dopo aver rilevato l'informazione attraverso la Banca dati centralizzata del Settore a cui compete la gestione del personale, provvede a revocare tutte le autorizzazioni all'accesso del lavoratore, ad eccezione dell'indirizzo di posta elettronica, e ne informa, attraverso l'apposita procedura informatica, il responsabile informatico dell'applicazione. Il lavoratore trasferito deve reindirizzare al Settore di provenienza tutta la corrispondenza di posta elettronica di competenza di quest'ultimo. Il Dirigente del Settore di nuova assegnazione/ responsabile delegato, sulla base del

nuovo incarico al trattamento dei dati conferito al lavoratore e delle competenze a quest'ultimo attribuite, provvede a richiedere le nuove abilitazioni, anche relative all'accesso a banche dati di un altro Settore, con le stesse modalità previste nel caso di nuova assunzione.

Nel caso di trasferimento di un lavoratore nell'ambito dello stesso Settore, il Dirigente di Settore/ responsabile delegato, sulla base del nuovo incarico al trattamento dei dati conferito e delle competenze a quest'ultimo attribuite, comunica al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, le autorizzazioni all'accesso da revocare e le nuove applicazioni, anche relative all'accesso a banche dati di un altro Settore, alle quali il lavoratore è autorizzato ad accedere. Il preposto alla



gestione delle credenziali disabilita le autorizzazioni all'accesso e per le nuove abilitazioni procede con le modalità previste nel caso di nuova assunzione informando, attraverso l'apposita procedura informatica, il Dirigente di Settore e il responsabile informatico dell'applicazione. Nel caso che il trasferimento del lavoratore (ad un altro Settore o nell'ambito dello stesso Settore) comporti il contemporaneo trasferimento del PC, il lavoratore è tenuto a consegnare al Dirigente i dati e le e-mail di interesse del Settore e successivamente a rimuoverli dalla propria stazione di lavoro. Nel caso invece in cui il trasferimento non comporti il contemporaneo trasferimento del PC, si deve seguire il comportamento previsto per il caso di cessazione del rapporto di lavoro.

3.2.4. Trattamento dei dati personali affidati a soggetti esterni

Sono considerati soggetti esterni tutti quei soggetti che non rientrano nel punto 3.2.3. (a puro titolo esemplificativo: società, enti, consorzi, professionisti, soggetti pubblici o gestori di pubblici servizi).

La titolarità del trattamento dei dati resta in capo al Comune.

Il Dirigente del Settore contraente nomina il soggetto esterno responsabile del trattamento dei dati.

Nel caso in cui l'oggetto del contratto o della convenzione comporti l'utilizzazione di applicazioni o banche dati di competenza di più Settori, la designazione del responsabile dovrà essere sottoscritta congiuntamente dal Dirigente del Settore contraente e dai Dirigenti delle banche dati interessate. All'inizio della collaborazione il soggetto esterno responsabile del trattamento fornisce al Dirigente del Settore l'elenco degli incaricati al trattamento dei dati da lui nominati. Il Dirigente di Settore/ responsabile delegato, comunica al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica:

1. a quali applicazioni l'incaricato è abilitato, richiedendo altresì, se necessario l'accesso ad Internet e l'utilizzo della posta elettronica;
2. la data di scadenza del contratto/ convenzione, se in suo possesso.

Nel caso in cui l'abilitazione riguardi banche dati di competenza di più Settori, nella comunicazione il Dirigente del Settore contraente dovrà altresì dare atto che i Dirigenti dei Settori interessati sono stati informati della richiesta.

Il preposto alla gestione delle credenziali imposta per l'utente un periodo massimo di validità pari alla durata del contratto/ convenzione, se conosciuta. In caso contrario il periodo di validità delle credenziali è di dodici mesi. Almeno 60 giorni prima della scadenza il preposto alla gestione delle credenziali comunica al Dirigente di Settore tramite e-mail che, scaduto il periodo di validità, le credenziali dell'utente, salvo diversa comunicazione, saranno disabilite. Trascorsi 30 giorni dalla scadenza del periodo di validità delle credenziali, senza che sia pervenuta una diversa comunicazione da parte del Dirigente di Settore, l'utente verrà dimissionato.

L'utente esterno che utilizza un PC di proprietà del Comune, prima della cessazione a qualsiasi titolo del suo incarico, deve eliminare dallo stesso i documenti e le e-mail che non siano di interesse del Settore, autorizzando per iscritto il Dirigente ad accedere ai documenti ed alle e-mail rimanenti. Il Dirigente di Settore/ responsabile delegato deve prontamente avvisare il soggetto preposto alla pulizia o recupero delle banche dati di cui al punto 3.1 concordando con lui le modalità di gestione della stazione di lavoro e dei dati in essa contenuti. Nel caso in cui, per esigenze contingenti, non sia stata



rilasciata la liberatoria, il Dirigente di Settore/ responsabile delegato richiede ed autorizza l'intervento del tecnico dell'Ufficio Sistema e Reti. Questo intervento verrà documentato mediante apposito verbale redatto a cura del Dirigente di Settore/ responsabile delegato. Nel caso in cui si provveda al ritiro della stazione di lavoro i dati legati al profilo dell'utente esterno verranno resi indisponibili dopo averne trattenuto una copia. Entro un mese il Dirigente di Settore/ responsabile delegato può richiedere il recupero delle banche dati e delle e.mail giacenti nella casella di posta disabilitata, esibendo la relativa autorizzazione dell'utente esterno. Trascorso tale periodo il preposto provvederà alla eliminazione definitiva dei suddetti dati.

Accesso alle banche dati

L'accesso telematico alle banche dati del Comune è consentito alle amministrazioni pubbliche e ai soggetti gestori o concessionari di servizi pubblici esclusivamente per finalità istituzionali.

3.2.5. Modalità di gestione delle password

Le password utilizzate nei sistemi di autenticazione sono assegnate dal preposto alla gestione delle credenziali all'atto della creazione delle credenziali stesse, sono identiche e vengono comunicate in forma riservata all'utente che deve provvedere, al primo utilizzo, alla sostituzione della password assegnata con una conosciuta solo dal medesimo.

Su ogni nuova stazione di lavoro assegnata viene creato un profilo con lo stesso userid che l'utente ha sui sistemi centralizzati di autenticazione ma con password provvisoria. Il dipendente ha l'obbligo di impostare la password seguendo la procedura di cambio password nel rispetto della normativa vigente.

Le password gestite tramite il sistema sono composte da almeno 8 caratteri e scadono automaticamente ogni tre mesi. All'approssimarsi della scadenza l'utente viene avvertito. Per motivazioni tecniche è opportuno avere un'unica password per l'accensione del PC, per l'accesso ad internet e per l'apertura della posta elettronica. Il lavoratore, qualora dimentichi la password d'accesso al proprio PC, dovrà rivolgersi al lavoratore da lui delegato alla custodia delle password (si veda paragrafo 3.3.3) o, in alternativa, al servizio di assistenza che si recherà sul posto e consentirà all'utente l'accesso al PC allo scopo di impostare una nuova password.

Qualora invece l'utente dimentichi la propria password, dovrà rivolgersi all'Ufficio Informatica che provvederà, previa identificazione personale, a fornire al lavoratore o a un suo delegato, una password provvisoria che consentirà di accedere alla procedura di modifica ed ottenere quella definitiva.

Qualora l'utente sia stato disabilitato per mancato uso delle credenziali per un periodo di almeno sei mesi, la procedura di riattivazione delle credenziali è quella di cui al successivo punto 3.2.6. Un utente che non sia stato disabilitato può, in qualsiasi momento, modificare la propria password autenticandosi con userid e vecchia password la nuova password verrà scelta dall'utente.

Ogni incaricato che riceve le proprie password ne è direttamente responsabile. Fatta eccezione per quanto previsto dal paragrafo 3.3.3., il lavoratore non deve in alcun modo comunicare le proprie password a persone diverse od altri incaricati; qualora avesse il timore che la propria password sia divenuta di conoscenza di altri soggetti deve prontamente provvedere a modificarla.



3.2.6. Disattivazione credenziali per disuso

Il mancato uso delle credenziali per almeno sei mesi continuativi determina la loro disattivazione.

Per riattivare le credenziali, l'utente dovrà rivolgersi all'Ufficio segreteria che provvederà, previa identificazione personale, a fornire in busta chiusa una password provvisoria che consentirà di accedere alla procedura di modifica della password ma che dovrà poi essere immediatamente sostituita da una definitiva.

3.3. Modalità di gestione delle stazioni di lavoro

3.3.1 Soggetto preposto alla pulizia o recupero delle banche dati su PC

Preposto alla pulizia o recupero delle banche dati su PC è il responsabile dei sistemi informativi, a cui compete la gestione del sistema informatico / telematico del comune, che provvederà alla designazione del personale incaricato.

3.3.2 Programmi antivirus

Su tutti i PC sono installati programmi antivirus che vengono aggiornati periodicamente in modo automatico, tramite l'accesso in rete al Server di gestione antivirus; l'antivirus installato sui singoli PC controlla in tempo reale i documenti utilizzati.

Oltre che sulle stazioni di lavoro sono installati sistemi antivirus sui server di posta elettronica, sistema di filtraggio della navigazione e file server, ovvero server che permettono la condivisione di documenti.

I Server di Gestione Antivirus si aggiornano in modo automatico. E' opportuno che l'utente, con periodicità almeno quindicinale, effettui con il software antivirus una scansione completa dei dischi interni della stazione di lavoro.

3.3.3 Interventi di accesso o manutenzione del PC

Durante l'assenza del lavoratore il Dirigente del Settore o il responsabile del trattamento può accedere a dati e procedure del pc del lavoratore assente e verificare il contenuto dei messaggi a quest'ultimo indirizzati, a condizione che ciò si renda indispensabile e indifferibile, per esclusiva necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa.

A tale scopo il Dirigente di Settore, sulla base delle scelte operative/organizzative effettuate, valuta i casi in cui il lavoratore deve consegnare ad un altro lavoratore da lui delegato per iscritto una busta chiusa contenente le proprie password, avendo cura di sostituirla ogni volta che esse vengono cambiate.

Il lavoratore delegato, su richiesta e alla presenza del Dirigente del Settore o del responsabile del trattamento, accede ai dati e alle procedure nonché ai messaggi di posta elettronica del lavoratore assente provvedendo a inoltrare al Dirigente del Settore o al responsabile da quest'ultimo indicato quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Dell'attività compiuta è redatto apposito verbale a cura del Dirigente/responsabile che ne informa il lavoratore assente alla prima occasione utile.

Nel caso in cui non sia stato delegato alcun lavoratore oppure nel caso in cui anche il



lavoratore delegato non sia presente, il Dirigente Responsabile di Settore/ responsabile delegato richiede ed autorizza l'intervento dei tecnici dell'Ufficio Informatica, che ne permettono l'accesso per il tempo necessario.

Questo intervento verrà documentato mediante apposito verbale redatto a cura del Dirigente Responsabile del Settore/ responsabile delegato e comunicato al lavoratore alla prima occasione utile.

Gli interventi dei tecnici possono avvenire senza conoscere e senza modificare la password del lavoratore, grazie ad una password di servizio custodita dal preposto, secondo le regole tecniche previste dalla legge.

Interventi di Manutenzione Quando per un PC occorre fare un intervento di manutenzione, ordinaria o straordinaria, sul loco o in laboratorio, sarà cura del lavoratore concordare modi e tempi di intervento con i tecnici addetti.

Se l'intervento necessita dell'accesso al PC con le credenziali del lavoratore, queste, se possibile, saranno inserite dallo stesso e non comunicate al tecnico.

Nel caso che il lavoratore non possa presenziare all'intervento, questi comunicherà le proprie credenziali al tecnico e provvederà a modificarle una volta terminato l'intervento

3.3.4. Società esterne o professionisti per la manutenzione e l'assistenza

Il Dirigente del Settore a cui compete la gestione del sistema informatico / telematico nomina la società che effettua la manutenzione dei sistemi hardware o software responsabile del trattamento dei dati il quale andrà integrato con una specifica assunzione di impegno da parte del responsabile stesso al rispetto delle seguenti disposizioni:

- a) non effettuare copie né procedere alla eliminazione degli archivi informatici di titolarità dell'ente detenuti.
- b) informare preventivamente gli interessati del giorno e dell'orario in cui saranno effettuati gli interventi tecnici.
- c) richiedere preventivamente l'autorizzazione ai tecnici dell'Ufficio Informatico nel caso di interventi di assistenza tramite collegamento remoto. Gli stessi tecnici dovranno essere avvisati al termine delle operazioni.
- d) usare riservatezza su dati ed informazioni addivenuti in loro possesso.
- e) trasmettere al Dirigente del Settore a cui compete la gestione del sistema informatico / telematico, all'inizio della collaborazione l'elenco degli incaricati al trattamento e successive variazioni
- f) trasmettere al Dirigente del Settore a cui compete la gestione del sistema informatico / telematico il nominativo degli amministratori di sistema affinché si possa provvedere al loro incarico

3.3.5. Dismissione delle stazioni di lavoro

In caso di dismissione di PC, il Dirigente che ha in carico la stazione di lavoro deve prontamente comunicare al soggetto preposto alla pulizia la presenza di banche dati da recuperare. Il soggetto preposto una volta recuperate le banche dati, conserva la stazione di lavoro per un mese quindi provvede a rendere illeggibili i dischi magnetici prima della rottamazione.

I dischi dei PC usati che il Comune cede in comodato d'uso prima della consegna



vengono riformattati impedendo l'accesso alle banche dati che vi erano contenute.

3.4. Salvataggio dei dati

Il salvataggio delle banche dati esistenti sui server è in carico all'Ufficio responsabile della banca dati.

Sui sistemi centralizzati vengono fatte copie almeno quotidiane degli archivi documentali e delle banche dati strutturate allo scopo di fornire almeno una versione aggiornata alla notte precedente.

L'esecuzione dell'operazione di salvataggio è verificata quotidianamente dagli operatori di sala macchine.

Ogni singola postazione di lavoro (client) non è soggetta a salvataggi quindi la formazione di eventuali archivi in locale, in caso di perdita dati, è di responsabilità dell'operatore.

Sono messe a disposizione cartelle di rete per settore, ufficio, utente ove poter depositare gli archivi di interesse comune o personali.

3.5. Locali

La sala macchine dove risiedono fisicamente i server su cui sono memorizzati i dati dell'Ente è dotata di impiantistica tale da garantire la sicurezza fisica dell'hardware, sia delle banche dati:

1. porta d'ingresso ad uso riservato;
2. gruppo di continuità esterno e di stabilizzazione della corrente;
4. impianto di rilevamento fumi e spegnimento automatico in caso di incendio;
5. impianto antintrusione collegato con il sistema di allarme centralizzato.

3.6. Cautele generali

3.6.1. Password

Il sistema centralizzato di autenticazione Active directory provvede in modo automatico alla scadenza trimestrale della password. Nel caso in cui le password siano impostate dall'utente, è sua responsabilità provvedere alla loro modifica almeno ogni tre mesi.

La password deve essere composta da almeno 8 caratteri contenuti numeri lettere maiuscole e minuscole.

Le password non devono contenere riferimenti agevolmente riconducibili all'incaricato e devono essere modificate almeno ogni tre mesi.

3.6.2. Uso del computer

Il PC una volta avuto l'accesso non deve essere lasciato incustodito.

In caso di assenza anche temporanea dall'ufficio, l'utente attivo al momento deve essere disconnesso o deve essere attivata la modalità salvaschermo con protezione mediante password. Il Dirigente di Settore/ responsabile delegato può impartire ulteriori istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro.



6.3. Custodia dei supporti

Devono essere impartite, da parte del Dirigente di Settore/ responsabile delegato, le istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati per motivi di sicurezza e al fine di evitare accessi non autorizzati e trattamenti non consentiti.