Approvato con delibera n. 208 del 17 maggio 2006

REGOLAMENTO SULLA SICUREZZA

PER IL TRATTAMENTO DEI DATI PERSONALI

CON STRUMENTI ELETTRONICI

Consiglio Regionale

Regione Friuli – Venezia Giulia

INDICE

1. Introduzione

1.1. Premessa al documento

Il presente documento raccoglie norme e linee guida da seguire per eliminare o ridurre i rischi derivanti da un uso scarsamente corretto ed a volte poco consapevole dell'utilizzo degli strumenti elettronici.

Un uso degli strumenti elettronici, difforme dalle regole contenute nel presente documento, può esporre il Consiglio regionale a rischi di accessi non autorizzati o alla divulgazione di informazioni relative al sistema informatico interno.

L'utilizzatore è la prima "vittima" della violazione della riservatezza e della sicurezza e per tale motivo il presente documento vuole innanzi tutto tutelare e salvaguardare chi con la propria attività lavorativa utilizza questi strumenti. I dati trattati per mezzo dei sistemi del consiglio regionale rimangono di proprietà dello stesso.

1.2. Campo di applicazione del documento

Il presente documento si applica a tutti i soggetti che utilizzano le risorse informatiche del Consiglio Regionale presso qualunque sede o ufficio riconducibile alla struttura, siano essi dipendenti a tempo pieno o parziale, collaboratori, consulenti, dipendenti di aziende esterne legate da contratti di fornitura di servizi o altri a cui ne è concesso l'uso.

1.3. Quadro normativo di riferimento

Decreto Legislativo 30 giugno 2003 n. 196. Codice in materia di protezione dei dati personali.

Legge 20 maggio 1970 n. 300. Norme sulla tutela della libertà e dignità del lavoratori, della libertà sindacale e dell'attivita' sindacale nei luoghi di lavoro e norme sul collocamento (*Statuto dei lavoratori*)...

Legge 18 agosto 2000 n. 248. Nuove norme di tutela del diritto d'autore.

Legge 7 agosto 1990 n. 241. Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

1.4. Definizioni

Autenticazione informatica: L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziale 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.

Codice identificativo personale: Il dato, componente di una Credenziale di autenticazione in possesso di una persona, da questa conosciuto o ad essa univocamente correlato, utilizzato per l'autenticazione informatica *(Es: Matricola).*

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 *(Password).*

Risorse informatiche consiliari. Qualsiasi combinazione di apparati tecnologici del Consiglio regionale hardware o software utilizzati per le comunicazioni elettroniche ed elaborazione dei dati.

Responsabile per la sicurezza. E' il soggetto a cui è conferito il compito di sovraintendere alle problematiche relative alla sicurezza informatica, definendo regole e comportamenti, criteri tecnici, organizzativi e procedurali atti a garantire un idoneo livello di sicurezza.

Amministratore di Sistema. Soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Utilizzatore. Qualsiasi persona fisica che utilizza le risorse informatiche del Consiglio regionale.

2. Indicazioni generali

2.1. Incaricati, trattamenti ed utilizzi consentiti

L'utilizzo delle risorse informatiche consiliari è riservato agli Incaricati al trattamento da parte del Consiglio Regionale del Friuli Venezia Giulia, come definito al paragrafo 1.2. Le risorse informatiche sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente professionali ed istituzionali. Ciò vale sia per le risorse condivise (risorse di rete, stampanti di rete, fax, ecc.), sia per quelle affidate al singolo dipendente (Personal Computer, periferiche, stampanti locali, ecc.).

Le risorse informatiche affidate al singolo Incaricato sono strumenti di lavoro appartenenti al patrimonio del Consiglio regionale e pertanto vanno custoditi in modo appropriato; il furto, il danneggiamento o lo smarrimento di tali strumenti debbono essere prontamente segnalati all'Ente.

2.2. Personal computer fissi e mobili

Le tipologie dei Personal Computer forniti quali strumenti di lavoro sono suddivise in Personal Computer fissi, strumenti che vengono utilizzati in maniera permanente sul proprio posto di lavoro, e in Personal Computer Mobili, strumenti che possono venir agevolmente trasportati ed utilizzati sia in sede che fuori sede.

2.2.1. Configurazioni di sistema

Il Personal Computer che viene consegnato all'Incaricato è comprensivo del software certificato e necessario a svolgere correttamente le mansioni affidate. Non è consentito modificare le configurazioni impostate sul proprio PC.

2.2.2. Software e hardware

Premesso che il Software e l'Hardware presenti sui PC permettono all'Incaricato di svolgere le proprie mansioni, ogni modifica sostanziale alla configurazione mediante l'alterazione dei parametri, l'aggiornamento del software presente oppure l'allacciamento e l'uso di risorse hardware non preventivamente fornite, possono compromettere la stabilità del sistema.

Non è consentito l'uso e l'installazione di programmi diversi da quelli presenti e previsti dagli standard del Consiglio regionale. Eventuali necessità che prevedano l'impiego di software non predisposto saranno autorizzate dal segretario generale.

Non è consentito l'utilizzo di programmi di origine esterna all'Ente introdotti attraverso Internet, Posta Elettronica od altri dispositivi di memorizzazione (Cd-rom, dischetti, ecc).

Non sono consentiti l'installazione e/o l'utilizzo di strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o di documenti informatici.

Non è consentita l'installazione autonoma di alcun dispositivo di memorizzazione, comunicazione o altro (masterizzatori, modem, ecc.) senza preventiva autorizzazione da parte del Segretario generale.

2.2.3. Accesso al Personal computer e controllo remoto

La facilitazione delle operazioni di aggiornamento del software e la garanzia la sicurezza dei dispositivi, delle applicazioni e dei dati può avvenire attraverso strumenti di controllo remoto che consentano di compiere le operazioni necessarie attraverso la rete locale.

L'assistenza tecnica per malfunzionamenti ordinari o diagnosi di sistema attraverso strumenti di controllo remoto deve avvenire solo previa autorizzazione dell'utilizzatore e di norma in presenza dell'utilizzatore stesso.

In caso di malfunzionamenti straordinari e in situazioni di emergenza il Responsabile della sicurezza ha la facoltà in qualunque momento di accedere a qualunque sistema informatico del Consiglio regionale per l'espletamento delle proprie funzioni.

2.2.4. Disposizioni ulteriori per Personal computer mobili

E' obbligo di ogni possessore di un PC mobile, custodire con la massima diligenza il proprio dispositivo e le periferiche ad esso correlate (stampanti, chiavi USB, unità di salvataggio, ecc.), sia esso fuori sede che in sede.

Colui che utilizza il Personal Computer fuori dall'ambito della rete locale, cioè non direttamente allacciato tramite scheda di rete o linea telefonica, dovrà adottare tutte le misure di sicurezza previste.

2.3. Rete del Consiglio Regionale

La possibilità di accedere alla rete interna da parte di ogni utilizzatore, rappresenta lo strumento più rilevante per il trattamento dei dati e per l'utilizzo dei servizi di accesso e condivisione delle risorse. L'utilizzo della complessa e diversificata gamma dei servizi erogati deve aderire ai compiti e alle attività assegnate per il raggiungimento del fine istituzionale dell'Consiglio regionale.

Le modalità di accesso richiedono sempre l'assegnazione di Credenziali di autenticazione, corredate da precise norme di attivazione, controllo e disattivazione.

Il corretto utilizzo delle risorse di rete è strettamente correlato a scopi strettamente lavorativi, per tale motivo ogni attività deve essere adeguata a questi vincoli. Sono vietate all'utilizzatore le seguenti attività:

- Trasgressione della riservatezza di altri utilizzatori o dell'integrità di dati personali.
- Compromissione dell'integrità dei sistemi e dei servizi.
- Consumo di risorse in misura tale da compromettere l'efficienza di altri servizi di rete.

Il Consiglio Regionale si riserva la facoltà di procedere alla verifica ed alla eventuale rimozione di qualsiasi file o applicazione memorizzato sulle cartelle di rete se ritenuto rischioso per la sicurezza dei sistemi, od anche acquisito e installato in violazione delle norme contenute nel presente documento.

2.4. Credenziali di autenticazione

Una Credenziale di autenticazione è lo strumento in possesso dell'utilizzatore che permette la sua autenticazione alla rete del Consiglio regionale all'utilizzo di banche dati. Una Credenziale è formata da almeno due elementi:

1. **Il Codice identificativo personale.** Un codice alfanumerico di lunghezza variabile, generalmente pubblico.

2. **La Parola chiave.** Un codice alfanumerico di lunghezza variabile assegnato dall'Amministratore del sistema, che deve essere mantenuto riservato.

Ogni Credenziale di autenticazione viene assegnata al singolo utilizzatore, in maniera tale da garantirne il riconoscimento e da assicurare che il Codice identificativo venga utilizzato solamente dal legittimo assegnatario. E' indispensabile che la Parola chiave, conosciuta esclusivamente dall'assegnatario e che tutela dagli utilizzi illeciti dei propri privilegi di accesso alle risorse hardware, software e dati non venga mai divulgata.

Gli obblighi per l'utilizzatore, derivanti anche dalla lettura del Codice in Materia di Protezione dei dati personali, non sono circoscritti solamente al buon uso dei programmi di accesso e di interrogazione del patrimonio informativo del Consiglio regionale ma, soprattutto ed in maniera non marginale, anche all'applicazione di misure personali tese a garantire la riservatezza dei dati utilizzati.

Nei seguenti paragrafi verranno illustrate alcune indicazioni pratiche volte a chiarire le attività a carico dei singoli utilizzatori consentendo un utilizzo sicuro ed idoneo delle Parole Chiave.

2.4.1. Indicazioni generali

Qualsiasi sistema di autenticazione utilizzato nell'ambito del Consiglio regionale deve rispondere alle seguenti specifiche.

Deve contenere almeno un elemento segreto (la Parola chiave), generato in maniera sicura e non disponibile in chiaro né all'utilizzatore né all'Amministratore del Sistema. Ove ciò non fosse possibile verrà imposto l'obbligo della sostituzione al primo accesso.

Ogni elemento segreto deve rispettare precise regole di composizione volte ad impedirne l'individuazione da parte di persone non autorizzate.

La parola chiave deve essere comunicata all'utilizzatore attraverso un canale di comunicazione sicuro ed in maniera separata dal Codice identificativo personale.

L'utilizzatore deve essere in grado di modificare la Parola chiave in maniera manuale o automatica; comunque sicura, in modo tale che nessuno ne sia a conoscenza o ne abbia la disponibilità, anche temporanea.

All'atto della modifica devono essere effettuati in maniera automatica e, in tempo reale, tutti i controlli utili a verificare il rispetto delle regole di composizione e, in caso contrario, a impedire la modifica.

Deve essere previsto un periodo massimo di validità per la Parola chiave, al termine del quale l'utilizzatore deve essere obbligato a modificarla.

Deve essere prevista una procedura di emergenza per consentire all'utente di accedere al Sistema anche in caso di dimenticanza/indisponibilità della propria Parola chiave. Tale procedura deve prevedere l'identificazione dell'utilizzatore e non deve essere attivata sulla base di una semplice richiesta telefonica.

La Parola chiave deve essere conosciuta solamente dall'utilizzatore, non vi devono essere pertanto Parole chiave *di gruppo*; come pure non può venir annotata accanto al Personal computer o riferita a colleghi, Amministratori di sistema o tecnici che eseguono interventi, sia interni che esterni. Ogni inadempienza a questo punto dovrà venir rapidamente ovviata modificando la Parola chiave o facendo disabilitare la Credenziale di accesso.

2.4.2. Assegnazione delle Credenziali di autenticazione

Ad ogni utilizzatore, previa richiesta da parte del proprio responsabile, vengono assegnate le Credenziali di autenticazione e i relativi profili di autorizzazione necessari e sufficienti all'attività che sarà tenuto a svolgere.

Tipicamente viene assegnata la Credenziale di accesso alla rete dell'Ente e le Credenziali necessarie all'utilizzo dei prodotti software utilizzati dal Consiglio Regionale

Il Codice di identificazione personale, associato alla Credenziale, non può venir assegnato ad altri incaricati, neppure in tempi diversi.

La Parola chiave della credenziale di autenticazione di accesso alla rete del Consiglio regionale deve venir cambiata almeno ogni 3 mesi.

La comunicazione del Codice di identificazione e della Parola chiave avviene mediante l'invio in busta chiusa e sigillata al richiedente che provvederà ad inoltrarla all'utilizzatore.

2.4.3. Ulteriori forme di protezione, limitazione e controllo dell' accesso

E' possibile attivare ulteriori forme di protezione per impedire accessi indesiderati o cautelarsi da accessi illeciti. Qualora ciò fosse necessario si elencano di seguito alcuni suggerimenti:

Protezione all'accensione. E' possibile attivare una Parola chiave all'accensione della macchina; ciò introduce un elemento di sicurezza a monte dell'attivazione del sistema operativo ed è legato all'hardware del Personal computer.

Salvaschermo. Il salvaschermo e' quella funzionalità presente sui sistemi Windows che viene innescata dopo un periodo predefinito di inattività del Personal computer, L'attivazione del salvaschermo con temporizzatore è obbligatoria e deve venir configurato su ogni Personal computer. Ulteriori informazioni vengono riportate al capitolo 6.2.

Protezione delle cartelle personali di Posta. Di norma l'accesso alla casella personale di Posta viene tutelato dalla Credenziale di autenticazione alla rete del Consiglio regionale, ma le cartelle poste sui server oppure sul

proprio Personal computer non prevedono un automatismo di protezione che, pertanto, è necessario attivare a posteriori.

2.4.4. Alcuni problemi in presenza di più Credenziali di autenticazione

Dal quanto riportato ai paragrafi precedenti si evince che ogni utilizzatore può possedere più di una Credenziale di autenticazione, ognuna con una Parola chiave diversa.

Consuetudine vuole che ogni utilizzatore cerchi di uniformare le proprie Parole chiave, ed anche se ciò viene sconsigliato, in quanto diminuisce la solidità delle Credenziali ed offre una possibilità di accesso ai sistemi ed ai dati, di fatto è una prassi consolidata, che sicuramente contribuisce a limitare problemi di ordine pratico.

L'omogeneizzazione delle Parole chiave deve venir limitata il più possibile, compatibilmente con il numero delle Credenziali di autenticazione possedute ed in armonia con i dati che vengono trattati.

2.4.5. Regole per la costruzione delle Parole chiave

Qui di seguito vengono elencati alcuni obblighi nella costruzione della Parola chiave:

- La lunghezza della Parola chiave deve essere almeno di 8 caratteri o, dove non fosse possibile, pari al massimo consentito.
- La Parola chiave non deve essere uguale ad una data (con i mesi espressi in numeri romani e con tutti i separatori di uso comune "- / .").
- La Parola chiave deve essere diversa da:
    - Codice identificativo personale.
    - Cognome o nome dell'utilizzatore.
    - Matricola (se diversa dal Codice identificativo personale).

Nel prosieguo vengono indicati alcuni suggerimenti che rafforzano la solidità della Parola chiave:

- La Parola chiave deve essere costruita utilizzano i caratteri numerici (1,2,3,ecc.), alfabetici (a,b,c,,ecc.), e i simboli speciali (!,§,ecc.) presenti su tutti i tipi di tastiere in uso.
- La Parola chiave deve contenere almeno un carattere appartenente a ciascuno degli insiemi sopra enunciati.
- La Parola chiave non deve contenere più di tre caratteri uguali consecutivi.
- La Parola chiave non deve contenere spazi vuoti in nessuna posizione.

- Devono esserci almeno 5 caratteri differenti tra la vecchia e la nuova Parola chiave.

2.4.6. Ciclo di vita delle credenziali di autenticazione

Gli eventi che caratterizzano il ciclo di vita delle Credenziali di autenticazione e delle Parole chiave sono i seguenti:

- Generazione
- Conservazione
- Utilizzo
- Sostituzione
- Cancellazione

2.4.6.1. Generazione

La Credenziale di autenticazione viene generata dagli Amministratori di sistema e comunicata secondo quanto previsto al Paragrafo 2.4.2. La Parola chiave può venir generata anche dall'utilizzatore stesso nel caso di protezione del Personal computer all'accensione oppure di protezione della cartelle personali di Posta. E' d'obbligo scegliere o reimpostare la Parola chiave al momento del primo conferimento di una Credenziale oppure all'attivazione di un nuovo servizio in cui viene previsto l'utilizzo di una Parola chiave.

2.4.6.2. Conservazione

La Parola chiave non deve venir rivelata a nessuno e deve essere custodita con tutta la cura necessaria dal legittimo proprietario. Non è pertanto opportuno mantenere traccia scritta della Parola chiave.

2.4.6.3. Utilizzo

Per un corretto utilizzo della Parola chiave l'utilizzatore dovrebbe adottare parole diverse per i diversi sistemi che usa. In particolare è buona norma che la Parola chiave di protezione all'accensione sia differente da quelle associate alle Credenziali di autenticazione ai sistemi di rete (vedi Paragrafo 2.4.3); questo impedisce che la compromissione della Parola chiave iniziale consenta anche il successivo accesso alla rete o al Personal computer stesso.

2.4.6.4. Sostituzione

La sostituzione della Parola chiave deve avvenire, come previsto dal Disciplinare Tecnico allegato al "Codice in materia di protezione dei dati personali (D.L. 196, dd. 30 giugno 2003)" ogni tre mesi. In ogni caso la sua sostituzione deve venir effettuata qualora risulti necessario, come nel caso di una sua rivelazione indesiderata o fortuita.

2.4.6.5. Cancellazione e Disattivazione

Le Credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate dagli Amministratori di sistema, salvo quelle autorizzate per soli scopi di gestione tecnica. Vengono ugualmente disattivate anche in caso del venir meno delle condizioni che consentono all'utilizzatore l'accesso ai dati personali.

Il Codice per l'identificazione non può venir assegnato ad altri incaricati, neppure in tempi diversi.

La cancellazione definitiva di una Credenziale viene effettuata qualora non venga più verificata la sussistenza delle condizioni per la sua conservazione. Ciò avviene periodicamente, e comunque a cadenza annuale, ed è a carico degli Amministratori di sistema.

2.5. Internet

2.5.1. Connessione alle rete Internet

È fatto divieto di:

- Connettersi autonomamente ad Internet con sistemi di dialup a numeri esterni al Consiglio regionale salvo autorizzazione del Segretario generale.
- Modificare le impostazioni o utilizzare browser diversi da quelli stabiliti.

2.5.2. Navigazione in rete Internet

L'utente deve utilizzare Internet in modo responsabile e secondo buona fede, al fine di garantire la sicurezza del sistema informatico del Consiglio regionale.

È fatto divieto di:

- Effettuare lo scarico gratuito o a pagamento di qualunque tipo di file, filmato, foto, che non sia inerente allo svolgimento delle mansioni affidate.
- Eseguire programmi scaricati da Internet o provenienti da altre fonti non sicure senza avere prima verificato che il programma sia privo di virus. Tutti i software scaricati attraverso la rete e i mezzi del Consiglio regionale devono essere controllati dall'antivirus prima di essere installati ed utilizzati.
- Effettuare ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili per scopi estranei allo svolgimento dell'attività lavorativa, salvo i casi direttamente autorizzati dal Segretario regionale e con il rispetto delle normali procedure di acquisto.
- Accedere a siti internet che abbiano un contenuto contrario a norme di legge ed a norme che tutelano l'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato.

- Effettuare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

- Disabilitare i sistemi adottati per bloccare l'accesso ad alcuni siti.

- Partecipare a forum non professionali, l'utilizzo di chat line (escluso gli strumenti autorizzati), di bacheche elettroniche e la registrazione in guestbook anche utilizzando pseudomini, con la sola esclusione di quelli espressamente autorizzati per iscritto.

- Gli utilizzatori sono invitati a limitare il rilascio di informazioni personali durante la navigazione via Web. L'utilizzatore è tenuto nel corso della navigazione a leggere con attenzione qualsiasi finestra, pop-up o avvertenza prima di proseguire nella navigazione e in particolare prima di accettare delle condizioni contrattuali o di aderire a delle iniziative online.

- Nel caso di comunicazione di dati sensibili o informazioni riservate via Web è necessario accertarsi che vi sia la protezione della comunicazione attraverso un opportuno protocollo di sicurezza. Ad esempio nel caso di Microsoft Explorer ciò può essere verificato controllando che nel bordo inferiore destro del browser appaia il disegno di un piccolo lucchetto chiuso di colore giallo.

2.6. Posta elettronica

La casella di posta, assegnata agli utilizzatori è uno strumento di lavoro e come tale può venir utilizzata, di norma, solo per scopi strettamente professionali e lavorativi.

Gli utilizzatori assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2.6.1. Norme d'uso della posta elettronica

Nella corrispondenza con altri utenti è bene:

- Scrivere i propri messaggi di posta elettronica in un formato congruente con il Programma di posta del destinatario, normalmente il formato di puro testo viene sempre accettato.

- Accertarsi che gli eventuali allegati dei propri messaggi non eccedano la dimensione massima prevista per il destinatario.

- Inviare allegati solo nei formati più usati: txt, rtf, doc, ppt, xls, pdf (possibilmente senza funzioni aggiuntive - macro), estensioni poco comuni potrebbe comportare la cancellazione del messaggio da parte del destinatario.

2.6.2. Divieti nell'utilizzo della posta elettronica

È fatto divieto di :

- Scaricare sul Personal Computer o sulle risorse condivise in rete messaggi di posta elettronica di caselle diverse da quelle assegnate all'utilizzatore.

- Accedere a caselle di posta personali attraverso la rete utilizzando apparecchiature del Consiglio regionale, ivi compreso l'inoltro automatico dei messaggi ricevuti all'indirizzo di posta assegnato verso indirizzi personali.

- Utilizzare le risorse informatiche per la comunicazione elettronica in modo anonimo o modificando la reale identità del mittente;

- Redigere messaggi di posta elettronica utilizzando l'indirizzo del Consiglio regionale, diretti sia a destinatari interni che esterni, in modo difforme dal modello predisposto dalla stessa.

- Creare, archiviare o spedire, anche solo all'interno della rete dell'Ente, messaggi pubblicitari o promozionali in nessun modo connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni,, mailing di massa di qualunque contenuto.

- Inviare messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità presunte.

Si ricorda che:

- Il messaggio di posta elettronica potrebbe essere ricevuto da destinatari diversi da quelli a cui era diretto, o potrebbe non essere recapitato o essere distrutto per problemi tecnici indipendenti dalla volontà del Consiglio regionale.

- Un messaggio di posta elettronica si configura, da un punto di vista giuridico, come corrispondenza aperta, potendo essere letto da chiunque durante il suo percorso sulla rete internet fino al destinatario. Nessuna aspettativa di tutela del proprio diritto alla privacy, relativa ai messaggi di posta elettronica in entrata ed in uscita utilizzando l'indirizzo del Consiglio regionale, potrà, dunque, fare capo all'utilizzatore, per tale motivo non deve essere usata per inviare documenti di lavoro "strettamente riservati".

2.6.3. Verifica sul contenuto dei messaggi

Gli utilizzatori assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Gli utilizzatori devono prestare attenzione:

- nell'invio di messaggi elettronici affinché non siano inserite inconsapevolmente delle informazioni dannose o pregiudizievoli per la sicurezza del Consiglio regionale. In particolare va usata la massima cautela nel rinvio a mezzo posta elettronica di pagine internet che per natura potrebbero contenere informazioni utili a risalire alla modalità di accesso utilizzata;

- a compilare correttamente i nomi dei file allegati alle email, controllandone accuratamente il contenuto.

- all'invio di documenti da considerarsi riservati;

- all'attendibilità dell'identità del mittente quando sia necessaria la certezza della stessa, in quanto è relativamente facile camuffare il mittente di una email. Si richiede pertanto, ogni qualvolta sia necessaria la certezza dell'identità del mittente, di verificarne l'identità con i mezzi appropriati;

- all'attendibilità della data ed ora esatta di invio di una email, in quanto è relativamente facile modificare questi dati.

Ogni utilizzatore ha a disposizione uno spazio limitato per il salvataggio e il mantenimento della propria casella di posta. Sua è la responsabilità di gestione dello spazio a disposizione. Nel caso sia raggiunto il limite di spazio, sarà bloccato l'invio della posta e mantenuta la ricezione della posta in ingresso finché non sarà liberato spazio nella casella.

2.6.4. Verifica sulle liste di destinatari

L'utilizzatore è invitato a prestare attenzione nell'utilizzo della funzione "Rispondi", "Rispondi a tutti" nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari. La stessa cautela è da applicare alla funzione "inoltra" e soprattutto nell'inviare allegati ad un elevato numero di persone.

Si consiglia di prestare attenzione nella selezione dei destinatari, se viene utilizzata l'opzione di completamento automatico dell'indirizzo.

L'utilizzatore deve prestare attenzione nell'organizzazione dell'agenda del proprio Programma di posta affinché non vi possano essere degli errori nella selezione dei destinatari dei messaggi.

L'utilizzatore è invitato a prestare la massima attenzione nell'utilizzo dei filtri con regole attive che consentono di inoltrare automaticamente determinati messaggi in arrivo ad altri destinatari.

Per l'invio di messaggi elettronici a molteplici destinatari, gli utenti sono tenuti a non utilizzare la funzione di invio per conoscenza nascosta ("bcc") che permette di occultare ai destinatari la lista degli altri destinatari del messaggio.

2.6.5. Riservatezza della posta elettronica

Si rammenta che la confidenzialità della posta elettronica è limitata in quanto i messaggi transitano nella rete pubblica di Internet e possono essere quindi visionati da terzi non autorizzati. Il livello di riservatezza di una email si avvicina di più a quello di una lettera aperta (cartolina), piuttosto che a quello di una lettera chiusa, a meno che non si sia utilizzato un sistema di cifratura.

L'invio di comunicazioni elettroniche con informazioni personali, si ricorda, è sottoposto alla disciplina prevista dal Decreto Legislativo 30 giugno 2003 n. 196 sul trattamento dei dati.

Si raccomandano gli utenti a prestare la massima attenzione nella stampa di messaggi di posta elettronica, soprattutto nel caso si utilizzino delle stampanti di gruppo o accessibili a più persone.

Si raccomanda di inserire la firma in calce all'email nonché, nei casi in cui non sia già inserita automaticamente, un'adeguata avvertenza sulla privacy e sulla riservatezza dei messaggi inviati, come nell'esempio successivo:

"Questo messaggio ed i suoi allegati è di carattere riservato ed è indirizzato esclusivamente al destinatario specificato. L'accesso, la divulgazione, la copia o la diffusione sono vietate a chiunque altro ai sensi delle normative vigenti, e possono costituire una violazione penale. In caso di errore nella ricezione, il ricevente è tenuto a cancellare immediatamente il messaggio, dandone conferma al mittente a mezzo email. "

"This message and its attachments (if any) may contain confidential, proprietary or legally privileged information and it is intended only for the use of the addressee named above. No confidentiality or privilegi is waived or lost by any mistransmission. If you are not the intended recipient of this message you are hereby notified that you must not use, disseminate, copy it in any form or take any action in reliance on it. If you have received this message in error, please, delete it (and any copies of it) and kindly inform the sender, of this email."

2.6.6. Come fare buon uso della posta elettronica

Si raccomanda di selezionare l'opzione attraverso cui i messaggi sono inviati immediatamente dal proprio Programma di posta. La funzione che permette di accodarli per un successivo invio può determinare casi di mancato o ritardato invio.

L'utilizzatore deve indicare con chiarezza nel campo oggetto l'argomento del messaggio. E' possibile richiedere una ricevuta di corretto ricevimento o lettura del proprio messaggio. A tale ricevuta va comunque assegnata un'importanza relativa poiché in taluni casi la conferma della ricezione avviene per la fase di consegna al mail server centrale e non per la consegna al destinatario finale del messaggio. La ricevuta di avvenuta lettura, ha comunque un'importanza relativa in quanto il destinatario può utilizzare la visione preventiva dei messaggi che ne permette la lettura senza l'inoltro della ricevuta.

L'utilizzatore deve periodicamente cancellare ed organizzare in opportune cartelle la posta già letta. Una quantità elevata di email nella cartella predefinita di arrivo della nuova posta può compromettere sensibilmente la stabilità del Programma di posta.

L'utilizzatore può fare uso degli appositi filtri per l'organizzazione delle email in arrivo, ed in particolare per ridurre le perdite di tempo associate all'arrivo di messaggi di posta non sollecitati.

Nel caso in cui ci sia l'arrivo sistematico di messaggi non sollecitati (spam-mail) da determinati indirizzi, l'utilizzare può segnalare il problema al Responsabile della sicurezza per richiederne l'eventuale filtraggio.

È permesso e consigliato l'uso della risposta automatica in caso di assenza e ferie.

2.7. Supporti rimovibili

Durante la normale attività produttiva ogni utilizzatore impiega supporti rimovibili di varia natura (magnetici, ottici, ecc.) per memorizzare e/o trasferire dati ed informazioni; tale utilizzo può comportare, anche inconsapevolmente,

problemi di sicurezza. Vengono pertanto indicate alcune prescrizioni per agevolare il buon uso dei supporti sopra citati.

Tutti i supporti rimovibili riutilizzabili (dischetti, cartucce, cd-rom, chiavi USB, ecc.) contenenti dati sensibili devono venir trattati con particolare cautela onde evitare che il loro contenuto possa venir recuperato, anche dopo la cancellazione dei dati in essi contenuti. Qualora non potessero venir recuperati dovranno venir distrutti.

I supporti magnetici contenenti dati sensibili devono venir custoditi in archivi chiusi a chiave.

Non è consentito scaricare file contenuti su supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

La consultazione di supporti magnetici, quando prevista, deve avvenire sempre e comunque da Personal computer dotati di antivirus aggiornato.

Supporti magnetici/ottici non più utilizzati devono venir cancellati e distrutti.

3. Disposizioni per il trattamento dei dati personali

3.1. Ciclo di vita dei dati personali

3.1.1. Elementi di sicurezza dei dati personali

Per proteggere le informazioni è necessario tutelarne tre qualità fondamentali: la riservatezza, l'integrità e la disponibilità.

3.1.2. I contenitori delle informazioni

Quando si parla di tutela delle informazioni vanno considerate quindi tutte le "forme" in cui esse si possono oggettivare.

Da questo punto di vista le informazioni possono trovarsi nelle seguenti tipologie di "contenitori":

- Cartaceo
- Informatico
- Verbale
- Altri supporti materiali (microfilm, prototipi e plastici, video, cassette, pellicole, informazioni riportate su lavagne o tabelloni, campioni di nuovi materiali, ecc.).

Per ciascun tipo di "contenitore" esistono specifiche modalità di interazione tra soggetto e informazione (lettura, scrittura, visione, ascolto, diffusione, ecc.) ed eventualmente sistemi di interazione specifici che consentano ad una pluralità di soggetti di trasmettere, ricevere, conservare, ecc. le informazioni.

Quando una stessa informazione risiede in più di un "contenitore", occorre proteggerla adottando contromisure adeguate alle diverse caratteristiche dei "contenitori" e del "sistema di interazione" utilizzato.

3.1.3. Le fasi del processo

Nel ciclo di vita dell'informazione, si possono individuare le seguenti fasi, non tutte necessariamente sempre presenti e talvolta non distinte nettamente tra loro:

Generazione	Acquisizione e/o produzione e/o elaborazione interna delle informazioni.
Classificazione	Definizione della criticità delle informazioni e attribuzione di una classe di rischio:

	• Dato Personale • Dato Sensibile • Dato Giudiziario • Dato Idoneo a rivelare lo stato di salute e la vita sessuale
Comunicazione	Trasmissione delle informazioni attraverso la diffusione, spedizione, pubblicazione, distribuzione.
Conservazione	Custodia ed archiviazione delle informazioni tra un momento di utilizzo e l'altro, in ogni fase del ciclo.
Cessione	Cessione di informazioni a terzi, su base volontaria o per obbligo contrattuale o legale, con rinuncia parziale o totale a diritti e privilegi su di esse.
Distruzione	Distruzione fisica o logica dell'informazione

3.2. Disposizioni specifiche

3.2.1. Generazione

- Non memorizzare sullo stesso supporto (cartaceo, cd-rom, dischi, cassette, ecc.) informazioni classificate diversamente. Nel caso in cui ciò risulti inevitabile, proteggere il supporto con le misure indicate per le informazioni di più alto livello di riservatezza in esso contenute.

- Le copie cartacee dei documenti o le riproduzioni di altri supporti fisici (ad es: audio/videocassette) devono essere predisposte da personale autorizzato al trattamento o da personale esterno nel cui contratto siano previste apposite clausole di riservatezza e/o accordi di non divulgazione.

- Quando l'elaborazione avviene su sistemi informatici in rete è necessario eliminare tutte le possibilità di accesso a cartelle condivise, seguendo le indicazioni disponibili.

3.2.2. Comunicazione

- Applicare il principio del "Conoscere solo ciò che è necessario", ovvero l'accesso ad un dato personale viene consentito solamente in presenza di una effettiva e comprovata necessità di utilizzo.

- Se vengono comunicate contemporaneamente (con lo stesso strumento o con la stessa modalità) informazioni con livelli di riservatezza diversi è necessario applicare le norme previste per il livello più alto (ad esempio nel caso si alleghino allo stesso testo email documenti con livelli di classificazione diversi).

- Se i destinatari della comunicazione delle informazioni non pubbliche sono esterni al Consiglio regionale è necessario assicurare l'adeguata tutela delle informazioni attraverso apposite clausole contrattuali o accordi di riservatezza concordati, caso per caso, con le funzioni amministrative competenti.

- Per la pubblicazione di dati personali su server in rete chiusa è necessario prevedere un'apposita area ad accesso limitato, con lista degli utilizzatori abilitati stabilita dal Responsabile del trattamento ed identificazione/autenticazione degli utilizzatori effettuata tramite Credenziale di autenticazione dotata di parola chiave. La lista deve contenere solamente utilizzatori nominati incaricati per quel trattamento.

- Se la rete è aperta (es. Intranet o Internet), valgono le stesse misure con l'aggiunta della verifica che gli utilizzatori abilitati siano stati formalmente incaricati del trattamento ai sensi della legge.

- Per l'invio di dati personali via e mail è necessario verificare che i destinatari siano stati formalmente incaricati del trattamento ai sensi del D.Lgs 196/2003.

- **Posta.**

    - E' utilizzabile liberamente sia il servizio interno che la Posta esterna (pubblica o privata). Se l'invio avviene tramite un servizio di consegna esterno e' richiesta l'attestazione della ricezione.

- **Protocollazione**

    - Tutti i dati personali in arrivo o in partenza devono essere protocollati.

- **Posta:**

    - E' utilizzabile liberamente sia il servizio interno che la Posta esterna (pubblica o privata).

    - Se l'invio avviene tramite un servizio di consegna esterno è richiesta l'attestazione della ricezione.

- **Fax**

    - Preavvertire il destinatario per evitare che i documenti rimangano incustoditi presso il fax di ricezione.

- **Intranet**

    - Prevedere un'apposita area ad accesso limitato, con lista degli utilizzatori abilitati stabilita dal proprietario dell'informazione ed identificazione/autenticazione degli utilizzatori effettuata tramite Credenziale di autenticazione e Parola chiave.

    - Attivare e controllare sistemi di logging degli accessi.

    - Memorizzare le informazioni sul server con le modalità previste al paragrafo "Strettamente Riservato" delle modalità di conservazione.

- **Internet**

    - Non è consentita la pubblicazione in Internet di dati personali senza il consenso dell'interessato.

- **Email (Intranet e Internet)**

    - Utilizzare strumenti di cifratura o firma digitale tramite certificati digitali.

    - Nel caso degli strumenti di cifratura (mediante l'utilizzo di programmi quali PkZip), non inoltrare la chiave di cifratura contestualmente ai dati personali.

3.2.3. Conservazione

- Conservare le informazioni negli archivi rispettando le misure previste per i diversi livelli di classificazione, i tempi di permanenza determinati dagli obblighi di legge, dal Titolare o dal Responsabile al trattamento e le correlate procedure in vigore.

- Assicurare l'adeguata conservazione delle informazioni riservate presso terzi esterni attraverso apposite clausole contrattuali o accordi di riservatezza concordati, caso per caso, con le funzioni interne competenti.

- Applicare, alla conservazione delle copie e ai duplicati di qualsiasi contenitore di informazioni, le stesse misure di sicurezza applicate agli originali.

- In caso di conservazione di documenti cartacei contenenti dati personali, selezionare l'accesso agli archivi attraverso un sistema di autorizzazione stabilito dal Responsabile dei relativi trattamenti.

- Utilizzare armadi, cassetti, ecc. chiusi a chiave, qualunque sia il contenitore dell'informazione (documento cartaceo, CD-ROM, DVD, videocassette, ecc.)

- In caso di conservazione su sistemi informatici:

    - Se si tratta di server web consiliari, configurare l'accesso ai dati come indicato al paragrafo 3.2.2 (Intranet).

- Se si tratta di server web esterni:

  - Richiedere esplicitamente al gestore l'utilizzo di strumenti software e hardware in grado di prevenire accessi illeciti e l'aggiornamento costante della configurazione attraverso la consultazione delle segnalazioni emesse dalla Funzione Sicurezza aziendale, nelle modalita' da convenire.

  - Proteggere i dati sul server con strumenti in grado di garantirne un adeguato livello di sicurezza.

- Se si tratta di Personal computer in rete è necessario eliminare tutte le possibilità di accesso a cartelle condivise. Abilitare all'accesso solo utilizzatori che siano stati formalmente incaricati del trattamento ai sensi del D.Lgs. 196/2003, fornendo loro Codice di Accesso Personale e Parola chiave.

- Le ditte esterne che si occupano della manutenzione dei PC (o parti di essi) che contengono informazioni esclusive devono avere sottoscritto contratti contenenti apposite clausole di riservatezza. Tali contratti dovranno prevedere, dove possibile, l'effettuazione delle operazioni presso i locali consiliari, senza l'asportazione di parti contenenti informazioni esclusive.

- In caso di trasporto fuori dalla sede di lavoro, custodire le informazioni in contenitori (borse, valigette portadocumenti, plichi, ecc.) idonei ad evitare perdite, acquisizioni indebite o manomissioni.

- Per archivi cartacei contenenti dati sensibili il Responsabile del trattamento deve prevedere un sistema di controllo degli accessi ai locali o ai singoli armadi o cassetti. In funzione dei casi specifici, del layout degli ambienti, della quantità dei dati ecc. tale sistema può essere manuale (es: registro cartaceo su cui riportare i dati relativi ai soggetti autorizzati e agli accessi) o elettronico. Il sistema prescelto deve consentire di selezionare e controllare gli accessi e registrarli fuori orario di lavoro. Se affidati agli incaricati autorizzati i documenti dovranno essere conservati, fino alla loro restituzione in contenitori muniti di serratura.

- Non è consentita la trasmissione di dati personali sensibili (D.Lgs 196/2003) via email o tramite Internet/Intranet (tranne nei casi esplicitamente autorizzati).

3.2.4. Cessione

- Può avvenire solo su autorizzazione del Titolare al trattamento per motivi istituzionali.

- Deve avvenire nel rispetto dei vincoli e degli obblighi imposti dal D.lgs. 196/2003.

3.2.5. Distruzione

- Va effettuata in caso risulti necessario o se scaduti i tempi di conservazione determinati dagli obblighi di legge.

- I supporti cartacei vanno resi non ricomponibili (se disponibile, utilizzare un tritadocumenti, oppure altre modalità di asporto e trattamento).

- I supporti rimovibili (dischetti, cd-rom, cartucce, ecc.) vanno cancellati e, dove tecnicamente possibile, cancellati in maniera definiva.

- Nei casi di dati sensibili o giudiziari, qualora non risultasse possibile la cancellazione definitiva dei supporti rimovibili, e' necessario provvedere alla distruzione degli stessi prima della dismissione.

4. Tutela della riservatezza dei dati dell'utilizzatore

4.1. Note sulla tutela della privacy dell'utilizzatore

Il Consiglio regionale garantisce la tutela della privacy di ogni Incaricato nell'ambito delle comunicazioni elettroniche effettuate utilizzando le risorse informatiche consiliari, provvedendo alle misure di sicurezza indicate nel D.Lgs. 196 del 30 giugno 2003.

Il Consiglio regionale si impegna a fornire agli Incaricati una informativa chiara e dettagliata sulle attività di monitoraggio del traffico di rete.

Il Consiglio regionale assicura una periodica informativa sulle modalità di utilizzo e fruizione delle risorse informatiche al fine limitarne l'uso scorretto e poco consapevole.

Il Responsabile della sicurezza verifica le prerogative degli Amministratori di sistema per quanto concerne il monitoraggio e l'accesso ai dati personali archiviati o comunicati attraverso il sistema informatico aziendale.

4.2. Accesso ai dati personali dell'utilizzatore senza assenso preventivo

Per dati utilizzatore vengono intesi:

- I dati utilizzatore presenti sulle risorse informatiche affidate (Personal Computer, dischetti, cd-rom, ecc.).
- La casella di Posta elettronica.

Vi può essere accesso, senza assenso preventivo, ai dati dell'utilizzatore in casi di estrema necessità quali:

- Situazioni di emergenza ove sia necessario tutelare la sicurezza del sistema informatico consiliare.
- Autorizzazione dell'Autorità Giudiziaria.
- Casi particolari di assenza dell'utilizzatore, quali dimissioni, ferie o malattia.

L'accesso senza assenso preventivo ai dati personali dell'utilizzatore può avvenire solamente nell'ambito di un protocollo ben definito che prevede:

- La richiesta da parte del referente gerarchico dell'utilizzatore.
- L'intervento diretto del Responsabile informatico (Responsabile della Posizione organizzativa "Nucleo informatico" o Responsabile della sicurezza), alla presenza del referente gerarchico dell'utilizzatore. Possono essere presenti i tecnici necessari a garantire l'accesso.
- Ogni partecipante prima, durante e successivamente all'atto ispettivo agli strumenti ed ai dati dell'utilizzatore dovrà garantire la riservatezza per tutto ciò che eventualmente potesse venir a conoscenza, nel rispetto e nella tutela dei diritti, delle libertà e della dignità dell'utilizzatore oggetto della verifica.

L'avvenuto accesso dovrà venir documentato dal Responsabile informatico:

- Mediante una relazione redatta sopra un apposito registro, in cui verranno evidenziati:
    - La data ed il luogo dell' ispezione.
    - Il dettaglio e gli strumenti oggetti dell'indagine.
    - I nominativi di tutti i presenti.
- Attraverso la comunicazione formale all'utilizzatore dell' evento occorso.

Successivamente all' ispezione il Responsabile informatico dovrà richiedere la disabilitazione delle Credenziali di autenticazione utilizzate all'Amministratore di sistema.

Il Responsabile informatico avrà inoltre il compito di essere garante della riservatezza e custode delle informazioni raccolte.

5. Evoluzione e supporto

5.1. Supporto tecnico

La struttura del Consiglio regionale, interessata nell'applicazione e nell'aggiornamento del presente documento, è la Posizione organizzativa "Nucleo informatico" della Segreteria generale, che coordina le azioni ed i comportamenti delle ditte esterne di manutenzione tecnica, si pone come interfaccia nei confronti delle esigenze del Consiglio regionale, offre le proprie competenze per migliorare ed implementare le misure idonee di sicurezza, interviene nel risolvere problemi contingenti legati a malfunzionamenti.

Il "Nucleo informatico" è quindi la struttura verso la quale convogliare gli interrogativi legati all'applicazione delle norme contenute nel presente documento.

Una breve nota merita anche l'eventuale apporto di Ditte esterne di manutenzione, per le quali le norme successive, devono venir applicate con estrema diligenza.

Le regole che qui vengono dettate sono circoscritte alla modalità di colloquio con i servizi tecnici di assistenza. Per ogni eventuale quesito e' necessario fare riferimento al Responsabile della Sicurezza.

Si raccomanda ad ogni utilizzatore di:

- Evitare nel modo più assoluto di comunicare per via e-mail, vocale o di altro tipo, informazioni riservate o Parole Chiave ai tecnici del supporto tecnico.

- Disattenzioni a queste indicazioni dovranno venir comunicare al Responsabile della Sicurezza, se di rilevanza consiliare, oppure agli Amministratori di sistema, se relative alla divulgazione della Parola chiave.

- Utilizzare per ogni richiesta di intervento tecnico, come malfunzionamenti, installazioni, Credenziali di accesso o Parole Chiave, lo strumento di comunicazione in Intranet previsto dal Sistema Informativo consiliare.

6. Allegati

6.1. Verifica dell' efficienza dell' Antivirus

Un Personal computer e' protetto dall' antivirus quando sulla barra in basso a destra appare una icona blu, come quella presente nella figura accanto.

L'icona standard può assumere una raffigurazione differente a seconda di determinate situazioni; come nell'esempio successivo:

ICONA	***Descrizione del Funzionamento***
	L'antivirus funziona normalmente
	Il file di riconoscimento dei virus e' obsoleto
	Il Personal computer e' scollegato dal server. Se l'immagine persiste l'antivirus non verra' aggiornato
	L'antivirus sta effettuando una scansione dei file presenti sul Personal Computer
	La scansione periodica e' stata disabilitata
	L'antivirus e' stato disabilitato

In determinate situazioni possono comparire altre Icone frutto di una combinazione grafica delle precedenti.

ATTENZIONE: Nei casi in cui non appare alcuna icona, oppure l'icona persiste ad apparire diversa da quella indicata per il funzionamento normale e' necessario interpellare il Nucleo informatico per la risoluzione del problema.

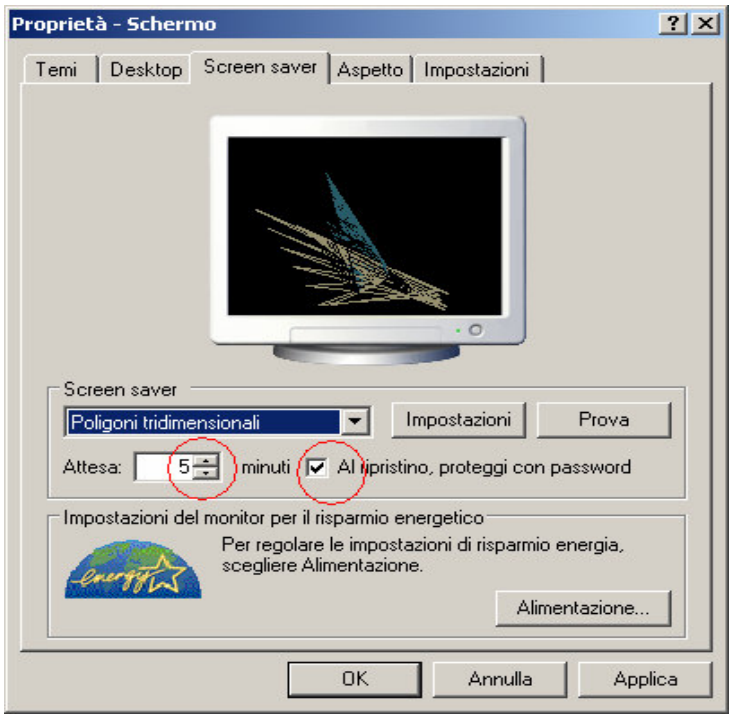
6.2. Configurazione del Salvaschermo

La funzionalità del salvaschermo e' attivabile seguendo la seguente sequenza:

1. Cliccare sul simbolo "Pulisci lo schermo" posto accanto al tasto "Start", come da figura. Se il tasto non e' presente chiudere o minimizzare tutte le applicazioni aperte in modo da liberare lo schermo.

2. Portare il puntatore del mouse sullo schermo vuoto e cliccare con il tasto Dx. apparirà una finestra denominata **Proprieta'-Schermo.**

3. Cliccare sulla cartella **Screen saver**. Selezionare il salvaschermo prescelto fra quelli proposti (l'immagine accanto ne suggerisce uno a titolo esemplificativo), poi regolare un tempo di **attesa** di 5 minuti e selezionare la casella **Al ripristino proteggi con password**. Poi cliccare sul tasto **OK.** Seguire l'esempio illustrato nella figura.



In caso di dubbi e' sempre possibile contattare il "Nucleo informatico" che provvederà a fornire le necessarie delucidazioni.