Uso sistemi e servizi informatici

Codice di comportamento per l'utilizzazione di sistemi e servizi informatici

Redatto da:

Carlo Cammelli – Dirigente del settore Tecnologie informatiche

0. INFORMAZIONI SUL DOCUMENTO

0.1. SCOPO DEL DOCUMENTO

Il presente documento ha la finalità di descrivere un codice di comportamento nell'uso degli strumenti informatici e servizi di rete.

0.2. SOMMARIO MODIFICHE

VERSIONE	DATA	DESCRIZIONE
1.0	10/07/2006	Emissione iniziale assieme a carta servizi
1.1	02/05/2007	Aggiornamento e revisione parti
1.2	31/03/2009	Aggiornamento e revisione parti

0.3. LISTA DISTRIBUZIONE

Inserimento in intranet consiglieri, dipendenti ed altri soggetti autorizzati all'uso di strumenti informatici

0.4. RIFERIMENTI

DLGS 196/2003	ALLEGATO B
DPS	CONSIGLIO REGIONALE DELLA TOSCANA

0.5. ACRONIMI

PM	Responsabile di Progetto
RNC	Rapporto di Non Conformità
ICT	Information and communication technology

0.6. Bibliografia

CNIPA	Manuale dei livelli di servizio nel settore ICT

1. DISPOSIZIONI DI CARATTERE GENERALE

Le disposizioni del presente codice operano nei confronti del presidente, dei consiglieri, del personale in forza presso i gruppi politici e dei dipendenti,
I consiglieri e il personale del Consiglio regionale della Toscana rispetteranno e faranno rispettare le norme ed i principi contenuti nel presente codice per l'intera durata del mandato o del rapporto di lavoro.
Il testo del presente codice è messo a disposizione anche in intranet ed è destinato ai consiglieri, ai dipendenti del Consiglio regionale della Toscana, agli altri soggetti autorizzati all'uso di strumenti informatici all'interno del Consiglio regionale.

2. ACCESSI ALLA RETE DEL CONSIGLIO REGIONALE

L' accesso alla rete e ai relativi servizi di rete del Consiglio regionale della Toscana può avvenire solamente mediante autenticazione del soggetto stesso che quindi appartiene agli utenti regolarmente registrati che hanno tale facoltà. L'autorizzazione per gli accessi viene sempre richiesta al responsabile della rete consiliare che provvede a registrare tale accesso fornendo le prime credenziali di autenticazione.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato (es. smart card), eventualmente associato ad un codice identificativo o a una parola chiave.

2.1. MISURE DI SICUREZZA PER GLI ACCESSI:

Le misure di sicurezza hanno efficacia se si matura un comportamento collaborativo che viene suggerito dalle indicazioni qui di seguito riportate:

a. la riservatezza della password è responsabilità dell'utente che ne è proprietario;
b. la password dovrà essere composta da almeno 8 caratteri;
c. la password fornita al primo accesso in rete deve essere modificata dall'utente al primo utilizzo e, successivamente, almeno ogni 3 mesi; la password è comunque modificabile dall'utente in qualsiasi momento (operazione periodicamente consigliata);
d. la password deve essere diversa dalle ultime 2 utilizzate e non deve contenere riferimenti agevolmente riconducibili all'utente;
e. i codici identificativi e/o le password non vanno per alcun motivo comunicati a terzi, nemmeno agli amministratori del sistema;
f. non è consentito trascrivere le password su supporti agevolmente accessibili da parte di terzi (post-it o altro sullo schermo o sulla scrivania);
g. le credenziali non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
h. le credenziali sono disattivate anche in caso di perdita dell'abilitazione che consente all'incaricato l'accesso ai dati personali;
i. il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi;
j. l'utente è tenuto a rendere inaccessibile la propria postazione di lavoro ogni volta che si assenta, utilizzando la funzione di blocco del sistema (che viene attivata premendo contemporaneamente i tasti Ctrl/Alt/Canc e cliccando sul bottone "blocca computer");

2.2. ACCESSO AI DATI IN ASSENZA DELL'INCARICATO

Qualora, in caso di assenza dell'incaricato assegnatario della dotazione informatica, si renda necessario, per ragioni improrogabili, l'utilizzo di dati accessibili in via esclusiva con i suoi codici di accesso è necessario rispettare le seguenti regole:

a. deve sussistere un'indispensabile ed indifferibile necessità di intervenire per esclusive necessità di operatività e di sicurezza del sistema;
b. il dirigente/responsabile del trattamento richiede alla persona del settore competente delegata alla custodia delle password le specifiche credenziali di accesso, in caso di mancanza di tale persona si può ottenere l'azzeramento delle password dal settore tecnologie per la sola parte relativa a utente e password di rete, non è possibile agire su specifiche applicazioni che non utilizzano l'autenticazione integrata mediante active directory;
c. ad accesso effettuato il dirigente/responsabile deve comunicare l'intervento effettuato al dipendente assente.

2.3. RIPRISTINO DELLA PASSWORD

Nel caso di perdita/dimenticanza della password da parte dell'utente, su richiesta dello stesso utente, l'amministratore di sistema deve impostare una nuova parola chiave e comunicarla all'utente che sarà obbligato dal sistema a definirne una nuova al primo utilizzo.
Per il ripristino della parola chiave di utenti interni del Consiglio regionale si segue la seguente procedura:

a. l'utente comunica la necessità di ridefinire la password al settore tecnologie via Intranet con la gestione richieste;
b. gli incaricati del settore tecnologie provvederanno ad assegnare una password temporanea che scade al primo accesso fatto dal diretto interessato che deve quindi cambiarla con una nuova;
c. Questa procedura va seguita anche qualora, a seguito del blocco dell'accesso per mancato utilizzo delle credenziali per più di 6 mesi, sia necessario richiederne lo sblocco.

2.4. AUTENTICAZIONE FALLITA (BLOCCO/SBLOCCO)

Dopo otto tentativi falliti di autenticazione, l'utente (o meglio il suo codice di identificazione) viene bloccato. In tal caso l'amministratore del sistema provvede allo sblocco a seguito di richiesta, anche telefonica, da parte dell'utente.
Nota bene: nell'ipotesi di sblocco la password non viene modificata dall'amministratore di sistema ma si attiva il solo sblocco.

3. PROTEZIONE DELLE POSTAZIONI DA ACCESSO FISICO NON AUTORIZZATO

Per accesso fisico s'intende l'accesso ai locali in cui vi sono uno o più postazioni di lavoro. Per evitare il rischio derivante da accesso fisico da parte di persone non autorizzate sono adottate le seguenti misure di sicurezza:

personale di struttura	le postazioni di lavoro sono accessibili solo da quanti ne hanno titolo, in qualità di responsabili o incaricati del trattamento, di amministratori del sistema, o altro, nei soli limiti in cui ciò sia funzionale allo svolgimento dei compiti o per lo svolgimento di attività di manutenzione, di pulizia, trasporto e facchinaggio.

personale esterno alla struttura	La persona esterna può accedere ai locali solo quando è presente qualche addetto; l'accesso fisico ai luoghi di lavoro è protetto tramite la presenza di personale di portineria ovvero tramite il presidio delle vie di accesso e registrazione dei relativi accessi autorizzati.
protezione dei portatili da accesso fisico non autorizzato	Il personale che ha in consegna un PC portatile è tenuto a evitare di lasciare incustodito il portatile per evitare il rischio di furto, custodire i portatili in luoghi o armadi protetti da serrature.

4. INTERVENTI DI ASSISTENZA E MANUTENZIONE

Assistenza in remoto.

Gli interventi di assistenza, installazione e aggiornamento dei software e, in generale, quelli volti a fronteggiare guasti nel funzionamento delle postazioni di lavoro, qualora possibile, sono di norma effettuati dagli amministratori del sistema tramite il servizio di assistenza e amministrazione remota dei PC, senza la necessità dell'intervento di un tecnico informatico presso la postazione di lavoro.
Il sistema di assistenza in remoto consente, previa autorizzazione del dipendente/utente, di condividere a distanza con l'operatore del supporto tecnico l'utilizzo di tastiera, mouse e schermo, senza che l'utente stesso perda il controllo di quanto avviene al proprio PC e ai dati eventualmente accessibili attraverso lo stesso.

Assistenza con intervento locale del tecnico

Se invece sono necessari interventi di manutenzione sulla macchina o di assistenza, adeguamento, ecc. presso la postazione di lavoro, è necessario che l'utente o, in sua assenza, altro dipendente della struttura, assista alle operazioni di manutenzione. Salvo autorizzazione, non possono essere asportate stampe o copie di archivi.
Gli interventi effettuati dai tecnici sono registrati nella intranet "richiesta di assistenza informatica". Ad ogni intervento viene assegnato un numero (codice) attraverso il quale richiamare le informazioni disponibili sullo stato di avanzamento o conclusione dello stesso.

5. PROTEZIONE DEI SUPPORTI RIMOVIBILI DI MEMORIZZAZIONE DA ACCESSI NON AUTORIZZATI

Ai sensi del punto 21 del Disciplinare tecnico allegato B in materia di misure minime di sicurezza, i supporti rimovibili (floppy disk, cd, dvd, memoria USB, etc.) utilizzati per la memorizzazione di dati personali sensibili o giudiziari devono essere conservati in modo tale da garantire la protezione da accessi non autorizzati e trattamenti non consentiti (armadi o cassetti chiusi a chiave).
Resta fermo l'obbligo per l'incaricato e il responsabile di verificare che gli elementi di arredo siano sempre chiusi.
Se non c'è immediata disponibilità di arredi muniti di serratura per l'archiviazione dei supporti contenenti dati personali sensibili, gli stessi devono in ogni caso essere ubicati in appositi locali chiusi a chiave.
Il personale diverso dagli incaricati del trattamento che accede a questi locali deve essere accompagnato da uno dei soggetti incaricati del trattamento che deve verificare che non vi sia un accesso ai dati sensibili contenuti sui supporti.

5.1. REIMPIEGO DEI SUPPORTI DI MEMORIZZAZIONE

Ai sensi del punto 22 del Disciplinare tecnico in materia di misure minime di sicurezza allegato al codice, i supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
Si riportano di seguito indicazioni operative da seguire relative ad alcuni supporti, nel caso in cui gli stessi siano consegnati a terzi:

a. floppy disk e cd-rom riscrivibili: prima di essere consegnati ai terzi, devono essere sottoposti ad una operazione di cancellazione delle informazioni precedentemente contenute con l'apposito comando di formattazione completa del supporto;
b. hard disk: prima di essere consegnato ai terzi, deve essere sottoposto ad una operazione di cancellazione delle informazioni precedentemente contenute con il comando FDISK (che rimuove la partizione) con una successiva formattazione;
c. nel caso in cui, a seguito di intervento tecnico, si presenti la necessità di sostituire l'hard disk, è necessario procedere al recupero dei dati contenuti nello stesso, ove possibile e opportuno; dopo aver effettuato tale operazione si potrà procedere alla cancellazione dei dati dall'hard disk sostituito; si ricorda che l'hard disk potrebbe costituire un mezzo di esportazione illegittima di dati personali qualora gli stessi fossero recuperati da personale non autorizzato; i fornitori dei servizi di manutenzione sono comunque impegnati per contratto al rispetto della normativa sulla protezione dei dati personali;
d. nel caso in cui i supporti rimovibili contenenti dati personali sensibili o giudiziari non siano destinati al riutilizzo, essi devono essere fisicamente distrutti mediante rottura.

6. PROTEZIONE DA MALINTENZIONATI

Ogni computer collegato in rete può essere oggetto di tentativi di connessione effettuati da soggetti che utilizzano altri computer collegati alla rete.
Per fare fronte a questo rischio i posti di lavoro consentono l'accesso tramite la rete solo agli amministratori del sistema.
Quando il computer è collegato a Internet le intrusioni possono teoricamente essere effettuate da computer connessi a Internet situati in un qualsiasi punto della rete mondiale.
La gestione della sicurezza rispetto a possibili intrusioni esterne viene garantita da un sistema di Firewall (gestito internamente) che controlla sia il traffico in ingresso che in uscita attraverso strategie definite di autorizzazioni che impediscono intrusioni dall'esterno.
Per motivi di sicurezza, l'amministratore del sistema provvede a mantenere temporaneamente il log di tutti gli accessi in entrata/uscita al firewall ed inoltre:

a. non vanno accettati collegamenti alla rete da parte di PC di terzi.
b. per i PC portatili per cui non è prevista la possibilità di collegarsi alla rete, è vietata la connessione fisica alla rete locale del Consiglio.
c. i PC portatili, quando collegati a rete diversa da quella del Consiglio regionale o connessi a Internet via modem ad un provider, non usufruiscono della protezione effettuata tramite firewall gestito dal Consiglio.

7. PROTEZIONE DAI VIRUS

I virus sono particolari programmi predisposti per essere eseguiti all'insaputa dell'utente. Possono causare danni ai dati memorizzati sul computer o al sistema operativo del computer stesso, violando potenzialmente la riservatezza dei dati. Su tutti i server sono installati programmi e applicazioni antivirus con aggiornamento automatico, minimo giornaliero, via Internet che garantisce una protezione idonea ad evitare il verificarsi di danni ai dati causati dai virus informatici. I PC connessi in rete sono protetti da un prodotto antivirus installato sulle singole postazioni e connesso al sistema server, con aggiornamento automatico, almeno giornaliero.
Sui PC stand alone (tra cui i portatili per cui non è prevista la possibilità di connessione alla rete es. aula consiliare) viene invece installato un prodotto antivirus che, per risultare efficace nel tempo, deve essere aggiornato periodicamente secondo le modalità richieste dal prodotto stesso. L'aggiornamento è a carico del settore tecnologie e può essere garantito solo se il sistema si connette regolarmente alla rete consiliare.

8. DESCRIZIONE DELLA CONFIGURAZIONE STANDARD DELLE UNITÀ LOGICHE DI MEMORIZZAZIONE

Le unità logiche a disposizione dell'utente ai fini della memorizzazione dei dati, in base alle configurazioni standard delle postazione di lavoro, sono le seguenti:

Unità locali del computer

C: = Unità logiche/disco installato fisicamente sul PC, altrimenti detti dischi fissi o locali.
Questa unità è esclusa dalla garanzia del salvataggio dei dati. Da ciò derivano rischi per la sicurezza dei dati e la loro conservazione, se non vi è un accorto utilizzo del computer e un salvataggio coscienzioso dei dati da parte dell'utente. Ai sensi dell'articolo 18 dell'Allegato B del d.lgs 196/2003 il salvataggio dei dati deve essere effettuato con cadenza almeno settimanale. L'utente deve evitare di conservare i dati di cui va garantita la sicurezza su queste unità.

Unità di rete comune delle singole strutture

Unità logica con lettera oltre D:\ = Unità logica/Disco dati degli utenti di una singola struttura. Unità garantita dal **salvataggio automatico dei dati** (backup notturno). Per le articolazioni organizzative del Consiglio, che ne hanno fatto richiesta, è stata creata una unità logica/disco accessibile in lettura/scrittura da tutti gli utenti assegnati alla struttura medesima. Questa Unità logica/Disco, accessibile per default da tutti gli utenti della struttura autorizzati**, consente una personalizzazione dei diritti di accesso**. Questa personalizzazione viene richiesta dal responsabile/dirigente per definire a carico dell'Informatica le abilitazioni opportune.

8.1. MISURE DI SICUREZZA INFORMATICHE RELATIVE ALL'ARCHIVIAZIONE DEI DATI

In base alla configurazione appena descritta risultano adottate le seguenti misure:

a. per la memorizzazione dei dati aventi caratteristiche e contenuti dichiarati sensibili va privilegiato l'utilizzo delle risorse di rete evitando l'uso delle unità logiche presenti fisicamente sul PC (dischi fissi/locali C); le l'unità logiche di rete sono infatti garantite da un salvataggio dei dati (backup). Contrariamente, quanto memorizzato sui dischi locali della propria postazione di lavoro (unità C) deve essere salvato su floppy disk o cd o memoria USB, a cura dell'utente, con cadenza almeno settimanale;
b. per la memorizzazione dei dati inerenti la propria funzione lavorativa, va data priorità all'utilizzo di cartelle del disco su rete (opportunamente abilitate); questo per agevolare l'accesso ai dati in assenza dell'incaricato, almeno da parte del responsabile del trattamento;

c. anche se alcuni programmi applicativi consentono la protezione dei singoli file mediante l'apposizione di specifiche password, tale pratica va evitata. La password sul file come misura di sicurezza non è adeguata e può essere controproducente. Infatti tali password possono essere perse o dimenticate, rendendo molto difficile il recupero dei dati.

8.2. CONDIVISIONE DELLE RISORSE IN RETE

Il responsabile/dirigente verifica che la configurazione e l'utilizzo spazio disco sul server di rete e messo a disposizione della propria struttura sia funzionale alle esigenze di riservatezza dei dati stessi. Tale verifica deve essere compiuta almeno una volta all'anno (ai sensi dell'art. 15 del Disciplinare tecnico).
In particolare il responsabile/dirigente dispone l'accesso differenziato a tali risorse, in base ad abilitazioni personali o per gruppi di lavoro, definite in relazione ai compiti svolti dal personale, comunicando all'amministratore del sistema le opportune abilitazioni da attivare. Il responsabile della struttura deve segnalare la variazione delle singole abilitazioni personali o della composizione dei gruppi, non appena queste si verifichino, all'amministratore di sistema per l'adeguamento delle autorizzazioni.
Per agevolare l'operatività delle persone, eventuali modifiche e/o integrazioni potranno essere comunicate attraverso il sistema di gestione richieste via Intranet dal dirigente/responsabile del trattamento al settore tecnologie.

9. RACCOMANDAZIONI

E' opportuno usare cautela con la posta elettronica in arrivo verificando, prima della sua apertura, la provenienza del messaggio. Per la posta elettronica valgono le indicazioni sulle modalità d'uso già riportate nella circolare del Segretario generale 26 maggio 2009 prot. n. 6907/6.6.4.
Anche il regolare spegnimento del personal computer al termine dell'utilizzo contribuisce a preservare il regolare funzionamento dello stesso e l'integrità dei dati.