Manuale per la sicurezza ed il corretto trattamento dei dati personali nel Consiglio Nazionale delle Ricerche

(D.lgs. 196/2003)

SOMMARIO

PREMESSA

Dal 1° gennaio 2004 è entrato in vigore il Decreto Legislativo 30 giugno 2003 n. 196, noto come Codice in materia di protezione dei dati personali.

Il nuovo codice riunisce in un solo corpus normativo la grande varietà di provvedimenti in materia stratificatisi nel tempo a livello nazionale e comunitario, provvedendo alla loro razionalizzazione e sistematizzazione e migliorando così di molto la fruibilità degli stessi da parte dell'interprete.

Il medesimo inoltre semplifica e snellisce gli adempimenti in precedenza previsti (eliminando molte incombenze a caratteristica prettamente formale) a carico dei titolari del trattamento di dati personali rendendo al tempo stesso tuttavia più stringenti e cogenti i comportamenti e gli obblighi rimasti, al fine di assicurare che la circolazione dei dati e delle informazioni relative alle persone, fisiche e giuridiche, oramai ineliminabile nella odierna società dell'informazione, avvenga nel massimo rispetto dei diritti e delle libertà fondamentali, quali soprattutto il diritto alla riservatezza ed alla identità personale.

E' necessario pertanto che ogni operatore sviluppi sempre più una consapevole cultura circa la "preziosità" e "delicatezza" delle informazioni che quotidianamente è chiamato a trattare e conservare, e che si adoperi affinché vengano compiutamente rispettate, nel suo settore di attività, tutte le misure di sicurezza previste a protezione dei dati stessi, anche per evitare di incorrere nelle pesanti sanzioni, a volte anche di carattere penale, previste dal legislatore a tutela della disciplina di riferimento.

OBBLIGHI DI SICUREZZA

Il diritto alla protezione dei dati personali mira a garantire che il trattamento delle informazioni si svolga "nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali" (art. 1 TU).

Il principio guida dell'azione amministrativa in questo settore è rappresentato pertanto dal "principio di necessità del trattamento", il quale, assieme ai correlati principi di "pertinenza e non eccedenza" , rappresenta un presupposto di liceità del trattamento medesimo.

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

Nell'ambito del predetto obbligo generale di contenere nella misura più ampia possibile determinai rischi, i titolari del trattamento sono tenuti in ogni caso ad assicurare un livello minimo di protezione dei dati mediante l'adozione delle "misure minime di sicurezza" individuate nel Titolo V, Capi I e II del Codice.

SCOPO DEL MANUALE

Nell'ottica di un efficace tutela delle informazioni e dei dati personali gestiti dal CNR, il presente Manuale per la Sicurezza ha lo scopo di fornire le prescrizioni e le istruzioni di massima circa il complesso delle misure organizzative, logistiche, tecniche, ed informatiche da adottare in tutte le strutture, affinché il livello di protezione dei dati personali oggetto di trattamento sia il più possibile conforme a quanto previsto, nel quadro dei più generali obblighi di sicurezza, dal Codice in materia di protezione dei dati personali, e sia tale in ogni caso da garantire il livello minimo di sicurezza previsto dal legislatore.

DEFINIZIONI NORMATIVE

Ai sensi di quanto previsto dal Codice si intende per:

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

dati personali: qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

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

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

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

diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

TRATTAMENTO DI DATI PERSONALI DA PARTE DELLE PUBBLICHE AMMINISTRAZIONI

Alle **Pubbliche Amministrazioni** è consentito:

a) **il trattamento di dati comuni** (diversi da quelli sensibili e giudiziari) se necessario per il perseguimento dei fini istituzionali.

Salvo quanto previsto per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici (parte II del Codice), le PA non devono pertanto acquisire il consenso dell'interessato.

E' tuttavia necessario fornire agli interessati una adeguata **informativa,** in cui si specifichino finalità e modalità del trattamento dei dati, l'eventuale obbligatorietà del loro conferimento, le conseguenze relative la rifiuto di fornire i dati, i diritti esercitabili dall'interessato, nonché i dati identificativi del titolare e del responsabile.

b) **il trattamento dei dati sensibili e giudiziari** se autorizzato da espressa disposizione di legge nella quale si specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

Nei casi in cui una disposizione di legge specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, le amministrazioni sono tenute ad adottare un apposito regolamento con il quale identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili, in relazione ai fini istituzionali perseguiti e nel rispetto dei principi affermati dal Codice.

In ogni caso, il trattamento dei dati sensibili e giudiziari da parte delle Pubbliche Amministrazioni è retto dal principio di indispensabilità, ossia possono essere trattati soltanto i dati sensibili e giudiziari indispensabili allo svolgimento di funzioni istituzionali che non potrebbero essere adempiute altrimenti (mediante il ricorso a dati anonimi o personali di diversa natura).

c) **la comunicazione di dati personali**

- a privati o enti pubblici economici soltanto se prevista da una norma di legge o di regolamento
- ad altri soggetti pubblici se prevista da una norma di legge o di regolamento ovvero, in mancanza, se necessaria per il perseguimento dei fini istituzionali previa apposita comunicazione al Garante per la protezione dei dati personali.

Non è in ogni caso consentita la diffusione dei dati idonei a rilevare lo stato di salute.

PROFILI ORGANIZZATIVI

TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

A termini di normativa è titolare del trattamento dei dati personali il soggetto (fisico o giuridico) cui competono, nell'ambito del trattamento medesimo, le decisioni in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

L'art. 28 del Codice precisa inoltre che, nel caso di trattamento effettuato da una pubblica amministrazione, titolare del trattamento è l'entità nel suo complesso.

Pertanto **titolare del trattamento dei dati effettuato nell'ambito di questo Consiglio è il CNR, nella persona del suo legale rappresentante pro tempore, il Presidente**.

RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI E RELATIVI COMPITI

Sono responsabili del trattamento, ai sensi di quanto disposto dal vigente Regolamento di organizzazione e funzionamento del Consiglio Nazionale delle Ricerche i , **i responsabili pro-tempore delle strutture amministrative, scientifiche e di servizio in cui si articola il CNR, con riferimento ai dati trattati nell'ambito delle Unità Organizzative (comunque denominate) alla cui direzione gli stessi sono preposti.**

Le Unità organizzative di riferimento sono:

- per l'Amministrazione centrale: Uffici delle Direzioni Centrali ed altre eventuali Unità Organizzative specificatamente individuate in quanto non incardinate negli Uffici;
- i Dipartimenti;
- gli Istituti
- le Aree della Ricerca

La nomina a responsabile è effettuata, in sede di prima applicazione della normativa di riferimento, con apposito provvedimento.

A regime, la nomina a responsabile del trattamento dei dati personali sarà contestuale al decreto (o altro provvedimento) di nomina alla direzione della struttura.

L'ambito di responsabilità si estende al trattamento dei dati effettuati, sia con l'ausilio di strumenti elettronici che in maniera cartacea, nell'ambito dell'Unità Organizzativa alla cui direzione il soggetto è preposto, e si riferisce alle tipologie di dati e di trattamenti indicati dal responsabile medesimo nell'apposita scheda di rilevazione fornita, in sede di prima applicazione, in risposta alla circolare pos. 6.9 prot. 0032307 del 16 Giugno 2005, e, successivamente indicati nella costituenda anagrafe elettronica dei trattamenti.

Il CNR si riserva di effettuare, comunque, ulteriori nomine di responsabili, laddove si rendesse necessario, per lo svolgimento di attività istituzionali, delegare a soggetti terzi esterni al CNR il trattamento di alcuni dati.

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare e contenute nel presente Manuale (e nei successivi aggiornamenti).

Sono compiti del responsabile del trattamento:

- assicurarsi che nell'Unità Organizzativa vengano rispettate le misure minime di sicurezza previste dalla normativa vigente, nonché le altre misure di sicurezza previste dal CNR e riassunte nel presente Manuale.
  Per l'attuazione delle misure di sicurezza in ciascuna unità organizzativa è assicurato il supporto per quanto riguarda il trattamento dei dati, dell'Ufficio Sistemi Informativi, e per quanto riguarda le misure di sicurezza della rete dell'Ufficio Reti e Telecomunicazioni.
  E' possibile contattare i soggetti di riferimento indicati alla pagina web www.cnr.it
  Per il supporto circa l'adozione di misure di sicurezza che non rivestano carattere informatico è possibile contattare l'Ufficio IV della Direzione Generale.

- procedere all'aggiornamento dell'"anagrafe elettronica dei trattamenti dei dati personali" ogni qualvolta si verifichi l'esistenza di un nuovo trattamento, la cessazione di uno precedente, la modifica delle caratteristiche di un trattamento, ovvero il nuovo ingresso, la cessazione o il cambiamento di mansioni di uno degli incaricati.
  L'aggiornamento dell'anagrafe, nella parte relativa ai soggetti incaricati, assolve gli obblighi previsti dalla normativa relativamente all'individuazione scritta del personale incaricato che afferisce (personale tecnico-amministrativo o ricercatore) o risulta assegnato (personale a contratto) alla struttura.
  Qualora il responsabile, nello svolgimento delle sue funzioni istituzionali, ritenga necessario autorizzare soggetti diversi dai precedenti al trattamento dei dati personali inerenti la sua struttura, dovrà provvedere a designare individualmente per iscritto i medesimi(Allegato A).

- comunicare al competente Ufficio dell'Amministrazione Centrale l'eventuale "esternalizzazione" (affidamento all'esterno) di trattamenti di dati personali al fine della predisposizione della nomina a responsabili di tali soggetti.
- comunicare al competente Ufficio dell'Amministrazione Centrale ogni comunicazione di dati personali ad altri soggetti pubblici, effettuata in qualsiasi modo anche tramite convenzione, non prevista da norme di legge o di regolamento ai fini delle necessarie comunicazioni in merito al Garante

- procedere alla richiesta di rilascio e revoca delle autorizzazioni all'accesso a banche dati elettroniche automatizzate.
  Per le banche dati dell'Amministrazione centrale è necessario provvedere ad inoltrare la richiesta al competente Ufficio, il quale poi inoltrerà la stessa al competente personale informatico.

- impartire istruzioni agli incaricati circa il corretto trattamento dei dati personali, dando idonea divulgazione presso gli stessi del presente Manuale per la sicurezza, con particolare riferimento all'appendice relativa alle istruzioni operative per gli incaricati.

- dare idonea diffusione presso i soggetti impegnati in attività di ricerca del "Codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici", affinché le attività medesime siano svolte nel rispetto dei principi e con l'osservanza dei criteri ivi indicati.

- fornire, al momento dell'acquisizione dei dati, per il tramite degli incaricati, ovvero mediante affissione nei locali aperti al pubblico o ancora mediante l'inserimento in moduli o formulari, l'informativa di cui all'art. 13 del Codice agli interessati (Allegato B).

  Il modello di informativa allegato contiene le informazioni generali ed essenziali valide per tutti i trattamenti effettuati all'interno del CNR.

Il suddetto dovrà pertanto essere opportunamente integrato qualora la specificità dei trattamenti effettuati nella singola struttura renda necessarie ulteriori precisazioni.

- evadere, le eventuali domande di accesso, rettifica, integrazione, cancellazione e blocco su istanza degli interessati al trattamento dei dati personali ai sensi degli artt. 7-10 del Codice, previa consultazione, ove lo si ritenga necessario, con l'ufficio competente in materia di disciplina circa il trattamento dei dati personali (Ufficio Sistemi Informativi)
- vigilare affinché l'accesso ai dati da trattare da parte degli incaricati sia limitato a quello strettamente necessari allo svolgimento delle mansioni loro assegnate.

INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

Ai sensi di quanto disposto dalla normativa, gli incaricati del trattamento dei dati personali sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

La designazione va effettuata per iscritto e deve individuare puntualmente l'ambito del trattamento consentito.

Si considera tale tuttavia anche la documentata preposizione della persona fisica all'Unità Organizzativa per la quale è stato individuato per iscritto, l'ambito del trattamento consentito agli addetti della medesima.

Nell'ambito del CNR si considera documentata preposizione l'indicazione degli incaricati preposti ad ogni specifico trattamento all'interno delle schede di rilevazione dei trattamenti inviate in risposta alla circolare n.4/05 del 16 Giugno 2005, ovvero, a regime, indicati nell'anagrafe elettronica dei trattamenti.

Si considerano incaricati pertanto nell'ambito del CNR il personale di ruolo (personale tecnico-amministrativo e ricercatore,) e personale operante ad altro titolo (personale a contratto , dottorandi, titolari di assegni di ricerca) nell'Unità Organizzativa medesima, sulla base di provvedimento o atto formale.

Qualora il responsabile, nello svolgimento delle sue funzioni istituzionali, ritenga necessario autorizzare soggetti diversi dai precedenti al trattamento dei dati personali inerenti la sua struttura, dovrà provvedere a designare per iscritto i medesimi consegnando agli stessi il modello di nomina (ALLEGATO)

Oltre che alle prescrizioni ed istruzioni di carattere generale contenute nel presente Manuale ogni incaricato deve attenersi alle istruzioni impartite dal responsabile dell'Unità Organizzativa cui afferisce od è assegnato relativamente alla specificità del trattamento dei dati personali effettuato nell'Unità Organizzativa medesima.

ANAGRAFE DEL TRATTAMENTO DEI DATI PERSONALI

L'anagrafe elettronica dei trattamenti dei dati personali, contiene i dati relativi alle tipologie ed alle caratteristiche di tutti i trattamenti svolti all'interno del CNR, così come comunicati dalle strutture in risposta alla circolare n.4/05 del 16 Giugno 2005 relativa al censimento generale dei trattamenti.

L'anagrafe costituisce l'unico riferimento circa i trattamenti svolti nel CNR ed i relativi incaricati.

La stessa è implementata e/o modificata, da parte di ciascuna struttura, ogni qualvolta si verifichi l'esistenza di un nuovo trattamento, la cessazione di uno precedente, la modifica delle caratteristiche di un trattamento, ovvero il nuovo ingresso, la cessazione o il cambiamento di mansioni di uno degli incaricati.

PROFILI TECNICI

LA SICUREZZA

Nell'ambito informatico, comunemente, il termine "sicurezza" si riferisce a tre aspetti distinti:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;

Integrità: Le informazioni non devono essere alterabili da incidenti o abusi;

Disponibilità Il sistema deve essere protetto da interruzioni impreviste.

Il TU sulla privacy pone una particolare attenzione, agli articoli 31 e seguenti, alle tematiche della sicurezza dei dati e sistemi.

In proposito le misure di sicurezza da adottare vengono distinte in:

- misure idonee e preventive volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- misure minime, indicate negli articoli 34 e 35 e analiticamente specificate nel Disciplinare Tecnico e diversificate a seconda che il trattamento sia effettuato o meno con strumenti elettronici.

Con l'approvazione del Codice i titolari di trattamento di dati (quindi anche il CNR) sono tenuti ad **adottare, quanto meno, le cd "misure minime di sicurezza"**, ossia gli accorgimenti, individuati negli artt. 34-35 e nel Disciplinare Tecnico del Codice, tesi ad assicurare un livello minimo di protezione dei dati personali.

La mancata osservanza di quanto stabilito in materia di misure minime di sicurezza e sanzionata penalmente (arresto fino a due anni o ammenda da diecimila a cinquantamila euro).

L'adozione delle misure minime di sicurezza non esonera tuttavia da responsabilità civile qualora l'eventuale danneggiato dimostri che, in base all'evoluzione tecnologica raggiunta, era possibile e raccomandabile l'utilizzo di misure di sicurezza ulteriori (le cd misure "idonee").

Per l'attuazione delle misure di sicurezza in ciascuna unità organizzativa è assicurato il supporto dell'Ufficio Sistemi Informativi.

Saranno concordati, presso ciascuna struttura, appositi incontri con personale tecnico - informatico, al fine di evidenziare eventuali criticità e predisporre un piano di adeguamento.

Per il supporto circa l'adozione di misure di sicurezza che non rivestano carattere informatico è assicurato il supporto dell'Ufficio .IV della Direzione Generale.

LE MISURE MINIME DI SICUREZZA

- **Trattamenti effettuati con strumenti elettronici**

Trattamento dati comuni

Sono **obbligatorie** le seguenti misure:

a) autenticazione informatica.
Il sistema informatico deve essere dotato di mezzi (le cd. credenziali di autenticazione) deputati alla verifica ed alla convalidazione dell'identità del soggetto che vi accede
Le credenziali di autenticazione consistono in un codice per l'identificazione (user id) dell'incaricato associato a una parola chiave riservata (password), conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave..

b) adozione di procedure di gestione delle credenziali di autenticazione;
Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali

c) utilizzazione di un sistema di autorizzazione;
E' il sistema che, dopo l'autenticazione, permette agli incaricati di trattare effettivamente i dati.
I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
E' effettuata tramite l'aggiornamento, almeno annuale, dell'anagrafe del trattamento dei dati personali.

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
Utilizzo di antivirus aggiornati almeno *semestralmente* (giornalmente) e adozione di *misure atte alla protezione dagli accessi dalla rete (firewall etc)*

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
Utilizzo di back up e strategie di disaster recovery

g) tenuta di un aggiornato documento programmatico sulla sicurezza (redatto annualmente dal CNR).

Trattamento dati sensibili o giudiziari

Ulteriori misure:

h) Adozione di idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni

i) Devono essere concordate con l'Ufficio Sistemi Informativi le misure organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti. 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.

- **Trattamenti effettuati senza l'ausilio di strumenti elettronici (dati su supporto cartaceo)**

Trattamento dati comuni

Sono **obbligatorie** le seguenti misure:

a) L'aggiornamento periodico dei dati il cui trattamento è consentito agli incaricati (tramite l'aggiornamento dell'anagrafe dei trattamenti)

b) Istruzioni circa un'idonea custodia degli atti e dei documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

E' compito di ciascun responsabile fornire istruzioni agli incaricati del trattamento affinché ai documenti contenenti dati personali non accedano persone prive di autorizzazione, dando idonea divulgazione presso gli stessi del presente Manuale per la sicurezza, per quanto riguarda le prescrizioni di carattere generale, nonché impartendo le istruzioni del caso relativamente alla specificità del trattamento dei dati personali effettuato nell'Unità Organizzativa medesima.

Trattamento dati sensibili o giudiziari

Ulteriori misure:

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, possibilmente utilizzando armadi o contenitori chiusi a chiave

Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

APPENDICE

ISTRUZIONI OPERATIVE PER GLI INCARICATI

A) Trattamenti senza l'ausilio di strumenti elettronici

1. UTILIZZATE LE CHIAVI!

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio quando l'ultima unità di personale lascia il locale e, comunque, alla fine della giornata e chiudete i documenti a chiave negli armadi ogni volta che potete.

2. NON COMUNICATE DATI PERSONALI A SOGGETTI NON LEGITTIMATI

L'utilizzo dei dati personali deve avvenire in base al cd "principio di necessità", è cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative.

I dati non devono essere comunicati all'esterno del CNR e comunque a soggetti terzi, se non previa autorizzazione del Responsabile nelle ipotesi consentite dalla normativa vigente.

3. FATE ATTENZIONE A COME DISTRUGGETE I DOCUMENTI

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

I documenti originali non possono in alcun caso essere distrutti senza la previa autorizzazione della Soprintendenza Archivistica.

4. RADDOPPIATE LE ATTENZIONI SE I DOCUMENTI CONTENGONO DATI SENSIBILI O GIUDIZIARI

I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi
molto attentamente in modo che non vi accedano persone prive di autorizzazione.

Ad esempio, la consultazione di documenti o certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattia, ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati.

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando possibilmente armadi o contenitori chiusi a chiave

Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

Riponete i documente contenenti dati sensibili o giudiziari negli appositi contenitori o scaffali al termine delle operazioni affidate e comunque a fine giornata.

In ogni caso di allontanamento dal proprio posto di lavoro, documenti devono essere riposti negli armadi o nei cassetti, possibilmente chiusi a chiave.

B) Trattamenti con strumenti elettronici

1. CONSERVATE I DISCHETTI (FLOPPY DISK) OVVERO I COMPACT DISC IN UN LUOGO SICURO

Per i dischetti e i compact disc si applicano gli stessi criteri che per i documenti cartacei. Riponeteli negli armadi o nei cassetti non appena avete finito di usarli.

2. UTILIZZATE LE PASSWORD

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

a) La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
b) La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
c) La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
d) La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.

Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di tipo *a*, che può dover essere resa nota, almeno temporaneamente, esclusivamente ai tecnici accreditati incaricati dell'assistenza. Scegliete le password secondo le indicazioni della sezione successiva.

3. ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe.

4. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i furti. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

5. NON FATEVI SBIRCIARE QUANDO STATE DIGITANDO LE PASSWORD

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

6. CUSTODITE LE PASSWORD IN UN LUOGO SICURO

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

7. NON UTILIZZATE APPARECCHI NON AUTORIZZATI

L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con l'Ufficio Sistemi Informativi.

8. **NON INSTALLATE PROGRAMMI NON AUTORIZZATI**
   Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con l'Ufficio Sistemi Informativi.

9. **APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS**
   La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi provenienti da fonti non ufficiali;
2. Attraverso le macro dei programmi di automazione d'ufficio.

COME *NON* SI TRASMETTE UN VIRUS:

1. Attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi;
2. Quando si copiano dati da dischetti;
3. Quando si scaricano dati o programmi da Internet.

QUALI EFFETTI HA UN VIRUS?

1. Effetti sonori e messaggi sconosciuti appaiono sul video;
2. Nei menù appaiono funzioni extra finora non disponibili;
3. Lo spazio disco residuo si riduce inspiegabilmente;

COME PREVENIRE I VIRUS:

1. **USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE**
   Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati.

2. **ASSICURATEVI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER DA DISCHETTO**
   Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

3. **PROTEGGETE I VOSTRI DISCHETTI (O COMPACT DISK) DA SCRITTURA QUANDO POSSIBILE**
   In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

4. **ASSICURATEVI CHE IL VOSTRO SOFTWARE ANTIVIRUS SIA AGGIORNATO**
   La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Informatevi con l'Ufficio Sistemi Informativi per maggiori dettagli.

5. **NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA**
   Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: i mail di questo tipo sono detti con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete.

6. **NON PARTECIPATE A "CATENE DI S. ANTONIO" E SIMILI**
   Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*, aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche.

SCELTA DELLE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

1. NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome
2. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
3. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.
4. NON usate il Vostro nome utente. È la password più semplice da indovinare
5. NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE

1. Cambiare la password a intervalli regolari.
2. Usare password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione.