2015 - Rev. 08

Documento Prescrittivo sulla Sicurezza

SIAF
Sistema Informatico
dell'Ateneo Fiorentino

Indice

1. Obiettivi

Il documento ha l'obiettivo di definire alcune regole comportamentali e le responsabilità connesse alla garanzia e alla manutenzione dell'efficacia delle misure di sicurezza; in particolare fornisce indicazioni atte a:

- garantire la sicurezza dei dati ai sensi del D.lgs.vo 30.6.2003 n.196 (recante il Codice in materia di protezione dei dati personali) e suo Disciplinare Tecnico (Allegato B);
- assicurare l'adempimento delle "Misure Minime" di sicurezza previste nel Disciplinare Tecnico;
- operare in modo da seguire le "Misure Idonee" a preservare i dati, in relazione ai rischi ai quali sono sottoposti.

Nel presente documento vengono fornite indicazioni per garantire la sicurezza nei suoi vari aspetti (riservatezza, integrità, disponibilità) attraverso misure di tipo logico e procedurale.

2. Definizioni

Definizioni utili ai fini della applicazione del documento:

- **"dato personale"**, qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- **"dati sensibili"**, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- **"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;
- **"titolare"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **cui competono**, anche unitamente ad altro titolare, l**e decisioni in ordine alle finalità, alle modalità del trattamento di dati personali** e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- **"responsabile"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **preposti** dal titolare al **trattamento di dati personali**;
- **"incaricati"**, le persone fisiche autorizzate a c**ompiere operazioni di trattamento** dal titolare o dal responsabile, se designato;
- **"autenticazione informatica"**, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- **"credenziali di autenticazione"**, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- **"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;
- **"profilo di autorizzazione"**, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- **"dati strategici"** per SIAF, i dati relativi ai servizi considerati strategici per le finalità e le attività svolte da SIAF;
- **"Regolamento di Ateneo"**: Regolamento di attuazione del Codice di Protezione dei Dati Personali in possesso dell'Università degli Studi di Firenze.

In base al "Regolamento di Ateneo" **SIAF è Responsabile del trattamento di tutti i dati da esso detenuti**, fatta eccezione per i dati contenuti nei siti WEB, database, applicazioni e dati utenti ospitati.

3. Riferimenti normativi

In materia di protezione dei dati personali le principali normative di riferimento sono le seguenti:
- Decreto legislativo 30 giugno 2003, n. 196 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" e suoi allegati.
- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

I testi completi e aggiornati di tali norme sono disponibili sul sito del Garante della Privacy www.garanteprivacy.it.
Sullo stesso sito sono presenti anche i vari provvedimenti emessi dal Garante relativamente ad ambiti specifici di trattamento.
Per quanto riguarda l'applicazione della normativa in Ateneo sono stati emanati due regolamenti:
- Regolamento di attuazione del codice di protezione dei dati personali in possesso dell'Università degli Studi di Firenze
- Regolamento per il trattamento dei dati sensibili e giudiziari in attuazione del D.lgs. 196/2003.

4. Campo di applicazione

Le regole comportamentali definite nella presente procedura sono orientate alla protezione dei dati personali, sensibili e strategici.

Esse hanno la seguente applicabilità:

❑ sono prescrizioni obbligatorie ai sensi del D.lgs.vo 30.6.2003 n.196 per tutti coloro che trattano i dati dei quali SIAF è **Responsabile**, in particolare per:

- gli incaricati di SIAF, con una o più delle funzioni di:
  - incaricato del trattamento;
  - incaricato della custodia delle credenziali;
  - incaricati della amministrazione di sistema, database e rete;

- incaricati del trattamento afferenti all'Università di Firenze, delle due tipologie:
  - per incarico scritto da parte del Responsabile;
  - per documentata preposizione;

- incaricati del trattamento esterni, appartenenti a società di consulenza relativamente a:
  - servizi in outsourcing;
  - supporto di sistemi;

- personale afferente a SIAF:
  - tutto il personale dipendente da SIAF;
  - tutto il personale che ha rapporti di collaborazione con SIAF a qualunque titolo;

❑ sono regole di accesso e di comportamento per tutti gli utenti di SIAF che non trattano dati personali.

Si sottolinea che:

- chiunque intraprende trattamento di dati personali è tenuto a comunicarlo al Responsabile della propria struttura di appartenenza che, ai sensi del "Regolamento di Ateneo", è Responsabile dei dati della struttura stessa;
- le stazioni di lavoro e le caselle di posta elettronica sono strumenti di lavoro 'aziendali' forniti dall'Ateneo; deve essere garantita la reperibilità delle informazioni (dati personali e non) di interesse comune in caso di assenza;
- ciascuno ha la responsabilità dei dati detenuti sulla propria stazione di lavoro e della loro protezione;
- la condivisione dei dati sulle stazioni di lavoro personali deve essere ristretta alle sole persone incaricate di trattare tali dati e deve essere conforme alle norme di sicurezza; per la condivisione di dati di interesse comune e/o personali si raccomanda l'utilizzo di file server opportunamente gestiti secondo le norme di sicurezza previste;
- le caselle di posta elettronica possono contenere, oltre a dati propri, anche dati di altri ed in quanto tali, devono essere preservate, anche sulle stazioni di lavoro personali; per comunicazioni di interesse comune si raccomanda l'utilizzo di indirizzi di funzione.

Le regole comportamentali relative all'utilizzo delle apparecchiature di lavoro valgono per :

- stazioni di lavoro personali nel luogo di lavoro;
- stazioni di lavoro comuni a più persone, nel luogo di lavoro;
- stazioni di lavoro portatili;
- stazioni di lavoro dalle quali ci si connette in modalità remota;
- stampanti.

I Responsabili e gli Incaricati sono inoltre tenuti a quanto altro specificato nella nomina o anche successivamente indicato dal Responsabile del Trattamento della Struttura e/o dai rispettivi Responsabili.

5. Gestione degli accessi

Chiunque tratti dati deve essere abilitato e poi riconosciuto dal sistema informatico, cioè autenticato tramite delle **credenziali di autenticazione**; possono anche essere definiti a livello applicativo diversi **"profili di autorizzazione"**, a seconda delle operazioni consentite a ciascuno degli incaricati del trattamento dei dati.

Tipicamente le credenziali sono composte da:

- un identificativo dell'utente (**User ID**), che è la parte pubblica delle credenziali;
- una parola chiave di autenticazione (**password**), che è la parte riservata delle credenziali.

La *password* è un elemento fondamentale per il sicuro funzionamento del sistema di autenticazione e per evitare accessi non autorizzati. La scelta ed il corretto utilizzo delle password da parte dell'utente è dunque un fattore fondamentale per la sicurezza di un sistema informatico.

5.1 - Modalità di scelta della password

Per garantire e mantenere l'efficacia delle misure di sicurezza, gli utenti devono essere consapevoli delle loro specifiche responsabilità nella **scelta delle password di accesso**. Affinché questa sia dotata di robustezza e quindi difficilmente intuibile da altri, è obbligatorio seguire le seguenti regole:

- la password deve essere 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;
- la password non deve contenere riferimenti aventi attinenza con la vita privata o professionale facilmente riconducibili all'utente (evitare ad es. nome, cognome, data di nascita, numero di telefono, codice fiscale, luogo di nascita, nome di parenti ecc.);
- le password non devono essere parole di senso comune presenti sul dizionario;
- la password non deve contenere una serie consecutiva di soli numeri o di sole lettere;
- la password, nel caso in cui lo strumento elettronico lo permetta, deve essere preferibilmente composta da una sequenza di lettere, numeri e caratteri speciali (es. di caratteri speciali: &;@*§ ? % £ = @ $);
- la password non deve essere costituita da una sequenza ovvia sulla tastiera (es. qwerty, 123456);
- la stessa password non deve essere riutilizzata per almeno quattro anni;
- la password deve essere facile da ricordare per l'utente.

5.2 - Cautele per la segretezza della password

Per garantire e mantenere l'efficacia delle misure di sicurezza, gli utenti devono essere consapevoli delle loro specifiche responsabilità nell'**utilizzo delle password di accesso**.

Nell'**utilizzo della password** devono quindi essere adottate le seguenti misure di sicurezza:

- utilizzare sempre esclusivamente le proprie credenziali di autenticazione;
- non condividere la propria password con altre persone;

- non comunicare ad altri le proprie credenziali;
- mantenere e custodire le proprie password con la dovuta riservatezza;
- evitare di scrivere le proprie password su foglietti di carta o agende, a meno che tali supporti cartacei non vengano custoditi in cassetti o armadi chiusi a chiave;
- nel digitare sulla tastiera la componente riservata della credenziale di autenticazione (password), prestare attenzione ad eventuali sguardi indiscreti che potrebbero far perdere alla password di accesso il requisito della segretezza
- comunicare immediatamente al Responsabile se per le credenziali si è verificata perdita della qualità in modo che siano subito disattivate.

5.3 - Obblighi relativi alla modifica della password

Per garantire e mantenere l'efficacia delle misure di sicurezza, gli utenti devono essere consapevoli delle loro specifiche responsabilità nella **modifica delle password di accesso**.

Per la **modifica della password** devono essere adottate le seguenti misure di sicurezza:

- modificare la password temporanea assegnata dall'amministratore, al primo utilizzo (primo log-on);
- cambiare immediatamente la password nel caso si sospetti abbia perso il requisito della segretezza;
- modificare la password di accesso alle applicazioni utilizzate per il trattamento di dati personali almeno ogni sei mesi;
- in caso di trattamento di dati sensibili (es. dati personali inerenti lo stato di salute) e giudiziari la password deve essere modificata almeno ogni tre mesi (art.5 – Disciplinare tecnico - dal D.lgs. 196/2003);
- comunicare all'incaricato della custodia delle credenziali la modifica, consegnandogli in busta chiusa le proprie credenziali (identificativo di utente e password).

5.4 - Sistema di Autenticazione Unico

Molti servizi SIAF utilizzano il sistema di autenticazione unico per cui la stessa coppia di credenziali di autenticazione (identificativo dell'utente e password) viene utilizzata per l'accesso a tutti essi.

Ciò rende ancora più critica la robustezza e la segretezza della password in quanto la sua conoscenza può dare ad altri la possibilità di accedere a più servizi per i quali può non avere incarico di accesso (dunque senza diritti) o accesso con profili diversi.

5.5 - Dimenticanza della password

Qualora un incaricato del trattamento dimentichi la propria password, la può recuperare presso il custode delle credenziali della propria struttura (v. § 5.3).

In caso ciò sia impossibile, per alcuni servizi può essere attivata una procedura di Recupero Password automatica; altrimenti può essere inviata la richiesta a SIAF sugli appositi moduli. La nuova password verrà

inviata da SIAF al Responsabile in busta chiusa.

Tutte le richieste pervenute e le relative risposte vengono protocollate.

- Per il servizio di Posta Elettronica

Può essere chiesto il ripristino della password iniziale (password di 'reset') attraverso lo specifico modulo "Richiesta Ripristino Password" disponibile sul sito di SIAF nel gruppo Posta Elettronica della sezione Modulistica.

- Per i servizi che utilizzano il Sistema di Autenticazione Unico

(v. URL www.csiaf.unifi.it > Attività e servizi - SOS utenti - Modalità di autenticazione servizi SIAF, raggiungibile dalla homepage di SIAF)

  - il personale dipendente di ruolo dell'Ateneo (docenti, ricercatori e personale T/A) può utilizzare il Servizio automatico di recupero password, purché abbia precedentemente impostato la Domanda e la Risposta personalizzate (operazione obbligatoria al momento del cambio password); il recupero viene attivato dalla apposita pagina "Servizio di Recupero Password", linkata dalla URL citata e la password viene inviata via posta elettronica all'indirizzo istituzionale. In alternativa, per riottenere la password occorre richiedere la riassegnazione della password iniziale inviando a SIAF il modulo "SI03-Richiesta ripristino password" disponibile sul sito di SIAF nella sezione Modulistica;
  - i collaboratori esterni, in possesso di credenziali per l'Autenticazione Unica, possono ottenere il ripristino facendone richiesta a SIAF, mediante lo stesso modulo "SI03-Richiesta ripristino password"
  - gli assegnisti di ricerca devono rivolgersi al Dipartimento di afferenza;
  - i dottorandi possono ottenere il ripristino rivolgendosi all'Ufficio Dottorato di Ricerca presso il Nuovo Ingresso di Careggi , l.go Brambilla, 3 - Firenze;
  - gli studenti possono utilizzare il Servizio automatico per il recupero della password, purché in precedenza abbiano impostato la domanda personalizzata (usando Cambia la password) e abbiano inserito il proprio indirizzo di posta elettronica (usando Inserisci la tue email). Altrimenti possono ottenere il ripristino della password iniziale recandosi personalmente alla rispettiva segreteria.

- Altri Servizi

In caso debba essere richiesta la assegnazione di una nuova password, deve essere seguita da parte del Responsabile la stessa procedura prevista per le altre variazioni.

6. Gestione degli incarichi e delle credenziali

Ciascun Responsabile del trattamento è tenuto ad assicurare la corretta gestione degli incarichi e delle credenziali del personale afferente alla propria struttura o ufficio.
I Responsabili del trattamento delle strutture diverse da SIAF possono designare degli **Incaricati del trattamento dati** (v. § 5.1)e degli **Incaricati della custodia delle credenziali** del personale afferente alla propria

struttura (v. § 5.3); questi ultimi, oltre alla custodia delle credenziali eventualmente potranno essere adibiti alla gestione dell'elenco degli incaricati (v. § 5.2).
I Responsabili degli uffici SIAF designano gli **Incaricati del trattamento dati**, gli **Incaricati con funzioni di Amministratore di Sistema** e gli I**ncaricati della custodia delle credenziali**.

6.1 - Assegnazione degli incarichi

Incaricati afferenti a strutture diverse da SIAF

Ogni volta che una unità di personale afferente ad un ufficio o struttura dell'Ateneo viene incaricata del trattamento di dati relativi ad un servizio informatizzato erogato da SIAF, il Responsabile del trattamento deve inoltrare a SIAF una specifica richiesta di *attivazione di utenza* (avvalendosi dei moduli predisposti e pubblicati sul sito web di SIAF), debitamente compilata e firmata, indicando:

- il trattamento, servizio, eventuale sottosistema per cui è stato conferito l'incarico e per il quale pertanto deve essere attivata l'utenza;
- i dati dell'incaricato;
- il profilo di autorizzazione (per i servizi che lo prevedono).

Sarà cura di SIAF:

- attivare le credenziali con il relativo profilo, comunicandole all'incaricato in busta chiusa
- inviare al Responsabile la notifica dell'avvenuta attivazione con eventuali specifiche,

Analogamente il Responsabile dovrà tempestivamente comunicare a SIAF mediante lo stesso modulo qualunque *variazione di stato* e in particolare:

- se un incaricato deve cambiare profilo;
- se un incaricato decade nei suoi diritti di accesso (ad esempio in caso di trasferimento ad altro ufficio).

Sarà cura di SIAF eseguire i relativi aggiornamenti.
Si fa presente che la richiesta di attivazione o disattivazione dell'utenza non ha valore di Nomina o Revoca dell'Incaricato.

Incaricati afferenti a SIAF

Ogni volta che una unità di personale di SIAF riceve un "incarico" di trattamento dati, il Responsabile del trattamento deve comunicarlo per scritto all'opportuno incaricato della gestione operativa delle credenziali (Amministratore di sistema), indicando:

- il trattamento, il servizio SIAF, l'eventuale sottosistema;
- i dati dell'incaricato;
- il profilo di autorizzazione (per i servizi che lo prevedono).

L'incaricato suddetto ha cura di:

- attivare le credenziali con il relativo profilo,

- comunicare la password all'incaricato,

Analogamente il Responsabile deve tempestivamente comunicare per iscritto all'incaricato della gestione delle credenziali (Amministratore di sistema) qualunque variazione di stato degli incaricati e in particolare:

- se un incaricato deve cambiare profilo;
- se un incaricato decade nei suoi diritti di accesso.

E' cura dell'incaricato con funzioni di Amministratore di sistema conservare le richieste e aggiornare i profili degli utenti configurati.

6.2 - Gestione degli incaricati

Incaricati afferenti a strutture diverse da SIAF

I Responsabili del trattamento in una struttura o in un ufficio sono tenuti a gestire un "*Elenco degli incaricati di trattamenti di dati*", nel quale devono riportare, per ogni trattamento / servizio / sottosistema i dati di tutti i relativi incaricati:

- nome e cognome dell'incaricato;
- rapporto con l'Università;
- identificativo dell'utente;
- profilo;
- data della richiesta di attivazione;
- data della conferma della attivazione;
- data della richiesta di disattivazione;
- data di conferma della disattivazione.

Si fa presente che il mantenimento delle credenziali di accesso a una persona che non è più incaricata del relativo trattamento dei dati, in caso di abuso è un rischio ed una responsabilità sia della persona stessa sia del Responsabile della struttura alla quale afferiva al momento della nomina.

Incaricati afferenti a SIAF

I Responsabili del trattamento di SIAF sono tenuti a gestire un "*Elenco degli incaricati di trattamenti di dati*", nel quale devono riportare, per ogni trattamento / servizio / sottosistema / tipo di incarico i dati di tutti i relativi incaricati:

- nome e cognome dell'incaricato;
- rapporto con l'Università;
- identificativo dell'utente;
- profilo;
- data della richiesta di attivazione;
- data della conferma della attivazione;
- data della richiesta di disattivazione;
- data di conferma della disattivazione.

Il Responsabile del trattamento deve comunicare all'incaricato della gestione operativa delle credenziali (tipicamente l'incaricato amministratore di sistema) ogni variazione relativa all'elenco degli incaricati e comunque con cadenza annuale fornire un elenco di tutti gli incaricati attivi afferenti al suo ufficio.

6.3 - Custodia delle credenziali

Incaricati afferenti a strutture diverse da SIAF

Il Responsabile del trattamento di ogni struttura deve assicurare la disponibilità dei trattamenti in caso di assenza di incaricati.
Ogni incaricato del trattamento è tenuto a affidare le proprie credenziali al Responsabile del trattamento o all'incaricato della custodia delle credenziali, se designato. L'incaricato della custodia delle credenziali le deve custodire in luogo sicuro.
Il Responsabile del trattamento curerà la definizione di una procedura per la custodia delle credenziali da parte dell'incaricato, e per l'accesso controllato in caso di assenza di un incaricato.

Incaricati afferenti a SIAF

Il Responsabile del trattamento di ogni ufficio deve assicurare la disponibilità dei trattamenti in caso di assenza di incaricati.
Ogni incaricato del trattamento è tenuto ad affidare le proprie credenziali all'incaricato della custodia delle credenziali. L'incaricato della custodia delle credenziali le deve custodire in luogo sicuro.
Il Responsabile del trattamento curerà la definizione di una procedura per la custodia delle credenziali da parte dell'incaricato, e per l'accesso controllato in caso di assenza di un incaricato, nella quale specifica:

- la modalità di custodia delle credenziali;
- l'obbligo di segnalazione all'incaricato assente della comunicazione ad altro incaricato temporaneo delle sue credenziali;
- le modalità di ripristino della riservatezza delle credenziali.

7. Gestione delle stazioni di lavoro

Dato che la stazione di lavoro è il punto di accesso ai dati, particolare cautela deve essere adottata sia nella sua custodia che nella sua manutenzione operativa atta a prevenire virus informatici ed intromissioni, da parte di tutto il personale, strutturato e non, dell'Ateneo.

7.1 - Custodia della stazione di lavoro

Per garantire e mantenere l'efficacia delle misure di sicurezza, gli utenti devono essere consapevoli delle loro specifiche responsabilità nella **custodia della propria stazione di lavoro**.

Le informazioni riservate (dati personali, dati sensibili, dati strategici), necessitano di una protezione più elevata e di particolare cautele da parte del personale incaricato del trattamento. In particolare, il personale è tenuto a seguire le seguenti istruzioni :

- evitare di lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- proteggere la stazione di lavoro attraverso cui si accede a sessioni di trattamento di informazioni riservate, utilizzando o key locks, password di qualità o screen saver (da attivare su richiesta o dopo un tempo prestabilito di inattività), nel caso in cui ci si assenti temporaneamente dall'ufficio;
- al termine della sessione di lavoro sui server centrali, effettuare la procedura di disconnessione ("log-off" / "logout" / "esci") ;
- al termine della sessione sulla stazione di lavoro, effettuare la procedura di arresto del sistema ed attendere che sia terminata prima di lasciare l'ufficio;
- effettuare (almeno una volta alla settimana) il backup dei dati personali e documenti essenziali presenti sulla propria stazione di lavoro o portatile tramite il servizio di file service fornito dal Centro e dai Servizi Informatici di Polo o, ove impossibile, su CD o altro supporto esterno.

7.2 - Credenziali delle stazioni di lavoro

Nei casi in cui:

- vengano mantenute informazioni di interesse comune sulla propria stazione di lavoro,
- la propria stazione di lavoro sia l'unica abilitata ad accedere ad uno specifico servizio,

il responsabile della stazione di lavoro è consapevole che deve essere garantito l'accesso alla stazione stessa in caso di assenza. L'accesso può essere garantito o attraverso la nomina di un collega fiduciario, opportunamente informato delle credenziali della stazione di lavoro o attraverso la consegna delle credenziali stesse al 'Custode delle credenziali' della propria struttura, secondo le modalità indicate al § "5.3 - Custodia delle credenziali".

7.3 - Prevenzione dei virus informatici

E' necessario prevenire l'introduzione di virus informatici che possano compromettere l'integrità del software e delle stazioni di lavoro, tenendo anche conto del fatto che tra un aggiornamento del programma

antivirus ed il successivo è presente una finestra temporale di rischio di introdurre virus non ancora noti dal programma antivirus stesso.

E' necessario pertanto:

- ❑ installare il software antivirus in dotazione;
- ❑ configurare la protezione permanente e l'aggiornamento automatico via rete;
- ❑ verificare il regolare funzionamento della procedura automatica di aggiornamento del programma antivirus, al fine di accertarsi che la procedura sia andata a buon fine;
- ❑ utilizzare il software rispettando le istruzioni del fornitore;
- ❑ verificare, tramite adeguato programma antivirus, i file, il software e i dispositivi di memorizzazione rimovibili (floppy disk, hard disk esterni, chiavette USB, ecc.) provenienti dall'esterno, prima del loro utilizzo;
- ❑ configurare il sistema operativo affinché sia possibile visualizzare l'estensione dei file: tale accorgimento rende più difficile il mascheramento da parte di file potenzialmente pericolosi (programmi EXE e script di vario tipo) che impiegano estensioni doppie (es. "leggimi.txt.vbs" oppure "logo.jpg.exe");
- ❑ ripulire immediatamente le stazioni che si rivelino o vengano segnalate come infette;
- ❑ segnalare tempestivamente al Responsabile dell'Ufficio Server Farm (per il personale SIAF) o al Responsabile del SIP locale (per il personale afferente ad altre strutture) qualsiasi presenza di virus sospetta che pregiudichi o abbia pregiudicato il sistema di sicurezza delle informazioni;
- ❑ nello scaricare dalla rete Internet programmi (es. software open source; freeware, shareware ecc.) e documenti (testi e tabelle che possono contenere dei "virus macro") necessari allo svolgimento della propria attività lavorativa, utilizzare unicamente i siti delle case produttrici dei medesimi o i link che esse stesse propongono sul loro sito;
- ❑ nell'utilizzo della posta elettronica :

  - evitare di aprire allegati che contengono un'estensione doppia o con estensione VBS, SHS, PIF, EXE, COM o BAT (a meno che non attesi e provenienti da mittente conosciuto e di fiducia);
  - se si ricevono e-mail non richieste o con contenuti pubblicitari, evitare di seguire i collegamenti a indirizzi Web eventualmente presenti nel testo delle e-mail;
  - nel caso si riceva un messaggio di e-mail da una persona conosciuta, ma con un contenuto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato; infatti alcuni virus sono in grado di trasmettere messaggi con allegati che sembrano spediti da mittenti conosciuti;
  - evitare di cliccare su icone dall'apparenza innocua che ricordano applicazioni associate ad immagini o musica, mostrate dagli allegati di posta elettronica in quanto possono nascondere "worm";
  - configurare il programma di posta elettronica in modo tale che non esegua automaticamente gli allegati.

7.4 - Politica di aggiornamenti software

E' necessario prevenire, sulla propria stazione di lavoro, accessi non autorizzati che violino il sistema e possano compromettere l'integrità del software ed indirettamente dei sistemi informativi.

E' pertanto necessario seguire una politica di aggiornamento dei software presenti sulla stazioni di lavoro in modo da introdurre regolarmente le modifiche o le nuove versioni emesse per proteggere i sistemi. Adottare quindi le seguenti norme:

- configurare, ove possibile, l'esecuzione automatica degli aggiornamenti del sistema operativo, ovvero
- configurare, ove possibile, lo scaricamento automatico dalla rete degli aggiornamenti (patch) del sistema operativo ed eseguire l'installazione non appena disponibile;
- ove non possibile un aggiornamento automatico, controllare almeno mensilmente la disponibilità di aggiornamenti e provvedere alla loro installazione;
- qualsiasi sospetta vulnerabilità nel sistema di sicurezza delle informazioni o la presenza di virus sulla propria postazione di lavoro;
- segnalare tempestivamente al Responsabile dell'Ufficio Server Farm (per il personale SIAF) o al Responsabile del SIP locale (per il personale afferente ad altre strutture) qualsiasi vulnerabilità o attività sospetta che pregiudichi o abbia pregiudicato il sistema di sicurezza delle informazioni.

8. Gestione del materiale

La sicurezza dei dati deve essere garantita anche quando questi non risiedono su server e stazioni di lavoro. In particolare deve essere protetto il materiale ottenuto come output da apparecchiature informatiche e non, ed il materiale cartaceo.

8.1 - Gestione del materiale di output

Per quanto riguarda il materiale ottenuto come output da apparecchiature informatiche e non, devono essere seguite le seguenti regole:

- se non utilizzati e quando ci si assenta dall'ufficio, provvedere a custodire in armadio o cassetto muniti di serratura i supporti removibili (es. floppy, cd) contenenti informazioni riservate o strategiche;
- controllare attentamente lo stato delle stampe di documenti riservati e rimuovere immediatamente tali copie dalla stampante, onde evitare che personale non autorizzato abbia accesso alle informazioni;
- provvedere a rendere inintelligibili eventuali stampe non andate a buon fine.

8.2 - Gestione del materiale cartaceo

Per quanto riguarda il materiale cartaceo, devono essere seguite le seguenti regole:

- conservare i supporti cartacei contenenti dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati stessi (stanze, armadi, cassetti chiusi a chiave);
- se si è in attesa di un documento contenente informazioni riservate via fax, non lasciare incustodito

l'apparecchio del fax ma rimuovere immediatamente il documento.

8.3 - Gestione delle apparecchiature dismesse

Le informazioni classificate come "riservate" (dati personali, dati sensibili ecc.) devono essere cancellate in maniera definitiva dai dispositivi di memorizzazione, prima che le apparecchiature vengano dismesse (trasferite per essere riutilizzate da altri utenti, riciclate o smaltite).
Il semplice comando di cancellazione o di formattazione non è spesso sufficiente per garantire una cancellazione permanente dei dati. Sono infatti disponibili diversi modi per recuperare i documenti che sono stati cancellati, anche dopo la formattazione dell'hard disk.
Occorre prestare particolare attenzione quando si gestiscono *dati personali e sensibili, informazioni strategiche o coperte da riservatezza*.
Per quanto concerne le vecchie stazioni di lavoro da dismettere, è compito di ciascun assegnatario provvedere alla permanente distruzione delle informazioni critiche e alla disinstallazione del software con licenza installato sulle stazioni di lavoro:

- nel caso di reimpiego o di riciclo la cancellazione sicura può essere effettuata tramite:
  - uno dei programmi di 'wiping' disponibili in rete (per es. DBAN, che si può scaricare dal sito http://www.dban.org, dove è disponibile anche la documentazione),
  - una formattazione a basso livello,
  - demagnetizzazione, che garantisce la demagnetizzazione anche per dispositivi non più funzionanti;

- nel caso di smaltimento la cancellazione può anche prevedere la distruzione dei supporti tramite:
  - sistemi di punzonatura o deformazione meccanica,
  - distruzione fisica o disintegrazione,
  - demagnetizzazione ad alta intensità.

Per quanto riguarda invece i server, gli storage system, le cartucce, in gestione all'Ufficio Server Farm di SIAF, è compito di quest'ultimo di provvedere alla cancellazione permanente delle informazioni riservate. Per garantire l'impossibilità di recupero dei dati, si utilizzano tecniche di formattazione profonda, oppure si provvede alla distruzione fisica dell'apparecchiatura, dopo aver completato la procedura di scarico del bene inventariale.

9. Informativa sui dati raccolti

In relazione ai servizi erogati di cui SIAF è Responsabile, vengono salvati i dati residenti sui sistemi e nei database, con finalità di ripristino in caso di perdita degli stessi.
Vengono inoltre archiviati i dati dei Log di sistema e degli applicativi, con le seguenti finalità:

- Monitoraggio della funzionalità dei servizi e della sicurezza

Per il servizio telematico di 'Accesso alla rete Internet" sono conservati i log relativi alla data e ora di autenticazione degli utenti che hanno richiesto il servizio tramite la rete wireless e il proxy con autenticanzione, con esclusione dei contenuti delle comunicazioni, per le finalità:

- Monitoraggio della funzionalità dei servizi e della sicurezza

Per i servizi telematici di fonia con tecnologia VoIP e di 'Posta elettronica' vengono archiviati anche i dati del traffico, esclusi i contenuti delle comunicazioni, per le finalità :

- Monitoraggio delle funzionalità del servizio
- Ripartizione di costi (solo per il servizio VoIP)
- Documentazione per accertamento e repressione dei reati

L'accesso ai sistemi per funzioni di amministrazione da parte degli incaricati è registrato su apposito log e conservato su nastro per le finalità:

- Controllo di sicurezza sugli accessi ai sistemi

I dati del traffico potranno essere acquisiti esclusivamente su richiesta giudiziaria da parte degli organi previsti dalla normativa vigente.
A tutti i dati dei Log hanno accesso solo gli incaricati a ciò adibiti; essi verranno utilizzati per le uniche finalità dichiarate che pertanto escludono qualunque controllo sulla attività svolta dai lavoratori durante il servizio.
I Log vengono conservati per i periodi previsti dalla normativa in materia.