Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Incaricato federale della protezione dei dati e della trasparenza
IFPDT

PROVVEDIMENTI TECNICI E ORGANIZZATIVI
GUIDA

Settembre 2011

Feldeggweg 1, 3003 Berna
Tel. 031 323 74 84, Fax 031 325 99 96
www.edoeb.admin.ch

Indice

INTRODUZIONE

Questa guida è nata su iniziativa dell'Incaricato federale della protezione dei dati e della trasparenza. Concepita come introduzione ai rischi legati alla protezione dei dati negli attuali sistemi d'informazione, rappresenta un ausilio all'implementazione di misure finalizzate a garantire una protezione dei dati personali ottimale e adeguata a condizioni specifiche. Gli aspetti più importanti della protezione dei dati sono presentati nell'ottica dei provvedimenti tecnici e organizzativi che devono essere previsti; tra questi, la cifratura dei dati, l'anonimizzazione, l'autenticazione, ecc.

La guida si rivolge innanzitutto ai responsabili dei sistemi d'informazione che, siano essi esperti o meno in ambito tecnico, si trovano a gestire dati personali. Essa fornisce tuttavia indicazioni utili anche a chiunque s'interessi della materia.

Le tematiche affrontate sono quattro: l'accesso ai dati, il loro ciclo di vita, la loro trasmissione e il diritto d'accesso. Per ogni tematica vengono sollevati i punti principali cui occorre prestare attenzione quando si concepisce e si implementa un sistema. Per ogni punto sono poi proposti alcuni provvedimenti da adottare; questi ultimi vanno intesi come linee guida generali, da adattare alle specificità del singolo progetto e della singola organizzazione.

Definizioni

Qui di seguito è riportata la definizione di alcuni termini al fine di assicurare l'esatta comprensione di quanto descritto nella guida.

Dati personali

- Sono **dati personali** tutte le informazioni relative a una persona identificata o identificabile.

- I **dati personali degni di particolare protezione** sono quelli concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali, la salute, la sfera intima o l'appartenenza a una razza, le misure d'assistenza sociale, i procedimenti o le sanzioni amministrativi e penali. Sono **pericolosi** (d'importanza vitali) i dati la cui diffusione può implicare rischi per la vita della persona interessata.

- Il **profilo della personalità** consiste in una compilazione di dati che permette di valutare caratteristiche essenziali della personalità di una persona fisica.

- La **persona interessata** è quella a cui si riferiscono determinati dati personali.

- Ai dati personali si applicano i seguenti quattro livelli di sicurezza:

1. ***Livello minimo***: si applica ai dati personali il cui abuso non sembra, in linea di massima, comportare conseguenze particolari per l'interessato. Si tratta, per esempio, del cognome, del nome, dell'indirizzo e della data di nascita (sempre che la combinazione di questi dati non consenta di individuare la persona in questione) oppure di informazioni diffuse nei media.
2. ***Livello medio****:* si applica ai dati personali il cui abuso può compromettere la situazione economica o la posizione sociale della persona interessata. Si tratta, per esempio, di dati relativi alla situazione personale di un affittuario o alle relazioni professionali.
3. ***Livello elevato***: si applica ai dati personali il cui abuso può compromettere seriamente la situazione economica della persona interessata o la sua posizione nella società. Si tratta, per esempio, di dati relativi allo stato di salute di un paziente, di dati personali degni di particolare protezione o di profili della personalità.
4. ***Livello molto elevato***: si applica ai dati personali il cui abuso può mettere in pericolo la vita della persona interessata. Si tratta, per esempio, di indirizzi di informatori della polizia o di testimoni implicati in determinati procedimenti penali o di indirizzi di persone minacciate per aver manifestato la propria opinione o appartenenza religiosa o politica.

Protezione dei dati

- La ***sicurezza dei dati*** include tutti i provvedimenti adottati in vista di assicurare l'integrità, la fruibilità e la riservatezza dei dati.

- La ***protezione dei dati*** include tutti i provvedimenti adottati in vista di evitare trattamenti inadeguati nonché qualsiasi conseguenza indesiderata di un determinato trattamento.

- Nel quadro della ***protezione delle informazioni*** sono definiti i livelli di riservatezza dei documenti (interno, confidenziale, segreto) nell'ottica di difendere gli interessi di un Paese o di un'organizzazione.

Collezione di dati

- Il termine ***collezione di*** **dati**, definito nel diritto svizzero, designa una raccolta di dati personali strutturata in modo tale da permettere di individuare le informazioni relative a una determinata persona.

Responsabilità

I ruoli riportati qui di seguito sono importanti in un'organizzazione che si occupa del trattamento di dati personali:

- il ***detentore di una collezione di dati*** è la persona privata o l'organo federale che decide in merito allo scopo e al contenuto dei dati utilizzati in un sistema d'informazione;

- il ***responsabile della protezione dei dati*** è la persona, interna a un'organizzazione, incaricata di controllare i trattamenti di dati personali e di proporre provvedimenti correttivi nell'ottica della protezione dei dati;

- l'***Incaricato federale della protezione dei dati e della trasparenza*** svolge compiti di sorveglianza e di consulenza presso persone private e organi federali. Tiene e pubblica inoltre un registro delle collezioni di dati che le persone private e gli organi federali sono tenuti a notificare;

- l'***Incaricato cantonale*** svolge compiti analoghi presso gli organi cantonali e comunali.

Basi legali

La guida si fonda sulla legge federale sulla protezione dei dati (LPD), in particolare sull'articolo 7, e sull'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD), in particolare sugli articoli 8-11 e 20-21.

Provvedimenti tecnici e organizzativi

L'adozione di provvedimenti tecnici e organizzativi consente di minimizzare i rischi connessi a un sistema d'informazione. Un sistema d'informazione che contiene dati personali deve cioè essere conforme a determinati criteri al fine di garantire la sicurezza dei dati. L'attuazione di questi provvedimenti consente di offrire una garanzia di sicurezza.

I provvedimenti tecnici sono legati direttamente al sistema d'informazione e interessano soltanto quest'ultimo. I provvedimenti organizzativi hanno invece a che fare solo indirettamente con il sistema d'informazione, interessando per esempio le persone che lo utilizzano.

Entrambe le categorie di provvedimenti sono indispensabili. Soltanto la loro adozione combinata consente di evitare la distruzione o la perdita di dati, gli errori, le falsificazioni, l'accesso non autorizzato, ecc.

Questi provvedimenti si iscrivono nel ciclo di vita di un sistema d'informazione e sono applicati a tutti i livelli del sistema.

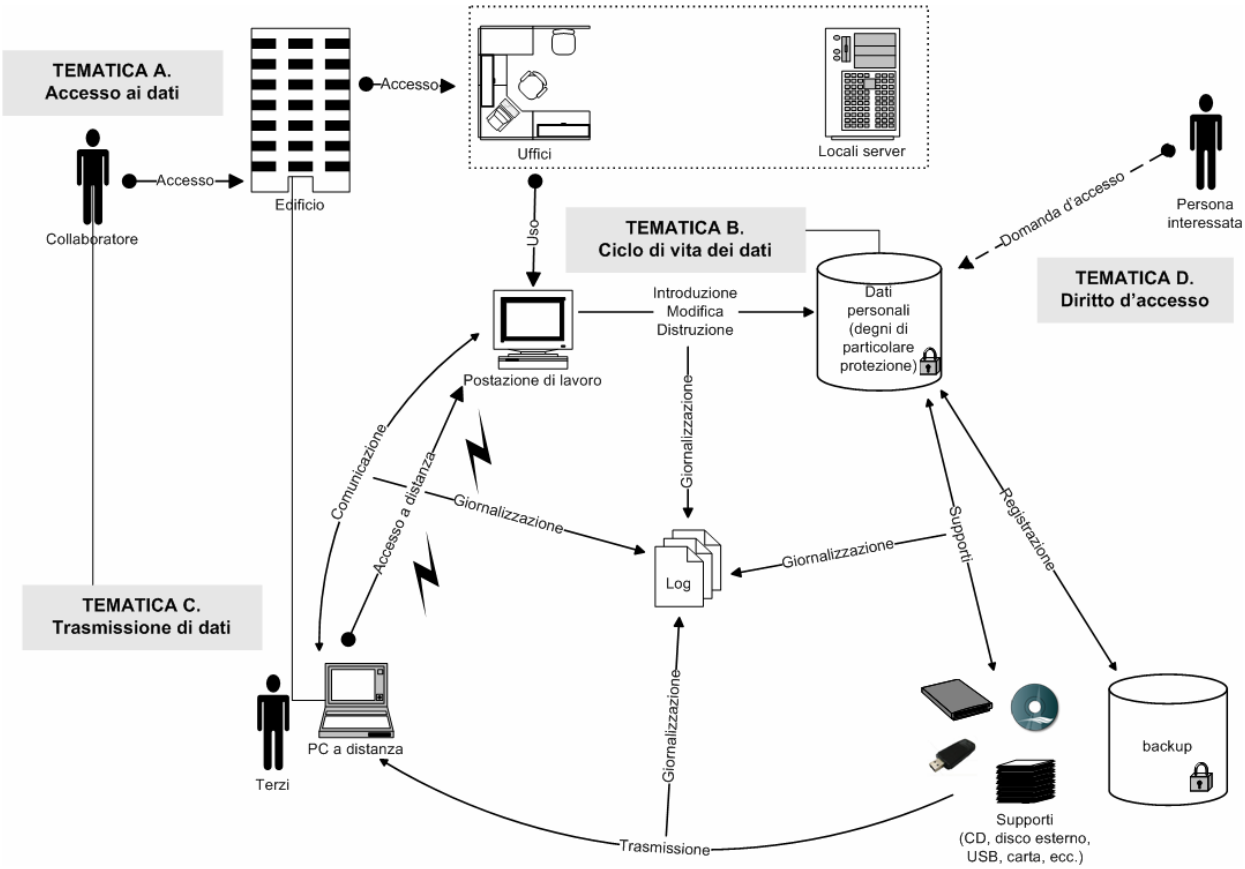
Nello schema 1 (pag. 6) è raffigurato il ciclo di vita di un sistema d'informazione; esso illustra varie operazioni (l'immissione dei dati, il loro trattamento, la loro comunicazione e registrazione, ecc.) nonché i livelli a cui possono intervenire terze persone (collaboratori, persone adibite al trattamento o persone i cui dati sono contenuti nel sistema).

Contenuto della guida

Dallo schema 1 emergono quattro tematiche principali, che sono poi le linee guida della guida, ovvero i provvedimenti tecnici e organizzativi legati: (1) all'accesso ai dati, (2) al loro ciclo di vita, (3) alla loro trasmissione e (4) al diritto d'accesso.

Per ogni tematica sono affrontati diversi aspetti e sono presentati i provvedimenti ad essi associati. Per ogni aspetto, vengono poi evidenziate alcune buone pratiche, da intendersi come suggerimenti per lo sviluppo di applicazioni che rispettino la sfera privata. I provvedimenti illustrati devono, ovviamente, essere adattati al grado di sensibilità dei dati, alla natura dei trattamenti, alla portata delle informazioni utilizzate, ecc.

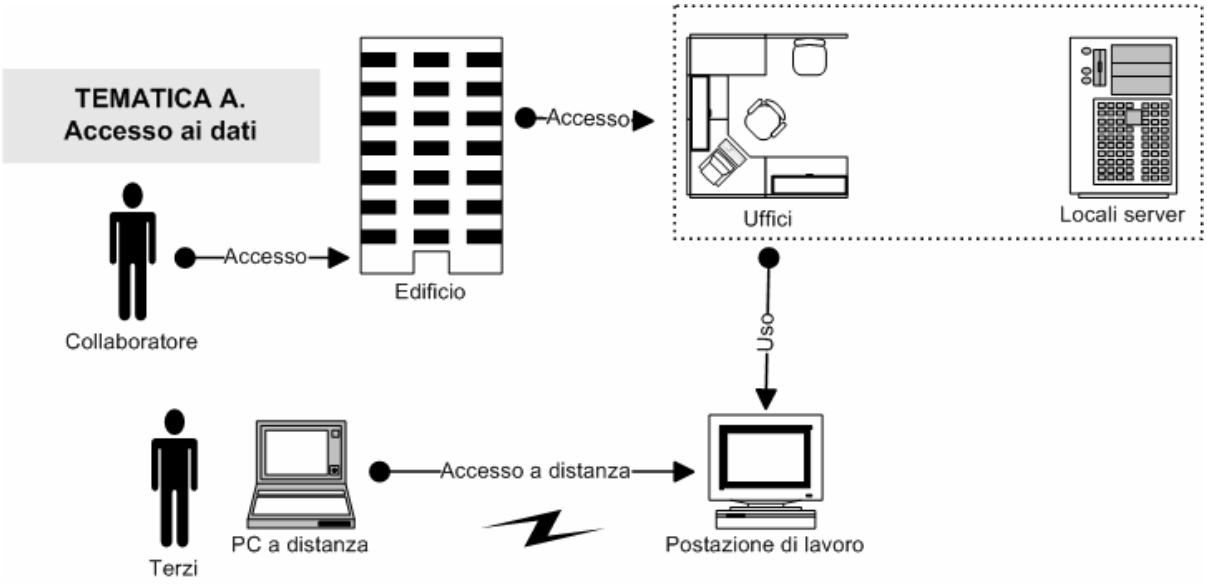
La guida si conclude riportando alcuni strumenti che consentono di prevedere i rischi legati alla protezione dei dati o di descrivere in modo formale i provvedimenti adottati.



Schema 1: Panoramica dei provvedimenti tecnici e organizzativi.
Le quattro sezioni dello schema riflettono le tematiche affrontate nei vari capitoli della guida.

TEMATICA A: L'ACCESSO AI DATI

La prima tematica riguarda l'accesso ai dati da parte dei vari gruppi di utenti. Poiché tale accesso va analizzato sotto più punti di vista, occorre innanzitutto valutare attentamente dove collocare i server di dati e quali strumenti adottare per garantirne la sicurezza tenendo conto di tutti i soggetti implicati. In secondo luogo, è necessario determinare le modalità di consultazione, modifica ecc. dei dati, il che presuppone più livelli di sicurezza: i computer utilizzati dai collaboratori devono essere accessibili soltanto alle persone autorizzate e devono essere protetti contro i tentativi d'intrusione esterni. Le intrusioni possono avvenire in loco (una persona non autorizzata accede ai locali) o a distanza (una persona non autorizzata accede al sistema attraverso la rete). Infine, occorre decidere quale traccia conservare degli accessi fisici ed elettronici.



***Schema** A: accesso ai dati*

Osservando lo schema A, emergono le domande riportate qui sotto. Queste domande sono approfondite nei capitoli che seguono e sono associate a proposte di provvedimenti concreti.

A.1 Come garantire la sicurezza dei locali?
A.2 Come garantire la sicurezza dei server?
A.3 Come garantire la sicurezza delle postazioni di lavoro?
A.4 Come garantire l'identificazione e l'autenticazione degli utenti?
A.5 Come proteggere l'accesso ai dati degli utenti?
A.6 Come controllare l'accesso a distanza?

A.1 Sicurezza dei locali

Per «locali» si intendono i luoghi in cui lavorano gli utenti del sistema ovvero chi ha accesso ai dati. Questi ultimi sono registrati nei locali server (cfr. sezione A2 - Sicurezza dei locali server); i computer personali sono periferiche che consentono di accedere ai dati. L'accesso ai computer, che fungono quindi da interfaccia verso i dati, deve essere controllato. Soltanto le persone autorizzate devono cioè poter accedere agli edifici e agli uffici. Poiché queste persone possono svolgere funzioni diverse, per poter definire diritti d'accesso specifici, occorre tenere conto di tutte le possibili funzioni (collaboratore dell'organizzazione, personale addetto alla manutenzione, alla pulizia dei locali, ecc.).

I provvedimenti da adottare vanno definiti in funzione del contesto globale. Se lo stesso edificio funge da sede di più organizzazioni, le esigenze in termini di sicurezza dei dati possono variare da un'organizzazione all'altra; sarà quindi necessario scegliere provvedimenti che soddisfino le esigenze specifiche, operando, per esempio, una suddivisione per piano. I server di dati, inoltre, possono essere esternalizzati, delegando pertanto a terzi la responsabilità della loro sicurezza.

Provvedimenti da considerare

- L'accesso all'edificio (o agli edifici) è soggetto a determinati controlli: le persone che desiderano entrare devono possedere un tesserino, eventualmente associato a un codice d'accesso, per poter essere identificate.
- Se lo stesso edificio è sede di più organizzazioni, occorre valutare la necessità di stabilire un sistema di controllo analogo per poter accedere ai locali adibiti all'organizzazione in questione: per esempio un sistema d'accesso elettronico installato sul piano o nella sezione dell'edificio in cui è ubicata l'organizzazione.
- I visitatori sono soggetti a misure di controllo specifiche e sono accolti secondo una procedura prestabilita, volta ad evitare che possano aggirarsi indisturbati all'interno dell'edificio.
- Al di fuori degli orari di presenza, gli uffici sono chiusi a chiave.
- Nei locali strategicamente più importanti sono, all'occorrenza, installati degli allarmi, attivati al di fuori degli orari di presenza.

A.2 Sicurezza dei locali server

Dal punto di vista strategico, i locali server sono i luoghi più importanti di un'organizzazione, dato che in esse sono collocati i contenitori fisici dei dati. L'integrità e la fruibilità dei dati possono essere assicurate soltanto se si adottano provvedimenti volti a impedire la loro perdita definitiva. Anche nel caso dei locali server, occorre definire le persone autorizzate ad

accedervi. Il livello di sicurezza è inversamente proporzionale al numero di persone autorizzate. Lo scopo è evitare che, effettuando intenzionalmente o meno operazioni errate sui server, vengano distrutti o cancellati dei dati. Per questa ragione è essenziale adottare provvedimenti particolari per garantire la sicurezza dei locali server.

Provvedimenti da considerare

- Soltanto una cerchia ristretta di persone deve poter entrare nei locali server. Autorizzare chiunque svolga una stessa funzione ad accedere a questi locali rispecchia un atteggiamento troppo lassista. I tecnici autorizzati ad accedervi per occuparsi della manutenzione dei sistemi devono essere in numero limitato. La pulizia dei locali dovrebbe essere affidata sempre allo stesso personale.

- Gli accessi ai locali server sono giornalizzati.

- Il locale è munito di un allarme costantemente in funzione, allo scopo di evitare qualsiasi intrusione non autorizzata.

- Idealmente, il locale server si trova nel sottosuolo, in modo da ridurre al minimo il numero delle vie d'accesso (porte, finestre, ecc.).

- Gli incidenti naturali, quali incendi o inondazioni, possono essere individuati in modo automatico e segnalati con allarmi.

A.3 Sicurezza delle postazioni di lavoro

I collaboratori accedono ai dati e li elaborano dalle postazioni di lavoro, dove si trova il loro computer personale. Per garantire la sicurezza dell'ambiente di lavoro, le periferiche devono essere disposte in modo strategico e vi deve essere un numero sufficiente di ripiani con chiusura a chiave.

Il computer personale deve essere protetto mediante password (che soltanto il collaboratore conosce) e gli appositi software anti intrusione. I provvedimenti adottati devono assicurare la protezione totale contro qualsiasi tipo di virus, i cosiddetti software malevoli (malware) e gli attacchi in senso lato.

Provvedimenti da considerare

- Le postazioni di lavoro sono allestite in modo tale che gli schermi dei computer non possano essere visti dalla porta dell'ufficio. Questo al fine di garantire che i visitatori esterni non siano in grado di osservare su cosa stanno lavorando i collaboratori.

- I documenti stampati non sono lasciati incustoditi in prossimità della stampante. Il collaboratore può, ad esempio, inserire un codice nella stampante quando decide di eseguire l'ordine di stampa.

- Il collaboratore colloca i documenti stampati e il materiale sensibile (chiavette USB, CD ROM, ecc.) in ripiani con chiusura a chiave.

- I computer portatili, e se necessario anche i desktop, sono fissati alla scrivania mediante un cavo antifurto.

- Su tutti i computer è stato installato e attivato un programma antivirus, aggiornato a intervalli regolari.

A.4 Identificazione e autenticazione

L'identificazione consente di stabilire l'identità di una persona e di distinguerla così da altre.

L'autenticazione consente invece di accertare che una persona sia effettivamente chi dice di essere; essa è effettuata sulla base di tre elementi: un oggetto che la persona *possiede* (p. es. un tesserino di riconoscimento), un'informazione che *conosce* (p. es. una password) oppure una *caratteristica propria* dell'utente (comportamentale, come la firma, o morfologica, come l'impronta digitale). Si parla di autenticazione forte quando sono combinati almeno due requisiti di base (p. es. password e tesserino).

L'autenticazione serve dunque a consentire agli utenti di entrare nei locali e di connettersi al proprio computer per accedere a determinati dati, mentre l'identificazione consente di individuare chi ha introdotto, modificato o distrutto dati nel sistema in un determinato momento.

L'autenticazione unica («Single Sign-On», SSO) è un metodo che permette a un utente di accedere a più applicazioni autenticandosi una volta sola.

Provvedimenti da considerare

- I conti utente che consentono l'autenticazione sono unici. I collaboratori non condividono lo stesso conto. Il conto è composto di un codice identificativo (nome utente) associato a una password, a un tesserino di riconoscimento, ecc.

- Idealmente, ogni utente utilizza conti diversi per identificarsi sul proprio PC e sulle applicazioni con cui lavora. In tal modo, se una persona con intenzioni dubbie riesce a connettersi al PC, non riuscirà ad accedere ai dati passando per le applicazioni installate.

- Se si usa l'autenticazione unica (SSO), mediante la quale l'accesso al PC si traduce nell'accesso alle applicazioni, occorre adattare le misure di sicurezza.

- La password deve essere sufficientemente sicura e cambiata di frequente. Una password è sufficientemente sicura se contiene almeno 8 caratteri e combina lettere (maiuscole e minuscole), cifre e caratteri speciali.

- La frequenza con cui è cambiata la password è inversamente proporzionale alla complessità della password stessa.

- L'autenticazione mediante dati biometrici deve essere utilizzata nel rispetto dei provvedimenti presentati nella «Guida ai sistemi di riconoscimento biometrico»[1].

A.5 Accesso ai dati

I dati sono conservati nei server centrali. In generale, i collaboratori non hanno bisogno di accedere a tutti i dati. Se l'accesso dei collaboratori è limitato ai soli dati necessari al loro lavoro si possono ridurre i rischi di un uso scorretto, sia questo intenzionale o meno. È inoltre possibile prevenire gli abusi. A tal fine, occorre definire regole d'accesso nonché un meccanismo d'autorizzazione in base alle funzioni svolte dai singoli collaboratori.

Provvedimenti da considerare

- Il sistema d'informazione è organizzato in modo tale da accordare agli utenti accessi differenziati.

- Il diritto d'accesso dei singoli collaboratori è definito internamente all'organizzazione secondo una matrice dei diritti di accesso.

- Il collaboratore procede alla propria autenticazione ogni volta che avvia il sistema. Il livello di autenticazione è direttamente proporzionale al grado di protezione dei dati.

- Gli accessi ai sistemi sono giornalizzati secondo le modalità esposte alla sezione B2 - Giornalizzazione.

A.6 Accesso a distanza

Gli accessi a distanza possono essere di diversi tipi: per ogni situazione distinta occorre prevedere determinate misure di protezione.

I collaboratori che desiderano lavorare esternamente all'organizzazione possono richiedere l'accesso a distanza al proprio PC dell'ufficio. Tale accesso va disciplinato secondo la

[1] www.lincaricato.ch > Temi > Protezione dei dati> Biometria

politica interna all'organizzazione e in considerazione della tipologia dei dati. Va pertanto definito un metodo sicuro di autenticazione. L'accesso ai dati può inoltre essere richiesto da terzi autorizzati, per esempio subappaltatori. Anche questi casi vanno disciplinati in modo chiaro; va inoltre richiesta un'autenticazione forte. La cosa più importante è comunque evitare qualsiasi accesso non autorizzato.

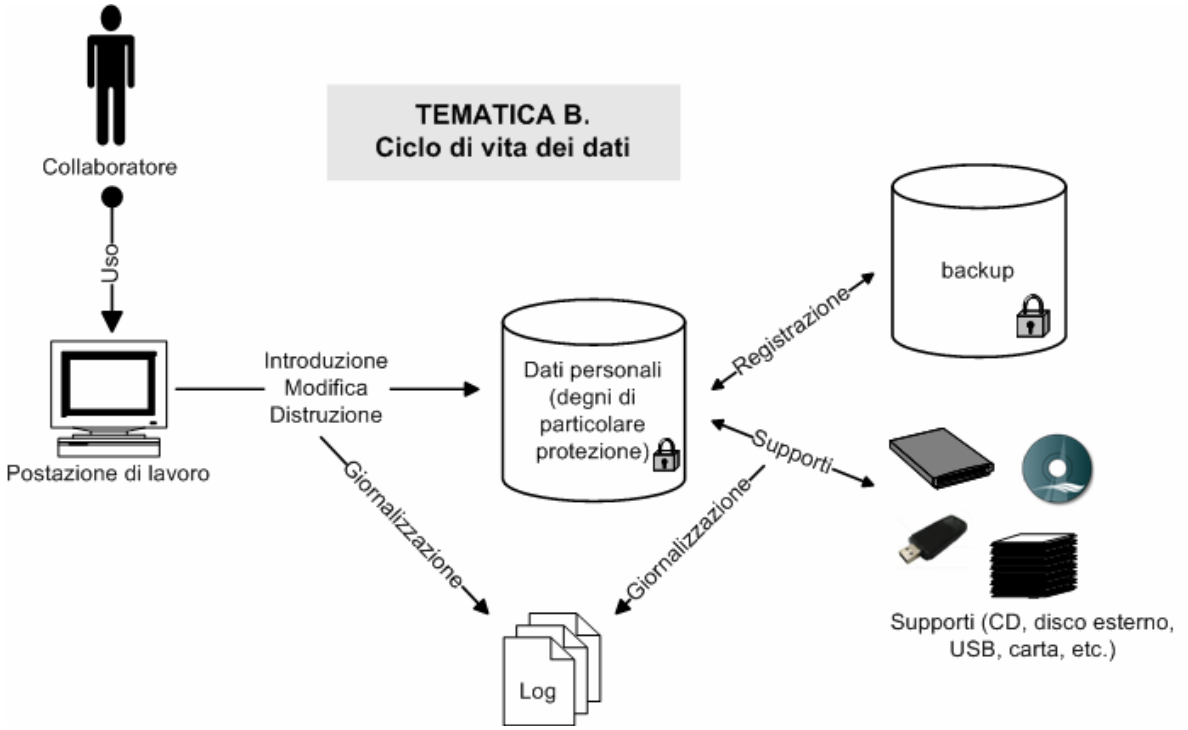
Nella sezione C1 - Sicurezza della rete sono riportate maggiori informazioni in materia di sicurezza della rete interna in caso di accesso a distanza da parte di terzi.

Provvedimenti da considerare

- Le persone che desiderano o devono connettersi a distanza si avvalgono di un accesso sicuro.
- L'autenticazione deve essere forte, ossia combinare almeno due requisiti di base.
- I computer personali sono protetti da un firewall.
- Gli accessi possono essere giornalizzati secondo le condizioni riportate nella sezione B2 - Giornalizzazione.

TEMATICA B: IL CICLO DI VITA DEI DATI

I provvedimenti riportati nella sezione precedente garantiscono l'accesso sicuro ai dati, consentendo di proteggere i computer che fungono da server centrali sia contro le intrusioni fisiche (accesso ai server centrali) sia contro i trattamenti illeciti (accesso ai computer personali). La tappa successiva consiste nel garantire la sicurezza dei dati durante il loro ciclo di vita. I dati devono cioè restare integri e affidabili da quando vengono immessi nel sistema fino a quando vengono distrutti e, ovviamente, in tutte le fasi di elaborazione intermedie (incluse la loro anonimizzazione e archiviazione).
In generale, i trattamenti di dati sono effettuati da collaboratori autorizzati all'interno dell'organizzazione, ma possono anche essere subappaltati a terzi.
Inoltre, durante le varie fasi di elaborazione, i dati sono spesso trasferiti su supporti mobili (chiavette USB, dischi duri esterni, ecc.): tenere traccia dei vari trattamenti permette, in caso di problemi, di risalire più facilmente alle cause.
Per evitare abusi dei dati, occorre studiare tutti gli aspetti e le situazioni menzionati.



Schema B: ciclo di vita dei dati

Nell'ambito di questa tematica vengono analizzate le domande riportate qui di seguito (cfr. schema B):

B.1 Come gestire l'immissione di dati nel sistema?
B.2 Come controllare i trattamenti di dati (giornalizzazione)?
B.3 Come pseudonimizzare o anonimizzare i dati?
B.4 Come cifrare i dati?
B.5 Come garantire la sicurezza dei vari supporti di dati?
B.6 Come garantire una copia di sicurezza dei dati?
B.7 Come distruggere definitivamente i dati?
B.8 Come gestire i progetti da dare in subappalto?
B.9 Come gestire la sicurezza delle informazioni e la protezione dei dati?

B.1 Immissione dei dati

L'immissione dei dati nel sistema è una tappa delicata: occorre assicurarsi che i dati immessi siano completi e corretti. In caso contrario, infatti, i risultati dei trattamenti saranno inesatti e condurranno a decisioni sbagliate. È importante sviluppare meccanismi d'assistenza atti a minimizzare i rischi d'errore durante l'immissione dei dati. Va inoltre fatta una distinzione tra l'immissione di dati reali e quella a titolo di test.

Provvedimenti da considerare

- I dati sono immessi unicamente da personale che ha ricevuto l'apposita formazione e autorizzazione.
- Il sistema prevede determinati meccanismi d'assistenza: segnala cioè le informazioni mancanti e, all'occorrenza, effettua test d'attendibilità.
- I dati utilizzati per i test sono fittizi o anonimizzati.
- L'immissione dei dati può essere giornalizzata secondo le regole riportate nella sezione B2 – Giornalizzazione.

B.2 Giornalizzazione

In alcuni casi è utile tenere traccia di tutti i trattamenti effettuati sui dati, ovvero dell'immissione di nuovi dati oppure della modifica o della distruzione di dati esistenti. In questo modo si può infatti risalire alla causa di un eventuale problema, sia essa un incidente tecnico, un accesso non autorizzato o un trattamento illecito di dati. Le singole operazioni possono essere giornalizzate: nei cosiddetti file di «log» (letteralmente, «giornali») sono registrati in ordine cronologico tutti gli eventi legati al sistema d'informazione; questi file sono conservati per un periodo di tempo proporzionale al grado di sensibilità dei dati e dei trattamenti.

Tutte le operazioni di cui sopra (accessi ai dati, immissione di nuovi dati, modifica o distruzione di dati esistenti) possono essere giornalizzate. La giornalizzazione diventa

obbligatoria soltanto nel caso in cui i dati trattati siano degni di particolare protezione e le misure preventive adottate non siano sufficienti a garantirne la sicurezza.

Negli altri casi, l'integrazione di un meccanismo di giornalizzazione è una scelta facoltativa, basata su una necessità chiara e su scopi ben determinati. Inoltre, la quantità di informazioni giornalizzate e la durata di conservazione dei file di log devono essere proporzionali.

Provvedimenti da considerare

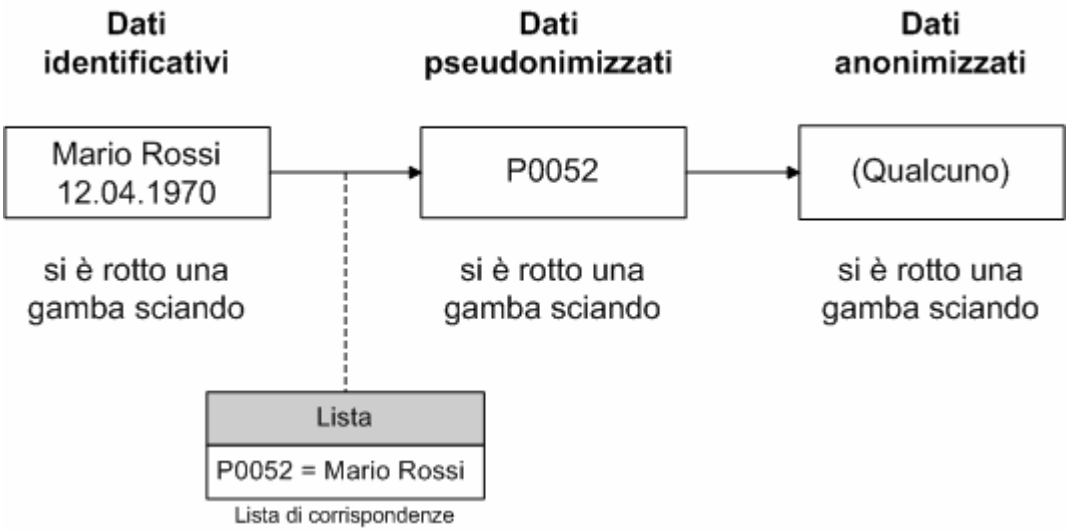
- Ragioni ben precise giustificano l'integrazione nel sistema di un meccanismo di giornalizzazione.
- Il contenuto e la durata di conservazione dei file di log sono proporzionali al grado di sensibilità dei dati e al tipo di trattamenti effettuati.
- I collaboratori sono informati del fatto che viene conservata una traccia delle operazioni effettuate sui dati.
- I file in cui sono registrate le varie operazioni (cosiddetti «giornali») sono protetti.
- I diritti di accesso ai file di log sono definiti in modo chiaro e sono limitati ai collaboratori che svolgono determinate funzioni all'interno dell'organizzazione.
- Il meccanismo di giornalizzazione è protetto contro attacchi o accessi illeciti finalizzati a modificare il contenuto dei file di log.

B.3 Pseudonimizzazione e anonimizzazione

La pseudonimizzazione e l'anonimizzazione servono a evitare l'identificazione di utenti i cui dati personali sono trattati dal sistema. Nel primo caso i dati identificativi di un utente sono sostituiti da un elemento identificante neutro (pseudonimo); l'anonimizzazione consiste invece nell'eliminazione di tutti i dati identificativi o di qualsiasi mezzo che consenta di risalire ai dati originali. La pseudonimizzazione è reversibile, mentre l'anonimizzazione è definitiva. Una volta anonimizzati, i dati non sono più personali.

I dati identificativi consentono di identificare facilmente una data persona. Per associare uno pseudonimo ai dati identificativi di una persona è utilizzata una lista di corrispondenze. Finché tale lista è disponibile, la pseudonimizzazione è un processo reversibile. Con l'anonimizzazione viene invece distrutto definitivamente qualsiasi dato identificativo (p. es. la lista di corrispondenze), cosicché la persona non può più essere identificata in alcun modo e il processo diventa irreversibile.

Nello schema riportato qui sotto questo processo è rappresentato graficamente:



Provvedimenti da considerare

- Di preferenza e nei limiti delle possibilità offerte dal progetto, vanno utilizzati dati anonimizzati. In presenza di dati anonimizzati non sono più applicabili né la legge federale sulla protezione dei dati né la maggior parte dei provvedimenti descritti in questa guida.
- Se i dati sono pseudonimizzati o anonimizzati, non è conservata nessuna informazione identificativa indiretta, ossia un'informazione ottenuta mettendo in relazione informazioni che, prese separatamente, non sono significative, ma che combinate consentono di identificare una persona.
- Nel caso in cui non sia opportuno optare per l'anonimizzazione, i collaboratori lavorano, nella misura del possibile, con dati pseudonimizzati.
- La lista di corrispondenze deve essere protetta: deve, cioè, essere accessibile a un numero limitato di collaboratori e, se possibile, cifrata.
- Nel caso in cui non sia opportuno optare per la pseudonimizzazione, i collaboratori lavorano con dati nominativi. Se sono degni di particolare protezione, i dati in questione devono essere cifrati (cfr. sezione B4 - Cifratura).

B.4 Cifratura

In linea generale, i dati sono memorizzati su un disco duro sotto forma di file oppure in una banca dati. La cifratura è un metodo per proteggere i dati personali ed evitare che siano letti o modificati in maniera abusiva. Essi sono cioè trasformati in un codice non comprensibile

per mezzo di una chiave di decifrazione. Chi non possiede o non conosce la chiave non è in grado di decifrarli.
Nella tematica che segue (C. Trasmissione di dati) viene affrontata la problematica del trasferimento di dati, nell'ambito del quale è possibile ridurre i rischi mediante un'apposita cifratura.

Provvedimenti da considerare

- L'algoritmo di cifratura e, in particolare, la lunghezza della chiave sono proporzionali al grado di sensibilità dei dati.
- Sullo stesso supporto di dati possono essere cifrati più gruppi di dati utilizzando chiavi specifiche.
- Le chiavi di cifratura sono protette.
- Soltanto un numero limitato di collaboratori ha accesso alle chiavi.

B.5 Sicurezza dei supporti di dati

Oltre che nei server centrali e nei computer personali, i dati vengono memorizzati in diversi supporti esterni, utilizzati per trasferire le informazioni tra collaboratori interni o tra questi e persone esterne all'organizzazione, senza dover passare per la rete. I supporti sono usati anche per fare copie di sicurezza temporanee e dalle dimensioni limitate.
I vari supporti (chiavette USB, dischi duri esterni, CD ROM, ecc.) hanno caratteristiche e quindi funzioni diverse: a differenza dei CD ROM, per esempio, le chiavette USB sono riscrivibili. Occorre inoltre sottolineare che è ormai possibile memorizzare sempre più dati in supporti sempre più piccoli; non si possono quindi sottovalutare i rischi legati a questi supporti.

Provvedimenti da considerare

- I collaboratori sono debitamente informati dei rischi legati all'uso di un supporto sconosciuto (chiavetta USB) sul proprio computer.
- I supporti esterni contenenti dati personali degni di particolare protezione o profili della personalità sono cifrati.
- I supporti esterni devono essere conservati in un luogo chiuso a chiave.
- È prevista un'apposita procedura da seguire per poter distruggere i supporti di dati e sono disponibili gli strumenti necessari per procedere alla distruzione.

B.6 Copia di sicurezza dei dati (backup)

Al fine di garantire l'integrità e la fruibilità dei dati contenuti nel sistema occorre definire una procedura di backup. Tale procedura deve cioè consentire di recuperare la versione più recente possibile dei dati persi o danneggiati a causa di operazioni errate o di trattamenti non autorizzati. Gli intervalli fra un backup e l'altro devono essere funzionali al numero di trattamenti effettuati nell'arco della giornata.

Provvedimenti da considerare

- Sulla base della tipologia dei dati, della loro quantità e della frequenza dei trattamenti viene definita una strategia di backup appropriata.
- I collaboratori vengono informati della strategia di backup.
- Per i server di backup vengono adottate le stesse misure di sicurezza previste per i server centrali.
- Il ripristino di dati è effettuato dai collaboratori che hanno ricevuto la formazione necessaria.

B.7 Distruzione di dati

I dati personali non vanno conservati a tempo indeterminato. Occorre pertanto stabilire la durata della loro conservazione e i meccanismi per la loro distruzione. Cancellare questi dati da un disco duro non basta ad assicurarne la distruzione definitiva; occorre assicurarsi che non siano più accessibili in alcun modo. Lo stesso vale per i dati disponibili in forma cartacea o su supporti mobili. Occorre infine distruggere anche le copie di backup.

Provvedimenti da considerare

- I dati disponibili in forma cartacea vanno distrutti mediante un distruggidocumenti.
- Anche i CD ROM e gli altri supporti mobili devono essere distrutti.
- I dati sono cancellati mediante programmi speciali in grado di garantirne la distruzione irreversibile.

B.8 Subappalto (trattamento di dati da parte di terzi)

Succede di frequente che un'organizzazione subappalti a terzi una parte dei suoi progetti, per esempio la fase di sviluppo del progetto, la manutenzione del sistema, il backup dei dati,

ecc. L'organizzazione appaltante assume la responsabilità dei suoi dati e deve assicurarsi che, in materia di protezione dei dati, l'appaltatore applichi regole equivalenti alle sue.

Provvedimenti da considerare

- Nel contratto d'appalto è stabilito che l'appaltatore deve rispettare le regole definite dall'organizzazione appaltante.
- L'organizzazione controlla a intervalli regolari che le condizioni di protezione dei dati siano rispettate.
- La trasmissione dei dati tra l'organizzazione e il subappaltatore segue regole precise.

B.9 Sicurezza e protezione

Per garantire la protezione dei dati, occorre tenere conto della classificazione secondo la loro tipologia (dati personali, degni di particolare protezione e pericolosi; cfr. definizioni riportate nel capitolo introduttivo) e quella secondo il livello di sicurezza (minimo, medio, elevato, molto elevato); questi due fattori vanno poi messi in relazione con il tipo di documento (interno, confidenziale, segreto). Si può quindi definire una matrice secondo il modello riportato qui sotto e, in base ad essa, stabilire un livello di protezione commisurato alla classificazione dei dati. La misura meno rigida si applica a tutti i livelli superiori.

	Dati non personali	Dati personali	Dati degni di particolare protezione	Dati pericolosi
		minimo/medio	elevato	molto elevato
Informazioni senza rischi		**Proteggere l'accesso al documento**	Proteggere **+ cifrare il documento**	Proteggere, cifrare **+ giornalizzare il trattamento + numerare le pagine del documento (*)**
Informazioni interne	**Proteggere l'accesso al documento**	Proteggere	Proteggere, cifrare **+ giornalizzare il trattamento**	Proteggere, cifrare, giornalizzare, numerare
Informazioni confidenziali	Proteggere **+ cifrare il documento**	Proteggere, cifrare	Proteggere, cifrare, giornalizzare	Proteggere, cifrare, giornalizzare, numerare
Informazioni segrete	Proteggere, cifrare **+ numerare le pagine del documento (*)**	Proteggere, cifrare, numerare	Proteggere, cifrare, giornalizzare, numerare	Proteggere, cifrare, giornalizzare, numerare

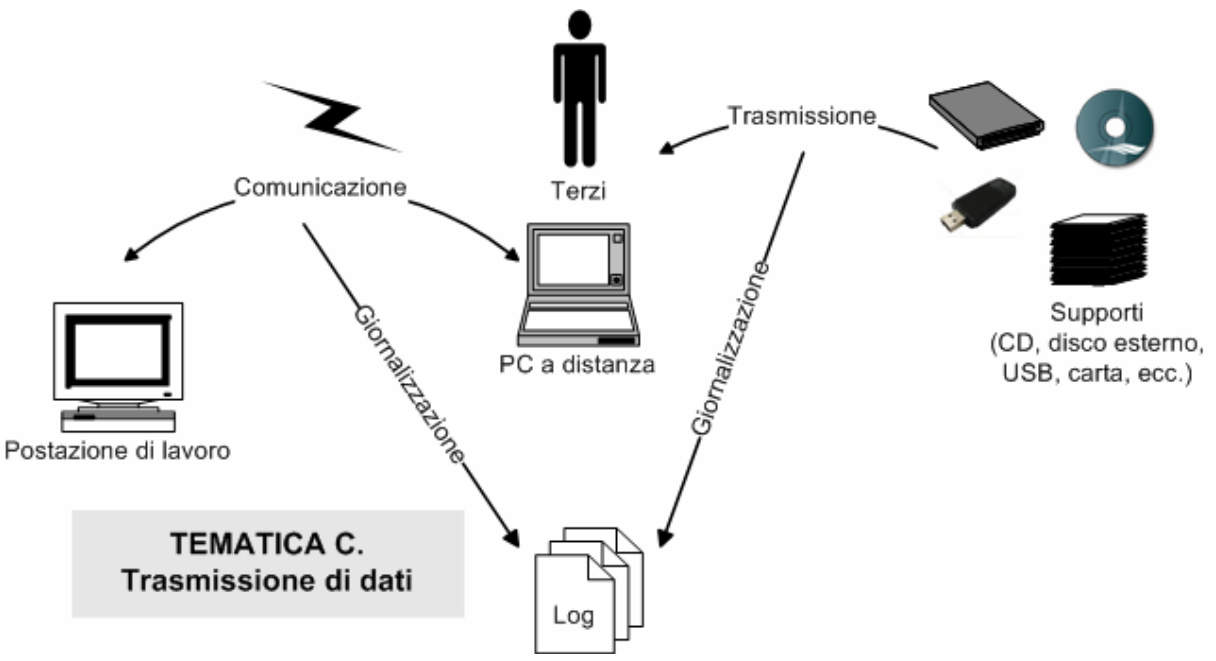
(*) La numerazione delle pagine dei documenti è una misura associata alla protezione delle informazioni.

Provvedimenti da considerare

- Il sistema è elaborato in funzione dei criteri fissati nella matrice.
- Sulla base della matrice sono adottati i provvedimenti appropriati.

TEMATICA C: TRASMISSIONE DI DATI

Gli odierni mezzi di comunicazione consentono di lavorare a distanza e di scambiarsi informazioni in modo semplice e rapido. Ciò significa che i dati non restano più all'interno dell'organizzazione, ma sono trasmessi all'esterno. È pertanto necessario garantire la protezione dei dati durante gli ormai frequenti trasferimenti a terzi.



Schema C: trasmissione di dati

Nell'ambito di questa tematica vengono analizzate le domande riportate qui di seguito (cfr. schema C):

C.1 Come garantire la sicurezza dei dati?
C.2 Come cifrare un messaggio inviato a utenti esterni all'organizzazione?
C.3 Come apporre la firma su un messaggio inviato a utenti esterni all'organizzazione?
C.4 Come trasmettere secondo modalità sicure un supporto mobile?
C.5 Come tenere traccia delle diverse comunicazioni?

C.1 Sicurezza della rete

La rete interna di un'organizzazione è sfruttata per diversi tipi di comunicazioni, per esempio dai collaboratori che fanno telelavoro oppure da terzi che la usano per accedere a determinati dati. Occorre dunque garantire la sicurezza della rete e delle comunicazioni. Poiché gli accessi avvengono generalmente via Internet, è indispensabile utilizzare protocolli di comunicazione sicuri. Il protocollo TLS (Transport Layer Security), successore del protocollo SSL (Secure Sockets Layer), permette di stabilire una comunicazione cifrata e quindi sicura tra client e server. Gli algoritmi e le chiavi crittografiche sono negoziati tra client e server. Il protocollo TLS permette inoltre alle due applicazioni (client/server) di autenticarsi reciprocamente scambiandosi i relativi certificati. Questo protocollo funge da substrato per i protocolli di comunicazione più comuni (http, ftp, ecc.). L'attivazione del protocollo avviene in maniera trasparente per l'utente; la sua presenza è segnalata semplicemente da un'icona a forma di lucchetto chiuso nella finestra della maggior parte dei browser.

Un altro modo per rendere sicuro l'accesso alla rete interna consiste nell'utilizzare connessioni VPN (Virtual Private Network – rete privata virtuale). Le reti private virtuali consentono di incapsulare i dati cifrati che devono essere trasmessi; queste reti si basano su protocolli crittografici forti (p. es. TLS, IPSec o SSTP).

Provvedimenti da considerare

- Le comunicazioni internet tra la rete interna e l'esterno devono essere limitate al minimo essenziale.
- Tenendo conto dei trattamenti da effettuare sui dati, occorre valutare la necessità di utilizzare un protocollo di comunicazione sicuro (TLS) e, all'occorrenza, procedere alla sua implementazione.
- Se collaboratori o terzi si collegano a distanza alla rete interna, deve essere stabilita una connessione VPN.

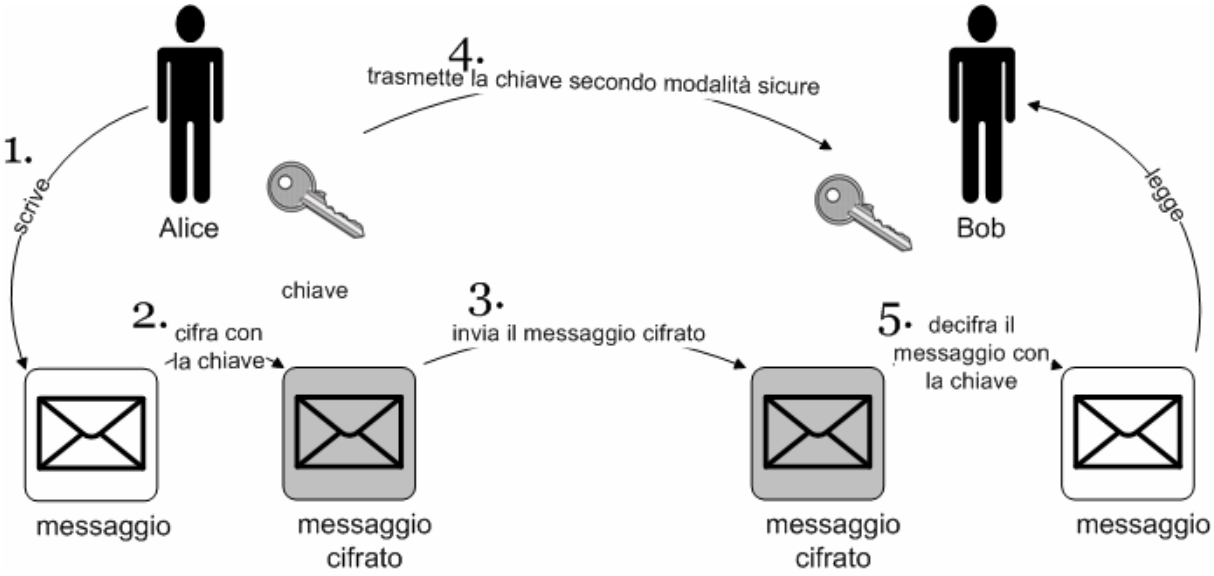
C.2 Cifratura dei messaggi

Oltre a cifrare i dischi duri e i file per impedire gli accessi indesiderati ai dati, occorre cifrare i messaggi in modo da evitare che, se la comunicazione è intercettata da terzi, il messaggio possa essere letto, modificato o cancellato.

Esistono due metodi per cifrare i messaggi: la cifratura simmetrica e quella asimmetrica.

La prima (illustrata nello schema qui sotto) funziona nel seguente modo:

1. Alice scrive un messaggio a Bob.
2. Alice cifra il suo messaggio per mezzo di una chiave pubblica.
3. Alice trasmette il messaggio cifrato a Bob.
4. Alice trasmette la chiave a Bob secondo modalità sicure.
5. Bob utilizza la chiave per decifrare il messaggio.



La cifratura simmetrica è più semplice perché prevede una sola chiave, che va tuttavia trasmessa secondo modalità sicure.

La cifratura asimmetrica è più complessa, ma evita i rischi di sicurezza legati alla trasmissione della chiave. Invece di una sola chiave, ogni utente ne genera due: una pubblica (a disposizione di tutti) e una privata (che soltanto l'utente conosce). La chiave pubblica è utilizzata per cifrare il messaggio e quella privata per decifrarlo. Questa tecnica consente inoltre di firmare i messaggi (cfr. sezione C3 − Firma dei messaggi).

La cifratura asimmetrica (illustrata nello schema qui sotto) funziona nel seguente modo:

1. Alice scrive un messaggio a Bob.
2. Alice utilizza la chiave pubblica di Bob per cifrare il messaggio e si assicura così che soltanto Bob possa leggerlo.
3. Alice invia il messaggio a Bob.
4. Bob utilizza la sua chiave privata per decifrare il messaggio.

Provvedimenti da considerare

- Occorre stabilire il tipo di cifratura più opportuno a seconda del grado di sensibilità dei dati e a seconda dei terzi che entrano in contatto con l'organizzazione.

- Se si opta per la cifratura simmetrica, occorre definire un protocollo sicuro per la trasmissione della chiave (l'e-mail, p. es., non è un mezzo sicuro).

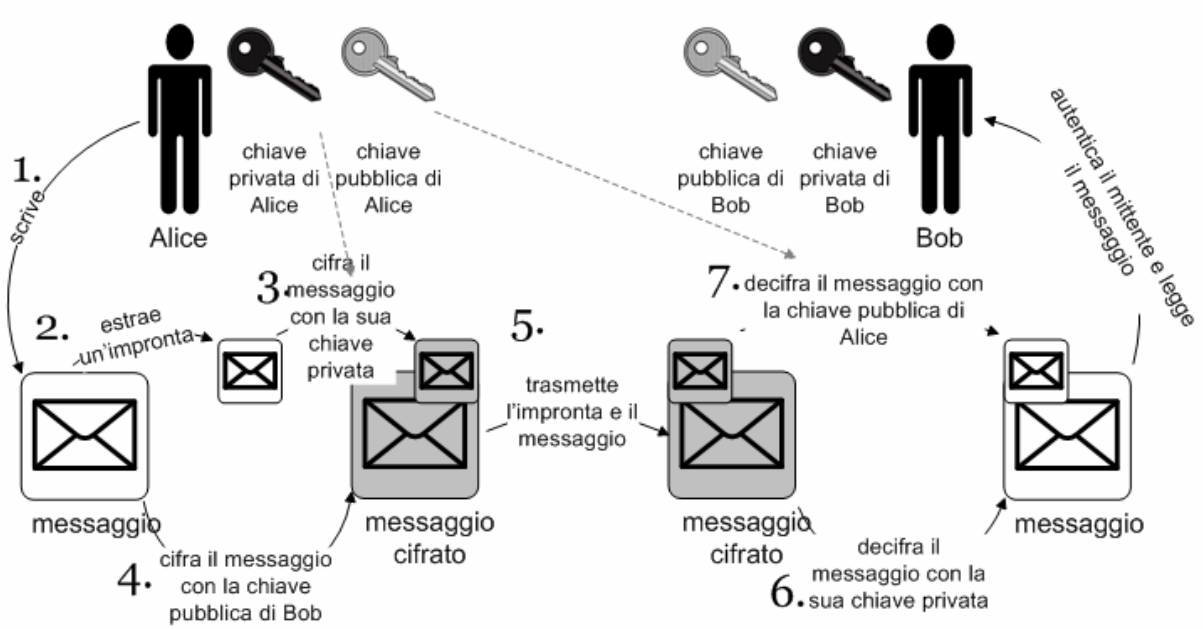
- Se si opta per la cifratura asimmetrica, occorre definire un meccanismo di cifratura dei messaggi, idealmente combinato con la firma dei messaggi (cfr. sezione C3 – Firma dei messaggi).

C.3 Firma dei messaggi

La cifratura dei messaggi (cfr. sezione C2 – Cifratura dei messaggi) consente di garantire che soltanto la persona che possiede l'apposita chiave sarà in grado di leggere il messaggio. Può tuttavia essere necessario fare anche in modo che il destinatario del messaggio possa confermare l'identità del mittente. La firma del messaggio consente di trasmettere questa informazione secondo modalità sicure.

Questa operazione è solitamente effettuata prima della cifratura del messaggio secondo il protocollo seguente:

1. Alice scrive un messaggio.
2. Alice estrae un'impronta dal messaggio. Questa impronta funge da firma.
3. Alice firma l'impronta utilizzando la sua chiave privata.
4. Alice cifra il messaggio seguendo la procedura descritta sopra.
5. Alice trasmette l'impronta e il messaggio a Bob.
6. Bob decifra il messaggio.
7. Bob verifica l'impronta con la chiave pubblica di Alice e si assicura così che Alice è effettivamente il mittente.



Provvedimenti da considerare

- I collaboratori sono debitamente informati delle situazioni in cui le comunicazioni devono essere firmate e cifrate.
- I collaboratori sanno come cifrare e firmare i messaggi.

C.4 Trasmissione dei supporti di dati

La trasmissione dei supporti di dati è un problema delicato poiché implica che una parte dei dati esca fisicamente dall'organizzazione per essere trasportata verso un altro luogo. È essenziale che questi supporti siano protetti durante il trasporto per evitare qualsiasi perdita o, nel caso più grave, furto, che si tradurrebbe nella divulgazione dei dati in questione. Quanto più i dati contenuti nei supporti sono degni di particolare protezione, tanto più è necessario che la trasmissione avvenga secondo modalità sicure.

Provvedimenti da adottare

- I destinatari dei supporti possono essere autenticati secondo modalità sicure.
- Prima di essere trasmessi, i supporti sono messi in busta chiusa seguendo una procedura sicura.
- Se necessario, i supporti mobili sono cifrati.
- Le modalità di trasporto dei supporti sono definite in modo chiaro (p. es. in valigette chiuse a chiave).
- Il principio dei quattro occhi permette di assicurare che la consegna e la ricezione dei dati avvengano correttamente. Per esempio, la persona che trasmette i dati e quella che li riceve combinano le loro password per accedere ai dati.

C.5 Giornalizzazione delle trasmissioni di dati

L'invio di dati via Internet e la trasmissione di supporti mobili possono essere protocollati e giornalizzati, così da poter risalire ai mittenti e ai destinatari nonché alle modalità di trasmissione. In caso di uso illecito, errato o di operazione inopportuna, è così possibile ritrovare una certa quantità di informazioni e ripercorrere il tragitto seguito dai dati dal momento in cui sono stati spediti a quello in cui si è presentato il problema.

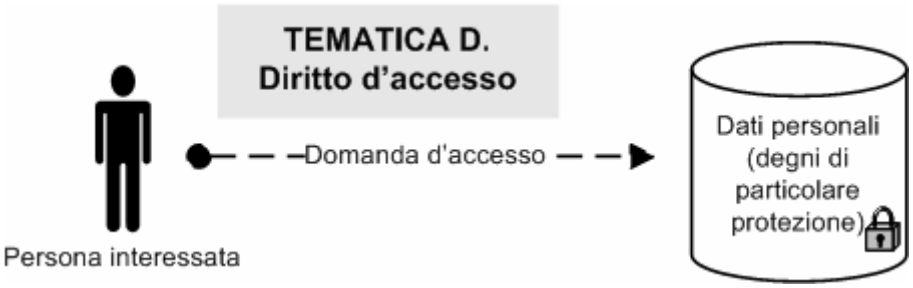
Le esigenze menzionate nella sezione B.2 – Giornalizzazione valgono ugualmente per la giornalizzazione delle trasmissioni di dati.

Provvedimenti da considerare

- Occorre definire una procedura di giornalizzazione molto precisa, nella quale siano riportati tutti i mittenti, i destinatari, il tragitto effettuato dai dati e i punti importanti del tragitto.
- La trasmissione dei supporti dovrebbe essere affidata sempre agli stessi collaboratori.
- La giornalizzazione va effettuata secondo il principio della proporzionalità, e in funzione della dimensione dei dati, della durata della trasmissione, ecc.

TEMATICA D: IL DIRITTO DI ACCESSO

Le persone interessate da questa tematica sono quelle i cui dati personali sono memorizzati nel sistema. Chiunque ha diritto di sapere se esistono dati personali che lo riguardano. In caso affermativo, la persona interessata può chiedere che questi dati siano distrutti o corretti nel caso in cui siano errati.



Schema D: diritto d'accesso

Nel quadro di questa tematica vengono analizzati i punti seguenti:

D.1 Come permettere alle persone interessate di esercitare il proprio diritto d'accesso?
D.2 Come garantire la riproducibilità delle procedure di esecuzione del diritto d'accesso?

D.1 Diritti delle persone interessate

Chiunque ha il diritto di accedere ai propri dati personali e di chiedere che vengano rettificati, bloccati o distrutti. L'organizzazione dev'essere in grado di ricevere ed elaborare queste richieste in modo appropriato. Le modifiche devono essere effettuate nel sistema al fine di garantire l'efficacia del meccanismo di ricerca dei dati personali. È inoltre importante che le operazioni siano espletate senza margine d'errore. Se, per esempio, qualcuno chiede che i suoi dati vengano distrutti, il sistema ne deve garantire la distruzione integrale.

Provvedimenti da considerare

- Occorre fornire informazioni chiare affinché tutti siano al corrente dei propri diritti.
- Esiste una procedura per le domande d'accesso e i collaboratori ne sono al corrente.
- Il sistema è munito di un meccanismo di ricerca affidabile.
- Le procedure di modifica, rettifica, blocco e distruzione dei dati sono documentate e affidabili.
- Tutti i trattamenti sono debitamente giornalizzati.

D.2 Riproducibilità delle procedure

La procedura che permette di rendere esecutivo il diritto d'accesso delle persone interessate deve essere definita in modo chiaro e riproducibile. Se il meccanismo è preimpostato nel sistema adibito al trattamento dei dati, tutti i collaboratori avranno la possibilità di rettificare, bloccare o distruggere dati, a seconda di quanto richiesto dalle persone interessate. La presenza di un meccanismo preimpostato è utile anche in caso di controlli da parte di autorità di sorveglianza in quanto permette di dimostrare l'applicabilità del diritto d'accesso.

Provvedimenti da considerare

- La procedura d'esecuzione del diritto d'accesso è preimpostata nel sistema.
- Tutti i collaboratori utilizzano la medesima procedura.
- Se necessario, l'autorità di sorveglianza può testare la procedura integrata nel sistema.

STRUMENTI ESISTENTI

Per ottimizzare l'applicazione dei provvedimenti tecnici e organizzativi sono disponibili alcuni strumenti.

Regolamento per il trattamento

Il regolamento per il trattamento è uno strumento previsto nel diritto svizzero e funge da ausilio nella definizione di provvedimenti tecnici e organizzativi adeguati. Lo scopo del regolamento consiste nell'assicurare la trasparenza necessaria durante l'elaborazione e la gestione di una collezione di dati personali. Nel regolamento vengono centralizzate le diverse informazioni, in quanto vi vengono riunite le varie procedure messe a punto dalle diverse unità incaricate del progetto. I responsabili della protezione dei dati e i fruitori del sistema possono così beneficiare di una giornalizzazione esaustiva, da cui attingere buone pratiche.

Il regolamento per il trattamento deve essere elaborato dal detentore di una collezione di dati.

Contenuto del regolamento

Se il detentore della collezione di dati è una persona privata, il regolamento per il trattamento deve contenere la descrizione dell'organizzazione interna e quella delle procedure di trattamento e di controllo dei dati, nonché i documenti relativi alla pianificazione, elaborazione e gestione dei mezzi informatici (hardware e software).

Se il detentore della collezione di dati è un organo federale, il regolamento per il trattamento deve essere elaborato soltanto se la collezione: contiene dati degni di particolare protezione o profili della personalità; è utilizzata da parecchi organi federali; è accessibile a terzi (p. es. Cantoni, autorità estere, organizzazioni internazionali o privati); è collegata ad altre collezioni di dati.

L'organo federale responsabile precisa il contenuto del regolamento. Questo include:

1. l'organizzazione interna – le operazioni effettuate dal sistema e la struttura dell'organizzazione – con menzione delle diverse responsabilità (protezione dei dati, detentore della collezione di dati, ecc.);
2. i documenti relativi alla pianificazione, all'elaborazione e alla gestione dei mezzi informatici, elaborati in modo trasparente;
3. una panoramica dei provvedimenti tecnici e organizzativi grazie alla quale sia possibile individuare quali provvedimenti sono già stati attuati;
4. la provenienza dei dati e lo scopo dei trattamenti;
5. tutte le indicazioni necessarie in ambito di obbligo di notifica;

6. la descrizione dei campi di dati, nonché una matrice che indichi le unità organizzative e gli utenti che hanno accesso ai dati;
7. la descrizione delle misure per l'esercizio del diritto d'accesso;
8. la configurazione dei mezzi informatici con menzione dei software e dell'hardware utilizzati.

Il regolamento è aggiornato periodicamente ed è messo a disposizione degli organi incaricati del controllo.

Per facilitare l'elaborazione del regolamento, l'IFPDT ha pubblicato sul suo sito il documento intitolato «Guida ai provvedimenti tecnici e organizzativi concernenti la protezione dei dati?» [2].

CONSIDERAZIONI FINALI

L'applicazione dei provvedimenti tecnici e organizzativi presentati in questa guida consente di assicurare una protezione adeguata dei dati. È tuttavia necessario tenere sempre in considerazione il contesto globale in cui si inserisce un progetto, la sua sensibilità, la quantità dei dati necessari, ecc.

Spetta al detentore della collezione di dati garantirne la protezione. Affrontando questo aspetto il prima possibile nella fase di elaborazione di un progetto, gli sarà possibile minimizzare i rischi. Grazie agli strumenti offerti dall'Incaricato federale della protezione dei dati e della trasparenza, il detentore della collezione potrà individuare tempestivamente i rischi intrinseci a un progetto e adottare quindi le misure preventive già in fase di definizione delle specifiche del progetto.

[2] www.lincaricato.ch > Documentazione > Protezione dei dati > Opuscoli > Provvedimenti tecnici e organizzativi