EOS di Manlio Morini
Soluzioni informatiche per l'impresa

Via dell'Argine, 11 (loc. Colignola)
56017 San Giuliano Terme (PI)

OSSERVAZIONI RIGUARDANTI IL DISCIPLINARE TECNICO

Terminologia

Il codice[1] distingue tra trattamenti effettuati con:

- strumenti **elettronici**, termine nel quale la lettera b) del comma 3 dell'articolo 4 fa rientrare gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- strumenti **diversi da quelli elettronici**: faldoni nei quali sono racchiuse pratiche, schedari nonché simili, e tuttora assai diffusi nonostante si sia in piena rivoluzione virtuale, mezzi tradizionali di annotazione, conservazione e consultazione di informazioni e dati.

Le misure minime di sicurezza per i trattamenti effettuati con strumenti elettronici sono prescritte dall'articolo 34 del codice privacy, e sviluppate nei punti da 1 a 26 del disciplinare tecnico: in tale categoria rientrano gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento. In sostanza il codice stabilisce "cosa fare" mentre al disciplinare è demandato il "come fare".

Il Codice intende per:

- "**autenticazione informatica**"[2], 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. Alcuni esempi di credenziale sono l'impronta digitale, la forma della mano, l'iride, la retina, la voce (caratteristiche **biometriche**), certificati digitali memorizzati su smart card, un codice identificativo (*username*) associato ad una *password*.
- "**profilo di autorizzazione**", l'insieme delle informazioni associate ad una persona, che consente di individuare a quali dati e a quali trattamenti la stessa può accedere.

E' bene precisare la differenza tra **autenticazione** ed **autorizzazione**: il sistema di autenticazione, si accerta dell'identità dell'utente, al fine di consentire o meno l'acceso al computer; **con il sistema di autorizzazione si stabilisce a quali dati del computer l'incaricato può accedere**, dopo che è entrato, e quali azioni (trattamenti) può compiere.

Autenticazione, codici identificativi e password

Visto che sistemi di autenticazione basati sulla coppia username+password, risultano fra i più rapidi ed economici da approntare, è utile approfondire l'argomento.
Il **codice per l'identificazione dell'incaricato** è il nome grazie al quale l'utente viene riconosciuto dal sistema; deve essere **unico per ogni incaricato**, non può essere assegnato a differenti incaricati anche in tempi diversi e, eventualmente, **deve essere disattivato se non usato per più di sei mesi o se l'incaricato perde tale qualifica**.

Esempio: uno studio si avvale di tre dipendenti Alberto, Giovanni e Maria; Alberto viene nominato responsabile e gli altri due incaricati al trattamento. A tutti e tre viene assegnato come nome utente il loro nome di battesimo e quindi: "Alberto", "Giovanni", "Maria". Dopo tre mesi Maria si licenzia. Il titolare dovrà preoccuparsi di disattivare l'account (il nome utente) "Maria", in quanto l'incaricato ha perso tale qualifica. Passano altri due mesi viene assunta una nuova

1 *Il decreto di legge sulla privacy con particolare riferimento all'allegato B ("Disciplinare tecnico").*
2 *Crittografia e Scienza dell'Informazione, definiscono "identificazione" quello che il disciplinare tecnico chiama "autenticazione" e attribuiscono al termine "autenticazione" un significato più forte: non solo identificazione ma anche verifica della correttezza del flusso di dati scambiati fra sistema ed operatore. In questo documento ci atteniamo alla terminologia del decreto di legge sulla Privacy e del relativo allegato tecnico.*

dipendente anch'essa dal nome Maria. Il titolare non può assegnarle come nome utente "Maria" perché già utilizzato in precedenza.

La **Parola chiave** è la tipica password. Si tratta di una parola segreta conosciuta solo dall'incaricato che permette di verificare che l'utente che chiede di accedere al sistema sia proprio la persona associata al codice identificativo di cui sopra. Il Disciplinare prevede che agli incaricati debbano essere impartite precise istruzioni scritte su come elaborare la password, e conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione. La parola chiave dovrà:

- essere costituita da almeno **otto caratteri** o comunque dal numero di caratteri consentiti dal sistema se inferiore a otto, e non deve contenere riferimenti direttamente riconducibili all'incaricato: non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici. E' buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica.
- **essere modificata al primo utilizzo**, non appena comunicata per la prima volta da chi amministra il sistema e, successivamente, **ogni sei mesi nel caso di dati personali**, mentre **nel caso di dati sensibili o giudiziari** la modifica dovrà intercorrere **ogni novanta giorni**. Nessun altro, neppure il titolare del trattamento, può accedere allo strumento elettronico, utilizzando la credenziale di autenticazione dell'incaricato. Eccezione a tale regola si ha solo se verificano congiuntamente le seguenti condizioni:
  - **prolungata assenza o impedimento dell'incaricato, l'intervento è indispensabile;**
  - **vi sono** concrete **necessità**, di operatività e di **sicurezza del sistema**. E' evidente che il titolare deve prendere le opportune misure, per essere in grado di accedere ai dati ed agli strumenti, al verificarsi delle condizioni sopra esposte. A tale fine, **agli incaricati devono essere fornite istruzioni scritte**, affinché:
    - predispongano una copia della parola chiave, provvedendo quindi a trascriverla, facendo però in modo che l'informazione resti segreta (ad esempio, inserendola in una busta chiusa e, possibilmente, sigillata);
    - consegnino tale copia ad un soggetto, che sia stato previamente incaricato della sua custodia (**l'incaricato per la custodia delle parole chiave**). Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere, all'incaricato per la custodia, la busta che la contiene. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

Inoltre, sebbene il disciplinare tecnico non entri in ulteriori dettagli, riteniamo importante che gli operatori siano edotti circa i rischi derivanti da:

- memorizzazione di credenziali per l'accesso a siti internet sfruttando l'apposito meccanismo offerto dai sistemi operativi Windows. Chiunque abbia accesso alla postazione di lavoro può recuperare dette credenziali con estrema facilità;
- utilizzazione delle stesse credenziali per l'autenticazione su sistemi differenti;
- principali tecniche di "spoofing" (furto di credenziali realizzato mediante e-mail e siti fraudolenti);
- installazione di software senza l'autorizzazione dell'amministratore di sistema. Oltre alle problematiche legate a virus ed affini, va evidenziata la perdita di sicurezza derivante dall'installazione di programmi per la condivisione di file o la tele-assistenza.

Profili di autorizzazione

L'individuazione di diversi profili di autorizzazione per gli incaricati può non sempre essere un obbligo: ad esempio, in uno studio professionale nel quale lavorano cinque impiegati in tutto, si può decidere di non impostare alcun profilo di autorizzazione, per cui ognuno potrà accedere a tutti i dati personali contenuti nella rete. Questa soluzione è sicuramente la più semplice e rapida da realizzare, specie considerando che determinati sistemi operativo e/o software applicativi non permettono una adeguata configurazione. D'altra parte, si deve considerare che, per ottemperare correttamente alle disposizioni privacy, con particolare riferimento a quella che impone di dare accesso agli incaricati ai soli dati personali

necessari per svolgere le mansioni lavorative, è generalmente necessario predisporre, profili di autorizzazione che coprano ambiti diversi: ad esempio, in una impresa relativamente piccola non sarebbe in alcun modo giustificabile che un impiegato dell'ufficio acquisti possa accedere ai dati personali relativi ai dipendenti.

Altre disposizioni dettate dal disciplinare tecnico

Lo strumento elettronico **non dovrà essere lasciato incustodito e accessibile durante una sessione di trattamento qualora l'incaricato debba assentarsi** dalla propria postazione per un periodo più o meno prolungato. Il "trattamento" non consiste infatti solo nella modifica o copia del dato: anche la semplice presa visione può essere considerata, a tutti gli effetti, trattamento. Da tale prescrizione non consegue l'obbligo di terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare. Si devono però mettere in atto accorgimenti tali, per cui anche in quei cinque minuti il computer non resti:

- **incustodito**, può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico;
- **accessibile**, può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno. Altra soluzione potrebbe essere l'utilizzo di uno screensaver con password.

Il disciplinare prevede l'obbligo di proteggere i dati personali **contro il rischio di intrusione** e dall'azione di programmi che possono portare al **danneggiamento di un sistema informatico**, dei dati o dei programmi in esso contenuti. Per ovviare al pericolo di intrusione informatica e cioè di tentavi dall'esterno di accesso non autorizzato al nostro sistema informatico ci si può affidare ai **firewall**. I firewall sono dei sistemi di tipo hardware o software. Il loro lavoro in sostanza lo si può paragonare ad un guardiano che vigila la porta che utilizziamo per "uscire" dal nostro sistema informatico per accedere ad altri (ad esempio ogni qualvolta navighiamo in internet), impedendo che "qualcuno" non autorizzato possa entrare di soppiatto.

Per quanto riguarda il pericolo di danneggiamento di un sistema informatico è chiaro che si sta facendo riferimento all'azione dei **virus informatici**. La norma impone di difendersi impiegando uno dei vari software antivirus in commercio, purtroppo conservando ancora per l'aggiornamento il lasso di tempo previsto dalla vecchia 675/96 che già fu motivo di ilarità tra gli operatori della sicurezza: ossia la cadenza **"almeno semestrale**". Fortunatamente gli antivirus di ultima generazione utilizzano un sistema di aggiornamento automatico che consente di essere tempestivamente protetti appena un nuovo virus viene messo in circolazione.
Ulteriori disposizioni riguardano l'aggiornamento dei "**programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti**", che dovrà essere effettuato **annualmente** o, nel caso si trattino dati sensibili o giudiziari, semestralmente. Tra i principali punti di debolezza di un sistema informatico va sicuramente annoverato il sistema operativo: sfruttando gli eventuali errori presenti (bug) degli estranei potrebbero, riuscire a guadagnare l'accesso al sistema. La contromisura da adottare è l'aggiornamento costante dei prodotti non appena viene scoperto un bug: tale procedura è nota come installazione di patch. I nuovi sistemi operativi, come ad esempio Windows XP, hanno incorporato una funzione automatica che avvisa quando la casa madre ha rilasciato una nuova "patch" sollecitando l'utente alla sua installazione.

Adozione tecniche di cifratura o di codici identificativi

Agli organismi sanitari, siano essi pubblici o privati, e agli esercenti le professioni sanitarie, che trattano dati sensibili idonei a rivelare lo **stato di salute o la vita sessuale**, si impone l'adozione di tecniche di cifratura o l'utilizzo di codici identificavi allo scopo di rendere i dati difficilmente interpretabili.
Riguardo agli algoritmi crittografici, non esistendo indicazioni precise nel disciplinare tecnico, riteniamo opportuno attenersi alle indicazioni del progetto europeo NESSIE (New European Scheme for Signatures, Integrity and Encryption).

EOS di Manlio Morini
Soluzioni informatiche per l'impresa

Via dell'Argine, 11 (loc. Colignola)
56017 San Giuliano Terme (PI)

Backup

Per quanto concerne la previsione di "**istruzioni organizzative e tecniche che prescrivano il salvataggio dei dati**" con una cadenza almeno **settimanale**, si devono impartire istruzioni che facilitino il cosiddetto **disaster recovery**: il recupero dei dati al verificarsi di eventi atti a distruggerli deve essere sempre previsto per far si' che, in caso di problemi, non venga meno uno degli obiettivi principali della sicurezza nel trattamento dei dati (la disponibilità dei dati stessi).
Ai supporti rimovibili (es: cdrom, floppy) contenenti dati sensibili o giudiziari è richiesta una particolare attenzione. Questi devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati e trattamenti non consentiti: ad esempio, si potranno impartire istruzioni, affinché essi vengano conservati in cassetti chiusi a chiave e successivamente, quando è cessato lo scopo per cui sono stati memorizzati, i dati dovranno essere cancellati. I cdrom non riscrivibili dovranno essere distrutti. Si consiglia di seguire le prescrizioni in commento anche per i supporti contenenti solo dati comuni.
Per quanto riguarda il backup di dati sensibili e giudiziari, l'organizzazione deve essere in grado di provvedere in ogni caso al ripristino dei dati entro **sette giorni**. I soggetti esterni che, professionalmente, assistono il titolare nella predisposizione ed installazione delle misure minime di sicurezza, devono rilasciare un certificato di conformità, nel quale devono descrivere quale sia stato l'intervento effettuato. La disposizione è atta a garantire la serietà degli interventi, rispetto a quanto richiesto dal disciplinare tecnico.

L'esperienza aziendale evidenzia come la "best practice" per minimizzare il MTTR (Mean Time To Recovery) consista nell'effettuare backup differenziali o incrementali infrasettimanali ed un backup completo settimanale, preferibilmente su dispositivi ottici.
L'opportunità di effettuare copie infrasettimanali dei dati di un elaboratore su un altro, collegato in rete, va valutata situazione per situazione, non perdendo di vista i rischi per la sicurezza che possono derivarne. Se lo scopo è quello di migliorare "availability" e "dependability" dell'impianto di elaborazione, solitamente risulta più opportuno investire in un sistema centralizzato ridondante.

Interventi formativi

Gli **interventi formativi degli incaricati del trattamento** devono essere programmati in modo tale, che essi abbiano luogo almeno al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti rispetto al trattamento di dati personali.

Gli interventi formativi, che possono avvenire all'interno e/o presso soggetti esterni specializzati, devono essere finalizzati a rendere gli incaricati edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

EOS di Manlio Morini
Soluzioni informatiche per l'impresa

Via dell'Argine, 11 (loc. Colignola)
56017 San Giuliano Terme (PI)

ALLEGATO B.
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA[1]

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata 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.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. 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.
5. 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.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

1 *Artt. da 33 a 36 del codice.*

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. 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.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19 Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1 l'elenco dei trattamenti di dati personali;

19.2 la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3 l'analisi dei rischi che incombono sui dati;

19.4 le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5 la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6 la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7 la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8 per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali

dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni 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.
22. 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.
23. Sono adottate 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.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone p rive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registra te. Quando gli archivi non sono dotati di strumenti

elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

EOS di Manlio Morini
Soluzioni informatiche per l'impresa

Via dell'Argine, 11 (loc. Colignola)
56017 San Giuliano Terme (PI)

STANDARD, PROGETTI ED ORGANIZZAZIONI D'INTERESSE

- NESSIE (New European Schemes for Signatures, Integrity and Encryption). In proposito si può consultare il sito http://www.cosic.esat.kuleuven.ac.be/nessie/
- ISO/IEC 17799:2005 (Information technology – Security techniques);
- ISO 27001:2005 (Information security management systems – Requirements);
- CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione). http://www.cnipa.it