INVITALIA

Agenzia nazionale per l'attrazione
degli investimenti e lo sviluppo d'impresa SpA

Tutela dei dati personali in Invitalia - Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa S.p.A.

Messa a Norma

Estratto del Documento Programmatico sulla Sicurezza dei Dati Personali

Roma, 26 marzo 2010

INVITALIA

Contenuto

1. Introduzione ... 5
1.1. Scopo del documento ... 6
1.2. Principi generali ... 7
1.3. Definizioni ... 8
1.3.1. Dato ... 8
1.3.2. Dato pubblico ... 8
1.3.3. Dato particolare (sensibile e giudiziario) ... 8
1.3.4. Banca dati ... 8
1.3.5. Misure di sicurezza ... 8
1.3.6. Risorse informative ... 8
1.3.7. Archivi ... 9
Archivi informatici ... 9
Archivi cartacei ... 9
Archivi critici ... 9
1.3.8. Aree aziendali ... 9
1.3.9. Aree ad accesso controllato ... 9
1.3.10. Risorse critiche del sistema operativo ... 10
1.3.11. Supporti di memorizzazione ... 10
1.3.12. Informazioni residue ... 10
1.3.13. Connessioni con l'esterno ... 10
1.3.14. Gateway ... 10
1.3.15. Zona demilitarizzata (DMZ) ... 11
1.3.16. Incidenti di sicurezza ... 11
1.4. Documentazione di riferimento ... 11
2. Organizzazione e responsabilità ... 12
2.1. Titolare del trattamento ... 12
2.2. Responsabile del trattamento di dati personali, di seguito chiamato Responsabile ... 13
2.3. Funzione privacy e responsabile gestione delle istanze degli interessati ... 13
2.4. Responsabile dei trattamenti informatici ... 14
2.5. Amministratori di Sistema ... 14
2.6. Incaricati del trattamento ... 15
2.7. Funzione amministratrice ... 15
2.8. Amministrazione della sicurezza degli Applicativi ... 15
2.9. Autorità di sistema e di amministrazione della sicurezza ... 16
2.9.1. Definizioni ... 16
3. Lista dei trattamenti ... 16
4. Analisi dei rischi ... 16
4.1. Aree di analisi ... 17
4.2. Valutazione delle minacce ... 20
4.3. Indici di rischi ... Errore. Il segnalibro non è definito.
4.4. Sintesi della valutazione del rischio ... Errore. Il segnalibro non è definito.
5. Prescrizioni di sicurezza ... 20
5.1. Definizione e protezione delle risorse ... 20
5.1.1. Proprietà delle risorse ... 20
5.1.2. Tipologia delle risorse ... 20
5.1.3. Protezione dei dati personali comuni e sensibili o giudiziari ... 21
5.1.4. Protezione dei dati riservati Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa ... 21
5.1.5. Risorse del sistema operativo ... 21

INVITALIA

5.1.6. Sistema di autenticazione 21
5.1.7. Assegnazione delle User-Id 22
5.1.8. Gestione del personale esterno 22
5.1.9. Revoca delle user-id 22
5.1.10. User-id inattive 22
5.1.11. User-Id di manutenzione 23
5.1.12. Convalida annuale 23
5.2. Password 23
5.2.1. Regole generali delle password 23
5.2.2. Numero tentativi di accesso con password invalide 24
5.2.3. Ripristino della password 24
5.3. Sistema di autorizzazione 24
5.4. Integrità e disponibilità dei dati 24
5.4.1. Access control 24
5.4.2. Integrità delle workstation e dei server 25
5.4.3. Integrità del sistema operativo 25
5.4.4. Ambienti di sviluppo e di manutenzione 25
5.4.5. Integrità delle librerie applicative 26
5.4.6. Programmi pericolosi 26
5.4.7. Aggiornamento dei programmi critici per la sicurezza 26
5.4.8. Altre Misure 26
5.5. Connessioni con l'esterno 27
5.5.1. Gateway 27
5.5.2. Caratteristiche di sicurezza 27
5.5.3. Server posti nella zona demilitarizzata (dmz) 28
Norme generali 28
5.6. Procedure di Backup 28
5.7. Piano di Backup/recovery 29
5.8. Sicurezza fisica 29
5.8.1. Aree Agenzia Nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa 29
5.8.2. Aree ad accesso controllato 30
5.8.3. Regole di gestione 30
5.8.4. Apparecchiature informatiche ed archivi critici 30
5.8.5. Supporti di memorizzazione 31
5.8.6. Informazioni residue 31
5.8.7. Stampanti e Fax 31
6. Piano di formazione 32
7. Sistemi dati in outsourcing 33
7.1. Norme di sicurezza aggiuntive 33
8. Attuazione del provvedimento sugli Amministratori di Sistema 35
9. Norme per gli incaricati del trattamento 36
9.1. Norme di carattere generale 36
9.2. Uso delle Workstation 36
9.3. Uso delle password 37
9.4. Uso dei modem 37
9.5. Internet 38
9.6. Antivirus 38
10. Archivi cartacei 39
10.1. Sicurezza fisica 39

INVITALIA

10.2. Accesso agli archivi 39
10.3. Copie e riproduzioni 39
11. Verifica dello stato della sicurezza 40
11.1. Verifiche dell'architettura di sicurezza 40
11.2. Test di intrusione 40
11.3. Processo di prevenzione e allarme (alert) 40
11.4. Attacchi sistematici 41
11.5. Incidenti di sicurezza 41
11.6. Gestione dei Log 41
11.6.1. Log degli accessi ai sistemi 41
11.6.2. Log di accesso ai dati e agli strumenti 41
11.6.3. Log delle attività 41
11.6.4. Login invalidi 42
11.6.5. Log di accesso alle risorse 42
11.6.6. Gestione dei archivi che contengono il log 42
12. Disponibilità, da parte dell'azienda, degli strumenti e dei dati affidati al dipendente 42
13. Controlli e audit 43
13.1. Audit formale 43
13.2. Verifiche periodiche 43
14. Società partecipate del Gruppo 43
14.1. Responsabile del trattamento 43
14.2. Trattamenti informatici 44
14.3. Incaricati del trattamento 44
14.4. Amministratori dei sistemi informatici 44
14.5. Norme per gli incaricati 44
14.6. Verifiche ed Audit 44
15. Società Regionali, di scopo e partecipate interessate dal processo di dismissione 45
16. Revisione del documento programmatico sulla sicurezza 45

1. Introduzione

Il "Piano di riordino, dismissione" e riassetto delle partecipazioni dell'Agenzia approvato dal Ministro dello Sviluppo Economico con decreto del 31 luglio 2007, è nell'anno in corso, ancora in fase di attuazione.

Infatti, l'articolo 23, comma 5 del D.L. 1° luglio 2009 n. 78, convertito dalla legge n. 102 del 2009, ha concesso una ulteriore proroga del termine per consentire il completamento delle attività connesse alla cessione delle società regionali dell'Agenzia alle Regioni.

Per quanto concerne, invece, le altre società partecipate dall'agenzia, come disposto dalla legge 296/2006 si segnala che sono state avviate attività di riordino volte all'accorpamento di alcune società del gruppo.

Il 21 dicembre 2009 ha avuto luogo la fusione per incorporazione di Sviluppo Italia Engineering in INVITALIA RETI. S.p.A, con efficacia dal 31 dicembre 2009, la quale ha emesso il primo Documento Programmatico della Sicurezza per il 2010 redatto nel rispetto della scadenza prevista dal punto 19 del Disciplinare tecnico in Allegato B al decreto legislativo 196/2003 (codice privacy, in seguito abbreviato D.lgs 196/2003), tenendo conto delle Misure di Sicurezza adottate dalla capogruppo, INVITALIA Agenzia nazionale per l'attrazione degli investimenti e la creazione di impresa.

Si evidenzia, inoltre, che il 30 novembre 2009 è stata istituita INVITALIA PARTECIPAZIONI S.p.A. la cui sede legale ed operativa si trova presso la sede di INVITALIA, Agenzia nazionale per l'attrazione degli investimenti e la creazione d'impresa S.p.A., e, pertanto, Invitalia Partecipazioni, che non ha proprio personale, si avvale in toto delle misure di Sicurezza adottate dalla Capo Gruppo.

Conseguentemente non tutte le implicazioni derivanti dai mutamenti societari sono state rese effettive nell'ambito dei trattamenti dei dati personali.

1.1. Scopo del documento

Scopo di questo documento (di seguito “DPS”) è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare presso Invitalia Agenzia per l’attrazione degli investimenti e lo sviluppo d’impresa S.p.a. (di seguito Agenzia) affinché siano rispettati gli obblighi, in materia di sicurezza, previsti dalla legge 196/2003 Codice della Privacy (di seguito chiamata Codice della Privacy o anche Legge), e dal Disciplinare tecnico relativo alle misure minime di sicurezza obbligatorie per il trattamento dei dati personali contenuti in qualsiasi documentazione, cartacea od in formato elettronico (di seguito Disciplinare).

È, inoltre, scopo del presente documento, definire le protezioni di sicurezza per le altre informazioni di cui la Agenzia è proprietaria e che non sono assoggettate alla suddetta Legge ma che sono critiche per l’attività di Agenzia (di seguito chiamate informazioni aziendali).

Questo documento è valido per tutti quei trattamenti di cui Agenzia è Titolare e per quelli di cui Agenzia è nominata Responsabile dalle altre società dello stesso Gruppo (Società Regionali/Soc. di scopo o Partecipate) o da altri Titolari terzi, senza avere ricevuto da questi ultimi esplicite indicazioni più restrittive in materia.

1.2. Principi generali

Il presente DPS si applica a tutte le strutture della Agenzia ed il suo contenuto deve essere divulgato a tutti anche attraverso adeguati momenti informativi e formativi.

Tutti i dipendenti della Agenzia devono rispettare le prescrizioni in esso contenute ed operare, nell'ambito della propria organizzazione, in modo da:

- Minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi cartacei contenenti dati personali o aziendali.
- Minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali o aziendali.
- Minimizzare la probabilità che i trattamenti dei dati personali o aziendali siano modificati senza autorizzazione.

NOTA: poiché dati personali, sia comuni, sia sensibili e giudiziari sono presenti negli stessi ambienti e sugli stessi supporti di elaborazione, l'Agenzia ha deciso che, in attesa di procedere ad una loro differenziazione, le misure indicate nel presente documento per i dati sensibili e giudiziari si applichino indifferentemente ad entrambi i tipi di informazioni.

1.3. Definizioni

1.3.1. Dato

Qualunque informazione relativa a persona fisica , persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

1.3.2. Dato pubblico

Dato proveniente da Pubblici Registri, elenchi, atti o documenti conoscibili da chiunque.

1.3.3. Dato particolare (sensibile e giudiziario)

Dato idoneo a rivelare:

- L'origine razziale ed etnica;
- Le convinzioni religiose, filosofiche o di altro genere;
- L'adesione a partiti, sindacati, associazioni, organizzazioni a carattere religioso, filosofico, politico o sindacale;
- Lo stato di salute e la vita sessuale;
- La posizione giudiziaria.

1.3.4. Banca dati

Qualunque complesso di dati, personali o di altro tipo, organizzati secondo una pluralità di criteri per il trattamento.

1.3.5. Misure di sicurezza

Il complesso delle misure tecniche, informatiche organizzative, logistiche e procedurali volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

1.3.6. Risorse informative

Le informazioni oggetto dei trattamenti dei dati personali sono chiamate "Risorse personali" e sono classificate in:

- Risorse o dati personali comuni;
- Risorse o dati personali sensibili e giudiziari.

Le informazioni oggetto dei trattamenti dei dati aziendali sono chiamate "Risorse aziendali" e sono classificate in:

- Risorse e dati aziendali pubblici;
- Risorse e dati aziendali per uso interno;
- Risorse e dati aziendali riservati.

Le risorse sono classificate, in base alle procedure in vigore, a cura dei rispettivi proprietari.
E' responsabilità dei proprietari individuare i dati personali sensibili e giudiziari e i dati aziendali riservati ed informare gli Amministratori di sistema della loro collocazione.

1.3.7. Archivi

Gli archivi che contengono le risorse informative possono essere informatici o cartacei.

Archivi informatici

Gli archivi informatici si presentano, ad esempio, nei seguenti supporti: dischi fissi e rimovibili di Personal Computer (Client e Server), dischi dell'elaboratore centrale, Compact Disk (CD), DVD, nastri magnetici, supporti ottici ed altri minori.

Archivi cartacei

Sono definiti archivi cartacei tutti i supporti, ad esclusione di quelli informatici, che contengono in qualunque forma dati o informazioni personali incluse le copie, su carta, di dati gestiti con supporti informatici. Sono inclusi in questa tipologia, oltre ai dati su carta o supporto analogo, le foto, le microfiches, i film, i video tape, ecc comprese le copie, anche parziali, su supporti non informatici, di banche dati gestiti in modo automatizzato.

Archivi critici

Sono definiti archivi critici gli archivi, informatici e non, che contengono dati o informazioni personali sensibili e giudiziari o informazioni aziendali riservate.

1.3.8. Aree aziendali

Sono definite "Aree aziendali" tutti i locali sotto la responsabilità di una delle strutture costituenti la Agenzia, nei quali si svolgono le normali operazioni aziendali.
Ai fini della sicurezza sono considerate aree aziendali anche i locali o gli armadi situati presso terzi (ad esempio presso fornitori, ….) e comunque utilizzati da personale dell' Agenzia.

1.3.9. Aree ad accesso controllato

Sono definite "**Aree ad Accesso Controllato**" quei locali all'interno delle "**Aree aziendali**" che contengono **archivi critici** o **apparecchiature informatiche critiche**, come in seguito definite.

1.3.10. Risorse critiche del sistema operativo

Gli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati (es. log di sistema, tabelle di servizio, cataloghi dei dati, etc.) sono chiamate "**Risorse critiche del sistema operativo**".

1.3.11. Supporti di memorizzazione

Sono considerati supporti di memorizzazione, a titolo esemplificativo, i nastri magnetici, i dischi magnetici (floppy disk) o ottici rimovibili o DVD e i CD-ROM che contengono informazioni personali o aziendali.

1.3.12. Informazioni residue

Sono definite "Informazioni Residue" quei dati personali ancora leggibili dopo la cessazione di un trattamento (es. registrazioni su nastri o dischi magnetici).

1.3.13. Connessioni con l'esterno

Sono considerate connessioni con l'esterno:

Interconnessioni tra il servizio IT di Agenzia o delle consociate incluse nella rete interna aziendale ed il servizio elaborazione dati di altre consociate, aziende terze, clienti, outsourcer o fornitori di servizi Internet.

Accesso remoto da parte di dipendenti di Agenzia o di altre aziende (fornitori, consociate, clienti).

1.3.14. Gateway

E' definito Gateway per le interconnessioni esterne l'insieme di hardware, software e applicazioni che permettono l'interconnessione o l'accesso remoto.

I gateway di interconnessione esterna devono essere sotto il controllo di Agenzia e approvati dal Responsabile dei trattamenti Informatici.

Caratteristiche di sicurezza:

Gli accessi in ingresso devono essere verificati con user-Id/password o altra tecnica di autenticazione.

Non deve essere permesso l'accesso ai Firewall da workstation collegate alla LAN interna, ma solo da workstation locali.

Deve esserci un processo per rilevare eventuali attacchi di massa al gateway.

Deve esserci un processo per disattivare gli utenti che non necessitano più del collegamento dall'esterno.

Le utenze abilitate devono essere verificate e riconfermate almeno ogni 12 mesi.

Nel caso di interconnessioni con altri sistemi esterni, deve esserci un controllo per verificare l'identità della controparte ad ogni attivazione del collegamento.

I collegamenti Dial dall'esterno devono avvenire tramite un gateway approvato dal Responsabile dei trattamenti Informatici.

Linee Dial da/per l'esterno non devono essere collegate alle Workstation individuali senza approvazione. Nel caso il collegamento sia di tipo TCP/IP tramite modem, non deve essere permesso il suo uso simultaneamente al collegamento interno, a meno che siano stati disattivati quei comandi che permettono l'utilizzo della workstation come link per collegarsi con la rete interna.

1.3.15. Zona demilitarizzata (DMZ)

E' definita zona demilitarizzata (DMZ) quella zona della rete informatica nella quale sono collegate alcune apparecchiature accessibili da reti esterne a quella aziendale.

I server posti nella zona demilitarizzata (DMZ) sono tipicamente Web Server e Data Server e per questi e per i Firewall valgono totalmente le regole definite in questo documento.

1.3.16. Incidenti di sicurezza

In linea generale è definito *incidente di sicurezza* qualunque evento inaspettato che riguardi l'integrità, la riservatezza o la disponibilità delle informazioni.

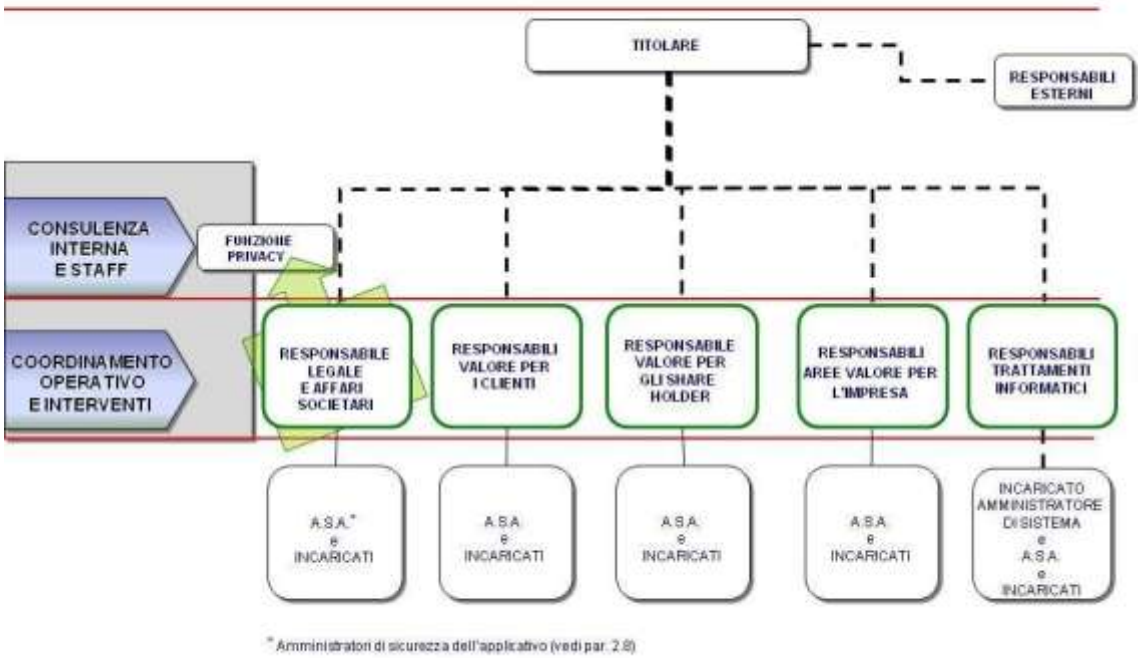
1.4. Documentazione di riferimento

Omissis

2. Organizzazione e responsabilità

I termini Titolare del trattamento, Responsabile del trattamento, Incaricato del trattamento e Dati Personali sono usati in conformità alle definizioni del Codice.

Modello Organizzativo di Invitalia - Agenzia nazionale per l'attrazione degli investimenti esteri e lo sviluppo d'impresa



2.1. Titolare del trattamento

Al Titolare competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali.

- Ha il compito di vigilare, anche tramite verifiche periodiche, sul rispetto, da parte dei Responsabili, delle proprie istruzioni, nonché sull'osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. A tal fine promuove e garantisce l'esecuzione del programma di audit.

Il Titolare, inoltre, garantisce, ai Responsabili di trattamento ed al Responsabile della sicurezza delle informazioni, il supporto in termini di adeguati budget e deleghe di autorità, affinché possano svolgere in autonomia e responsabilità i compiti affidati.

2.2. Responsabile del trattamento di dati personali, di seguito chiamato Responsabile

Il Responsabile dei trattamenti dei dati personali ha le seguenti responsabilità:

- Promuovere lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel Documento Programmatico sulla Sicurezza dei Dati Personali.
- Informare il Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.
- Garantire lo svolgimento di un continuo processo di addestramento degli Incaricati del Trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza.
- Monitorare il rispetto delle misure di sicurezza relative agli archivi non automatizzati
- Collabora al programma di audit
- Valutare almeno annualmente, nell'ambito della proprie responsabilità, il livello di rischio cui sono soggetti i dati personali oggetto di trattamento .

2.3. Funzione privacy e responsabile gestione delle istanze degli interessati

La Funzione Privacy – all'interno della Direzione affari legali e dismissioni ha il compito di curare il collegamento dei ruoli privacy aziendali alla struttura aziendale, in grado di attraversare tutta l'organizzazione, a partire dal vertice aziendale e presidiare la corretta gestione dei rapporti con i fornitori di servizi, che fanno un significativo utilizzo di informazioni per conto dell'Azienda.

In azienda la Funzione privacy coincide con il Responsabile Gestione delle istanze degli interessati che ha il compito di gestire:

La raccolta delle informazioni contenute nelle istanze di accesso e negli altri tipi di istanze avanzate da parte dell'interessato;

La comunicazione di queste istanze agli altri Responsabili e/o Incaricati nominati dal Titolare che si presume trattino o abbiano trattato dati personali dell'istante, al fine di raccogliere le informazioni necessarie per la soddisfazione delle istanze o comunicare le richieste di blocco o di cancellazione o le altre richieste che possano giuridicamente ritenersi accettabili;

La raccolta di eventuali informazioni da parte degli altri soggetti che operano per conto del Titolare;

Il successivo trasferimento delle informazioni raccolte agli interessati o a chi per loro (vale a dire i soggetti che siano muniti di procura speciale ai sensi di quanto disposto dall'art. 9, comma II, del Codice);

La catalogazione delle istanze ricevute e delle risposte rilasciate nonché degli eventuali atti rilasciati a seguito dell'eventuale attivazione di procedimenti giudiziari.

2.4. Responsabile dei trattamenti informatici

Il Responsabile dei Trattamenti Informatici, oltre a quanto illustrato per i responsabili del trattamento (Par 2.2), ha anche le seguenti responsabilità aggiuntive:

- Operare, nel rispetto delle procedure aziendali, come il custode delle applicazioni, delle banche dati, e della rete assegnate alla propria gestione;
- Definire le procedure di gestione delle user-Id – normali e con privilegi - e delle Password;
- Garantire l'attuazione delle misure di sicurezza descritte nel DPS e mantenere aggiornato il DPS secondo l'evoluzione tecnologica;
- Nominare gli amministratori di sistemi server, di basi dati, di rete e apparati di sicurezza, di software e applicativi, secondo l'ambito di competenza e responsabilità ad essi attribuite.

2.5. Amministratori di Sistema

Gli amministratori di sistema operano per la gestione e la manutenzione dei Sistemi Informatici Aziendali, quali amministratori di sistemi server, amministratori di basi dati, amministratori di rete e apparati di sicurezza, amministratori sistemi software e applicativi.

Gli amministratori di sistema, designati in conformità a quanto previsto dal provvedimento del Garante 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (v. paragrafo 8 "Attuazione del provvedimento sugli Amministratori di Sistema") e generalizzati in apposito documento, hanno le seguenti responsabilità:

- Agire nel rispetto delle procedure aziendali;
- Sviluppare, realizzare e mantenere aggiornate, per le banche dati gestite con sistemi informatici, le misure di sicurezza in accordo con le norme contenute nel DPS;
- Monitorare, se richiesto, i piani di adeguamento sulla sicurezza;
- Amministrare e gestire la sicurezza informatica operando anche come gestore delle password.
- Il personale appartenente alle funzioni Operation Management e Application Management della Direzione Sistemi Informativi è nominato individualmente Amministratore di Sistema in linea con quanto previsto nel provvedimento del Garante.

2.6. Incaricati del trattamento

Gli Incaricati del trattamento dei dati personali, nell'ambito del trattamento assegnato, hanno le seguenti responsabilità:

- Svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel Documento Programmatico sulla Sicurezza e le direttive del Responsabile.
- Non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento.
- Rispettare le norme di sicurezza per la protezione dei dati personali.
- Informare il proprio Responsabile e/o Il Responsabile Sicurezza Informazioni, secondo le procedure in vigore, in caso di incidente di sicurezza che coinvolga dati personali o aziendali riservati.

2.7. Funzione amministratrice

La funzione amministratrice è la funzione responsabile del processo che utilizza uno o più applicativi a supporto della propria attività.

La funzione amministratrice ha la responsabilità di individuare e definire i ruoli degli utenti che debbono accedere, in ragione della propria attività o necessità (personale interno, consulenti e/o soggetti terzi ad esempio beneficiari) alle informazioni gestite dalle applicazioni.

2.8. Amministrazione della sicurezza degli Applicativi

Gli amministratori di sicurezza degli applicativi (ASA) sono custodi delle applicazioni, sono figure non necessariamente tecniche che si avvalgono di uno strumento software per l'abilitazione e la profilazione delle utenze sui diversi applicativi su indicazioni delle funzioni amministratrici. Gli ASA generalmente risiedono presso le funzioni amministratrici e sono pertanto conoscitori del processo che si serve dell'applicazione per lo svolgimento della propria attività, garantendo così sicurezza nell'attività di abilitazione, disabilitazione e/o modifica ruolo delle utenze sulle applicazioni.

Gli ASA hanno inoltre il compito di aggiornare periodicamente l'effettivo accesso alle varie applicazioni delle risorse come sopra definite e di mantenere una traccia di audit di tutte le operazioni effettuate.

L'attività è regolata dalla citata procedura GR-PO-SQ-0045 Accesso ai Sistemi Informativi.

Per quei sistemi, che non possiedono uno strumento applicativo strutturato per la profilazione e l'abilitazione degli utenti sulle applicazioni, tale funzione è svolta direttamente dall'Amministratore di sistema che funge in questo caso da ASA.

Per quanto gli ASA non siano figure tecniche e non abbiamo poteri di controllo sulle applicazioni particolarmente penetranti l'Agenzia applica nei loro confronti gli standard prescritti dal garante nel provvedimento del citato provvedimento sugli Amministratori di Sistema ed in particolare:

- Nomina individuale su base fiduciaria;
- Elenco aggiornato degli ASA nominati;
- Controlli sull'operato.

2.9. Autorità di sistema e di amministrazione della sicurezza

2.9.1. Definizioni

Autorità di sistema:

Le autorità date ad una persona (amministratore del sistema) tramite l'assegnazione di attributi, privilegi o accessi che sono associati col sistema operativo o data base e che sono richiesti per svolgere attività di system supporto o di manutenzione.

Autorità di amministrazione della sicurezza:

Le autorità date ad una persona tramite l'assegnazione di attributi o privilegi che sono associati con il sistema di controllo accessi e che sono richiesti per attivare ed amministrare i controlli di sicurezza.

Chi possiede l'autorità di sistema può impropriamente operare in modo da alterare il sistema di controllo accessi, così come un amministratore di sicurezza può impropriamente alterare i componenti del sistema.

Le attività che competono a tali persone devono essere esplicitamente autorizzate dal Responsabile dei Sistemi Informativi e le persone messe al corrente delle loro responsabilità.

3. Lista dei trattamenti

Omissis

4. Analisi dei rischi

L'analisi dei rischi, basata su valutazioni formali recenti e su rilevazioni ad hoc, ha rilevato le minacce possibili e le aree di maggior rischio per la sicurezza dei dati personali come sotto riportate.

L'analisi dei rischi è stata focalizzata sulle circostanze, possibili o probabili, che possono determinare il verificarsi di rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta.

L'analisi dei rischi è finalizzata alla verifica del livello di sicurezza in merito ai principi di:

- *integrità dei dati*: intesa come la gestione dell'accuratezza e completezza delle informazioni e delle relative applicazioni, la salvaguardia dell'esattezza dei dati, la difesa da manomissioni o modifiche non autorizzate, ecc.;
- *riservatezza*, o *confidenzialità dei dati*: intesa come la garanzia che le informazioni siano accessibili solo alle persone autorizzate, la protezione delle trasmissioni, il controllo degli accessi, ecc.;
- *disponibilità dei dati*: intesa come l'assicurazione che l'accesso ai dati sia disponibile quando necessario, quindi la garanzia per gli utenti della fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi stessi.

La valutazione di rischio è frutto del giudizio degli analisti, ed è stata basata su criteri di efficacia rapportati all'odierno sviluppo tecnologico ed alle correnti security practices diffuse a livello internazionale. In questo ambito, si è fatto ricorso alla metodologia di analisi ISO 27001 al fine di avvalersi di un sistema internazionalmente riconosciuto, facilmente replicabile e suscettibile di comparazione anno su anno.

Poiché le informazioni siano soggette ad un **rischio** occorre che una **minaccia** (vedere cap.4.2) sfrutti una o più debolezze o **vulnerabilità** (vedere cap.**Errore. L'origine riferimento non è stata trovata.**) presenti nel sistema di sicurezza.

È ovvio che a parità di minaccia, livelli di vulnerabilità diverse, generano livelli di rischio differenti; così come a parità di vulnerabilità, livelli di minaccia differenti, generino livelli di rischio differenti.

Il metodo utilizzato non si sofferma ad analizzare in dettaglio le centinaia di minacce possibili, ma le sintetizza raggruppandole per grandi famiglie (vedere cap.4.2). La sempre maggiore diffusione di sistemi aperti e l'utilizzo generalizzato di Internet tende oggi a rendere omogenee, per settori di attività, le minacce e la probabilità che si concretizzino.

Il livello di vulnerabilità è valutato, per ogni singola area presa in esame, sulla base di interviste e sulla valutazione della documentazione fornitaci.

4.1. Aree di analisi

L'analisi dei rischi prende in esame l'intera struttura aziendale ed è stata suddivisa nelle seguenti aree:

Politica della sicurezza

Il Sistema di sicurezza aziendale si deve basare su taluni principi fondamentali che la Società fa propri come valori ineludibili.

Scopo primario è quello di diffondere la consapevolezza sui rischi che corrono le informazioni personali e definire le responsabilità in materia.

Organizzazione della sicurezza

Qualsiasi sistema di sicurezza adeguato si fonda su una corretta distribuzione di ruoli e di responsabilità.

Una organizzazione della sicurezza è efficace se gode del supporto del top management e di adeguati budget. Occorre, inoltre, evitare, nel posizionare tale organizzazione nel contesto aziendale, i conflitti di interesse.

Classificazione e controllo degli asset

La sicurezza delle informazioni presuppone la conoscenza, la gestione ed il controllo delle stesse. Un sistema di sicurezza non basato su concetti di classificazione è debole.

I dati personali comuni, quelli sensibili o giudiziari e gli altri dati aziendali vanno classificati per poterli distinguere e proteggere in modo selettivo.

Rischi connessi con la condotta del personale

Le rilevazioni internazionali delle casistiche degli accessi non autorizzati ai sistemi informatici indicano che le effrazioni sono prevalentemente di origine interna aziendale.

Per migliorare l'efficacia dei sistemi di protezione è fondamentale poter contare su adeguati e consapevoli comportamenti di tutto il personale.

Sicurezza fisica e ambientale

Le apparecchiature critiche e gli archivi dovrebbero essere sempre posti in ambienti sicuri, con accesso controllato e dotati di sistemi di protezione ambientali. La gestione degli accessi sia del personale interno sia di quello di terzi dovrebbe essere sempre regolato da rigorose procedure.

Gestione dei computer e della rete

Gli ambienti Internet, Intranet ed Extranet sono sempre più complessi e richiedono molta attenzione, così come ogni connessione con l'esterno (linee telefoniche, modem) nonchè la crescente minaccia di virus e di altri programmi pericolosi.

Nel caso di outsourcing di servizi di vario genere è necessario predisporre chiari contratti in materia di sicurezza.

Procedure ed accesso ai sistemi ed ai dati

Non basta usare User-id e password occorre che le autorizzazioni siano date a ragion veduta e soprattutto ritirate quando non più necessarie. Una gestione non rigorosa di tali elementi è segnale di basso livello di sicurezza.

E' essenziale, inoltre, che i log siano registrati e regolarmente controllati. Gli utenti devono avere la consapevolezza che gli accessi e i tentativi di accesso sono rilevati.

Sviluppo e manutenzione dei sistemi

Una delle principali regole in materia di efficacia nella sicurezza impone che la progettazione delle relative misure avvenga con una chiara definizione degli obiettivi che le stesse devono

conseguire e che l'adozione delle stesse avvenga nella fase di progettazione delle attività che devono da queste essere presidiate.

Piano di continuità / disaster recovery

Il piano di continuità dovrebbe comprendere il deposito dei dati di backup degli archivi e degli ambienti applicativi, in locali separati da quelli dei dati originari e l'effettuazione di test periodici per verificarne l'efficacia e lo stato di aggiornamento.

Attività di audit e controllo

Il sistema Data Protection si fonda su specifici presidi imposti dal legislatore e sulla verifica che tali presidi rispondano effettivamente ai requisiti stabiliti.

Un'eventuale carenza in tal senso vanifica spesso gli investimenti e gli sforzi fatti nell'area della sicurezza.

I controlli, inoltre, sono essenziali per rilevare eventuali intrusioni dall'esterno o un uso non appropriato delle apparecchiature informatiche.

Archivi cartacei

La sicurezza degli archivi cartacei, oltre che con opportune apparecchiature, si raggiunge con una intensa azione di formazione ed addestramento. Anche i migliori armadi corazzati risultano inutili se gli incaricati del trattamento lasciano l'ufficio incustodito senza adottare le necessarie misure di sicurezza.

Gestione workstation

Dal punto di vista della sicurezza le workstation rappresentano una debolezza di non facile contenimento.

Non sempre il sistema operativo utilizzato dispone di adeguate misure di sicurezza ed a volte è facilmente modificabile dall'utente. Inoltre è sempre possibile riprodurre e registrare sulle workstation copie, anche voluminose, di porzioni di banche dati con scarse possibilità di controlli.

Servizi in outsourcing

Con il termine "outsourcing" si intende l'affidamento a terzi di servizi per conto della Società.

La Legge prevede che, qualora tali servizi prevedano trattamento di dati personali, i fornitori del servizio siano inquadrati in specifici ruoli da cui discendono diverse forme di responsabilità. Eventuali carenze in questa area possono avere ripercussioni legali e di immagine per la Società.

Omissis

4.2. Valutazione delle minacce

Omissis

5. Prescrizioni di sicurezza

Obiettivo: definire le regole fondamentali per la realizzazione delle misure di sicurezza per le informazioni personali ed aziendali oggetto di trattamento sotto la responsabilità dell'Azienda.
Aderenza: il rispetto del presente documento è obbligatorio e oggetto di verifiche ed audit.
Eccezioni: sistemi isolati (non in rete) che non contengono dati personali o aziendali.
Allegati tecnici: sarà cura dell'Amministratore di sistema definire per ogni piattaforma i parametri tecnici che rendono concreto su ogni singolo sistema e sulla rete/LAN quanto richiesto dalle presenti prescrizioni.

5.1. Definizione e protezione delle risorse

Gli oggetti informatici si presentano sotto la forma di dati, testi, o programmi.

Gli oggetti che fanno parte dei trattamenti dei dati personali sono chiamati «risorse **personali**».
Gli oggetti che fanno parte dei trattamenti dei dati aziendali sono chiamati «risorse **aziendali**».
Gli oggetti che si riferiscono alle funzioni del sistema ed al servizio di elaborazione dati sono chiamate «**Risorse del sistema operativo**».
Le Procedure Organizzative interne richiamate sono consultabili nella Tabella procedure organizzative – Sistema Qualità pubblicate nella intranet aziendale.

5.1.1. Proprietà delle risorse

Per ogni risorsa deve essere definito un proprietario o una Funzione Amministratrice. I proprietari delle risorse personali coincidono con i Responsabili dei trattamenti. I proprietari delle risorse aziendali, non individuate come Personali, sono i Dirigenti cui è assegnata la responsabilità delle risorse stesse (Funzione Amministratrice).

5.1.2. Tipologia delle risorse

Le risorse personali sono suddivise in:

- Risorse o dati personali comuni.
- Risorse o dati personali sensibili o giudiziari.

Le risorse aziendali sono suddivise in:

- Risorse e dati pubblici dell'Agenzia.

- Risorse e dati riservati dell'Agenzia.

Le risorse sono classificate, in base alle procedure in vigore, a cura dei rispettivi proprietari.

E' responsabilità dei proprietari individuare i dati personali sensibili o giudiziari e i dati aziendali riservati ed informare gli Amministratori di sistema della loro tipologia e collocazione.

5.1.3. Protezione dei dati personali comuni e sensibili o giudiziari

I dati personali comuni e sensibili o giudiziari devono essere messi a disposizione solo delle persone che hanno la necessità di accedervi ai soli fini di trattamento. L'accesso deve essere esplicitamente permesso, solo con le modalità previste dal trattamento e limitato ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.

La validità della richiesta di accesso deve essere verificata prima di consentire l'accesso.

Le autorizzazioni di accesso devono risultare da appositi documenti ed essere a disposizione dell'audit.

5.1.4. Protezione dei dati riservati Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa

I dati riservati, classificati secondo le guide definite dalle procedure aziendali, sono protetti con le regole definite dai rispettivi proprietari.

L'applicazione di questa norma è condizionata all'emissione della relativa Procedura Organizzativa.

5.1.5. Risorse del sistema operativo

Di norma, le risorse del sistema operativo sono accessibili agli utenti ordinari in modalità di «sola lettura o esecuzione».

Fanno eccezione quelle risorse che, se conosciute, potrebbero consentire di aggirare i sistemi di sicurezza (es. log, archivi contenenti le password, ecc.). Queste risorse sono inaccessibili all'utenza ordinaria.

5.1.6. Sistema di autenticazione

Ogni sistema e/o banca dati contenente dati personali o aziendali, deve essere dotata di una funzione di Identificazione ed Autenticazione basata su User-Id e password.

Ogni identificativo (user-id) deve essere univocamente e direttamente associato ad un singolo utente. La User-Id è costituita secondo le regole in vigore.

Una volta assegnata la User-Id ad una persona, questa User-Id non deve essere più assegnata, anche in tempi diversi, ad altra persona.
La Procedura Organizzativa: Accesso ai Sistemi Informativi Aziendali, definisce le modalità operative per il sistema di autenticazione.

5.1.7. Assegnazione delle User-Id

L'User-Id, che permette l'accesso alle banche dati ed alla rete, è definita dall'amministratore di sistema e abilitata dal relativo ASA.

5.1.8. Gestione del personale esterno

Personale non direttamente dipendente da una azienda controllata del Gruppo Agenzia può essere utilizzato per le attività connesse con il servizio di elaborazione dati. In tal caso non sono richieste ulteriori misure oltre quelle descritte nel presente DPS. Tuttavia, nel caso tali risorse siano nella posizione di accedere a informazioni personali o riservate, ovvero ai sistemi o alla rete interna eludendo i sistemi di controllo, è richiesta la preventiva approvazione dell'incaricato al trattamento individuato dal Responsabile del trattamento informatico per il loro intervento.
A solo titolo di esempio si elencano i ruoli tipici di un Information System che hanno la possibilità di eludere i sistemi di controllo:

- Personale che utilizza utenze privilegiate di sistema.
- Personale che utilizza utenze privilegiate di sicurezza.
- Personale che utilizza utenze privilegiate per la manutenzione HW e SW.
- Personale che utilizza utenze privilegiate per la manutenzione delle librerie applicative.

5.1.9. Revoca delle user-id

Quando un incaricato non ha più la necessità di accedere ad una banca dati, o lascia l'azienda, il Responsabile del trattamento cui risponde l'Incaricato o, nel caso si tratti di un terzo, la direzione Gestione e Sviluppo Risorse Umane, deve chiedere tempestivamente all'Amministratore di sistema di disabilitare l'utenza non più necessaria.

5.1.10. User-id inattive

Le user-id inutilizzate per più di 6 mesi devono, a cura degli Amministratori di sistema, essere disattivate. Fanno eccezione le User-Id di manutenzione che non scadono mai e le User-Id di applicazioni per le quali sono specificatamente definite differenti specifiche.

5.1.11. User-Id di manutenzione

L'Amministratore di sistema mantiene aggiornata, per ogni sistema e apparecchiatura di rete, la lista delle User-Id abilitate alla sola manutenzione del sistema. Tale lista è autorizzata dal Responsabile dei trattamenti informatici.

5.1.12. Convalida annuale

Gli ASA devono, con cadenza annuale, procedere alla convalida dei diritti di accesso alle risorse sotto la propria responsabilità. Ciò può essere fatto anche tramite liste che devono essere predisposte a cura dell'amministratore di sistema. La lista degli utenza abilitate alle applicazioni, risultanti ancore attive al termine del processo di revisione, deve essere condivisa con la Funzione Amministratrice e/o Responsabile del trattamento ed essere a disposizione su appositi documenti (cartacei e/o digitali) di eventuali revisori (interni o esterni) per i necessari controlli e verifiche, per almeno due anni.

5.2. Password

La robustezza delle password è il meccanismo più importante per proteggere i dati.

Le regole di seguito elencate sono vincolanti per tutti i sistemi e workstation con cui si accede alle banche dati contenenti dati personali o aziendali.

Le password di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione.

5.2.1. Regole generali delle password

- La lunghezza minima è di 8 caratteri (lettere e numeri o caratteri speciali).
- Per una corretta protezione delle informazioni, la password:
- Non deve essere comunicata ad altri utenti.
- Non deve essere banale o facilmente indovinabile (es. non contenere dati facilmente riconducibili all'utente). A tale scopo devono essere definite opportune regole di composizione.
- Non deve essere riutilizzata in tempi ravvicinati, cioè la sequenza delle password utilizzate deve essere controllata.
- Non deve contenere l'user-id al suo interno.
- Deve essere cambiata almeno ogni 90 giorni.

Le regole sono vincolanti per tutti i sistemi e Workstation tramite i quali sia possibile accedere alle banche dati contenenti dati personali.

Note: se la tecnologia lo permette, le regole sono rese obbligatorie dal software; altrimenti è responsabilità dell'utente rispettarle.

5.2.2. Numero tentativi di accesso con password invalide

Dopo 5 errori consecutivi nella digitazione della password, l'utenza viene disabilitata per evitare un numero illimitato di tentativi per indovinarla.

5.2.3. Ripristino della password

Il ripristino della password deve essere fatto, a cura dell'Amministratore di sistema, dopo diligente e positiva identificazione del richiedente e a cura dell'utente deve essere cambiata subito dopo.

5.3. Sistema di autorizzazione

L'accesso ai dati personali è concesso solo dopo esplicita autorizzazione, data per iscritto o con strumenti informatici specificatamente predisposti, da parte della Funzione Utente.

Il criterio di assegnazione dei profili deve essere basato sulle effettive necessità di lavoro.

L'accesso deve essere esplicitamente permesso, solo con le modalità previste dal trattamento e limitato ai soli dati la cui conoscenza è necessaria per lo svolgimento delle operazioni di trattamento o di manutenzione.

Le autorizzazioni di accesso devono risultare da appositi documenti (cartcei e/o digitali) ed essere a disposizione di eventuali revisori (interni o esterni) per i necessari controlli e verifiche, per almeno due anni.

La Procedura Organizzativa: Accesso ai Sistemi Informativi Aziendali, definisce le modalità operative per il sistema di autorizzazione.

5.4. Integrità e disponibilità dei dati

Al fine di garantire l'integrità dei dati devono essere messe in atto le contromisure seguenti.

5.4.1. Access control

Tutti i server ed i sistemi operativi devono essere dotati di una funzione di Access Control. Il software utilizzato deve essere certificato almeno C2 secondo lo standard TCSEC o FC2E3 secondo lo standard ITSEC o l'equivalente secondo lo standard ISO/IEC 15408. Il Responsabile dei trattamenti informatici ha la facoltà di derogare dall'utilizzo di software certificato.

Nel caso in cui dati personali, sensibili o giudiziari sono trasmessi in reti non affidabili (es. Internet), è obbligatorio l'utilizzo di funzioni che li rendano inintelligibili (es. crittografia). È responsabilità del Responsabile dei trattamenti informatici definire le caratteristiche e le modalità operative della funzione utilizzata.

5.4.2. Integrità delle workstation e dei server

Ogni workstation e server deve essere dotato di un software antivirus. L'antivirus deve essere aggiornato, secondo le procedure in vigore, e mantenuto costantemente attivo.

Gli utenti delle workstation e dei laptop non hanno privilegi superiori a quelli definiti dal gruppo User di Windows.

Le eccezioni a tale norma devono essere approvate per iscritto dal responsabile dei trattamenti informatici. Il Responsabile della sicurezza mantiene una lista aggiornata di tali eccezioni.

Inoltre l'Amministratore di sistema, in presenza di situazioni di emergenza provvede a fornire agli utenti adeguate informazioni di allerta e indicazioni sulle contromisure da adottare.

5.4.3. Integrità del sistema operativo

È fondamentale che le parti critiche del sistema operativo siano a loro volta integre. Anche il migliore sistema di crittografia, può venire compromesso se installato in un sistema operativo compromesso. Per ridurre tali rischi devono essere adottate le seguenti norme:

- Devono essere utilizzati meccanismi che permettano di verificare che i software da installare siano originali ed integri.
- Non devono essere mai utilizzati software di provenienza dubbia o scaricati da siti non affidabili.
- Le modifiche al sistema operativo devono essere effettuate secondo adeguati processi di "change and configuration management ".
- L'utilizzo remoto di utenze di amministratore di sistema dall' esterno deve essere ridotto al minimo e, se necessario, utilizzando collegamenti sicuri (es. VPN, IPSEC).

5.4.4. Ambienti di sviluppo e di manutenzione

Nel sistema informativo sono presenti gli ambienti di seguito descritti. E' opportuno rilevare che non sempre sono fisicamente distinti tra loro, ma di sicuro sono logicamente distinguibili.

Sviluppo: per lo sviluppo di nuovi moduli o personalizzazione di moduli esistenti.

Collaudo o test: per la verifica preliminare della corrispondenza tra quanto richiesto e quanto realizzato.

Manutenzione: per apportare le correzioni rese necessarie dal verificarsi di anomalie alla produzione.

Produzione: e' l'ambiente in cui si svolgono le attività operative quotidiane.

Il processo di sviluppo, sia che venga svolto all' interno sia che venga affidato a fornitori esterni, deve prevedere metodologie formali e documentazione appropriata per garantire il rispetto dei requisiti voluti.

In questo processo devono essere considerati anche gli aspetti di sicurezza, perché il risultato sia in linea con questo DPS.

5.4.5. Integrità delle librerie applicative

Ovviamente un programma applicativo manomesso compromette l'integrità dei dati a cui accede. Per ridurre tali rischi devono essere adottate le seguenti norme:

- Gli ambienti di sviluppo e test devono essere separati da quelli di produzione.
- Le librerie di produzione (master) devono essere protette e accessibili unicamente da personale autorizzato.
- Le librerie devono essere gestite secondo appropriati processi di "change and configuration management ".
- Le procedure di trasferimento delle librerie dall'ambiente di test a quello di produzione devono essere basate solo su applicazioni specializzate e mai al di fuori di queste.

5.4.6. Programmi pericolosi

Dalle librerie dei server sono eliminati quei programmi che possono modificare i dati aggirando i sistemi di sicurezza. Se necessario, tali programmi sono utilizzati da personale opportunamente addestrato e protetti o rimossi dopo l'utilizzo.

I sistemi sensibili ai virus devono essere protetti con opportuni programmi (antivirus). Tali programmi devono essere, a cura dell'Amministratore di sistema, mantenuti costantemente aggiornati.

5.4.7. Aggiornamento dei programmi critici per la sicurezza

È compito degli amministratori di sistema mantenere aggiornati i software in base agli aggiornamenti rilasciati dalle case fornitrici. Qualora un aggiornamento critico per la sicurezza, non è implementato, l'amministratore informa il Responsabile dei trattamenti informatici, motivando la decisione.

5.4.8. Altre Misure

Ai fini di ridurre i rischi dell'integrità del sistema, viene utilizzato il sistema di IDS e IPS (sniffing) che lavorano sulla rete allo scopo di prevenire e/o monitorare virus, trojan, ect.

Per ridurre i rischi legali connessi all'uso improprio degli strumenti informatici e della navigazione internet da parte dei dipendenti, e per finalità di sicurezza informatica, è attivato un

sistema di URL *filtering* che blocca l'accesso ai siti web dai contenuti contrari alla legge o al buon costume oppure ritenuti pericolosi dalle *best practices* internazionali.

5.5. Connessioni con l'esterno

Sono considerate connessioni con l'esterno:

- Interconnessioni tra il servizio I/T di Agenzia ed il servizio elaborazione dati di altre aziende, clienti, outsourcer e fornitori di servizi Internet.
- Accesso remoto da parte di personale dell'azienda o di altre aziende (fornitori, consociate, clienti).

5.5.1. Gateway

E' definito Gateway per le interconnessioni esterne l'insieme di hardware, software e applicazioni che permettono l'interconnessione o l'accesso remoto.

I gateway di interconnessione con l'esterno devono essere sotto il controllo di Agenzia e approvati dal Responsabile dei trattamenti informatici.

5.5.2. Caratteristiche di sicurezza

- Gli accessi in ingresso devono essere verificati con user-Id/password o altra tecnica di autenticazione.
- Non deve essere permesso l'accesso ai Firewall da workstation collegate alla LAN interna aziendale, ma solo da workstation locali connesse ad una LAN sezionata logicamente
- Deve esserci un processo per rilevare eventuali attacchi di massa al gateway.
- Deve esserci un processo per disattivare gli utenti che non necessitano più del collegamento dall'esterno.
- Le utenze abilitate devono essere verificate e riconfermate almeno ogni 3 mesi.
- Nel caso di interconnessioni con altri sistemi esterni, deve esserci un controllo per verificare l'identità della controparte ad ogni attivazione del collegamento.
- I collegamenti Dial dall'esterno devono avvenire tramite un gateway approvato dal Responsabile dei trattamenti Informatici.
- Linee Dial da/per l'esterno non devono essere collegate alle Workstation individuali senza approvazione. Nel caso il collegamento sia di tipo TCP/IP tramite modem, non deve essere permesso il suo uso simultaneamente al collegamento interno, a meno che siano stati disattivati quei comandi che permettono l'utilizzo della workstation come link per collegarsi con la rete interna.

5.5.3. Server posti nella zona demilitarizzata (dmz)

Norme generali

- I server posti nella zona demilitarizzata (DMZ) sono tipicamente Web Server e Data Server e per questi e per i Firewall valgono totalmente le regole definite in questo documento.
- Però per il fatto di essere più esposti verso l' ambiente esterno (es. Internet) richiedono qualche attenzione aggiuntiva. Per i dettagli tecnici si rimanda all' allegato specifico, qui si definiscono regole generali e comportamentali.
- Il primo aspetto da considerare è di garantire l' integrità dei dati, cioè evitare che per errore, disattenzione o dolo le informazioni messe a disposizione degli utenti siano modificate senza autorizzazione.
- Poi occorre garantire la riservatezza, cioè che le informazioni immesse dagli utenti non siano intercettate da terzi non autorizzati.
- Per questo le autorità di accesso al sistema devono essere attentamente assegnate in relazione all' attività ed alla responsabilità di ogni incaricato, distinguendo i seguenti ruoli:
- Web administrator: amministratore del sistema
- Web Master: gestore dell' applicazione web server
- Autore Web: inserisce e aggiorna le informazioni
- Sviluppatore: sviluppa e mantiene le applicazioni
- Utente: accede solo per consultare o per utilizzare le applicazioni disponibili.

5.6. Procedure di Backup

- E' responsabilità dell'Amministratore di sistema effettuare, in base alle procedure operative aziendali, periodicamente una copia di backup dei dati personali e aziendali e delle informazioni in genere.
- I backup devono essere effettuati con frequenza quotidiana.
- I supporti di backup devono essere prontamente riposti nei locali/armadi appositamente predisposti.
- Periodicamente, secondo le procedure in vigore, i supporti devono essere trasferiti in locali separati situati in una sede separata rispetto a quella che contiene gli archivi originali.
- Almeno annualmente, deve essere effettuato un test per verificare la capacità di rilettura dei supporti e la ricostruzione delle banche dati.

- Solo il Responsabile del trattamento dei dati informatici può autorizzare la non esecuzione (eccezionalmente) dei backup.

5.7. Piano di Backup/recovery

A cura del Responsabile dei trattamenti informatici devono essere predisposte opportune procedure per assicurare la ripresa del servizio informatico in tempi e con livelli adeguati alla criticità aziendale delle operazioni automatizzate. Il tempo minimo di ripristino, per i trattamenti con dati sensibili e giudiziari, non deve essere superiore a 7 giorni.

5.8. Sicurezza fisica

Il furto o il danneggiamento delle apparecchiature informatiche, la diffusione o distruzione non autorizzata di informazioni e l'interruzione dei processi informatici, oltre che a danneggiare l'azienda, possono esporre il Titolare dei trattamenti delle informazioni personali al rischio di violare la legge 196/2003. Per tale motivo sono istituiti controlli per limitare l'accesso fisico ad alcune aree.

5.8.1. Aree Agenzia Nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa

Sono definite aree di Agenzia tutti i locali sotto la responsabilità di una delle strutture Agenzia nei quali si svolgono le normali operazioni aziendali.

- Gli accessi ai locali sono controllati da una reception, da un servizio di guardia o dagli addetti che normalmente lavorano in detti locali.
- L'accesso, è consentito solo ai dipendenti di Agenzia ed alle persone autorizzate.
- I visitatori occasionali possono accedere agli uffici solo se accompagnati da un dipendente o da una persona preposta. Questa regola non si applica per le aree aperte al pubblico. Da tali aree non è permesso l'accesso dei visitatori agli uffici delle aziende del Gruppo.
- I visitatori individuati come abituali possono accedere agli uffici anche se non accompagnati.
- È compito del Responsabile del trattamento coinvolto individuare i Visitatori abituali e nominarli incaricati.
- Ai fini della sicurezza sono considerate aree di Agenzia anche i locali o gli armadi situati presso fornitori di servizi ed utilizzati dal personale dell'Agenzia stessa
- E' compito della direzione Servizi Generali rilasciare le procedure che regolamentano la definizione e la gestione di tutte le aree del Gruppo Sviluppo Italia.

5.8.2. Aree ad accesso controllato

Sono definite «aree ad accesso controllato» quei locali all'interno delle aree di cui al punto 1.3.9 che contengono apparecchiature informatiche critiche ed archivi critici (informatici o non automatizzati), come definiti nel paragrafo 0, contenenti dati personali sensibili e giudiziario aziendali riservati.

- Apparecchiature ed archivi devono essere all'interno di aree soggette al controllo dell'Agenzia.
- Deve essere chiaramente identificato un responsabile.
- Il locale deve essere chiuso, anche se presidiato.
- L'accesso deve essere consentito solo alle persone autorizzate dal responsabile dell'area.
- L'accesso deve essere possibile solo dall'interno dell'area soggetta al controllo del Gruppo Agenzia ed eventuali uscite di sicurezza devono essere allarmate.
- L'area deve essere protetta con barriere pavimento/soffitto o con sistema anti-intrusione.

5.8.3. Regole di gestione

Il Responsabile della «area ad accesso controllato» deve mantenere un effettivo controllo sull'area di sua responsabilità.

- Deve esserci una lista delle persone autorizzate ad accedere.
- La lista deve essere periodicamente controllata.
- I visitatori occasionali devono essere accompagnati.
- Gli ingressi al di fuori del normale orario di lavoro devono essere registrati e successivamente controllati a cura del Responsabile dell'area.
- Il Responsabile deve assicurare l'esecuzione di periodici test sull'efficacia degli allarmi.

5.8.4. Apparecchiature informatiche ed archivi critici

Ai fini della sicurezza, sono considerate apparecchiature informatiche critiche - se costituiscono parte del trattamento di dati personali - le seguenti apparecchiature:

- Computer (escluse le workstation ad uso esclusivamente personale), apparecchiature per il collegamento dei canali, system o master console, unità dischi e nastri;
- Sistemi per la gestione delle LAN e WAN;
- Bridge, IDS, IPS; Gateway, Repeater, Router, Wiring hub, URL FILTERING;
- Performance e trace tool, Sniffer, protocol analyzer;

- Porte di collegamento principali (backbone);
- Eventuali apparecchiature per la crittografia.

Le chiavi dei sistemi e delle apparecchiature devono essere rimosse.

Le apparecchiature delle LAN (Switch) non facenti parte del backbone e non situate nelle aree ad accesso controllato, devono essere riposte all'interno di armadi chiusi a chiave.

Si definiscono critici quegli archivi (informatici e non) che contengono quantità elevate di dati o informazioni personali sensibili e giudiziari o aziendali riservate. È compito dei rispettivi Responsabili/Proprietari individuare detti archivi ed informare il Responsabile dell'area che li contiene.

5.8.5. Supporti di memorizzazione

I supporti contenenti dati sensibili e giudiziari possono, su valutazione e richiesta del Responsabile di quel trattamento, essere marcati con un'etichetta recante la dicitura: «Può contenere dati personali sensibili o giudiziari secondo la legge 196/2003. Rispettare quanto previsto dalla procedura aziendale».

I supporti contenenti dati sensibili e giudiziari o aziendali riservati devono essere custoditi in un'area ad accesso controllato o in un ufficio non accessibile quando non presidiato o in un armadio/cassetto chiuso a chiave.

I supporti contenenti i backup destinati al recovery devono essere custoditi in un luogo presidiato situato in un edificio diverso da quello che contiene gli archivi originali.

5.8.6. Informazioni residue

Computer, supporti di dati e simili devono essere smaltiti correttamente per evitare che vengano cestinate o divulgate involontariamente informazioni personali.

Sono definite «informazioni residue» quei dati personali ancora leggibili dopo la cessazione di un trattamento (es. nastri o dischi magnetici).

I dati personali e aziendali riservati devono essere resi illeggibili prima del riutilizzo dei supporti in un altro trattamento o prima della alienazione dei supporti stessi.

E' compito dell'Amministratore di sistema definire e tenere aggiornate le appropriate modalità di cancellazione secondo i supporti utilizzati.

5.8.7. Stampanti e Fax

Gli incaricati al trattamento devono controllare il processo di stampa dei documenti al fine di ridurre al minimo il rischio che persone non autorizzate possano accedere agli stessi.

La stampa di documenti contenenti dati personali sensibili e giudiziari o aziendali riservati deve, pertanto, essere effettuata su stampanti o Fax posti in locali ad accesso controllato o su stampanti presidiate dall'Incaricato durante le fasi di stampa.

6. Piano di formazione

Il Servizio Formazione (Area Risorse Umane) ha il compito di erogare una sessione di formazione operativa sulla sicurezza dei dati a singoli Incaricati. Tale sessione individuale viene erogata al verificarsi di una delle tre seguenti circostanze:

1. Ingresso in servizio di nuovo personale
2. Cambio di mansioni (turn over interno)
3. Introduzione di un nuovo, significativo strumento elettronico di lavoro (es. nuova piattaforma elettronica di condivisione di dati e documenti).

La sessione viene erogata dal Servizio Formazione nel contesto dell'affiancamento al nuovo dipendente o al dipendente che cambia mansioni, oppure in sede di primo utilizzo aziendale del nuovo significativo strumento elettronico. Essa ha ad oggetto i rischi che incombono sui dati, le misure disponibili per prevenire eventi dannosi, le modalità per aggiornarsi sulle misure minime adottate.

I materiali utilizzati dal Servizio Formazione ai fini dell'erogazione di queste sessioni individuali viene messo a disposizione dall'Ufficio Legale e dal Responsabile dei trattamenti informatici.

Inoltre, allo scopo di rendere edotti gli incaricati e, ove opportuno, anche i Responsabili del trattamento, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività e delle responsabilità che ne derivano, l'Agenzia organizza periodiche sessioni di aggiornamento sulle evoluzioni della normativa a protezione dei dati e sui provvedimenti del Garante, focalizzati in particolare sulle direttive e sulle procedure privacy adottate. Tali sessioni formative sono erogate da professionalità qualificate dell'Ufficio Legale o da professionisti esterni di comprovata esperienza. Infine, a completamento del piano formativo, e per garantire all'utenza la possibilità di una formazione permanente è stato messo a disposizione di tutto il personale un corso multimediale di sensibilizzazione sulla normativa. che permette di realizzare un modello di autoapprendimento in grado di coniugare varie tecnologie multimediali rendendo i percorsi cognitivi interattivi e consentendo la verifica dei livelli di conoscenza dei temi.

7. Sistemi dati in outsourcing

I sistemi che contengono dati personali, se affidati in outsourcing devono rispettare le regole del presente DPS in ogni sua parte. Un estratto del DPS, contenente le parti caso per caso applicabili, deve essere allegata al contratto di servizio e farne parte a tutti gli effetti.

7.1. Norme di sicurezza aggiuntive

I contratti con gli Outsourcer devono, in base alle valutazioni di rischio effettuate caso per caso dal Titolare o dal Responsabile del trattamento coinvolto, contenere clausole sui seguenti punti:

- Separazione delle responsabilità/attività di sicurezza
- Devono essere concordate dettagliate tabelle che specifichino, in materia di sicurezza, le attività di pertinenza dell'outsourcer, quelle di pertinenza dell'affidatario e quelle eccezionalmente in comune.
- Standard di sicurezza del servizio di outsourcing.

Nel caso di trattamento di dati sensibili e giudiziari l' outsourcer deve predisporre un documento che precisi le norme e le soluzioni di sicurezza adottate per il servizio fornito all'Agenzia. Tale documento, che non deve essere in contrasto col DPS e con quanto prescritto dalla D.LGS. 196/2003, deve essere vincolante per l'outsourcer. In particolare devono essere precisate le modalità di attuazione delle misure minime previste dal Disciplinare tecnico allegato alla citata legge.

- Isolamento della rete/LAN:

L'outsourcer deve garantire che per la parte di rete/LAN di sua responsabilità, con un'opportuna segmentazione della rete, sia evitato il rischio che altri suoi clienti o persone non autorizzate accedano ai sistemi o ai dati dell'Agenzia.

- Controlli e audit:

Deve essere concordata con l'outsourcer la possibilità di effettuare o far effettuare controlli e audit, anche senza preavviso, per verificare lo stato della sicurezza del servizio prestato all' Agenzia ed il rispetto delle misure minime obbligatorie.

Inoltre l' Agenzia potrà effettuare autonomamente o fare effettuare - secondo modalità concordate - test di intrusione per verificare la impossibilità di accedere alla rete ed ai sistemi della stessa, se non autorizzati.

I test potranno essere condotti senza preavviso con frequenza e durata a discrezione dell'Agenzia che informerà l'outsourcer all'inizio ed al termine di ogni test.

Nel caso in cui i test mettano in evidenza carenze, l'Outsourcer dovrà provvedere a correggere le criticità in un tempo non superiore a 20 giorni lavorativi.

- Osservanza del provvedimento sugli Amministratori di sistema

Nei confronti degli outsourcer che operano sui sistemi dell'Agenzia con funzioni di amministratori di sistema, l'Agenzia ha individuato specifiche clausole contrattuali o una specifica nomina di responsabile esterno. Con tali atti l'Agenzia richiede all'outsourcer la conformità al provvedimento e l'attuazione dei punti d) ed e) del provvedimento stesso. In particolare, l'obbligo di conservazione della lista dei nominati amministratori di sistema che concorrono alle attività di trattamento dell'Agenzia, nonchè la verifica del loro operato. La lista, mantenuta costantemente aggiornata a cura dell'Outsourcer, dovrà essere resa disponibile al Garante per eventuali attività di ispezione o direttamente all'Agenzia per attività di audit.

8. Attuazione del provvedimento sugli Amministratori di Sistema

Con il provvedimento del 27 novembre 2008 "Misure ed accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema", il Garante per il trattamento dei dati personali ha individuato specifiche misure organizzative e tecniche per disciplinare sia il ruolo dell'amministratore di sistema (figura generalmente attribuita a coloro che sono impegnati nell'attività di gestione e manutenzione di sistemi di elaborazione o sue componenti), sia quello di altre figure tecniche assimilabili agli amministratori di sistema, ossia tutti «coloro che svolgono mansioni analoghe in rapporto a sistemi di elaborazione e banche di dati», come «gli amministratori di basi di dati (*data base administrator*), gli amministratori di reti e di apparati di sicurezza (*network administrator*) e gli amministratori di sistemi software complessi».

Nel dare attuazione al provvedimento suddetto, l'Agenzia ha individuato in maniera puntuale i soggetti dotati di profili amministrativi: tale identificazione si è effettuata accedendo alle singole componenti dei sistemi, e verificando quegli account definiti, con particolari ruoli di autorità sui sistemi, tali da consentire attività di gestione ed amministrazione.

La società ha predisposto una lista organizzata sulla base dei seguenti criteri:

- applicazioni;
- database;
- server;
- apparati di rete

e, per ciascun settore, l'Agenzia ha individuato il personale dipendente che svolge o ha le autorizzazioni per svolgere le attività proprie di un amministratore di Sistema server/Database/Reti e apparati di sicurezza/Software.

La lista così ottenuta, è stata elaborata in modo da mettere in risalto l'effettivo ruolo svolto da ogni singolo soggetto individuato, secondo quanto richiesto dal Garante con l'indicazione anche dell'ambito di operatività Sistema server/Database/Reti e apparati di sicurezza/Software e applicativi.

Il censimento eseguito è stato inoltre arricchito di ulteriori informazioni di dettaglio, relative a:

- tutti i sistemi affidati in outsourcing;
- tutti i sistemi contenenti dati relativi al personale dipendente dell'Agenzia;
- tutti i sistemi contenenti dati personali ed aziendali riservati e, dunque, soggetti all'applicazione del provvedimento;
- lo stato e la modalità di registrazione dei log degli accessi amministrativi a tutti i sistemi censiti.

9. Norme per gli incaricati del trattamento

9.1. Norme di carattere generale

- Il trattamento di dati personali deve avvenire da parte degli Incaricati solo se richiesto dal Responsabile di quel trattamento.
- L'uso delle apparecchiature informatiche che contengono dati personali o aziendali è permesso solo per svolgere le attività previste nelle istruzioni scritte impartite agli Incaricati.
- Copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi.
- I raccoglitori con documenti cartacei contenenti dati personali devono essere riposti, dopo il loro utilizzo, in armadi chiusi.
- Al termine dell'orario di lavoro il dipendente, nell'abbandonare il proprio posto di lavoro, deve lasciare la scrivania sgombra e con tutti i cassetti/armadi chiusi a chiave.
- In caso si constati o si sospetti un incidente di sicurezza, secondo le procedure in vigore, deve essere data immediata comunicazione al Responsabile del trattamento dei dati informatici e/o al responsabile del trattamento coinvolto.
- Tutte le norme del presente capitolo si applicano anche ai terzi autorizzati ad accedere dall'esterno (fornitori, consulenti ecc.).

9.2. Uso delle Workstation

Ogni dipendente è responsabile di fornire il proprio contributo al fine di minimizzare la possibilità che i dati personali e aziendali contenuti nella propria *workstation*, o trattati tramite la *workstation,* siano esposti a rischi di sicurezza e dovrà osservare le regole di seguito illustrate.

Nel caso in cui si lasci incustodita la scrivania durante l'orario di lavoro:

- Spegnere la *workstation* o se l'apparecchiatura deve restare accesa, attivare una password (*keyboard o screen lock*)
- Assicurare i portatili con gli appositi strumenti o riporli in un armadio/cassetto chiusi a chiave.

Al termine della giornata di lavoro:

- Spegnere la workstation o attivare una password (*keyboard o screen lock*)
- Se si dispone di un portatile riporlo sotto chiave.

In viaggio:

- Proteggere il portatile con la password (*keyboard o screen lock*);
- Tenere il portatile sempre presso di se e non lasciarlo incustodito in auto o in albergo;
- Rendere inintelligibili, secondo le procedure in vigore, i dati personali sensibili o giudiziari e aziendali riservati.

9.3. Uso delle password

La password è un elemento fondamentale della sicurezza delle informazioni. La *password* identifica in modo univoco l'utente del computer e dei servizi informatici. Per la protezione dei dati personali è essenziale che la password sia mantenuta riservata e non comunicata ad altri.

Le regole base da rispettare sono:

- La lunghezza minima della *password* è di 8 caratteri;
- La password deve essere mantenuta riservata e non comunicata ad altri utenti. Se, eccezionalmente, dovesse essere necessario fornirla, in caso di emergenza, ad altra persona, va cambiata subito dopo;
- La password non deve essere banale o facilmente individuabile. A tale scopo devono essere seguite le regole di composizione emesse dai Sistemi Informativi;
- Non contenere *l'user-id*, o il proprio nome, come parte della *password*;
- La password deve essere cambiata almeno ogni 90 giorni;
- Se si accede dall'esterno non utilizzare per l'accesso alla rete la stessa *password* valida per l'accesso alle banche dati.

Note: è responsabilità dell'utente rispettarle queste regole anche se la tecnologia non le rende obbligatorie sulla propria *workstation*.

9.4. Uso dei modem

Le connessioni, con modem o linee dirette, tra i sistemi e la rete dell' Agenzia , con reti e sistemi esterni, possono presentare un serio rischio per l'intero Gruppo. Come conseguenza di collegamenti non corretti dal punto di vista della sicurezza, è possibile che si esponga l'intero sistema informativo dell' Agenzia ed i dati in esso contenuti, ciò può avvenire senza che il dipendente se ne renda conto.

Per tale motivo, ogni collegamento dall'interno verso l'esterno e viceversa, deve essere approvato dal Responsabile dei trattamenti Informatici.

9.5. Internet

Nel caso si utilizzi la rete Internet per collegarsi con altre organizzazioni e si trasmettano dati personali, bisogna tenere presente quanto previsto dalle *policy* di Gruppo e tenere conto delle seguenti avvertenze:

- Internet è usato da milioni di persone nel mondo, non tutte meritevoli di fiducia.
- Ogni informazione trasmessa può essere letta da un elevato numero di persone sconosciute.
- Non trasmettere all'esterno dati personali sensibili e giudiziari o aziendali riservati se non resi inintelligibili.
- Non trasmettere posta elettronica interna del Gruppo tramite Internet, ma usare il sistema ufficiale.
- Non è permesso prelevare software da Internet senza l'autorizzazione del Responsabile dei Trattamenti Informatici.
- Non prelevare o inserire in Internet materiale inappropriato, offensivo o pregiudizievole per altre persone o organizzazioni.

Per una maggior consapevolezza, le regole di comportamento per l' utilizzo di Internet sono state recepite in una policy aziendale pubblicata sulla intranet aziendale per la diffusione al personale dipendente.

9.6. Antivirus

È obbligatorio che ogni workstation sia dotata di un antivirus. L'antivirus deve essere aggiornato, secondo le procedure in vigore, almeno semestralmente e mantenuto costantemente attivo.

Inoltre il responsabile dei trattamenti informatici, in presenza di situazioni di emergenza provvede a fornire agli utenti adeguate informazioni di allerta e indicazioni sulle contromisure da adottare.

10. Archivi cartacei

Ai fini del presente DPS sono definiti «archivi cartacei» tutti gli altri supporti, ad esclusione di quelli informatici, che contengono in qualunque forma dati o informazioni personali incluse le copie, su carta, di dati gestiti con supporti informatici.
Sono inclusi in questa tipologia, oltre ai dati su carta o supporto analogo, le foto, i dischi ottici, i film, i videotape, ecc comprese le copie, anche parziali, su supporti non informatici, di banche dati gestiti in modo automatizzato.

10.1. Sicurezza fisica

I locali o gli archivi che contengono dati personali sensibili e giudiziari o aziendali riservati devono essere protetti da chiusure munite di chiavi. Se non presidiati o fuori orario di ufficio devono comunque essere chiusi a chiave.
I documenti che si riferiscono a trattamenti facenti capo a Responsabili diversi sono conservati in contenitori o locali separati, laddove se ne ravvisi la necessità.
Gli accessi fuori orario ai locali devono essere espressamente autorizzati dal Responsabile del trattamento: chi accede deve essere identificato e l'accesso deve essere registrato.

10.2. Accesso agli archivi

L'accesso agli archivi cartacei contenenti dati personali sensibili o giudiziari è consentito solo al personale espressamente autorizzato per iscritto dal Responsabile del trattamento. Tale accesso deve essere limitato esclusivamente ai dati che sono strettamente necessari per adempiere ai compiti assegnati.
I documenti contenenti dati sensibili o giudiziari, se affidati all'Incaricato del trattamento dal Responsabile, vengono dall'Incaricato conservati in contenitori muniti di serratura e restituiti al termine delle operazioni affidate.

10.3. Copie e riproduzioni

Le copie e le riproduzioni di documenti contenenti informazioni personali o aziendali sono, a loro volta, dati personali o aziendali e pertanto devono essere trattate e custodite come tali.
La documentazione, tecnica o di altro genere, relativa al trattamento di dati personali sensibili e giudiziari (es. chiavi logiche o fisiche di accesso ai siti contenenti tali informazioni) deve essere gestita adottando le stesse misure richieste per i dati presidiati.

11. Verifica dello stato della sicurezza

11.1. Verifiche dell'architettura di sicurezza

Almeno ogni 6 mesi il Responsabile della sicurezza delle informazioni deve effettuare controlli per verificare che gli elementi chiave, ai fini della sicurezza dei sistemi, siano integri.

I controlli per i sistemi critici (contenenti applicazioni su dati sensibili e giudiziari, aziendali riservati, firewall, ecc.) devono avere una frequenza trimestrale.

Le verifiche devono comprendere:

- I parametri del sistema di controllo accessi;
- La lista delle persone con autorità di sistema o di sicurezza;
- I parametri di sicurezza dei sistemi operativi;
- L'aggiornamento del programma antivirus.

I controlli effettuati ed il loro esito, nonché le azioni pianificate per correggere eventuali deviazioni, devono essere riportati in un apposito verbale e comunicate al Responsabile dei trattamenti Informatici.

11.2. Test di intrusione

Almeno una volta l'anno il Responsabile della sicurezza delle informazioni deve assicurare che sia condotto un test di intrusione sui sistemi e sulla LAN.

Tale verifica deve essere condotta con l'ausilio di uno specialistico tecnico esterno.

L'uso dei tool di intrusione è riservato a chi è autorizzato dal Titolare o dal Responsabile, ed è proibito al di fuori dei test autorizzati.

11.3. Processo di prevenzione e allarme (alert)

Il Responsabile del trattamento Informatico deve predisporre un programma che permetta di anticipare i possibili problemi legati alla sicurezza delle informazioni.

- Con cadenza annuale, o in occasione di significativi cambiamenti alle architetture informatiche, deve essere effettuata una valutazione di rischio.
- Deve essere mantenuto un collegamento con il CERT, o altra istituzione che abbia le stesse finalità, per essere informati riguardo alle esposizioni di sicurezza dei principali prodotti software utilizzati.

- Nel caso siano segnalate dal CERT, o altra istituzione che abbia le stesse finalità, esposizioni definite ad alto rischio, sui prodotti installati, deve essere subito valutata l'opportunità di intervento.

11.4. Attacchi sistematici

Deve essere attivato almeno un sistema che permetta di rilevare quando il numero dei tentativi non riusciti di login superano una determinata soglia di pericolo oltre il quale si deve indagare su possibili attacchi.

11.5. Incidenti di sicurezza

Definizione: In linea generale viene definito incidente di sicurezza qualunque evento inaspettato che riguardi l'integrità, la riservatezza o la disponibilità delle informazioni. È compito del Responsabile della Sicurezza delle informazioni rilasciare una procedura che definisca una articolazione degli incidenti per gravità e la relativa gestione.

Una appropriata gestione degli incidenti è fondamentale per tenere sotto controllo questo fenomeno e mettere in atto le opportune contromisure per ridurli.

11.6. Gestione dei Log

L'Amministratore di sistema deve predisporre un processo per garantire che i log elencati siano attivi e protetti da accessi non autorizzati. I log devono essere conservati per almeno 2 mesi.

11.6.1. Log degli accessi ai sistemi

Se il sistema operativo lo consente, tutti i tentativi di login - sia che abbiano avuto successo sia che siano stati rifiutati - devono essere registrati.

11.6.2. Log di accesso ai dati e agli strumenti

Se il sistema di controllo accessi lo consente, il Responsabile del trattamento può chiedere che siano registrati gli accessi alle singole risorse.

11.6.3. Log delle attività

Se il sistema operativo lo consente, le attività svolte dalle persone con autorità di sistema o di amministrazione della sicurezza devono essere registrate.

11.6.4. Login invalidi

La lista dei login invalidi è fornita da parte degli Amministratori di sistema su richiesta del Responsabile del trattamento.

11.6.5. Log di accesso alle risorse

Se il sistema di controllo accessi lo consente, il Responsabile del trattamento può chiedere che siano registrati gli accessi alle singole risorse.

11.6.6. Gestione dei archivi che contengono il log

Le registrazioni che compongono i log, in quanto dati personali, devono essere oggetto di uno specifico trattamento che ne preveda l'utilizzo solo per finalità di sicurezza in caso di pericolo o di incidente.

12. Disponibilità, da parte dell'azienda, degli strumenti e dei dati affidati al dipendente

Per garantire al Titolare, in caso di assenza dell'incaricato e per urgenti necessità, l'accesso agli strumenti ed ai dati ivi contenuti devono essere rispettate le seguenti modalità:
Solo i Responsabili dei trattamenti possono autorizzare un altro incaricato a sostituirsi alla persona assente e ad utilizzare la sua User-ID ed il relativo profilo di accesso.

Solo i Responsabili dei trattamenti possono autorizzare gli Amministratori di sistema a fornire all'incaricato autorizzato le credenziali di accesso.

Se il sistema lo permette, per fornire le nuove credenziali, si deve utilizzare la stessa metodologia usata per il reset delle password. In tal modo viene mantenuta la segretezza delle credenziali della persona assente.

Le autorizzazioni di accesso devono risultare da appositi documenti (cartecei o digitali) conservati dagli Amministratori di sistema oltre dagli ASA (Amministratori Sistemi Applicativi) ed essere a disposizione del Servizio Revisione Interno per i necessari controlli e verifiche.

A cura dell'Amministratore del sistema coinvolto, devono essere attivate, limitatamente al periodo di tempo necessario, le registrazioni dei log delle attività della User-Id interessata.
A cura del Responsabile di trattamento, la persona assente, deve essere informata al suo rientro, su quanto avvenuto.

13. Controlli e audit

Il sistema di controllo si articola su due livelli:

- Audit formale;
- Verifiche periodiche.

13.1. Audit formale

Almeno annualmente il Titolare fa verificare con appropriati controlli audit l'aderenza dello stato della sicurezza al presente DPS.

Al termine dell'audit l'Amministratore di sistema o il Responsabile interessato, nel caso in cui siano state riscontrate deviazioni, deve formulare un piano che preveda il rientro nel più breve tempo possibile.

Situazioni di non aderenza, per periodi superiori a 6 mesi, possono essere accettati solo con l'esplicita autorizzazione scritta del Responsabile di riferimento il quale ha comunque l'obbligo di informare per iscritto il Titolare.

13.2. Verifiche periodiche

È compito del Responsabile della sicurezza delle informazioni effettuare verifiche periodiche sullo stato della sicurezza in azienda e presso gli outsourcer esterni ed i terzi (fornitori, consulenti …) che trattano dati personali o aziendali riservati.

Un rapporto sullo stato della sicurezza, anche in base agli esiti dei self assessment, deve essere predisposto almeno semestralmente e inviato al Titolare ed ai Responsabili.

14. Società partecipate del Gruppo

Qualora una Società di Scopo o Partecipata nomini l' Agenzia Responsabile del trattamento dei propri dati, l' Agenzia oltre a trattare i dati di tale azienda come se fossero propri, applica le seguenti norme aggiuntive:

14.1. Responsabile del trattamento

Il responsabile del trattamento dei dati della Società del gruppo ha gli stessi compiti definiti nel Cap.2.2.

14.2. Trattamenti informatici

Il responsabile dei trattamenti informatici dell'Agenzia svolge lo stesso ruolo anche per i trattamenti informatici cui sono soggetti i dati delle Soc. del gruppo. (Rif. Cap.2.4).

14.3. Incaricati del trattamento

I dipendenti Agenzia che trattano i dati delle Soc. di Scopo o Partecipate sono nominati Incaricati di detti trattamenti e hanno gli stessi compiti definiti nel Cap. 2.6.

14.4. Amministratori dei sistemi informatici

Gli amministratori dei sistemi informatici dedicati ad una Soc. di Scopo o Partecipata ha gli stessi compiti definiti nel cap 2.5. Nel caso il sistema informatico gestisca i dati di una Soc. di Scopo o Partecipata insieme a dati dell' Agenzia o di altre Soc. di Scopo o Partecipate, l'Amministratore designato opera con le stesse regole nei confronti di tutti i trattamenti presenti nel Sistema stesso.

14.5. Norme per gli incaricati

Sia che un dipendente Agenzia sia nominato, in forma dedicata, quale incaricato di un trattamento di una Soc. di Scopo o Partecipata, o svolga questo compito contemporaneamente ad altri incarichi di trattamento di dati personali di Agenzia o di altre Soc. di Scopo o Partecipate, il dipendente Agenzia applica le norme contenute nel Cap.9.

14.6. Verifiche ed Audit

Le attività di Audit e di verifiche periodiche svolte dell'Agenzia includono normalmente i trattamenti di cui sono Titolari le Soc. di Scopo o Partecipate. Da parte dell'esecutore della verifica o Audit sarà formulato un report separato per ogni Soc. di Scopo o Partecipata oggetto di verifica. Il report deve essere consegnato al Titolare o al Responsabile della Soc. di Scopo o Partecipata interessata. Nell'esecuzione dell'Audit o della verifica, l'area dell'Agenzia che la esegue, deve operare nell'interesse del Titolare della Soc. di Scopo o Partecipata, cercando di minimizzare ogni eventuale conflitto d'interessi che dovessero sorgere.

15. Società Regionali, di scopo e partecipate interessate dal processo di dismissione

Alle società partecipate dall'Agenzia (cfr Premessa del presente Documento), per le quali la legge Finanziaria 2007 ha disposto il riordino e il riassetto, per le quali l'Agenzia di fatto continua ad erogare servizi e trattamenti di diversa natura (Informatici, Legali e Amministrazione del Personale) si applica l'Articolo 13 del presente documento, in virtù dei Ruoli Privacy (Titolare e Responsabile del Trattamento) reciprocamente attribuiti.

16. Revisione del documento programmatico sulla sicurezza

Il presente DPS è valido per un anno. Trascorso tale termine deve essere oggetto di revisione, a cura del Responsabile della Sicurezza, per adeguarlo ad eventuali variazioni del livello di rischio cui sono soggetti i dati personali e ad eventuali modifiche della tecnologia informatica. In ogni caso il DPS deve essere aggiornato entro il 31 marzo di ogni anno.
Nell'attesa dell'adeguamento conservano validità le istruzioni in vigore.

Roma, li 26 Marzo 2010 Titolare del Trattamento