Ministero per i Beni e le Attività Culturali

DIPARTIMENTO PER LA RICERCA, L'INNOVAZIONE E L'ORGANIZZAZIONE
DIREZIONE GENERALE PER L'INNOVAZIONE TECNOLOGICA E LA PROMOZIONE

Roma, 31 marzo 2006

Prot. N. **1787** *Allegati*

Documento Programmatico sulla Sicurezza per il MINISTERO PER I BENI E LE ATTIVITA' CULTURALI

Redatto ai sensi e per gli effetti dell'articolo 34. comma 1. lettera g) del D.Lgs.196/2003 e del disciplinare tecnico (allegato B del D.Lgs. n. 196/2003)

Sommario

1 Premessa Metodologica

Il presente Documento Programmatico sulla Sicurezza per l'anno in corso è redatto dal Ministero per i Beni e le Attività Culturali (di seguito semplicemente MINISTERO), con sede in Roma in via del Collegio Romano 27, a cura del Responsabile dei sistemi informativi con il concorso dei Capi dei Dipartimenti che hanno partecipato alle attività di ricognizione dei trattamenti dei dati.

Il Documento è stato elaborato in considerazione della nuova disciplina in materia di tutela dei dati personali entrata in vigore il 1 gennaio 2004 con l'attuazione del D.Lgs. 196/03 e delle disposizioni in materia si sicurezza contenute nel Disciplinare Tecnico di cui all'Allegato B della medesima Legge.

Per la compilazione del presente Documento Programmatico sulla Sicurezza *(nel seguito DPS)* è stata effettuata una ricognizione dei trattamenti di dati personali svolti presso il MINISTERO e/o affidati a soggetti terzi.

A tal fine è stata adottata una metodologia di sviluppo del documento che ha portato a rilevare i processi lavorativi, sia negli uffici centrali che in quelli periferici, al fine di individuare le basi dati utilizzate per i trattamenti e i soggetti fisici e giuridici (sia interni sia esterni) che svolgono le operazioni di trattamento e che sono abilitati a farlo.
La rilevazione dei processi di trattamento ha consentito la contestuale individuazione dei sistemi, delle infrastrutture tecnologiche sottese al trattamento e delle aree relative alla loro localizzazione.
L'analisi del ciclo di lavorazione dei dati ha riguardato, sia i trattamenti svolti con strumenti elettronici, sia i trattamenti relativi ad atti e documenti cartacei.

A seguito delle attività di rilevazione effettuate, è stato accertato il risultato dell'analisi dei rischi per stabilire l'efficacia e la completezza delle misure di sicurezza rispetto alle minacce di distruzione e perdita, anche accidentale, dei dati, di accessi non autorizzati, di trattamenti non consentiti o non conformi rispetto alle finalità della raccolta.
La descrizione dei controlli effettuati e dei criteri adottati per garantire l'efficacia delle misure e la loro adeguatezza nel tempo è contenuta nell'apposito capitolo, così come il risultato degli accertamenti con le relative considerazioni emerse.

Per ogni trattamento, infatti, sono state censite e valutate le misure di sicurezza poste in essere al fine di determinarne la corrispondenza e l'adeguatezza con quanto previsto dal D.Lgs. 196/03 e correlato Disciplinare Tecnico; allo scopo, sono state riviste anche le deliberazioni e le istruzioni normative interne che disciplinano la politica aziendale sulla *Privacy* e sono stati esaminati e classificati gli ambienti e i locali di lavoro nei quali avvengono i trattamenti

Si è, inoltre, proceduto alla previsione e predisposizione di interventi formativi destinati agli incaricati al fine di renderli edotti sui contenuti della legge e sulle politiche aziendali in materia di privacy.

A fronte di quanto sopra descritto, viene redatto il presente Documento Programmatico sulla Sicurezza per l'anno 2006. Tale documento, che sarà costantemente aggiornato nel tempo, costituisce la base per le successive e più analitiche versioni per i prossimi esercizi.

Il documento è stato impostato in diversi capitoli, organizzati in maniera da rappresentare le disposizioni di cui alla regola 19 del Disciplinare tecnico della Legge.

1.1 Politica interna sulla riservatezza dei dati

Lo scopo del presente documento è quello di descrivere le modalità di trattamento dei dati effettuato da MINISTERO, sotto il profilo della sicurezza e riservatezza dei dati, al fine di attestarne la qualità, la puntualità e l'osservanza alle previsioni di legge.

Per questo motivo il MINISTERO dedica la dovuta attenzione ed il massimo impegno alla tematica della sicurezza dei dati, adottando le misure tecnologiche, organizzative e logistiche più adeguate a garantire una appropriata copertura dei rischi derivanti dalla perdita, sia dolosa che accidentale, dell'integrità, della riservatezza e della disponibilità dei dati stessi.

Il MINISTERO è altresì consapevole che la sicurezza non è un processo statico, ma dinamico, che necessita di costanti aggiornamenti in base alle diverse e mutate esigenze quali, ad esempio, il rilascio di nuovi servizi informatici, l'affacciarsi di nuovi rischi, la disponibilità di nuove tecnologie, nuovi scenari operativi, ecc.

1.2 Normativa di riferimento

- D.Lgs. 29 luglio 2003 N. 196 Codice in materia di protezione dei dati personali e Disciplinare Tecnico in materia di misure minime di sicurezza e successive modificazioni ed integrazioni;
- Provvedimento del Garante del 29 aprile in tema di video sorveglianza;
- Legge23 dic. 1993, n°. 547 "Reati informatici";
- Regio decreto 22 aprile 1941 n° 633, come modificato ed integrato dal decreto legislativo n° 518 del 29 dicembre 1992;
- Codice Civile – art. 2050.
- Codice penale – art. 615-*ter*

1.3 Definizioni

Sono definite di seguito le terminologie richiamate nel presente documento:

- Archivi: Archivi cartacei o informatici conservati presso MINISTERO oggetto di trattamento da parte dello stesso.
- Trattamenti: Tutte le operazioni (ad es: l'elaborazione, la modificazione, la conservazione, consultazione, la comunicazione, la diffusione, la cancellazione ….) definite dall'art. 4 comma 1 lettera a), che il MINISTERO effettua sui dati degli interessati per i propri fini istituzionali.
- Piattaforme: Elaboratori, sistemi automatizzati o strumenti per l'elaborazione e/o archiviazione dei dati e/ o delle informazioni contenute negli archivi di cui sopra.
- Risorse: Tutti gli altri mezzi - a titolo esemplificativo la rete di trasmissione dati per il collegamento degli elaboratori - utilizzati per la corrente operatività.
- Locali: Locali, edifici, strutture logistiche di MINISTERO che ospitano, anche temporaneamente, le Piattaforme e/o le Risorse necessarie all'operatività Amministrativa-Gestionale.

Ai fini del D.lgs. 196/03 si intende:

- per "**trattamento**" qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- per "**dato personale**" qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
- per "**dati identificativi**" i dati personali che permettono l'identificazione diretta dell'interessato;

- per "**dati sensibili**" i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- per "**dati giudiziari**" i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
- Per "**strumenti elettronici**" gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

1.4 Revisioni

Il MINISTERO si riserva la facoltà di modificare il presente documento ove le condizioni tecnico/organizzative e normative applicabili dovessero variare.
In particolare:

- ogni qualvolta dovessero cambiare le tecnologie e gli strumenti elettronici soggetti a protezione e misure di sicurezza;
- ad ogni controllo periodico cui le misure di sicurezza sono sottoposte per verificarne la validità e l'efficacia;
- a seguito di variazioni della normativa interna e/o di legge.

2 Trattamenti dei dati svolti (Regola 19.1)

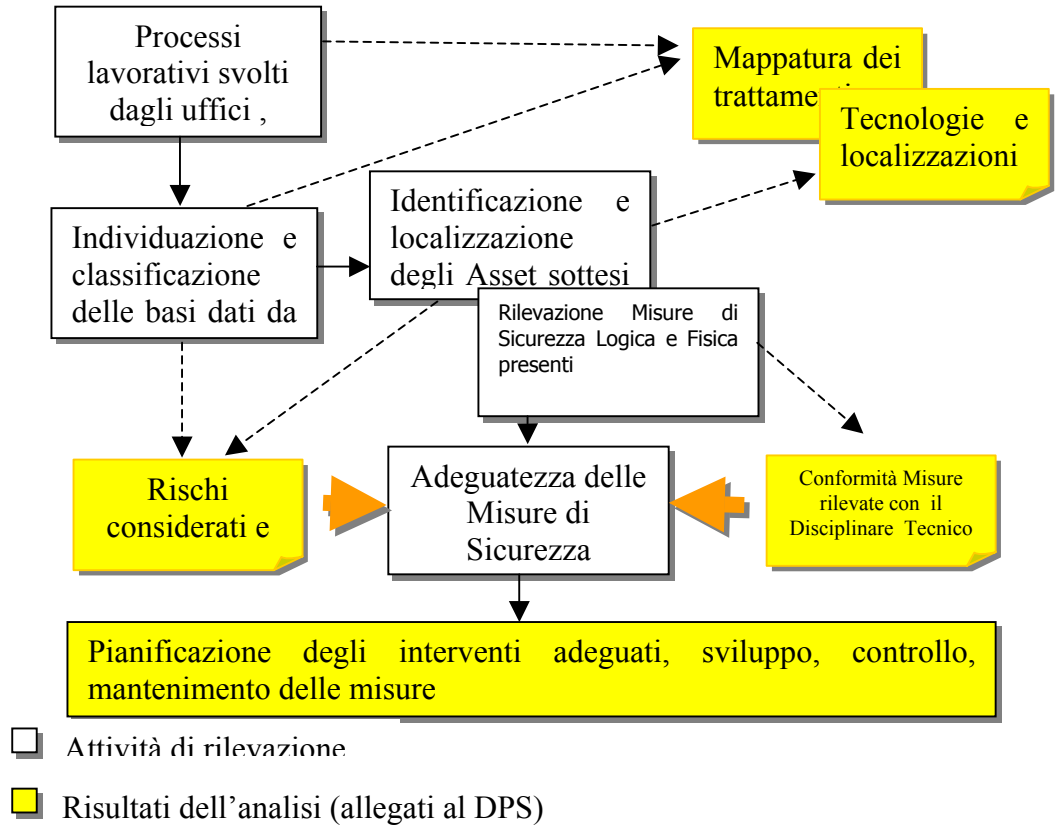
Per giungere alla efficace ed esaustiva compilazione del DPS è stata avviata preventivamente una ricognizione generale dei trattamenti svolti dal MINISTERO o affidati, in conformità alle prescrizione legislative, ad entità esterne.

2.1 Metodologia adottata per la rilevazione

Nello schema che segue viene descritta sinteticamente la metodologia adottata ai fini delle rilevazioni delle informazioni utili alla ricognizione dei trattamenti effettuati dal MINISTERO.

Allo scopo sono state censite le banche dati, individuati i processi operativi negli uffici centrali e periferici, censite le misure di sicurezza per la protezione dei dati, individuati i soggetti fisici e giuridici che svolgono le operazioni di trattamento dei dati e che sono abilitati a svolgerle, esaminate le deliberazioni e le istruzioni normative interne che disciplinano l'operatività, osservati e classificati gli ambienti e i locali di lavoro nei quali avvengono i trattamenti.

L'analisi del ciclo di lavorazione dei dati ha riguardato sia i trattamenti svolti con strumenti elettronici, sia i trattamenti relativi ad atti e documenti cartacei.
Come punto di partenza sono stati presi in considerazione i processi lavorativi svolti dalle diverse Funzioni e unità organizzative, sono state, in successione, individuate e classificate, secondo le previsioni di Legge, le basi dati di interesse ai fini della privacy.
Sono state rilevate le tecnologie sottese al trattamento e gli ambienti in cui le stesse sono localizzate al fine di individuare le misure di sicurezza tecniche implementate.
Le fasi finali del processo di rilevazione hanno posto in relazione le misure di sicurezza già presenti con i rischi considerati al fine di valutarne la loro adeguatezza e corrispondenza con quanto previsto dalla Legge.



2.2 Tipologie di dati trattati

Le finalità del trattamento effettuato dal MINISTERO sono riconducibili alle seguenti macro-categorie:

- Finalità istituzionali – ambito di missione
- Finalità istituzionali – ambito di autoamministrazione (amministrative e contabili)

Il MINISTERO, *nello svolgimento delle proprie attività istituzionali*, procede al trattamento di dati personali, reddituali, finanziari, sensibili, e a volte anche giudiziari, relativi a:

- personale dipendente, per la gestione del rapporto lavorativo, ivi comprese le malattie, gli infortuni, i pagamenti di quote associative, etc.;
- familiari del dipendente, per il riconoscimento delle indennità relative allo stato familiare;
- collaboratori e fornitori, per la gestione del rapporto contrattuale;
- soggetti che accedono alle biblioteche e agli archivi per motivi personali e/o di ricerca e di studio;
- soggetti, privati e/o giuridici, che ricevono contributi dal Ministero per lo svolgimento di attività culturali, siano esse di carattere letterario che cinematografico che sportivo;
- soggetti, privati e/o giuridici, che hanno attinenza con le attività istituzionali del Ministero.

A seguito dell'analisi compiuta sulle categorie di dati trattati, sono stati identificati i seguenti trattamenti svolti con o senza ausilio di strumenti elettronici (nel caso di trattamento con strumenti elettronici è indicata la sigla delle applicazioni utilizzate):

- SIAP - Gestione carriera del personale (costituzione del rapporto di lavoro, mobilità, estinzione del rapporto di lavoro)
- SIAPWEB- Visualizzazione del personale in servizio effettivo presso ciascun Istituto
- EUROPA-Sistema rilevazione presenze, gestione assenze per malattia,congedo per maternità,diritto allo studio,aspettative sindacali, motivi personali,maternità
- SICOGE-Gestione contabile
- PART -TIME-gestione rapporto di lavoro part –time
- GESTIONE INCARICHI- incarichi extraistituzionali art. 53 Dlgs n. 165/2001:incompatibilità
- GESTIONE FONDI- trattamento economico dirigenti
- RIQUALIFICAZIONE DEL PERSONALE- gestione delle procedure di riqualificazione
- SPT-Trattamento economico e previdenziale
- attuazione misure di sicurezza (d.lgs. N°626/94)
- Gestione del personale (tenuta fascicoli personali,gestione del contenzioso,procedimenti disciplinari)
- Sistema rilevazione presenze, gestione assenze per malattia,congedo per maternità,diritto allo studio,aspettative sindacali, motivi personali,maternità
- WTIME-Sistema rilevazione presenze, gestione assenze per malattia,congedo per maternità,diritto allo studio,aspettative sindacali, motivi personali,maternità
- Acquisizione di beni e servizi, esecuzione di lav. pubblici
- Concessioni finanziamenti a terzi
- Interventi economici in favore di soggetti che abbiamo attinenza con il settore dei beni e delle attività culturali - Legge Onesti
- Sistema Arca-Hugnot automation.s.p.a.-Sistema rilevazione presenze
- gestione assenze per malattia, congedo per maternità,diritto allo studio,aspettative sindacali, motivi personali,maternità
- Manifestazioni culturali
- Sistemi di VideoSorveglianza

Per ciascun trattamento sono riportate le seguenti informazioni.

- Identificativo del Trattamento: attività che implicano dati personali oggetto del trattamento;
- Categoria del dato: indica la presenza di dati personali, identificativi, sensibili, giudiziari;
- Categorie di soggetti cui si riferiscono i dati:
- "funzione Owner": Unità organizzativa preposta alla raccolta del dato: rappresenta la responsabilità organizzativa che gestisce il trattamento;
- Altre Unità Organizzative: sono le eventuali altre Direzioni e/o Uffici rispetto a quella preposta alla raccolta che contribuiscono all'effettuazione del trattamento;
- Descrizione sintetica del trattamento: Indica la tipologia di operazione che viene effettuata sul dato: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, interconnessione, blocco, comunicazione, diffusione, cancellazione, distruzione.
- Banca dati: indica la banca dati di riferimento su cui insiste il trattamento. In caso di trattamento di tipo cartaceo indica l'archivio di riferimento.

Tali informazioni sono state ottenute attraverso l'utilizzazione di questionari inviati alle Unità organizzative, interviste effettuate ai diversi responsabili delle funzioni e documentazione interna già esistente.

Codice Trattamento	Categoria del dato				Categoria soggetti		Funzione Owner					Altre unità organizzative					Descrizione sintetica del trattamento											
	Personale	Identificativo	Sensibile	Giudiziario	Pers.le dipendente	Altro	Dip. BAL	Dip. BCP	Dip. SS	Dip. RIO	D.G.AFF.GEN.	Dip. BAL	Dip. BCP	Dip. SS	Dip. RIO	D.G.AFF.GEN.	raccolta	registrazione	organizzazione	conservazione	consultazione	elaborazione	modificazione	selezione	estrazione	comunicazione	diffusione	cancellazione
T01.0 - SIAP	X	X			X						X				x		X	X	X	X	X	X	X	X	X	X		X
T02.0 - SIAPWEB	X	X			X						X	x	x	x							X			X	X	X		
T03.0 - EUROPA	X	X	X		X					X							X	X	X	X	X	X	X	X	X	X		X
T04.0 - SICOGE	X	X			X	X[1]	X	X	X	X							X	X	X	X	X	X	X	X	X	X		X
T05.0 - PART TIME	X	X			X		X	X	X		X						X	X	X	X	X	X	X	X	X	X		X
T06.0 - INCARICHI	X	X			X		X	X	X		X						X	X	X	X	X	X	X	X	X	X		X
T07.0 - FONDI	X	X			X						X						X	X	X	X	X	X	X	X	X	X		X
T08.0 - Riqualificazione	X	X			X						X	x	x	x	x		X	X	X	X	X	X	X	X	X	X		X
T09.0 - SPT	X	X			X						X						X	X	X	X	X	X	X	X	X	X		
T10.0 - L. 626/94	X	X	X		X		X	X	X		X						X	X	X	X	X	X				X		
T11.0 - Personale	X	X	X	X	X		X	X	X		X				x		X	X	X	X	X	X				X		
T12.0 - Presenze	X	X	X		X		X										X	X	X	X	X	X				X		
T12.5 - Assenze	X	X	X		X			X									X	X	X	X	X	X				X		
T13.0 - Arca	X	X			X			X									X	X	X	X	X	X	X	X	X	X		X

Codice Trattamento	Categoria del dato				Categoria soggetti		Funzione Owner					Altre unità organizzative					Descrizione sintetica del trattamento											
	Personale	Identificativo	Sensibile	Giudiziario	Pers.le dipendente	Altro	Dip. BAL	Dip. BCP	Dip. SS	Dip. RIO	D.G.AFF.GEN.	Dip. BAL	Dip. BCP	Dip. SS	Dip. RIO	D.G.AFF.GEN.	raccolta	registrazione	organizzazione	conservazione	consultazione	elaborazione	modificazione	selezione	estrazione	comunicazione	diffusione	cancellazione
T14.0 - Beni e Servizi	X	X				X[1]		X	X								X	X	X	X	X	X				X		
T15.0 - Manifestazioni	X	X				X[1]		X									X	X	X	X	X	X				X		
T16.0 - WTIME	X	X	X		X				X								X	X	X	X	X	X	X	X	X	X		X
T17.0 - Finanziamenti	X	X				X[2]			X								X	X	X	X	X	X				X		
T18.0 - Onesti	X	X		X		X[3]			X								X	X	X	X	X	X				X		
T19.0 - Videosorveglianza	X	X			X	X[3]	X	X	X	X	X							X	X	X	X					X		X

Tabella 1 - Elenco dei trattamenti

In relazione alla tabella 1, si precisano le seguenti abbreviazioni:

- DIP. BAL: Dipartimento per i Beni Archivistici e Librari
- DIP.BCP: Dipartimento per i Beni Culturali e Paesaggistici
- DIP. SS: Dipartimento per lo Sport e lo Spettacolo
- DIP. RIO: Dipartimento per la Ricerca, l'Innovazione e l'Organizzazione
- D.G.AFF.GEN.: Direzione Generale Affari Generali, Bilancio, Risorse Umane e Formazione

[1] Fornitori beni e servizi; Esecutori di lavori pubblici
[2] Privati; Associazioni Culturali
[3] Privati

2.3 Mappa di trattamenti effettuati

I dati sono trattati sia in maniera automatizzata sia in forma cartacea.

Il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi.
L'architettura del sistema informativo deputata ai trattamenti del MINISTERO si avvale di sistemi collegati in LAN presenti sia nelle Sedi e uffici centrali sia presso le sedi distaccate. Essi sono finalizzati al supporto alle attività operative ed istituzionali del MINISTERO ed all'automazione d'ufficio.
La piattaforma tecnologica utilizzata comprende sistemi MS/Windows, prevalentemente, e sistemi Unix, Microsoft Office per i sistemi distribuiti.
Le applicazioni sono basate sia su architettura Client/Server che su tecnologie Web.

Non sono adottati sistemi per la raccolta di dati personali attraverso siti Web disponibili al pubblico.

Il sito web istituzionale del MINISTERO, oltre a fornire informazioni di carattere generale, eroga un insieme di Servizi on-line, che rappresentano l'interfaccia più innovativa tra l'Amministrazione e i principali stakeholders: Cittadini, Aziende, Consulenti, Professionisti, Rappresentanze Diplomatiche e Consolari, Comuni d'Italia, Istituti Nazionali, Istituti Internazionali.
Il sito web fornisce i seguenti servizi, differenziati per classe di utenza :

- Prenotazione Musei:
  - Prevendita Ingressi
  - Prevendita Mostre
- Acquisto Pubblicazioni
- Multimedialità
- Biblioteche
- Archivi
- Paesaggi

Il Trattamento dei dati è affidato a personale del Ministero.

Tali soggetti operano con la qualificazione giuridica di Incaricati del trattamento ai sensi dell'Art. 30 della legge
Insieme all'atto di nomina, ai soggetti incaricati del trattamento sono impartite chiare istruzioni su come svolgere il compito assegnato.

Per lo svolgimento delle proprie attività, tuttavia, il MINISTERO affida l'elaborazione di alcune fasi di lavorazione dei dati a soggetti esterni.

Tali soggetti esterni operano con la qualificazione giuridica di Incaricati del trattamento ai sensi dell'Art. 30 della legge
Insieme all'atto di nomina, ai soggetti incaricati del trattamento sono impartite chiare istruzioni su come svolgere il compito assegnato.

Comunicazione
Viene effettuata la comunicazione dei dati solo ed esclusivamente ai soggetti previsti per legge o regolamento (MEF, INAIL, PARLAMENTO ecc)

Diffusione dei dati

L'Amministrazione non diffonde in alcuno modo i dati oggetto di trattamento

Riepilogo dei dati trattati

Dal riepilogo dei dati trattati (tabella di riferimento numero 1) e dall'identificazione degli strumenti utilizzati si deriva il seguente schema:

Identificativo trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia dei dispositivi di accesso	Tipologia di interconnessione
T01.0 - SIAP	Applicativo :SIAP Database: NEWSIAP	• Server c/o DIP. RIO • Archivi cartacei	• Client/Server • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T02.0 - SIAPWEB	Applicativo: SIAPWEB Database: NEWSIAP	• Server c/o DIP. RIO • Archivi cartacei	• Web • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T03.0 - EUROPA	applicativo: EUROPA database: EUROPASQL	• Server c/o DIP. RIO • Archivi cartacei	• Client/Server • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T04.0 - SICOGE	Applicativo: SICOGE Database: SICOGE_MBAC	• Server c/o DIP. RIO • Archivi cartacei	• Web • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T05.0 - PART TIME	Applicativo: PARTTIME Database: PARTTIME	• Server c/o DIP. RIO • Archivi cartacei	• Client/Server • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T06.0 - INCARICHI	Applicativo: GESTIONE INCARICHI Database: GESINCARICHI	• Server c/o DIP. RIO • Archivi cartacei	• Client/Server • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T07.0 - FONDI	Applicativo: GESTIONEFONDI Database: GESFONDI	• Server c/o DIP. RIO • Archivi cartacei	• Client/Server • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T08.0 - Riqualificazione	Applicativo: RIQUALIFICAZIONE DEL PERSONALE Database: RQP	• Server c/o DIP. RIO • Archivi cartacei	• Web • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T09.0 - SPT	Applicativo:SPT	• Server c/o MEF • Archivi cartacei	• Web • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T10.0 - L. 626/94	archivio cartaceo	• Archivi cartacei	• Accesso manuale agli archivi cartacei	
T11.0 - Personale	archivio cartaceo	• Archivi cartacei	• Accesso manuale agli archivi cartacei	
T12.0 - Presenze	archivio cartaceo	• Archivi cartacei	• Accesso manuale agli archivi cartacei	
T12.5 - Assenze	archivio cartaceo	• Server c/o DIP. SS • Archivi cartacei	• Accesso manuale agli archivi cartacei	
T13.0 - Arca	applicativo: sistema Arca-Hugnot automation s.p.a.	• Server c/o DIP. BCP • Archivi cartacei	• Client/Server • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T14.0 - Beni e Servizi	archivio cartaceo	• Archivi cartacei	• Accesso manuale agli archivi cartacei	
T15.0 - Manifestazioni	archivio cartaceo	• Archivi cartacei	• Accesso manuale agli archivi cartacei	
T16.0 - WTIME	Applicativo: WTime Database: File Sequenziale	• Server c/o DIP. SS • Archivi cartacei	• Client/Server • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T17.0 - Finaziamenti	Applicativo: FUS Database: Danza; Musica; Cinema; Sport; Luoghi dello spettacolo	• Server c/o DIP. SS • Archivi cartacei	• Client/Server • Accesso manuale agli archivi cartacei	Personal computer connesso alla rete lan o intranet geografica del Ministero
T18.0 - Onesti	Applicativo:	• Server c/o DIP. SS	• Client/Server	Personal computer connesso

Identificativo trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia dei dispositivi di accesso	Tipologia di interconnessione
	Commissione Onesti Database: ONESTI	• Archivi cartacei	• Accesso manuale agli archivi cartacei	alla rete lan o intranet geografica del Ministero

Tabella 2 - Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti

3 Distribuzione dei compiti e delle responsabilità (Regola 19.2)

3.1 Il Modello Organizzativo Privacy

Il MINISTERO, in qualità di Titolare del trattamento dei dati personali e nella persona del Ministro per i Beni e le attività culturali, dopo aver esaminato le responsabilità interne della propria struttura organizzativa, con particolare riferimento a quelle afferenti il trattamento dei dati personali, ha definito un proprio modello organizzativo Privacy, individuando contestualmente i soggetti responsabili del trattamento.

Ai sensi dell'Art. 29 ed in considerazione della particolare struttura del Ministero, suddivisa in Dipartimenti e dislocata su tutto il territorio nazionale, il Titolare ha ritenuto di costituire un apposito organismo, denominato 'Organismo Privacy e Sicurezza'' al quale affidare l'incarico di Responsabile del trattamento.

Il Ministero per i Beni e le attività culturali, sulla base delle disposizioni contenute nel D.Lgs 196/2003 ed al fine di ottemperare al meglio agli obblighi da esso derivanti, ha adottato il modello organizzativo rappresentato in Figura 1:

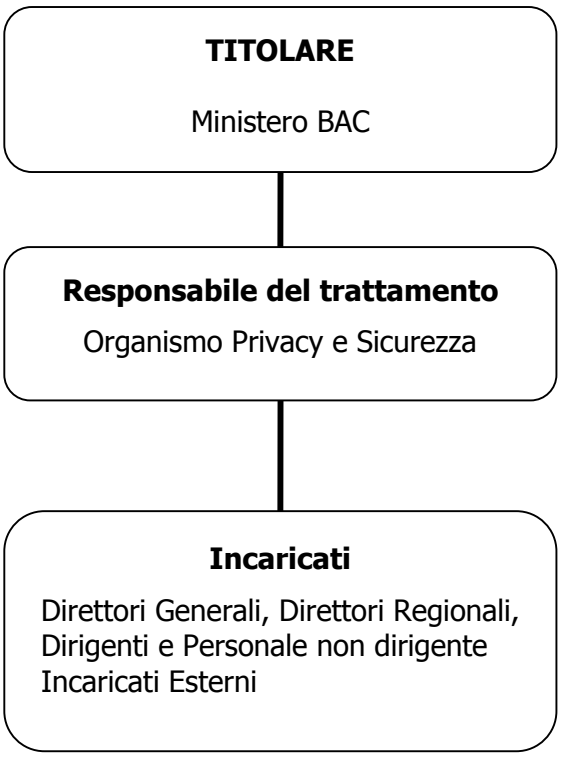


Figura 1. Modello Organizzativo Privacy adottato dal Ministero per i Beni e le attività culturali

3.2 Responsabile del Trattamento

Il Ministero per i Beni e le attività culturali, ai sensi dell'art. 29 del D.Lgs 196/2003, ha individuato in qualità di Responsabile un apposito organismo, che sarà designato con atto scritto, del quale faranno parte soggetti scelti tra coloro che per esperienza, capacità ed affidabilità, sono in grado di fornire idonee garanzie di rispetto delle vigenti disposizioni in materia di trattamento dei dati personali.

A questo ''organismo'' il Titolare, contestualmente al conferimento scritto della nomina, detterà le istruzioni alle quali lo stesso dovrà attenersi nell'espletamento delle funzioni ad esso affidate.

Periodicamente, ed ogni qualvolta se ne presenti la necessità, l'Organismo Privacy e Sicurezza' riferirà al Ministro aggiornandolo in merito allo stato di adeguatezza delle misure di tutela e/o sulle nuove rischiosità che incombono sui dati e proporrà le soluzioni più opportune per poterle contenere o eliminare.

3.3 Incaricati del trattamento dei dati

In esecuzione dei compiti assegnati, il Responsabile provvederà a conferire, ai sensi dell'art. 30 del D.Lgs. 196/2003, la nomina di Incaricato del trattamento ai Direttori, al personale Dirigente e non dirigente, in servizio presso gli Uffici di pertinenza, addetto a trattamenti di dati personali rilevanti ai fini della normativa in materia di Privacy.

La nomina ad Incaricato del trattamento sarà conferita con atto scritto.

Al personale incaricato è affidato il compito di trattare i soli dati personali necessari per lo svolgimento delle funzioni ad esso affidate, anche collettivamente, e di compiere le sole operazioni di trattamento a ciò strumentali, attenendosi anche ad eventuali ulteriori istruzioni contenute negli Ordini di servizio, ovvero impartite nel corso dell'attività e nel rispetto delle pertinenti disposizioni contenute in specifiche comunicazioni interne indirizzate alle categorie di incaricati interessati.

Le nomine ad incaricato sono estese, con analoghi criteri e modalità e per il solo periodo necessario, anche ai non dipendenti che occasionalmente svolgono operazioni di trattamento, compreso il personale esterno di società fornitrici di servizi, consulenti, manutentori, eventuali stagisti, che possono trovarsi a trattare dati sia necessariamente per le attività connesse all'espletamento delle mansioni, sia incidentalmente.

Istruzioni per gli incaricati

L'Incaricato, con l'atto di nomina, riceve chiare istruzioni e autorizzazioni per il trattamento e la gestione dei dati necessari ed indispensabili a svolgere le mansioni affidategli nel rispetto delle competenze dell'unità organizzativa di appartenenza.

Inoltre è stato predisposto e sarà pubblicato sul sito Intranet del Ministero il documento riportante le istruzioni per il trattamento, con e senza l'ausilio di strumenti elettronici, dei dati personali.

4 Analisi dei Rischi (Regola 19.3)

L'analisi dei rischi valuta sia eventi tecnici sia organizzativi e ciò anche in considerazione delle previsioni degli 'Artt. 11 e 15 del D.Lgs. 196/2003 e del richiamato art. 2050 del c.c..

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

L'esame dei rischi viene effettuato tenendo conto della natura dei dati, distinti tra dati identificativi, personali, sensibili e giudiziari, e delle caratteristiche del trattamento.

L'obiettivo generale della sicurezza delle informazioni consiste nel garantire tre proprietà fondamentali ad esse associabili:

- Riservatezza, ovvero assicurare che le informazioni siano accessibili solo alle persone autorizzate;
- Integrità, cioè tutelare l'esattezza e la completezza delle informazioni e dei metodi con cui sono elaborate e/o processate;
- Disponibilità, ovvero assicurare che gli utenti autorizzati possano accedere alle informazioni e ai beni, quando è richiesto.

Tutti i rischi esaminati sono quindi individuati, classificati e descritti, nei seguenti principali raggruppamenti:

1. rischi sull'integrità dei dati;
2. rischi sulla riservatezza dei dati, di trattamenti non consentiti o non conformi alle finalità della raccolta;
3. rischi sulla disponibilità dei dati.

In relazione alla tipologia di rischi considerati, nel capitolo dedicato alle Contromisure Adottate, sono descritti gli accorgimenti tecnici e organizzativi implementati, quali contromisure idonee alla riduzione e/o eliminazione del livello di rischio.
Nei paragrafi che seguono, per ogni classe di rischio, sono indicati gli eventi o le circostanze, ritenuti possibili o probabili, che possono dar luogo ad incidenti sull'integrità e la disponibilità dei dati.
Il capitolo sull'Analisi dei Rischi conclude con una tabella di riepilogo che, a fronte dei rischi considerati, indica la valenza di impatto.

4.1 Rischi sull'Integrità dei dati

Sulla base del concetto di integrità dei dati, riportato precedentemente, l'accertamento della stessa riguarda la protezione dei dati dai rischi di possibili modifiche o distruzione accidentali o deliberata.

I rischi possibili circa le minacce all'integrità dei dati possono essere classificati in:

1. rischi di carattere accidentale: riguardano l'involontaria distruzione dei dati imputabili ad azioni umane errate oppure a guasti delle apparecchiature dedicate alla memorizzazione;
2. rischi da programmi di cui all'art.615 quinquies del codice penale: rischi connessi alla diffusione dei virus e di programmi pericolosi;

3. rischi di carattere volontario: alterazioni dell'integrità conseguenti ad una teorica azione deliberatamente perpetrata allo scopo di modificare, inserire o distruggere volontariamente i dati.

4.2 Rischi sulla Riservatezza dei dati

In questa categoria rientrano i rischi di trattamenti non consentiti o non conformi alle finalità della raccolta.
I possibili eventi, posti in relazione al rischio di accesso non autorizzato, sono collegabili a due fattispecie:

1. rischi di accessi fraudolenti dall'interno: sono dovuti a:
   - profilo di autorizzazione all'accesso non aderente al ruolo assegnato o conseguente all'attribuzione di privilegi di accesso eccessivi;
   - inferenza ossia cattura di informazioni che consentono, correlate tra loro, di giungere alla conoscenza indiretta di dati;
   - utilizzo dei privilegi di amministratori di sistema per l'accesso ad archivi;
   - manomissione delle autorizzazioni da parte del personale addetto al controllo e all'amministrazione dei profili di accesso.
2. rischi di accessi fraudolenti dall'esterno: sono dovuti a:
   - accessi tramite sistemi di collegamento remoto installati per la manutenzione o la trasmissione di software;
   - intercettazione di comunicazioni telematiche.

4.3 Rischi sulla Disponibilità dei dati

I dati devono essere sempre disponibili al momento di una richiesta effettuata da personale (o sistemi) in possesso delle autorizzazioni necessarie.
I rischi di non disponibilità sono determinati da:

1. eventi di natura accidentale: in questa tipologia di rischi è stata compresa l'eventualità che le informazioni non siano disponibili a causa di eventi non volontari e/o non previsti,
2. eventi di natura intenzionale: in questa tipologia di rischi rientrano i casi in cui le informazioni non sono disponibili a causa di azioni volontarie, poste in essere con lo scopo preciso e determinato di impedire l'accesso alle informazioni da parte dei soggetti che detengono il pieno diritto di farlo.

4.4 Riepilogo dell'analisi dei rischi

Sulla base delle considerazioni fatte in precedenza, di seguito vengono indicati i livelli di rischio individuati. Per alcuni assets (es. edifici, applicazioni), non classificabili come direttamente contenenti dati, il rischio è indicato in relazione al danno che, potenzialmente, può essere provocato sui dati in conseguenza del verificarsi di eventi rischiosi cui tali assets sono soggetti.

La tabella seguente riepiloga gli eventi considerati nell'analisi dei rischi esposta nei paragrafi precedenti, evidenziandone la gravità dell'impatto, che è stimata nei tre livelli riportati.

	Minaccia	ASSET								
		edifici	uffici e locali	locali tecnici	archivi cartacei	Web Server	banche dati su Server	banche dati su Client	Altri Server	Reti
Errori e malfunzionamenti	Errori in fase di progettazione					Basso	Medio	Basso	Medio	Medio
	Errori in fase di back-up					Alto	Alto	Alto	Alto	
	Errori in fase di aggiornamento e manutenzione del software					Medio	Medio	Basso	Medio	Medio
	Errori in fase di aggiornamento e di manutenzione dell'hardware					Medio	Medio	Medio	Medio	Medio
	Errori in fase di aggiornamento e di manutenzione della rete									Medio
	Malfunzionamento software (sia di sistema sia applicativo)					Medio	Medio	Medio	Medio	Medio
	Malfunzionamento hardware					Medio	Medio	Medio	Medio	Medio
	Malfunzionamento della rete					Basso	Basso	Basso	Basso	Alto
	Sovrascrittura della memoria di massa					Basso	Alto	Alto	Basso	
	Sovraccarico elaborativo del sistema					Medio	Alto	Medio	Medio	Medio
Frodi e furti	Furto di hardware					Basso	Basso	Basso	Basso	Basso
	Acquisizione di dati da supporti cartacei				Basso					
	Acquisizione dati su supporti magnetici					Medio	Medio	Medio	Medio	Medio
	Manipolazione di software e dati					Basso	Basso	Basso	Basso	Basso
	Uso improprio di privilegi					Basso	Basso	Basso	Basso	Basso
Danneggiamenti fisici	Indisponibilità dei sistemi in seguito a eventi ineluttabili (naturali e non)					Basso	Basso	Basso	Basso	Basso
	Inagibilità dei locali					Basso	Basso	Basso	Basso	Basso
	Danneggiamento delle reti					Basso	Basso	Basso	Basso	Basso
	Danneggiamento hardware (dispositivi, schede)					Basso	Basso	Basso	Basso	Basso
	Interruzione servizi elettrici, condizionamento d'aria					Basso	Basso	Basso	Basso	Basso
Altre minacce	Accesso non autorizzato al sistema					Medio	Medio	Medio	Medio	Medio
	Modifica non autorizzata dei privilegi					Medio	Medio	Medio	Medio	Medio
	Alterazione instradamento di rete					Basso	Basso	Basso	Basso	Medio
	Intercettazione del traffico di rete									Medio

	Minaccia	ASSET								
		edifici	uffici e locali	locali tecnici	archivi cartacei	Web Server	banche dati su Server	banche dati su Client	Altri Server	Reti
	Introduzione di software dannoso					Medio	Medio	Alto	Medio	Medio
Altre minacce interne	Manipolazione di software					Basso	Basso	Basso	Basso	
	Abuso di privilegi					Medio	Medio	Alto	Medio	Medio
	Utilizzo illecito del sistema (hardware/software/rete)					Medio	Medio	Alto	Medio	Medio
	Sovraccarico del sistema elaborativo/trasmissivo.					Medio	Medio	Alto	Medio	Medio
Comportamenti degli operatori	sottrazioni di credenziali di utenticazione non correttamente custodite					Alto	Alto	Alto	Alto	Alto
	carenza di consapevolezza disattenzione o incuria (comportamento colposo)					Medio	Medio	Alto	Medio	Alto
	comportamenti sleali o fraudolenti (comportamenti dolosi)					Alto	Alto	Alto	Alto	Alto
	errore materiale commesso dall' operatore nell'espletamento della attività					Alto	Alto	Alto	Alto	Alto
Eventi relativi al contesto fisico ed ambientale	accessi non autorizzati a locali/reparti ad accesso ristretto	Medio	Medio	Medio	Medio	Medio	Basso	Alto	Basso	Medio
	sottrazione di strumenti contenenti dati	Medio	Medio	Medio	Medio	Medio	Basso	Alto	Basso	Medio
	eventi distruttivi, naturali o artificiali (movimenti tellurici, incendi, allagamenti, scariche atmosferiche, condizioni ambientali, ecc..), nonché dolosi, accidentali o dovuti ad incuria	Basso	Basso	Basso	Basso	Medio	Medio	Medio	Medio	Medio
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Basso	Basso	Basso	Basso	Medio	Medio	Medio	Medio	Medio
	errori umani nella gestione della siicurezza fisica	Basso	Basso	Basso	Basso	Medio	Medio	Medio	Medio	Medio

Tabella 3: valutazione dei rischi

	Minaccia	IMPATTO		
		Riservatezza	Integrità	Disponibilità
Errori e malfunzionamenti	Errori in fase di progettazione	x	x	x
	Errori in fase di back-up		x	
	Errori in fase di aggiornamento e manutenzione del software		x	x
	Errori in fase di aggiornamento e manutenzione hardware		x	x
	Errori in fase di aggiornamento e manutenzione della rete	x		x
	Malfunzionamento software (sia di sistema sia applicativo)		x	x
	Malfunzionamento hardware		x	x
	Malfunzionamento della rete			x
	Sovrascrittura della memoria di massa		x	
	Sovraccarico elaborativo del sistema			x
Frodi e furti	Furto di hardware	x		x
	Acquisizione di dati da supporti cartacei	x		x
	Acquisizione dati su supporti magnetici	x		
	Manipolazione di software e dati	x	x	x
	Uso improprio di privilegi	x	x	x
Software dannoso	Introduzione di software dannoso	x	x	x
Danneggiamenti fisici	Indisponibilità dei sistemi in seguito a eventi ineluttabili (naturali e non)		x	x
	Inagibilità dei locali			x
	Danneggiamento delle reti			x
	Danneggiamento hardware (dispositivi, schede)		x	x
	Interruzione servizi elettrici, condizionamento d'aria		x	x
Altre minacce esterne	Accesso non autorizzato al sistema	x	x	x
	Modifica non autorizzata dei privilegi	x	x	
	Alterazione instradamento di rete	x	x	
	Intercettazione del traffico di rete	x		
	Sovraccarico del sistema elaborativo/trasmissivo			x
Altre minacce interne	Manipolazione di software		x	
	Abuso di privilegi	x	x	x
	Utilizzo illecito del sistema (hardware/software/rete)	x	x	x
	Sovraccarico del sistema elaborativo/trasmissivo.			x

	Minaccia	IMPATTO		
		Riservatezza	Integrità	Disponibilità
Comportamenti degli operatori	sottrazioni di credenziali di autenticazione (sottrazione di nome utente e password non correttamente custodite)	x	x	x
	carenza di consapevolezza disattenzione o incuria (comportamento colposo da parte dell'operatore)	x	x	x
	comportamenti sleali o fraudolenti (comportamenti dolosi da parte dell'operatore)	x	x	x
	errore materiale (errore commesso dall' operatore nell'espletamento della sua attività)	x	x	x
Eventi relativi al contesto fisico ambientale	accessi non autorizzati a locali/reparti ad accesso ristretto	x	x	x
	sottrazione di strumenti contenenti dati	x		x
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc..), nonché dolosi, accidentali o dovuti ad incuria		x	x
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc..)		x	x
	errori umani nella gestione della sicurezza fisica	x	x	x

Tabella 4: Individuazione dell'impatto

5 Contromisure di Sicurezza (Regola 19.4)

Di seguito vengono descritte le misure di sicurezza in essere e da adottare, in conformità alla regola 19.4. I dettagli relativi all'analisi dello stato della sicurezza delle informazioni gestite dal MINISTERO sono riportate nell'allegato 1.
Si precisa che sono in atto le attività necessarie alla implementazione delle misure di sicurezza sulle diverse piattaforme e nel frattempo sono state attivate procedure, normative e soluzioni organizzative nel senso auspicato dalla norma.

5.1 Misure di sicurezza logica

Le misure di sicurezza logiche riguardano i criteri che sono seguiti dai diversi programmi software, di sistema o applicativi, per controllare l'accesso degli utilizzatori alla rete locale (ed eventuali interconnessioni esterne), alle stazioni di lavoro individuali, agli Elaboratori ed alle funzionalità applicative.
Le misure di sicurezza logica possono essere sinteticamente riassunte nelle seguenti categorie:

- Identificazione e Autenticazione: misure atte a verificare l'identità di un incaricato/utente nel momento in cui richiede un accesso al sistema. Detta verifica è vincolante, ai fini della sicurezza, per l'accesso alle risorse informatiche da parte dell'utente stesso. Solo in caso di esito positivo, il sistema concederà all'utente l'accesso alla normale operatività; in caso contrario l'accesso non sarà consentito. L'affidabilità del controllo dell'identità dipende da informazioni conservate all'interno del sistema, informazione che devono essere memorizzate in modo protetto.
- Controllo autorizzazione alle funzionalità/servizi: misure che garantiscono che un incaricato/utente possa espletare le sole operazioni di sua competenza. Fra tali funzionalità vanno previste quelle di amministrazione dei diritti di accesso e della loro verifica.
- Controllo autorizzazione ai dati: misure che garantiscono che il processo e/o l'incaricato/utente possano operare solo sui dati di propria competenza. Tra tali funzioni vanno previste quelle di amministrazione dei diritti di accesso e della loro verifica.
- Tracciamento: misure mirate a registrare gli accessi alle varie risorse (dati e programmi) del sistema informatico rilevanti per gli aspetti di sicurezza.
- Sistemi che evidenziano eventi anomali: misure che permettono di investigare sugli eventi che possono rappresentare una minaccia alla sicurezza. Tali strumenti devono consentire di identificare selettivamente le azioni eseguite da uno o più utenti. Periodicamente controllano le registrazioni per verificare casi anomali o sospetti. Permettono l'Alert on line o differito del superamento di opportune soglie di sicurezza predefinite.
- Oscuramento dati d'archivio: misure tese ad inibire la lettura delle informazioni memorizzate nella base dati (ad esempio tramite cifratura) per garantirne la riservatezza.
- Sistemi di riutilizzo supporti magnetici: misure che permettono l'analisi del software e dei dati al fine di identificare, segnalare e correggere violazioni all'integrità. Fra tali funzioni vi sono quelle di identificazione ed eliminazione dei Virus, di analisi della integrità degli indici di una base dati.
- Duplicazione dati/risorse: misure tese a garantire la ridondanza dei dati e delle risorse al fine di un ripristino in caso di indisponibilità. Tra tali funzioni vi sono quelle di salvataggio periodico (backup), mirroring dei dischi, jogging.
- Controllo interscambio dati: misure tese a garantire la sicurezza nelle trasmissioni di dati attraverso l'autenticazione dell'originatore, l'integrità e la riservatezza del contenuto del messaggio, il non ripudio dell'originatore e del destinatario.

5.1.1 Controllo Accessi

L'accesso alle risorse informatiche avviene attraverso differenti modalità, secondo gli ambienti applicativi disponibili.
In generale è previsto un profilo di abilitazione che definisce per ogni soggetto incaricato del trattamento:

- l'accesso agli archivi presenti sugli Elaboratori e i relativi diritti (sola lettura, modifica, ecc..);
- l'accesso alle applicazioni presenti sugli Elaboratori e le relative funzionalità applicative abilitate;
- la possibilità di interconnessioni con reti esterne e/o piattaforme di altri Enti;
- l'accesso, limitatamente ai trattamenti autorizzati che prevedono l'utilizzo di dati sensibili, alle stazioni di lavoro dalle quali è possibile trattare tali dati.

L'accesso diretto agli Elaboratori è consentito esclusivamente agli Incaricati muniti di autorizzazione.
Ogni utilizzatore del sistema è identificato mediante una credenziale composta da un codice identificativo personale (pubblico) congiuntamente ad una password (privata); in caso di necessità, a seguito di vincoli tecnici, ad uno stesso soggetto possono essere assegnate più credenziali.

5.1.2 Autenticazione e identificazione degli utenti

- Codice identificativo (User-id): A tutti i destinatari di un incarico per il trattamento viene attribuito un codice identificativo personale per l'utilizzo delle risorse informatiche. Lo stesso codice non può, neppure in tempi diversi, essere assegnato a persone diverse. Ad ogni codice è associato un profilo di abilitazione. In caso di revoca dell'incarico e/o dell'autorizzazione, intervengono le procedure organizzative al fine di rendere inutilizzabile, o di modificare, a seconda delle necessità, sia il codice che il profilo stesso.
- Password: Ad ogni codice identificativo è associata una parola chiave. Al primo utilizzo, il dipendente ha l'obbligo di modificarla attenendosi alle seguenti regole e, comunque, tenendo presente che la password:
  - deve essere alfanumerica, di 8 caratteri o del numero massimo previsto dalle procedure;
  - non deve essere composta utilizzando lo user-id;
  - non deve essere ottenuta anagrammando la precedente;
- Profili di accesso: Ogni utente ha accesso alle sole informazioni che risultano necessarie allo svolgimento del proprio compito aziendale. I profili di accesso alle risorse informatiche devono essere stabiliti in base al ruolo ricoperto da ciascun utente. Ciò avviene anche attraverso i limiti stabiliti e le istruzioni impartite ai dipendenti attraverso la lettera di incarico per il trattamento loro consentito.

Relativamente ai profili di accesso, l'Amministrazione si propone di verificare l'attuale organizzazione delle autorizzazioni e, dove necessario, di apportare le opportune razionalizzazioni.

In merito alle regole di gestione della password (lunghezza, complessità, scadenza, etc.), l'Amministrazione provvederà ad una puntuale verifica dei sistemi e delle applicazioni per verificare il possibile adeguamento a quanto disposto dalla normativa.
Sull'argomento, sono fornite chiare istruzioni agli incaricati del trattamento anche attraverso la lettera di incarico.

5.1.3 Sviluppo e gestione dei progetti applicativi

Tutti i progetti applicativi gestiti in autonomia dal MINISTERO, che riguardano il trattamento di dati personali, prevedono una verifica di congruità con le prescrizioni indicate nel presente documento.
Le altre applicazioni in dotazione al MINISTERO, rese disponibili da Enti esterni, sono depositarie della completa gestione anche sotto il profilo della sicurezza.
Le procedure informatiche realizzate, prima di essere inserite in ambiente di produzione, vengono sottoposte ad una verifica sulla qualità/affidabilità del software e successivamente ad autorizzazione da parte del MINISTERO.
L'accesso all'ambiente di produzione è consentito ai soli soggetti autorizzati. I dati presenti negli archivi sono protetti secondo le misure di sicurezza identificate.

5.1.4 Archivi sulle stazioni di lavoro individuali

In generale, per quanto riguarda le stazioni di lavoro individuali, la presenza di archivi sulle stesse viene considerata di tipo eccezionale, a fronte di esigenze particolari, di elaborazioni individuali e, comunque, a carattere temporaneo. L'accessibilità ed integrità di detti archivi non è garantita e le responsabilità in materia di sicurezza sono di carattere personale del soggetto assegnatario della stazione di lavoro.
Non è consentito dalle singole stazioni di lavoro condividere in rete archivi mediante funzionalità server.
Per quanto attiene le stazioni di lavoro portatili (laptop), le stesse sono dotate di sistema operativo atto a garantire la protezione degli archivi mediante utilizzo di identificativo-password. Particolari indicazioni circa l'adeguato utilizzo del sistema, soprattutto in caso di dati personali sensibili, sono impartite attraverso le istruzioni allegate alla nomina.

5.1.5 Gestione dei supporti di memorizzazione

Per evitare la diffusione di informazioni e' necessario, non solo garantire la sicurezza degli accessi ai sistemi informativi, ma anche un corretto approccio nella gestione e nel trattamento dei supporti magnetici sui quali risiedono le informazioni, in modo da verificare che non siano danneggiati o obsoleti. A tale proposito il regolamento interno, in corso di diffusione, per gli incaricati e per gli addetti all'amministrazione dei sistemi, contiene le indicazioni relative alla gestione dei supporti utilizzati.

5.1.6 Protezione antivirus

Tutti i sistemi sensibili ad attacchi, di cui al di cui all'articolo 615 quinquies del codice penale, sono protetti mediante idonei programmi, la cui efficacia e il cui aggiornamento sono verificati con cadenza almeno semestrale.
Le contromisure adottate per la protezione da virus via posta elettronica sono affidate e garantite dall'attuale gestore.

5.2 Misure di sicurezza fisica

Le misure di sicurezza fisica riguardano gli aspetti relativi al controllo degli accessi fisici ed alla protezione dei locali.
Le misure di sicurezza fisiche possono essere sinteticamente riassunte nelle seguente categorie:

- Sistemi di rilevazione passiva: impianti che rilevano la presenza di situazioni logistiche anomale (accessi, incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo senza attivare contromisure.

- Sistemi di rilevazione attiva: impianti che rilevano la presenza di situazioni logistiche anomale (incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo e attivando una specifica contromisura.
- Sistemi di controllo accessi fisici: impianti che regolano l'accesso fisico in determinate aree riservate alle sole persone e mezzi autorizzati.
- Sistemi di continuità di alimentazione: impianti che garantiscono una continuità dell'alimentazione elettrica ai sistemi, almeno per una chiusura ordinata.
- Infrastrutture: accorgimenti generici sugli edifici e disposizione dei locali al fine di garantire la sicurezza (edifici antisismici, uscite di sicurezza allarmate, separazione ambienti a rischio, ecc.).

5.2.1 Controllo accessi agli edifici

Gli edifici sono protetti, nel normale orario lavorativo, mediante servizio di vigilanza.
L'accesso del personale agli edifici è consentito mediante esibizione alla vigilanza dell'apposito badge.
I visitatori/ospiti che accedono agli edifici devono essere identificati presso il servizio di vigilanza, che provvederà a dotare il visitatore di apposito badge.

Aree in Sicurezza

Per Area di Sicurezza si intende: sala macchine, locali tecnici, nastroteche, archivi di sicurezza, etc..
L'accesso alle aree di Sicurezza è riservato al personale autorizzato.

Organizzazione dei Locali di Sicurezza

Nei Locali di Sicurezza sono custodite le apparecchiature ed i supporti magnetici e/o cartacei per i trattamenti automatizzati. In particolare:

- le apparecchiature di elaborazione dei trattamenti con esclusione delle stazioni di lavoro individuali e delle apparecchiature passive di rete (hub, cavi, ecc..);
- i supporti magnetici e/o cartacei utilizzati nei trattamenti (documenti, tabulati, supporti di backup, ecc.), con esclusione di quanto elaborato o prodotto localmente presso le stazioni di lavoro individuali.

Dispositivi di sicurezza e allarme.

Il MINISTERO prevede, per i propri Locali di Sicurezza, i seguenti dispositivi:

- allarme antincendio;
- allarme anti-intrusione;
- estinzione automatica di incendio;
- presenza di gruppi di continuità e di condizionamento.

5.3 Misure di sicurezza organizzativa

Le misure di sicurezza organizzative sono sinteticamente riassunte nelle seguenti categorie:

- Ruoli e responsabilità: descrizione di figure aziendali operative che gestiscono aspetti di sicurezza evidenziando la responsabilità ed attività di loro competenza in ambito IT.
- Norme di utilizzo e comportamento: documentazione rivolta agli incaricati/utenti che descrive le norme comportamentali e procedurali da applicare per un utilizzo sicuro del sistema e delle informazioni.
- Procedure di gestione: documentazione rivolta agli incaricati dedicata alla gestione degli aspetti di sicurezza descrivente le modalità di svolgimento delle attività di loro competenza.

- Formazione: attività tesa a istruire gli incaricati e gli utenti che operano su dati personali e sensibili al fine di utilizzare al meglio i dispositivi di sicurezza progettati e di far conoscere ed applicare la norma relativa.
- Sensibilizzazione e comunicazione: attività rivolta a tutti gli utenti per sensibilizzarli alle problematiche generali di sicurezza e alle relative norme.

5.3.1 Riutilizzo controllato dei supporti

Gli incaricati sono autorizzati per iscritto a svolgere operazioni di trattamento di dati personali.
In particolare, debbono custodire e controllare i supporti magnetici sui quali sono registrati i dati sensibili in maniera che nessun soggetto non autorizzato possa venirne a conoscenza, neppure accidentalmente.
I citati supporti non devono assolutamente essere utilizzati da soggetti privi di adeguata autorizzazione.

5.3.2 Installazione di software non autorizzato

E' vietato l'utilizzo di software non ufficialmente rilasciato dall'Amministrazione e preventivamente testato nella sua integrità.
È parimenti vietata l'installazione, senza preventiva autorizzazione, sui sistemi del MINISTERO anche di software distribuito con la formula del freeware (ovvero in forma gratuita) o shareware (ovvero in prova).

5.3.3 Risorse condivise

Per i sistemi che governano risorse condivise, come per esempio le stampanti, sottosistemi condivisi, fax, ecc. il servizio preposto fornisce precise istruzioni per garantire la protezione dei dati e delle transazioni senza bloccare l'operatività degli altri utenti.
In generale, prima di abbandonare il proprio posto di lavoro, l'utente dovrà provvedere a chiudere tutte le connessioni attive che sono state aperte con il suo codice identificativo lasciando attive solamente le applicazioni condivise.
La stazione di lavoro deve essere quindi protetta con il programma salvaschermo.

5.3.4 Salva- schermo (screen saver)

Su tutte le stazioni di lavoro deve essere installato, in ambiente Windows, uno *salva-schermo* che entra in funzione automaticamente dopo un numero prefissato di minuti di inattività.
L'utente deve attenersi a precise norme, quali:

- impostare una password da digitare per la ripresa dell'attività;
- non disattivare lo strumento salva-schermo;
- impostare un tempo di attesa per l'entrata in funzione del salva-schermo non superiore a 10 minuti.

5.3.5 Trattamento dei Dati Personali con strumenti diversi da quelli elettronici

I dati personali devono essere custoditi in archivi dotati di meccanismi di chiusura che permettono l'accesso agli stessi ai solo Incaricati che debbano conoscere i dati in essi custoditi in relazione allo svolgimento delle proprie mansioni.
In ogni caso, gli Incaricati non debbono accedere ai Dati Personali la cui conoscenza non sia strettamente necessaria per adempiere alle mansioni loro assegnate.
Gli Incaricati devono custodire i documenti contenenti i Dati Personali in contenitori muniti di serratura fino all'archiviazione nell'archivio di provenienza.

Le riproduzioni, anche parziali, di documenti contenenti dati personali e sensibili e/o informazioni relative al trattamento devono essere conservati e custoditi con le medesime modalità previste per i documenti originali.

Tali documenti possono essere resi disponibili a terzi soggetti esterni al MINISTERO, solo nel caso in cui i medesimi soggetti siano stati nominati incaricati del trattamento dal MINISTERO. I documenti contenenti dati personali possono essere comunicati all'esterno qualora sussistano le seguenti condizioni: consenso dell'Interessato, obbligo di legge o contrattuale, necessità di far valere un diritto in giudizio, dati pubblici o conoscibili da chiunque, ecc.

5.3.6 Istruzioni e regole di comportamento

Contestualmente all'atto di nomina gli Incaricati ricevono le istruzioni, sul trattamento dei dati personali, alle quali devono attenersi durante lo svolgimento delle proprie attività lavorative.
Ulteriori istruzioni sono contenute nel regolamento interno, portato a conoscenza di tutti gli incaricati.
Le principali regole di comportamento, e le relative modalità di attuazione, riguardano:

- custodia e utilizzo della password di accesso al sistema informativo aziendale;
- accessibilità agli strumenti elettronici che non devono essere lasciati incustoditi durante una sessione di lavoro;
- salvataggio dei dati sulla postazione di lavoro;
- custodia dei supporti, informatici e cartacei, sui quali sono registrati i dati;
- maggiori cautele in materia di trattamento dei dati sensibili e giudiziari, siano essi presenti in formato elettronico che cartaceo;
- modalità di custodia e conservazione dei documenti contenenti dati sensibili e giudiziari;
- custodia degli archivi informatici e cartacei;
- aggiornamento sulle misure di sicurezza disposte dal Titolare.

5.4 Misure da adottare

5.4.1 Misure di sicurezza logica

Le attività di gestione della sicurezza logica, ossia di autorizzazione e controllo dell'accesso alle funzioni applicative e ai dati, all'aggiornamento degli stessi da parte degli utenti, sono effettuate tramite le funzionalità messe a disposizione dai sistemi operativi e dalle applicazioni. Il MINISTERO si propone di avviare le opportune attività di verifica e normalizzazione per quanto concerne la corretta definizione ed attribuzione di profili di autorizzazione all'utilizzo delle risorse informatiche.

Relativamente alle modalità di gestione della password (lunghezza, modifica, scadenza, etc.) sono in atto le attività necessarie alla implementazione delle misure di sicurezza sulle diverse piattaforme e nel frattempo sono state attivate procedure, normative e soluzioni organizzative nel senso auspicato dalla norma".

Per quanto riguarda la gestione delle vulnerabilità degli strumenti elettronici, il MINISTERO stà valutando l'opportunità di utilizzare strumenti tecnologici.

5.4.2 Misure di sicurezza fisica

Gli accessi agli edifici e ai locali presentano una rischiosità di tipo medio, il MINISTERO si ripropone di verificare la corretta predisposizione di idonei dispositivi di controllo, quali:

- impianti che rilevano la presenza di situazioni logistiche anomale (incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo per la segnalazione e/o l'attivazione di specifiche contromisure;
- impianti che garantiscono una continuità dell'alimentazione elettrica ai sistemi, almeno per operazioni indispensabili;
- accorgimenti generici sugli edifici e disposizione dei locali al fine di garantirne la sicurezza (uscite di sicurezza allarmate, separazione ambienti a rischio, ecc.).
- impianti che regolano l'accesso fisico in determinate aree riservate alle sole persone e mezzi autorizzati;

Sono installate, anche se non in modo generalizzato, videocamere atte a monitorare il perimetro degli edifici del MINISTERO o di sue sedi periferiche (musei, archivi di Stato, biblioteche, etc.) e a controllare gli ingressi ai locali. Allo scopo, il MINISTERO, si propone di aggiornare e dettagliare la tipologia e le modalità di utilizzo dei sistemi di videosorveglianza.

Particolare attenzione viene riservata alla custodia degli archivi e dei documenti cartacei.

Allo scopo, il MINISTERO provvede a:

- destinare ad archivi solo locali dotati di meccanismi di chiusura che consentano un accesso selezionato e riservato ai soli Incaricati autorizzati;
- emanare apposita normativa per l'utilizzo e la custodia dei documenti personali, contenenti dati sensibili, in modo che gli Incaricati:
    - durante il ciclo di lavorazione, custodiscano i documenti cartacei in contenitori muniti di serratura;
    - al termine del citato ciclo, provvedano a riportare la documentazione nell'archivio di provenienza;
    - non possano, in alcun modo, accedere ai dati personali la cui conoscenza non sia strettamente necessaria per adempiere alle mansioni loro assegnate;
    - dopo l'orario di chiusura degli uffici, vengano identificati e registrati, in un apposito registro tenuto dagli addetti al ricevimento, i soggetti che accedono ai citali locali.
- le riproduzioni, anche parziali, di documenti contenenti dati personali e sensibili e/o informazioni relative al trattamento devono essere conservati e custoditi con le medesime modalità previste per i documenti originali.

I responsabili degli uffici operativi agiscono e vigilano sulla corretta applicazione delle presenti procedure.

5.4.3 Misure di sicurezza organizzativa

Il MINISTERO provvederà a formalizzare la costituzione del "Organismo Privacy e Sicurezza" informando tutta la struttura sulle motivazioni della scelta e sulle finalità della costituzione stessa.
Il "Comitato Privacy e Sicurezza" provvederà, attraverso i propri componenti ad attivarsi per tutte le incombenze che gli competono in materia di trattamento dei dati personali e ampiamente descritte nel capitolo allo stesso dedicato.
Particolare risalto sarà dato alla informazione e formazione di tutti gli incaricati al fine di pervenire ad un adeguamento organizzativo e di comportamento in linea con quanto prescritto dal D.Lgs. 196/03 e al Disciplinare Tecnico in Allegato B).

6 Criteri e modalità di ripristino della Disponibilità dei dati (Regola 19.5)

Le attività svolte per la garanzia della continuità e della sicurezza fisica del servizio sono quelle rivolte esclusivamente all'integrità fisica dei dati, basate cioè sul salvataggio, con cadenza giornaliera o secondo necessità, di tutti i dati e sul relativo corretto ripristino di tutte le informazioni salvate.
Il salvataggio di sicurezza dei dati viene attualmente effettuato, per ogni server, con l'ausilio degli strumenti software messi a disposizione dai sistemi operativi, su dischi secondari che periodicamente vengono riversati su nastro magnetico.
La scelta di utilizzare i dischi secondari per il salvataggio delle informazioni è scaturita dalla possibilità di semplificare e ridurre i tempi di ripristino in caso di malfunzionamento o perdita (anche parziale) delle informazioni.
L'ulteriore copia su nastro magnetico, permette di avere una ubicazione differenziata dei dati e quindi di ridurre i rischi ambientali, oltre che di ripristinare le informazioni su supporti hardware sostitutivi (in casi di indisponibilità di quelli primari). Le copie su nastro magnetico vengono, infatti, conservate nell'armadio ignifugo sito nei locali tecnici.

7 Piano di Formazione (Regola 19.6)

Le misure minime di sicurezza previste dall'articolo 31 del D.Lgs. 196/03 ed analiticamente individuate dall'allegato B (D.Lgs.196/03), prevedono che sia realizzato per gli incaricati un piano di formazione per renderli edotti dei rischi che incombono sui dati.

Il MINISTERO, in conformità alla legge e in considerazione delle diverse figure professionali, stà predisponendo programmi diversi per la formazione dei Responsabili e per quella degli Incaricati.

Attualmente è stata erogata la formazione ai Dirigenti Generali nell'ambito delle iniziative svolte dal Ministero delle Comunicazioni.

8 Trattamenti affidati all'esterno (Regola 19.7)

La sicurezza dei trattamenti affidati a soggetti esterni è garantita dal contratto di servizio tra le parti.

Tali soggetti operano con la qualifica di "Incaricato del trattamento" ai sensi dell'art. 30 del D.Lgs. 196/03 e ricevono idonee e analitiche istruzioni su come proteggere i dati ai quali hanno accesso.

Inoltre, è richiesto, ai soggetti esterni, un attestato di conformità alla legge.

L'incaricato esterno è autorizzato a procedere all'organizzazione delle operazioni di trattamento dei dati personali in esecuzione del vigente contratto.

Il Titolare, anche attraverso il Responsabile, quando ne ravvisi l'opportunità, effettua le verifiche atte ad appurare la conformità delle misure di sicurezza in essere e l'osservanza delle istruzioni impartite.

9 Cifratura dei dati o separazione dei dati identificativi (Regola 19.8)

Non applicabile in quanto il MINISTERO non rientra nelle categorie di titolari per i quali è previsto tale obbligo.

10 Piano di Audit

Il Titolare, per tramite del Responsabile, verifica periodicamente l'efficacia delle misure adottate relativamente a:

- accesso fisico a locali dove si svolge il trattamento;
- procedure di archiviazione e custodia dati trattati;
- efficacia e utilizzo misure di sicurezza strumenti elettronici;
- integrità dei dati e delle loro copie di backup;
- distruzione dei supporti magnetici non più riutilizzabili;
- livello di informazione degli interessati.

11 Dichiarazione di impegno e firma

Il presente documento redatto in data 31/03/2006 viene firmato in calce dal Direttore Generale per l'Innovazione tecnologica e la promozione, in qualità di Responsabile dei sistemi informativi, e verrà aggiornato periodicamente entro il 31 marzo di ogni anno.
L'originale del presente documento è custodito presso la sede del MINISTERO, per essere esibito in caso di controllo.

Roma, 31/03/2006

Firmato
IL DIRETTORE GENERALE
Arch. Antonia Pasqua Recchia