I processi sono raggruppati nello schema per aree omogenee in base alle tipologie di trattamento e di dati trattati come di seguito descritto:

Area ❶: processi che trattano dati personali sensibili relativi a:
- le attività istituzionali dell'Istituto;
- gestione del personale (sistema strumentale SAP HR)

Area ❷: altri processi strumentali, quali i sistemi contabile, protocollo e documentale e patrimonio che trattano dati personali comuni;

Area ❸: distribuzione su Internet di servizi alla comunità degli utenti (contribuenti e pensionati). Questi servizi hanno ad oggetto dati personali sensibili;

Area ❹: servizi transazionali disponibili sulla rete e accesso non strutturato a file system condivisi e alla messaggistica, con il trattamento di dati, anche personali sensibili;

Area ❺: scambio nei due sensi di informazioni tra l'Istituto ed organizzazioni partner di informazioni anche personali sensibili, ed anche accesso transazionale da stazioni di lavoro interne a servizi informatici di partner istituzionali (Esempio: Poste Italiane S.p.A., INPS, ecc.);

Area ❻: accesso di fornitori esterni al database centrale (es. referenti delle Poste presso gli uffici provinciali) per il trattamento di informazioni personali anche sensibili.

3. METODOLOGIA ADOTTATA E PROCESSI GENERALI DI GESTIONE DELLA SICUREZZA

Le misure di sicurezza adottate dall'IPOST e questo DPSS, che costituisce una di tali misure, sono stati definiti sulla base di un'analisi dei rischi condotta, con la collaborazione di una società del settore.

Come parte della politica di sicurezza adottata dall'Istituto, questo DPSS è riveduto periodicamente e ogni qual volta si verifichi un cambiamento significativo del contesto nel quale la politica vigente in un dato momento era stata disegnata.

4. SICUREZZA INFORMATICA

Misure tecniche

La sicurezza del sistema informativo dell'IPOST si basa sull'impiego di profili di sicurezza applicativa, attuati attraverso particolari configurazioni di dispositivi di rete (router, proxy, gateway, firewall, ecc.), hardware specializzato per l'autenticazione e procedure software di registrazione ed autenticazione dell'utente.

L'Ente applica una politica di controllo accessi alle risorse che si basa sulla definizione delle informazioni, del loro grado di sensibilità e sulla valutazione delle necessità operative degli incaricati dei trattamenti che, in base alle loro responsabilità, devono essere messi in grado di accedere a certe parti della base dati. Ne risulta un sistema di controllo che mira a dare accesso alle informazioni in base al ***profilo*** di ciascun utente e che si fonda sui seguenti elementi:

- una procedura formale di registrazione degli utenti;
- un sistema combinato di misure tecniche, applicato su client, server, apparati di rete e strumenti specifici di sicurezza volto a garantire l'accesso ai dati soltanto a coloro i quali sono legittimati in base al proprio profilo;
- la revisione sistematica delle credenziali, per tutta la durata dell'utenza;
- il monitoraggio sistematico degli accessi.

Criteri di definizione, di attribuzione e di gestione dei codici identificativi personali

Per semplicità di utilizzo, sia per l'accesso al dominio Microsoft Windows™ 2000 che caratterizza l'ambiente operativo dell'Istituto sia per l'accesso alle procedure, è definito uno standard aziendale di attribuzione di un codice identificativo personale univoco.

Modalità di attivazione, variazione e gestione delle parole chiave per l'accesso ai dati personali.

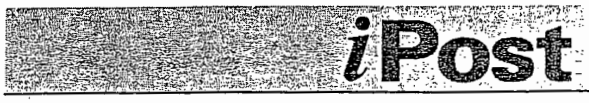
Le parole chiave di accesso al dominio Microsoft Windows™ 2000 possono essere variate in modo autonomo da parte degli utilizzatori operando nell'apposita funzionalità in pannello di controllo/password all'interno dei sistemi Microsoft Windows™ in uso.

Una volta attribuita un' utenza, l'utente è invitato a modificare al più presto la propria password. È stabilito un periodo di validità di una password, scaduto il quale l'utente viene invitato a modificarla.

E' stata fornita congrua istruzione al personale interessato per l'autonoma sostituzione della password di accesso al sistema impostata a livello BIOS.

Criteri di utilizzo e aggiornamento dei programmi antivirus

L'Istituto ha installato il software antivirus Symantec AntiVirus™ Corporate Edition.
Agli utilizzatori di software per la posta elettronica via Internet sono state impartite istruzioni sull'utilizzo del software Microsoft Outlook™ e sulla potenziale pericolosità di apertura di file allegati ai messaggi di e-mail, soprattutto da mittenti sconosciuti.
I sistemi sono configurati per la scansione dei file di programma creati, modificati, cancellati dall'utente oltre a prevedere una scansione settimanale delle unità disco locali.
I software vengono aggiornati tramite procedure automatiche con distribuzione dei file da parte della Gestione Tecnica dell'Istituto.



5. APERTURA AD INTERNET

L'IPOST dispone di un portale Internet che dà accesso diretto alla comunità degli assistiti e pensionati (area 3 nella figura precedente). Gli utenti sono registrati attraverso un processo formale, con il riconoscimento fisico all'atto della presentazione della domanda.

Il Server è posto su DMZ ed è accessibile da Internet solo tramite protocollo HTTP sulla porta 80. Il protocollo SSL è utilizzato per l'autenticazione del server e il "criptamento" dell'informazione.

6. MONITORAGGIO DELLA RETE E DELL'UTILIZZO DEI SERVIZI

Il gruppo di gestione tecnica dell'IPOST utilizza report prodotti dai vari sistemi per effettuare regolarmente attività di auditing di sicurezza, che includono analisi dei file di log dei vari database, con produzione di tracciati di accesso alla base informativa, dei log di sistema operativo e del traffico da e verso Internet, con registrazione e monitoraggio degli indirizzi IP e, su particolari applicazioni, degli utenti.

7. MISURE DI SICUREZZA FISICA

L'IPOST utilizza una serie di misure di sicurezza sia per l'accesso fisico ai locali della propria sede che per la salvaguardia dell'integrità dei dati in essa custoditi.

In particolare:

- Con un contratto stipulato da Poste Italiane con un istituto di vigilanza, è garantito il presidio della sede durante la notte nei giorni lavorativi dal lunedì al venerdì e per le intere giornate di sabato, domenica e altre festività infrasettimanali; per questa attività di presidio è disponibile per la sede centrale un impianto TV a circuito chiuso che copre le aree di accesso ai corridoi di accesso agli uffici e alla sala macchine (CED).
- Gli accessi al CED sono soggetti ad abilitazione e registrazione elettronica. L'accesso al locale adibito a sala server è esclusivamente riservato al personale della gestione tecnica debitamente abilitato, ad eccezione degli addetti alla pulizia dei locali. Il servizio di guardiania gestisce la consegna delle chiavi dei locali.
- Il controllo degli accessi delle zone non protette è effettuata dal personale addetto. Il sistema prevede terminali presenza per personale interno e la tenuta di registri cartacei per visitatori, tecnici della manutenzione, accesso straordinario in sede fuori orario di lavoro e personale mancante di badge.
- E' installato ed operativo un sistema di rilevazione allarme impianti tecnologici (impianto elettrico e condizionatori). La sede dell'Istituto è dotata di estintori a polvere e ad anidride carbonica per l'utilizzo con apparecchiature informatiche. Un estintore ad anidride carbonica è situato nei pressi della sala server dell'Istituto.

Nelle aree protette (centro di elaborazione dati, sala server, sala fonia/dati e nastroteca) sono in funzione dispositivi antincendio e antiallagamento.

- Gli allarmi sono fatti confluire in un quadro sinottico presso la vigilanza, sempre sotto controllo.
- Le aree CED sono alimentate attraverso un gruppo di continuità, gestito da Poste Italiane. L'intera sede dell'Istituto è climatizzata. Un impianto di condizionamento controlla la temperatura della sala macchine secondo le specifiche tecniche delle apparecchiature.
- La base dati e le principali applicazioni risiedono su macchine cluster completamente ridondanti (alimentatore, scheda di rete, ecc.). Le unità adottano la tecnologia RAID che consente la ricostruzione dei dati.

8. ASSICURAZIONE DELL'INTEGRITÀ DEI DATI

Ogni notte sono programmati backup delle basi dati e, una volta al mese, le copie effettuate vengono trasferite nella sede di Pesaro.

I nastri giornalieri vengono utilizzati a rotazione nell'arco della settimana (dal lunedì al venerdì). I dispositivi di backup ritenuti obsoleti vengono formattati e archiviati. Sia il backup giornaliero che il mensile prevedono, alla conclusione, procedure di verifica della corretta esecuzione della procedura.

La corretta esecuzione dei backup viene verificata ogni mattina dall'addetto alla gestione dei sistemi informatici dell'Istituto.

I server dell'Istituto sono collegati al gruppo di continuità di Poste Italiane S.p.A. che consente la salvaguardia dei sistemi in caso di momentanei sbalzi di tensione con spegnimenti automatici in caso di prolungata mancanza di tensione elettrica.

9. MISURE MINIME PER I TRATTAMENTI CARTACEI

Vengono adempiute le seguenti prescrizioni:

- La validità delle richieste di accesso ai dati personali è verificata prima di consentirne l'accesso stesso;
- Gli atti e i documenti contenenti i dati vengono conservati in archivi ad accesso selezionato e, se affidati agli incaricati, vengono da questi ultimi conservati e restituiti al termine delle operazioni affidate;
- Il responsabile, nel designare gli incaricati, autorizza preventivamente per iscritto il solo accesso ai dati la cui conoscenza sia strettamente necessaria all'adempimento dei compiti assegnati;
- Gli atti e i documenti contenenti i dati, se affidati agli incaricati del trattamento, vengono conservati, fino alla restituzione, in contenitori muniti di serratura;

- L'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi: l'adempimento di tale prescrizione si concreta nel consentire l'accesso agli archivi solo ed esclusivamente al responsabile del trattamento o ad un suo incaricato;
- Eventuali supporti informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali vengono conservati e custoditi a cura del responsabile del trattamento.

10. MISURE ORGANIZZATIVE - RUOLI E RESPONSABILITÀ RISPETTO AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI

Corretto utilizzo delle risorse informatiche

E' stata inviata comunicazione agli utilizzatori di posta elettronica e di accessi Internet inerente un corretto utilizzo delle applicazioni. È previsto un programma di rinnovo su base annuale.

Definizione e pubblicazione di norme

L'istituto predispone e divulga a tutti i propri dipendenti tramite la Intranet aziendale le proprie policy in materia di sicurezza.

E' definita una specifica policy sull'uso delle risorse, portata immediatamente a conoscenza dei nuovi assunti, che fissa norme sui comportamenti individuali e regole di processo in relazione al trattamento dei dati personali tramite le funzioni offerte dal sistema informativo.

Modalità di accesso ai dati particolari (sensibili e del casellario).

Le informazioni relativi a dati sensibili (origine razziale ed etnica, adesione a sindacati, stato di salute, eventuali procedimenti penali) vengono trattate su supporto informatico solo ed esclusivamente dagli addetti dell'ufficio Organizzazione e Personale e dal Servizio Previdenza.

11. FORMAZIONE

L'Ente organizza sistematicamente corsi di formazione interna per i responsabili e gli incaricati del trattamento. La formazione viene programmata dal Responsabile del Servizio Organizzazione e Personale, che ne tiene registrazione formale sulla lista dei corsi di formazione sostenuti.

La formazione include corsi finalizzati ad illustrare il sistema di sicurezza adottato dall'Istituto, tra i quali corsi specifici per gli incaricati di trattamento. Questa formazione viene effettuata in occasione dell'inserimento in Azienda, e comunque prima dell'assegnazione del codice identificativo e della parola chiave.

La formazione degli incaricati viene programmata dal Responsabile che ne raccoglie registrazione formale tramite sulla lista dei corsi di formazione sostenuti, che viene inviata all'Area Risorse Umane.

In occasione di cambiamenti apportati alle procedure di gestione della sicurezza viene di volta in volta valutata l'opportunità di procedere a ulteriori interventi di formazione.

12. NOMINA A RESPONSABILE DEL TRATTAMENTO

La procedura viene attivata dal Consiglio di Amministrazione dell'Ente che fa predisporre una "Lettera di nomina a Responsabile del trattamento dei dati".

Ad ogni cambiamento organizzativo che comporti lo spostamento ad altra struttura viene predisposta nuova nomina.

Ogni servizio nomina gli incaricati dei trattamenti, i quali sono gli unici abilitati al trattamento dei dati di propria competenza, siano essi in formato cartaceo che elettronico. Gli incaricati del trattamento vengono informati degli obblighi derivanti dai requisiti di legge e invitate al rispetto dei principi e delle regole di seguito riassunti:

- Tutti gli incaricati, nel trattare i dati personali, sia se riferiti a persone, sia se riferiti a soggetti giuridici, dovranno operare garantendo la massima liceità, correttezza, pertinenza e non eccedenza delle informazioni di cui vengono in possesso, con particolare cautela ai dati sensibili e giudiziari, nonché ai dati di cui all'art. 17 del Testo Unico della Privacy (c.d. dati semi-sensibili).
- Le singole fasi di lavoro e la condotta tenuta, dovranno evitare che i dati siano soggetti a rischi di perdita o distruzione; che ai dati possano accedere persone non autorizzate; che vengano svolte operazioni di trattamento non consentite o non conforme ai fini per le quali i dati stessi sono stati raccolti.
- Gli incaricati dovranno perciò operare con la massima diligenza in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, all'eventuale loro aggiornamento, così per la conservazione ed eventuale distruzione.
- Non potranno eseguire operazioni di trattamento per fini non istituzionali.

Gli incaricati devono custodire i dati con diligenza, evitando azioni che possano far conoscere a persone non incaricate i dati medesimi.

13. NOMINA A INCARICATO DEL TRATTAMENTO

La procedura viene attivata dal Responsabile del trattamento in occasione della prima assegnazione alla struttura, attraverso la predisposizione di una lettera che viene archiviata in luogo protetto. Ad ogni cambiamento organizzativo che comporti lo spostamento ad altra struttura viene fatto sottoscrivere un nuovo modulo.

iPost

14. FUNZIONE PRIVACY

Per la cura degli adempimenti legati al trattamento dei dati personali, l'Ente ha istituito un Ufficio Privacy, con il compito di monitorare la corretta applicazione della politica di sicurezza dell'Istituto affiancando affiancare il titolare nelle funzioni di vigilanza e controllo che esso deve esercitare nei confronti dei responsabili e degli incaricati da esso stesso designati all'interno ed all'esterno dell'Istituto.