6 Misure da adottare

La scelta di adottare tali misure deriva in parte dagli obblighi di legge, in termini di misure minime ed idonee, ed in parte da studi specifici effettuati dai vari settori dell'Ente per migliorare la sicurezza globale del sistema informativo dell'Ente. In particolare per ciò che riguarda le misure idonee, queste sono in gran parte derivate dall'attività di analisi e gestione del rischi, che l'Ente reitera annualmente così come imposto dalla normativa sulla privacy.

6.1 Misure di sicurezza logica

6.1.1 Identificazione/Autenticazione e controllo accessi

Un processo di Autenticazione implementa la fase di riconoscimento necessaria per accedere al posto di lavoro, gestisce l'interazione con l'utente controllandone le attività in base ai diritti dello stesso definiti dalle politiche di sicurezza allo scopo di prevenire l'accesso a risorse non autorizzate.

In ENPALS il controllo accessi attualmente è diversificato in funzione della tipologia del sistema operativo, dell'applicazione e della rete. La gestione delle attività di identificazione, autenticazione ed autorizzazione si sono stratificate nelle singole applicazioni con svariati sistemi che vanno dalla identificazione con codice fiscale, identificativo di rete e matricola per il personale interno, all'autenticazione tramite password, pin, certificato digitale.

Le iniziative intraprese in ambito sicurezza e controllo accessi dovranno essere in grado di consentire autenticazioni di tipo debole (UserId e Password, PIN) e autenticazioni di tipo forte (firma digitale, Smart card).

Attività da realizzare o in via di realizzazione:

Progettazione e realizzazione dell'Identity Management con la matrice dei profili:
La progettazione della matrice deve tener conto anche dei profili assegnati ai dipendenti in qualità di incaricati del trattamento di dati. (Attività In fase di rilascio del primo modulo).

Inserimento della firma digitale all'interno di applicazioni Mission-Critical:
In un contesto in cui il servizio erogato dall'Ente (processo) è la risultante di molteplici interventi operati in tempi ed uffici diversi, assume rilevanza fondamentale la possibilità di attribuire univocamente la responsabilità di ogni passo procedurale che concorre al processo. In tal senso l'Ente ha adottato la firma digitale all'interno di alcuni processi critici, quali il recupero crediti.
La componente architetturale di sicurezza già disponibile, inclusa la capacità di operare su più piattaforme, permette all'Ente una completa integrazione dei nuovi dispositivi di firma (smart card e lettori) all'interno dei processi di sicurezza in essere o da implementare. Sono stati acquisiti smart card, lettori (dal CNIPA).

Autenticazione con Pin o Password

Tutte le altre applicazioni dell'Ente utilizzeranno il sistema federato di autenticazione basato su UserId e pw o PIN, adeguando le applicazioni per renderle coerenti con le corrispondenti politiche di sicurezza.

6.1.2 Accountability e gestione dei Log

Parallelamente alle modalità di identificazione l'Ente ha provveduto ad istituire fasi di registrazione delle operazioni in dipendenza delle classi di utenza e delle tipologie di operazioni. Le modalità sono purtroppo polverizzate in modo perfettamente speculare a quelle di identificazione ed autenticazione per cui esistono tanti archivi di Log per quasi tutti gli accounts. I dati registrati non sono normalizzati e non sempre afferiscono al soggetto che ha effettuato l'operazione, all'oggetto dell'operazione, al tempo e alla localizzazione della stazione di lavoro da cui è partita l'operazione. Si impone pertanto la necessità di pervenire nel più breve tempo possibile ad una "consolidation" dei log, centralizzando e normalizzando i log medesimi.

Per ottenere un sistema di log logicamente centralizzato dovranno essere implementate le seguenti funzioni:

- Raccolta centralizzata
- Normalizzazione dei log di diversa provenienza funzionale
- Consultazione ed il reporting procedurale
- Consultazione ed il reporting non proceduralizzato.

Solo la disponibilità di un tale strumento consentirà di superare la concezione tradizionale secondo la quale, la massa dei log è considerata solo un onere in termini di conservazione a fini più o meno realistici di documentare a posteriori incidenti già avvenuti. Infatti, disponendo di un sistema di gestione centralizzato del log, sarà possibile:

- Prevenire eventi dannosi
- Migliorare la disposizione e la configurazione delle difese
- Verificare la rispondenza dell'attività operativa alla politica della sicurezza dell'Ente.

L'attività di analisi del sistema di log centralizzato è stata completata ed il progetto che coinvolge tutte le applicazioni ed i sistemi presenti in ENPALS non potrà essere sviluppato all'interno per oggettive impossibilità di immediato intervento da parte di tutti i responsabili delle procedure esistenti. Si è provveduto pertanto a redigere un capitolato tecnico che è in via di rilascio all'Ufficio competente.

6.1.3 Sicurezza delle reti

La sicurezza della rete primaria è in modo parziale a carico della Rete Unitaria Per la Pubblica Amministrazione, mentre la protezione dell'Intranet è a carico dell'Ente; tuttavia anche per la componente gestita da RUPA, fenomeni quali il "nomadismo" (esistenza di utenti mobili) generato dagli Ispettori di vigilanza, dai Dirigenti, medici, avvocati o da personale di ditte esterne si creano delle falle che non potendo essere controllati da RUPA stessa restano a carico dell'Ente; in modo analogo, per i rischi derivanti dall'uso di strumenti quali USB flash memory, compact disk, dischetti e qualsiasi altro tipo di unità esterna le responsabilità restano a carico dell'Ente.

Strumenti di protezione della rete

Antivirus

Questo strumento protegge server e client dagli assalti dei virus informatici. Oltre alla qualità in termini di quantità di virus riconosciuti, le caratteristiche peculiari di un simile Software sono:

- Diffusione a server e client via rete
- Gestione centralizzata
- Aggiornamento via INTERNET
- Generazione di un log
- Utilizzo di regole euristiche a difesa da virus non conosciuti

L'Ente ha già un sistema di sicurezza antivirus gestito centralmente

Firewall

Questo elemento costituisce il componente principale delle difese perimetrali della rete aziendale nei confronti di internet ed Intranet. Oltre alla qualità in termini di quantità di diverse tipologie di attacchi riconosciuti, le caratteristiche peculiari di una simile installazione sono:

- La continuità del servizio
- La gestione centralizzata e remotizzata
- L'aggiornamento via INTERNET
- La generazione di un log.

L'analisi dei rischi ha evidenziato la necessità di dispositivi di difesa perimetrale delle reti ENPALS sia rispetto agli accessi esterni via Internet sia rispetto agli accessi interni attraverso la Intranet aziendale. Rispetto ad Internet esiste un sistema di difesa perimetrale costituto dai firewall gestiti in ambito RUPA, viceversa risulta deficitaria la difesa perimetrale della Intranet. Rispetto a questo aspetto è in corso l'acquisizione di sistemi firewall per la protezione di Intranet.

Sicurezza delle connessioni wireless

I collegamenti wireless sono consentiti ad alcune categorie di utenti: Ispettori e Dirigenti. È presente un sistema che assicura la messa in sicurezza del sistema e delle WLAN (wireless lan) già installate o in via di installazione.

6.1.4 Sicurezza dei supporti di memorizzazione

Un aspetto molto importante che impatta notevolmente sulla sicurezza delle informazioni è rappresentato dall'uso sempre più pesante di dispositivi di memorizzazione esterni quali gli USB memory flash. È in corso uno studio per l'individuazione di dispositivi dotati di meccanismi di protezione quali Password o PIN per l'accesso al dispositivo e di crittografia per la cifratura dei dati in essi contenuti. Parallelamente la soluzione dovrà provvedere al recovery dei dati e delle chiavi.

6.1.5 Distribuzione, Gestione e Sicurezza del Software

Questi sono sistemi di distribuzione a client e server dei Software da utilizzare. Si tratta sia di Software di sistema sia di Software applicativo.
Questi strumenti devono essere in grado di:

- Riconoscere la versione di Software installato e da sostituire
- Documentare le configurazioni di ogni singola stazione
- Verificare l'integrità dei Software installati e da diffondere
- Generare un accurato log.

6.1.6 Disaster Recovery

Garantisce affidabilità, sicurezza dei dati e ripristino in caso di disastro garantendo la continuità del servizio. L'Ente è già dotato di un tale sistema che tuttavia pur coprendo tutto il mondo legacy non copre ancora tutto il mondo distribuito (cfr. cap. 7)

6.2 Misure di sicurezza organizzativa

La messa in sicurezza dei sistemi e la protezione del patrimonio informativo si può ricondurre, da un punto di vista organizzativo, a tre specifiche funzioni tra loro indipendenti:

1. Definizione delle politiche in tema di Sicurezza Informatica
2. Progettazione, implementazione e gestione delle misure di sicurezza in attuazione delle politiche di cui al punto precedente
3. Verifica e controllo della corretta attuazione e dell'efficienza delle misure di sicurezza adottate.

Analisi del rischio

L'analisi del rischio consente di avere una mappa delle possibili contromisure di sicurezza da realizzare mediante investimenti sostenibili. Nel corso del 2007 sarà condotta un'approfondita analisi dei rischi, ricorrendo ad esperti con riconosciute competenze in materia di sicurezza informatica.

7 Criteri e modalità di ripristino della Disponibilità dei dati (regola 19.5)

In relazione ai rischi individuati, oltre alle misure già indicate, tese ad ottemperare alle prescrizioni di Legge, costituiscono prassi aziendale le seguenti ulteriori modalità operative:

- l'analisi delle esigenze in termini di tipologia dei dati oggetto di recovery, se previsto nell'ambito dei servizi offerti, per dimensionare opportunamente i supporti di memorizzazione da utilizzare, le scorte e gli eventuali strumenti aggiuntivi finalizzati al miglioramento e velocizzazione dei processi;
- l'aggiornamento delle procedure operative di recovery, se previsto nell'ambito dei servizi offerti, dei dati atte a garantire la ripresa dei dati entro i limiti stabiliti dalla legge;
- la predisposizione di regole e istruzioni aggiuntive per gli incaricati;
- la miglior dislocazione delle copie di salvataggio in locali separati dagli ambienti di produzione.

È compito dei vari Uffici interessati di concerto formalizzare le procedure di salvataggio e verificarne la loro rispondenza alle esigenze e ai relativi obblighi di Legge.

È cura dei Responsabili degli Uffici dichiarare la presenza di dati sensibili, giudiziari o particolari ai sensi della Legge negli archivi di competenza dell'ENPALS, in modo tale che funzione ICT possa adeguare le modalità di gestione dei relativi supporti.

Le misure adottate consentono il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici entro sette giorni.

8 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 piano di formazione è stato gia predisposto dall'Ente per ottemperare alla L.675/96 e al DPR 318/99 e per il 2007 è previsto l'aggiornamento del piano in conformità al nuovo D.Lgs. 196/03. Di seguito si riportano le informazioni relative al nuovo piano

8.1 Obiettivi

Il piano formativo predisposto con riferimento alla D.Lgs. 196/03 ha l'obiettivo di fornire alle figure professionali interessate le necessarie conoscenze su:

1. la normativa specifica in materia di trattamento dei dati personali;
2. le problematiche di carattere generale inerenti la sicurezza informatica;
3. le attività necessarie al mantenimento del livello di sicurezza;
4. le procedure redatte allo scopo di garantire il rispetto delle misure minime;
5. i compiti cui l'incaricato è chiamato ad attenersi durante l'attività di trattamento.

9 Trattamenti affidati all'esterno (regola 19.7)

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

Il trattamento dei dati in esecuzione delle prestazioni contrattuali predette potrà interessare ogni tipologia di dati secondo le definizioni comma 1), dell'articolo 4) del d.lgs. n.196/2003 (dato personale, dati identificativi, dati sensibili, dati giudiziari).

Il soggetto che gestisce i trattamenti esternalizzati opera con la qualificazione giuridica di responsabile ed ha ricevuto idonee ed analitiche istruzioni per garantire la sicurezza dei dati.

La tabella descrive in maniera sintetica il tipo di attività esternalizzata, il tipo dei dati interessati al trattamento e quali sono i criteri e gli impegni assunti per l'adozione delle misure.

Descrizione sintetica dell'attività esternalizzata	*Trattamenti dei dati interessati*	*Soggetto esterno*	*Descrizione dei criteri e degli impegni assunti per l'adozione delle misure*
Rilascio cedolini stipendi	Sensibili	Data Management	Elaborazione cedolini stipendi

I cedolini vengono elaborati e inviati dalla DATAMANAGEMENT per posta elettronica in formato file zippato. La connessione tra il client e il Mail Server usa il protocollo https che garantisce lo scambio di dati in maniera criptata.

10 Cifratura dei dati (regola 19.8)

Non applicabile in quanto l'ENPALS non rientra nelle categorie di titolari per i quali è previsto tale obbligo.