Il sito web è gestito, in ambito RUPA (a breve Servizio Pubblico di Connettività), in outsourcing e fornisce i seguenti servizi, differenziati per classe di utenza:

- Per il Cittadino
  - estratto contributivo e calcolo simulato della pensione;
  - verifica sulle informazioni anagrafiche personali;
  - domanda di pensione;
  - duplicato CUD.

- Per le aziende, i consulenti delegati e i lavoratori autonomi:
  - invio denuncia contributiva mensile e trimestrale;
  - richiesta di agibilità;
  - immatricolazione lavoratori;
  - ricerca informazioni anagrafiche dell'impresa;
  - ricerca lavoratori Enpals;
  - gestione deleghe.

- Per i Patronati (su delega del lavoratore):
  - gestione delle deleghe;
  - informazioni anagrafiche patronato;
  - estratto contributivo;
  - duplicato CUD;
  - inoltro domanda di pensione.

- Per la SIAE (che in convenzione opera come front-office per le aziende e i lavoratori iscritti all'Enpals):
  - invio denuncia contributiva mensile;
  - richiesta di agibilità;
  - ricerca denunce trimestrali e agibilità;
  - immatricolazione lavoratori;
  - ricerca informazioni anagrafiche dell'impresa;
  - ricerca lavoratori Enpals;
  - gestione deleghe.

3 Distribuzione dei compiti e delle responsabilità (regola 19.2)

3.1 Definizioni dei "Ruoli di Legge"

Di seguito si indicano i ruoli e le competenze per ognuna delle figure previste dalla Legge.

- **Art. 28 - Titolare dei Trattamenti**
  ENPALS è Titolare del trattamento per i dati di sua proprietà e per le correlate responsabilità di legge; esercita un potere decisionale del tutto autonomo sulle finalità e modalità del trattamento ivi compreso il profilo della sicurezza.

- **Art. 29 – Responsabile del Trattamento**
  I Responsabili del trattamento dei dati personali sono tutti i Dirigenti delle unità operative della Direzione Generale e delle Sedi Compartimentali nonché i Coordinatori delle Consulenze, ciascuno per le competenze e per le Aree di relativa assegnazione, al fine di poter vigilare sulla concreta e capillare applicazione della normativa di riferimento.
  I Responsabili dovranno inoltre assumere le necessarie iniziative atte ad assicurare che il trattamento dei dati e gestione degli stessi, in forma cartacea o con l'ausilio di mezzi elettronici, avvenga nell'ambito della propria struttura nel rispetto della Legge e delle disposizioni interne impartite in materia.

- **Art. 30 - Incaricati**
  Le operazioni di trattamento dei dati personali sono affidate esclusivamente ad Incaricati individuati per ruolo e mansione tra i dipendenti dell'Ente ovvero a personale esterno di società fornitrici di servizi quali consulenti, manutentori, eventuali stagisti o interinali. L'incaricato con l'atto di nomina riceve chiare istruzioni in ordine alle cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato, anche al fine di assicurare che lo strumento elettronico non sia lasciato incustodito ed accessibile durante una sessione di trattamento.
  L'incaricato è autorizzato a trattare e gestire i dati necessari ed indispensabili per svolgere le mansioni allo stesso affidate nel rispetto delle competenze dell'unità organizzativa di appartenenza, assicurando che gli atti ed i documenti contenenti dati personali o giudiziari non siano acceduti da persone prive di autorizzazione e siano restituiti al termine delle operazioni affidate.

  Gli Incaricati vengono identificati attraverso lettere di incarico a cura del Responsabile, individuando l'ambito del trattamento consentito. La nomina avviene singolarmente o per classi omogenee di incaricati quando gli stessi risultino appartenenti ad una stessa unità organizzativa e svolgano nell'ambito dei ruoli assegnati, identiche tipologie di trattamento.
  L'elenco degli incaricati ed il loro profilo di accesso ai dati è periodicamente aggiornato a cura della Direzione del Personale.

3.1.1 Sicurezza informatica

Le responsabilità della sicurezza delle informazioni rientrano, come già indicato, nei compiti specifici della Direzione Sistemi Informativi e Telecomunicazioni.

In condizioni ordinarie:

- predispone la Politica di sicurezza delle informazioni e le sue successive revisioni;
- predispone ed attribuisce i ruoli e le responsabilità definite all'interno del presente documento e richiamate dalla politica;
- definisce l'approccio dell'Ente per la gestione del rischio avendo cura di identificare il livello di rischio accettabile
- recepisce le valutazioni derivanti dall'analisi del rischio effettuata durante gli incontri periodici;
- propone il budget necessario per le soluzioni alle non conformità rilevate ed evidenziate dall'analisi del rischio;
- promuove la realizzazione di interventi formativi e di sensibilizzazione sulla sicurezza in tutto l'Ente;
- definisce gli obiettivi di controllo.

In condizioni di emergenza:

- in funzione del tipo di emergenza, da avvio a tutte le attività atte alla soluzione dell'evento occorso, recependo costantemente le informazioni relative all'evolversi della situazione al fine di pervenire al ripristino della normalità.

Per l'espletamento di tali compiti si tengono riunioni periodiche, almeno due volte l'anno in condizioni di normalità e ogni volta che si renda necessario in casi di emergenza; Lo svolgimento di tali riunioni segue, orientativamente, la disamina di uno o più punti tra quelli presenti nell'elenco che segue:

- redazione ed aggiornamento dei documenti richiesti dalla legge sulla tutela dei dati personali quali, ad esempio il DPS sulla base delle indicazioni fornite dai Responsabili del Trattamento dei dati sensibili o giudiziari per quanto riguarda la parte relativa al loro trattamento senza l'ausilio di strumenti informatici, sottoponendoli all'adozione del titolare del trattamento;
- presentazione e discussione dei nuovi piani di intervento e/o controllo dello stato di avanzamento delle realizzazioni dei piani precedentemente approvati;
- gestione del budget specifico;
- varie ed eventuali.

4 Analisi dei Rischi (regola 19.3)

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

L'analisi è stata condotta dal personale della DSIT con il supporto di esperti ed 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 personali ordinari, sensibili e giudiziari, e delle caratteristiche del trattamento.

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.

La legge classifica le Banche Dati come quegli asset che contengono i Dati Personali.
Risulta evidente che alcuni asset di seguito riportati (es. edifici, applicazioni) non sono classificabili come direttamente contenenti Dati Personali e/o Sensibili.

Per tali asset il rischio è stato calcolato sulla base del danno potenziale indotto sulle banche dati dai rischi cui sono soggetti tali asset. Ad esempio, il rischio di accesso non autorizzato ad un edificio, induce i rischi di violazione della riservatezza e/o di disponibilità di archivi contenuti in tale edificio, così come la mancanza di documentazione di un'applicazione, nel caso di manutenzione evolutiva, può causare errori di programmazione e/o controllo dei diritti di accesso ad una banca dati che, pur protetta dal sistema operativo, potrebbe così essere soggetta a rischi indotti di perdita di riservatezza e/o di integrità.

L'attribuzione del grado di rischio – per ciascun di essi e per ciascun sistema – è stata effettuata sulla base di considerazioni puramente qualitative, considerando le prassi attuali dell'Ente e le contromisure rilevate e successivamente elencate. Di seguito la tabella di riepilogo dei rischi:

Evento		Descrizione dell'impatto sulla sicurezza (Livello di gravità)	Misure d'azione
Comportamenti degli operatori	Sottrazione di credenziali di autenticazione	Alta	Cambio mensile della password
	Carenza di consapevolezza, disattenzione o incuria	Media	Formazione operatori
	Comportamenti sleali o fraudolenti	Media	Monitoraggio continuo (rete e software)
	Errore materiale	Bassa	Verifica periodica dei dati
Eventi relativi agli strumenti	Azione di virus informatici o di codici malefici	Bassa	Server antivirus (no dati su client)
	Spamming o altre tecniche di sabotaggio	Bassa	Software specifico
	Malfunzionamento, indisponibilità o degrado degli strumenti	Bassa	Assistenza tecnica
	Accessi esterni non autorizzati	Bassa	Firewall switch
	Intercettazione di informazioni in rete	Bassa	Firewall Switch
	Intercettazione di informazioni tramite e-mail	Media	Antivirus Antispam
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	Media	Porta blindata
	Sottrazione di strumenti contenenti dati	Bassa	Telecamere
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti a incuria	Bassa	Disaster Recovery (IBM)
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione,...)	Media	Gruppo di continuità
	Errori umani nella gestione della sicurezza fisica	Bassa	Vigilantes

5 Contromisure di Sicurezza adottate (regola 19.4)

Di seguito vengono descritte le contromisure in uso presso l'ENPALS, in considerazione delle tipologie di rischio considerate.
Nei paragrafi che seguono vengono delineate le soluzioni adottate in relazione ai rischi individuati, quali:

- Rischi specifici
- Rischi per l'integrità dei dati
- Rischi per la riservatezza dei dati
- Rischi per la disponibilità dei dati.

5.1 Contromisure a fronte di Rischi specifici

Con riferimento ai rischi prevedibili o probabili, valgono le seguenti considerazioni generali e contromisure di prevenzione:

- La zona in cui sono ubicati i CED dell'INPS e dell'EDS (sui cui sistemi sono ospitate gran parte delle applicazioni ENPALS) risultano in fascia territoriale geografica, che nelle carte di pericolosità sismica risulta classificata tra le zone a grado di pericolosità 3, vale a dire uno dei valori più bassi.

- Nella zona limitrofa gli edifici dell'ENPALS a Roma non sono presenti vie d'acqua che potrebbero esondare.

Nel caso di disastri imprevedibili dovuti cioè a calamità naturali o assimilabili l'ENPALS usufruisce delle contromisure di maggior tutela attraverso la ridondanza delle risorse, così come previsto dalle politiche di sicurezza dell'INPS. In particolare si provvede quotidianamente al salvataggio dei dati che, in funzione, delle particolarità dei dati e della criticità del processo, può garantire una ripresa del servizio compatibilmente alle prescrizioni di Legge.
Per quanto attiene alle applicazioni ed ai dati residenti in hosting sui sistemi serventi EDS, sono assicurati livelli di salvataggio e backup quotidiani.

5.1.1 Passaggio in produzione dei progetti applicativi

Nella prassi operativa dell'ENPALS, le applicazioni software prima di essere inserite in ambiente di produzione vengono sottoposte ad una verifica sulla qualità/affidabilità del software.
Il passaggio in produzione di un componente software di qualsiasi tipologia, richiede il superamento di una autorizzazione, generalmente concordata tra il fornitore e l'ENPALS.

5.1.2 Procedure applicative documentate

Gli incaricati che devono trattare dati personali attraverso le applicazioni gestionali dispongono di una documentazione adeguata in merito alle procedure da utilizzare.

5.1.3 Contratti di manutenzione hardware

Con la finalità di minimizzare eventuali problemi dovuti a guasti hardware sono previsti costanti interventi di manutenzione sugli apparati attraverso specifici contratti con i fornitori di riferimento.

5.1.4 Protezione antivirus

L'aggiornamento dei sistemi Antivirus è garantita giornalmente attraverso automatismi che non richiedono l'intervento degli utenti.
Si precisa che le contromisure adottate per la protezione da virus via posta elettronica sono affidate e garantite da EDS gestore della rete.
Per poter contenere e prevenire ulteriormente i rischi di integrità dei dati, vengono segnalate alle funzioni interessate le vulnerabilità dei sistemi al fine di promuovere l'eventuale necessità di aggiornamento degli stessi con le patch raccomandate dai costruttori.

5.2 Contromisure per la riservatezza dei dati

I Paragrafi seguenti descrivono le contromisure adottate a fronte di rischi inerenti la Riservatezza dei dati.

5.2.1 Sviluppo e gestione dei progetti applicativi

Tutti i progetti applicativi gestiti in autonomia dall'ENPALS che riguardano il trattamento di dati personali devono prevedere una verifica di congruità con le prescrizioni indicate nel presente documento.
Le altre applicazioni in dotazione all'ENPALS, rese disponibili da Enti esterni quali l'INPS, l'Anagrafe Tributaria e Infocamere sono depositarie della completa gestione anche sotto il profilo della sicurezza.
Onde garantire la corretta coesistenza della produzione con lo sviluppo e la manutenzione delle applicazioni, si definiscono due ambienti tecnici virtuali:

- ambiente di produzione;
- ambiente di sviluppo.

5.2.2 Ambiente di produzione

L'ambiente di produzione opera in modalità totalmente controllata e l'accesso è consentito ai soli soggetti singolarmente autorizzati. I dati presenti negli archivi sono dati reali e vengono protetti secondo le misure di sicurezza identificate. Dove possibile i sistemi e i programmi informatici sono configurati in modo da ridurre al minimo l'utilizzo di dati personali e identificativi degli interessati.

5.2.3 Ambiente di sviluppo

Generalmente lo sviluppo delle applicazioni è affidato a società esterne che utilizzano i propri sistemi e per i test non utilizzano quindi dati reali. Quando, in casi limitati, sia necessario disporre di un ambiente di sviluppo vengono approntati temporaneamente sistemi isolati dalla rete di produzione che non contengono dati reali.
L'accesso all'ambiente di sviluppo non richiede procedure specifiche al fine del rispetto delle disposizioni del Codice.

5.2.4 Profili abilitativi

Ogni utente ha l'accesso, con le relative modalità, alle sole informazioni che risultano necessarie allo svolgimento del proprio compito presso l'ENPALS.
I profili abilitativi dovranno 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.
Nel caso di utenti che detengono il massimo dei privilegi sono predisposti, per garantire i corretti livelli di sicurezza implementati, dei controlli e delle verifiche degli accessi ai servizi e alle risorse, in modo da individuare eventuali utilizzi impropri o non consentiti.

5.3 Misure di Sicurezza Logiche, Fisiche ed Organizzative

Le misure di sicurezza che vengono elencate nel prosieguo del presente capitolo sono atte a garantire l'insieme dei requisiti di sicurezza dei sistemi in termini di integrità, disponibilità e confidenzialità dei dati in conformità alle disposizioni indicate nel Disciplinare Tecnico. Per la loro natura e applicabilità possono soddisfare uno o più dei requisiti tra quelli indicati e quindi in alcuni casi possono non connotarsi univocamente ai medesimi.
Vengono, quindi, applicate le misure di sicurezza di seguito elencate:

- Fisiche, riguardanti la sicurezza ed il controllo degli accessi ai locali dell'ENPALS contenenti apparecchiature e supporti di memorizzazione;
- Logiche, adottate dal personale dell'ENPALS riguardanti il controllo dell'accesso alle piattaforme, agli archivi, ai database ed alle applicazioni;
- Logiche, adottate dal personale dell'ENPALS relative all'utilizzo delle stazioni di lavoro ed alla protezione degli archivi informatici mantenuti su di esse al fine di limitarne la perdita ed assicurarne la riservatezza ed integrità;
- relative alla rete, alla rete locale ed alla interconnessione con servizi esterni quale Internet, limitatamente alle terminazioni presso i locali dell'ENPALS e gestiti dal medesimo;
- organizzative,adottate dal personale dell'ENPALS relative alla salvaguardia delle informazioni che risiedono su supporto informatico e/o cartaceo;
- organizzative, relative alle regole, procedure e policy valide per tutti i dipendenti.

5.4 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 al 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 sarà inibito. L'affidabilità

del controllo dell'identità è dipendente da informazioni conservate all'interno del sistema, le quali devono essere memorizzate in modo protetto.

Controllo Accessi - 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 Accessi - 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.

Accountability - Tracciamento: misure mirate a tenere traccia delle azioni effettuate da utenti e processi in modo che sia possibile risalire a chi ha svolto le azioni. Non deve essere permesso agli utenti non autorizzati di accedere alle informazioni registrate. Deve essere inoltre possibile registrare selettivamente le azioni di uno o più utenti.

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, 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 loro 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: autenticazione dell'originatore, integrità e riservatezza del contenuto del messaggio, non ripudio dell'originatore e del destinatario.

5.4.1 Identificazione/Autenticazione e Controllo Accessi

In ENPALS il processo di identificazione/autenticazione e controllo accessi è attualmente 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.
In generale è previsto un profilo di abilitazione che definisce per ogni soggetto incaricato del trattamento:

- l'accesso agli archivi presenti sugli elaboratori, ed i relativi diritti (sola lettura, modifica, etc.);
- 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.

Allo stato attuale i più importanti sistemi di controllo accessi realizzati dall'Ente sono di seguito descritti.

Autenticazione forte (certificato digitale) via Internet o Intranet

Accesso ad applicazioni critiche: il sistema consente l'accesso alle applicazioni dell'area recupero crediti.

Autenticazione con Pin o Password

Con questo sistema si accede a tutte le altre applicazioni dell'Ente.

Credenziali: a) Codice identificativo (User-id) / PIN

A tutti coloro cui è rilasciato 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 abilitazioni.
In caso di revoca dell'incarico e/o delle autorizzazioni, è compito del responsabile gerarchico dell'incaricato comunicare immediatamente il codice identificativo che deve essere reso inutilizzabile, o, a seconda delle necessità, il profilo di abilitazioni modificato.
È prevista, inoltre, la disattivazione del codice identificativo nel caso di mancato utilizzo dello stesso per un periodo superiore a sei mesi.

Credenziali: b) Password
Ad ogni codice identificativo è associata una parola chiave. Al primo utilizzo, il dipendente ha l'obbligo di modificarla tenendo presenti le seguenti regole:

- deve essere alfanumerica, di non meno di 8 caratteri;
- non deve essere composta utilizzando lo user-id;
- non deve essere ottenuta anagrammando la precedente;
- la password decade automaticamente ogni 30 giorni.

La password può essere sostituita autonomamente dagli incaricati.

5.4.1.1 Archivi sulle stazioni di lavoro individuali

In generale per quanto riguarda le stazioni di lavoro individuali, è in corso di attivazione un sistema di archiviazione su elaboratori serventi in modo che possano venir assicurate le funzioni di backup centralizzato.
Non sarà consentito dalle singole stazioni di lavoro condividere in rete archivi mediante funzionalità server, salvo quando espressamente convenuto tra gruppi omogenei di utenti di una determinata unità organizzativa.
La presenza di archivi sulle singole stazioni di lavoro deve essere considerata di tipo eccezionale, a fronte di esigenze particolari di elaborazioni individuali, e comunque a carattere temporaneo. L'accessibilità ed integrità di detti archivi e le conseguenti responsabilità in materia di sicurezza sono di carattere personale del soggetto assegnatario della stazione di lavoro.
Per quanto attinente le stazioni di lavoro portatili, questi sono dotati di sistema operativo atto a garantire la protezione degli archivi mediante utilizzo di identificativo-password.

5.4.2 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) legato agli Ispettori di vigilanza, ai Dirigenti o a personale di ditte esterne non possono essere controllati da RUPA stessa e pertanto devono essere a carico dell'Ente.
La RUPA inoltre non controlla lo spamming in quanto legato a contenuti aziendali difficilmente decifrabili da una terza parte.

Di seguito sono descritte le misure di sicurezza adottate dall'Ente ed aggiornate semestralmente per la protezione delle reti.

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 possiede un sistema di sicurezza antivirus.

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

Sono presenti i firewall per la protezione da Internet gestiti attraverso la RUPA, dovranno essere acquisiti quelli per la protezione di Intranet.

Sicurezza connessioni wireless
I collegamenti wireless sono consentiti ad alcune categorie di utenti: Ispettori e Dirigenti.

5.4.3 Distribuzione del software

Questi sono sistemi di distribuzione *client* e *server* dei *Software* da utilizzare. Si tratta sia di *Software* di sistema sia di *Software* applicativo e sia di *Software* di tipo *legacy*.

Questi strumenti sono 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.

Il sistema è in corso di attivazione.

5.5 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, etc.).

5.5.1 Controllo accessi agli edifici

Gli edifici sono protetti mediante servizio di vigilanza generalmente disponibili nel normale orario lavorativo.
L'accesso del personale agli edifici è consentito mediante esibizione alla vigilanza dell'apposito badge.
Per il personale dipendente, al di fuori del normale orario di lavoro o turnazione, è effettuata la registrazione da parte del servizio di vigilanza, previa autorizzazione rilasciata dal Direttore Generale.
I visitatori/ospiti che accedono agli edifici devono essere identificati presso il servizio di vigilanza, che, previa autorizzazione del personale interno referente, provvederà a dotare il visitatore di apposito badge.
Per i soggetti esterni che accedono abitualmente ai locali, può essere, su autorizzazione preventiva di un responsabile, predisposto e tenuto a disposizione presso la vigilanza un badge nominativo.
Il personale che valida l'ingresso del visitatore/ospite è responsabile di qualsiasi inosservanza da parte del visitatore/ospite durante la sua permanenza nei locali dell'ENPALS.

5.5.2 Dispositivi di sicurezza e allarme.

L'ENPALS prevede per i propri Locali di Sicurezza i seguenti dispositivi:

- sistema di rilevazione fumi;
- di rilevazione di eccessiva umidità;
- allarme antincendio;
- allarme aumento temperatura;
- allarme anti intrusione;

- estinzione automatica di incendio;
- presenza di gruppi di continuità e di condizionamento.

5.6 Misure di Sicurezza Organizzative

Le misure di sicurezza organizzative possono essere 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 risorse 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.

Di seguito sono elencate le misure organizzative adottate ed implementate dall'ENPALS, con particolare riferimento alle procedure di gestione.

5.6.1 Cancellazione dei dati dell'interessato per decaduti termini di mantenimento

Per i dati trattati al di fuori di quelli istituzionali, per qualsiasi tipologia di dato trattato secondo la classificazione indicata dalla Legge, è compito del responsabile dell'Ufficio preposto al trattamento di concerto con il Responsabile ICT, provvedere alla cancellazione fisica dei dati personali privi delle caratteristiche che ne consentano il mantenimento negli archivi di produzione o storici.

5.6.2 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 venire a conoscenza, neppure accidentalmente, dei contenuti di tali supporti.
Tali supporti non devono essere utilizzati da altri soggetti che non possiedono l'incarico scritto per poterli trattare.

Nel caso di trattamento dei dati sensibili o giudiziari, i supporti già utilizzati per il trattamento potranno essere riutilizzati, solo nel caso in cui sia possibile tecnicamente cancellare le informazioni precedentemente contenute, in modo tale da non poter essere recuperabili, in caso contrario dovranno essere distrutti.

Per poter trasportare all'esterno supporti che contengano dati sensibili o giudiziari si dovranno utilizzare contenitori sigillati muniti di chiusure di sicurezza.

5.6.3 Sicurezza nella trasmissione dei dati

La connessione tra le sedi dell'ENPALS, avviene tramite la rete RUPA nazionale, la cui gestione anche sotto il profilo della sicurezza è demandato alla RUPA stessa. Il trasporto è gestito per convenzione con le società fornitrici di banda.

All'interno delle sedi è presente una rete locale LAN che collega la quasi totalità delle stazioni di lavoro presenti presso l'ENPALS. Questa rete è gestita da personale interno, lo schema è tenuto costantemente aggiornato dalle strutture preposte. L'adeguamento è affidato a fornitori esterni con i quali sono stipulati appositi contratti.

Grazie alla nuova piattaforma tecnologica di prossima adozione, le totalità delle apparecchiature saranno sottoposte a censimento e monitoraggio tramite messaggi ad una console presidiata.

Tutte le connessioni della rete con altre reti sono protette tramite appositi dispositivi (firewall) che impediscono accessi non autorizzati. Come già detto le garanzie di protezione sono offerte da RUPA e dai fornitori di banda. ENPALS ha chiesto ed ottenuto che le protezioni fossero rinforzate con protezioni di tipo VPN, Intrusion Detection Prevention, Firewall, Content filtering, Anti-Spam, Antivirus.

Nei compiti della gestione interna è previsto il costante monitoraggio degli allarmi trasmessi dai dispositivi anzidetti (che dovranno coprire nel corrente anno tutta la rete) in modo da poter verificare le possibili scoperture e/o la presenza di tentativi di intrusione.

5.6.4 Restrizione degli accessi per via telematica

L'installazione di modem per comunicazione su linee commutate è proibito.

5.6.5 Installazione di software non autorizzato

È vietato l'utilizzo di software non ufficialmente rilasciato dall'ENPALS e preventivamente testato nella sua integrità. Tale norma assicura, peraltro, il rispetto dei contenuti del D. Lg. 518/1992 e successive modifiche sul diritto d'autore e la tutela legale del software.
È parimenti vietata l'installazione senza preventiva autorizzazione sui sistemi dell'ENPALS anche di software distribuito con la formula del freeware (ovvero in forma gratuita) o shareware (ovvero in prova). Tali divieti sono anche prescritti attraverso le istruzioni fornite agli incaricati mediante la lettera di incarico.

5.7 Istruzioni e regole di comportamento

5.7.1 Definizione di policy e procedure di sicurezza

Per poter garantire un adeguato livello di sicurezza sono state definite e aggiornate delle policy e procedure alle quali tutti i dipendenti si dovranno attenere.
Di seguito un elenco delle più importanti che l'ENPALS prevede di rendere pubbliche nel breve:

- Classificazione delle Informazioni.
- Utilizzo strumenti di lavoro.
- Utilizzo Posta elettronica.
- Gestione visitatori.
- Gestione Incidenti di sicurezza.

È prevista inoltre la creazione delle caselle postali:

- Area Security, utilizzata da coloro che hanno dubbi o domande inerenti la sicurezza delle informazioni;
- HD Security, di supporto alla gestione degli incidenti di sicurezza.

5.7.2 Criteri e Procedure di rilascio delle credenziali

Le credenziali (costituite congiuntamente dal codice identificativo user-id e dalla password iniziale) vengono assegnate ai dipendenti a cura degli Uffici preposti a tali attività su richiesta del responsabile gerarchico del dipendente.
Il dipendente deve provvedere a sostituire la password iniziale con una di sua scelta.
I responsabili hanno il compito di vigilare su tali criteri.

5.7.3 Criteri e Procedure di controllo accessi agli archivi informatici

L'accesso agli archivi informatici è regolamentato da un apposito sistema di controllo che, sulla base delle abilitazioni corrispondenti ai vari profili utente, consente l'accesso ai soli elaboratori/archivi/dati necessari e sufficienti per il trattamento.
Il Responsabile ha il compito di vigilare sul corretto utilizzo delle procedure.

5.7.4 Criteri e Procedure di controllo accessi agli archivi cartacei

Gli archivi cartacei si distinguono in:

- archivi di lavoro: mantenuti a cura dei singoli incaricati negli uffici operativi;
- archivi operativi: archivi ufficiali mantenuti a cura di responsabile in Locali di Sicurezza.

Eventuali fotocopie devono essere autorizzate e custodite con le stesse modalità dei documenti originali.

Archivi di lavoro
Il personale incaricato segue le procedure previste dall'ENPALS:

- gli armadi, o altre strutture di conservazione, sono tenuti chiusi;
- nel corso del trattamento i documenti sono protetti ed eventualmente chiusi in appositi contenitori di lavoro.

Archivi operativi
Nell'accedere ai documenti cartacei, l'incaricato deve seguire le seguenti regole:

- gli armadi, o altre strutture di conservazione, sono tenuti chiusi;
- nel corso del trattamento i documenti sono protetti ed eventualmente chiusi in appositi contenitori di lavoro;
- i documenti sono prelevati dagli archivi per il tempo strettamente necessario allo svolgimento della mansione.

5.7.5 Criteri e Procedure per i supporti magnetici rimovibili

Supporti magnetici presso il CED

I supporti registrati non possono lasciare i locali di sicurezza del CED se non a seguito di apposita autorizzazione.

Criteri e Procedure per assicurare l'integrità dei dati

I dati contenuti negli archivi informatici sono protetti contro il rischio di perdita, anche accidentale, attraverso apposite procedure che consentono il veloce ripristino delle informazioni perdute o danneggiate.

In linea di massima, le suddette procedure prevedono:

- la conservazione delle copie degli archivi in locali di sicurezza diversi;
- il ripristino selettivo dei soli dati danneggiati;
- l'esecuzione di prove di ripristino.