U.O.S. Sistema Informatico
Via Portuense, 240
00149 – Roma
Tel 06 45482304 - Fax 06 5593560
E-mail : lmarro@ares118.it

CODICE DELLA PRIVACY

(D.L.vo N. 196/2003)

DISPOSIZIONI MINIME SULLA SICUREZZA

E

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente documento si compone di n. 43 pagine (inclusa la presente)

Data di emissione: 30/03/2011

U.O.S. Sistema Informatico
Via Portuense, 240
00149 – Roma
Tel 06 45482304 - Fax 06 5593560
E-mail : lmarro@ares118.it

Premessa

Il presente Documento è stato redatto sulla base delle "Disposizioni inerenti l'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dagli articoli 33-36 e allegato B del D.Lgs. 196/03".

Le citate disposizioni impongono la predisposizione e l'aggiornamento, con cadenza almeno annuale (entro il 31 marzo di ogni anno), di un **Documento Programmatico sulla Sicurezza** dei dati, per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi, i seguenti elementi:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Tale documento deve essere obbligatoriamente predisposto nel caso di trattamento di dati sensibili o giudiziari. Questo è il caso di una Pubblica Amministrazione qual è l'Azienda Regionale per l'Emergenza Sanitaria ARES 118, che tratta, per mandato istitutivo, per la adempimento delle disposizioni normative e per la gestione delle attività a favore dei cittadini del Lazio, una insieme di dati fra cui sicuramente alcuni rientranti nella tipologia "sensibili", altri, anche se in misura limitata, "giudiziari".

Con apposito incarico il Direttore dell'UOS Sistema Informatico è stato designato come responsabile per la redazione entro il 31 marzo del Documento programmatico della Sicurezza di cui all'allegato B del DLvo 196/03, coadiuvato, al fine di ottemperare a tale incarico da tutti i responsabili delle strutture complesse, nominati dal titolare quali soggetti tenuti ad effettuare il trattamento dei dati personali

Il presente documento è il frutto di una ampia revisione concettuale e operativa che ha considerata la necessità

- identificare i tipi di dati e le operazioni eseguibili da parte nello svolgimento delle proprie funzioni istituzionali
- definire l'assetto documentale relativo alla gestione dei dati e in modo specifico per le applicazioni delle disposizioni del DLvo 196/03
- rivedere il contenuto del Documento programmatico, rispetto alle indicazioni normative, trasferendo la trattazione degli elementi prima richiamati nel regolamento

Il presente documento focalizza l'attenzione sul mandato legislativo evidenziando le principali misure adottate in relazioni alla tipologia delle varie banche dati, secondo una articolazione che segue la "Guida operativa per redigere il Documento programmatico sulla sicurezza" elaborata dal Garante e le modalità di lavoro del gruppo prima ricordato:

1. Censimento dei flussi informativi per i trattamenti interni; censimento delle banche dati costituite presso le strutture aziendali designate, coordinamento con la loro tipizzazione al fine della notifica al Garante.
2. Censimento delle singole banche dati ed archivi presenti in ogni servizio al fine dell'analisi dettagliata dei rischi e delle misure di sicurezza da adottare.
3. La descrizione delle modalità operative di gestione delle varie componenti e sistemi preposti alla gestione delle banche dati.
4. Analisi dei rischi connessi alla gestione delle banche dati, anche sulla scorta delle modalità operative di cui sopra.
5. L'individuazione di un piano con le principali misure di controllo necessarie per ciascun rischio in precedenza individuato.
6. Attività di informazione e formazione di tutti i soggetti interessati.
7. Indicazioni per le verifiche e l'aggiornamento periodico del piano stesso.

La redazione del documento ha visto il coinvolgimento in diversi incontri svoltisi nell'anno di diversi responsabili delle Unità Operative dell'Azienda.

Mediante la modulistica, allegata al presente documento – e descritta nelle Linee Guida prima ricordate -, i Dirigenti delle diverse UOC dell'ARES 118 sono stati invitati a rivedere il censimento delle varie banche dati esistenti. Attraverso tale censimento è stato possibile ricavare l'elenco dei vari trattamenti di dati in essere e la loro relazione con le stesse banche dati.

La modulistica consente anche di ottenere, per ciascuna banca dati rilevata, informazioni circa:

- Il trattamento/i per i quale viene impiegata
- la tipologia dei dati trattati
- i soggetti ai quali i dati si riferiscono
- le operazioni di trattamento eseguite su di esse
- la natura dei dati
- le modalità di trattamento dei dati contenuti con varie tipologie di strumenti e mezzi
- le eventuali comunicazioni dei dati contenuti ad altri soggetti

- l'eventuale diffusione dei dati
- l'eventuale intervento di terzi nella manipolazione della banca dati
- la correttezza comportamentale nel trattamento dei dati contenuti
- i soggetti coinvolti, a vario titolo, nella manipolazione dei dati contenuti
- le modalità di gestione delle copie dei dati (ove necessarie)
- i trattamenti affidati all'esterno dell'Ente

In sintesi nella redazione del presente DPS, sono stati utilizzati i precedenti documenti integrandoli, dove possibile, con gli aggiornamenti forniti dai responsabili del trattamento secondo le modalità descritte e si è proceduto a ricollocare alcuni temi alla luce del nuovo assetto documentale, riorganizzando la suddivisione del testo e approfondendo alcuni temi in modo più aderente al mandato normativo, trattando alcuni aspetti in modo metodologicamente più corretto nel regolamento e nelle specifiche procedure e istruzioni.

Il Mandato

Ai sensi della L.R. 03 Agosto 2004, n. 9 "Istituzione dell'azienda regionale per l'emergenza sanitaria ARES 118." l'ARES 118 è ente dipendente della Regione, dotato di personalità giuridica di diritto pubblico.

L'ARES 118 espleta le attività di gestione e coordinamento della fase di allarme e di risposta extraospedaliera alle emergenze sanitarie, ivi compresa l'emergenza neonatale, di trasporto del sangue, degli organi e di trasporti secondari legati al primo intervento.

L'ARES 118 provvede, inoltre, al raccordo con le attività svolte dai medici di medicina generale addetti alla continuità assistenziale nell'ambito del sistema di emergenza sanitaria territoriale.

Nell'esercizio delle proprie competenze l'ARES 118: a) si raccorda con le aziende sanitarie e con tutti gli altri enti ed organismi pubblici e privati accreditati che operano nell'ambito del sistema di emergenza sanitaria, al fine di garantire l'integrazione delle rispettive attività e di assicurare la continuità assistenziale in emergenza, disponendo in tempo reale di informazioni relative alla disponibilità della struttura più idonea al trattamento; b) cura la gestione ed il coordinamento dell'attività di elisoccorso e del personale sanitario dell'ARES 118 operante sui mezzi addetti all'elisoccorso; c) esprime parere preventivo sull'accreditamento degli organismi a scopo non lucrativo iscritti nell'elenco regionale previsto dall'articolo 2, comma 18, del decreto legislativo 30 dicembre 1992, n. 502 (Riordino della disciplina in materia sanitaria a norma dell'articolo 1 della l. 23 ottobre 1992, n. 421) e successive modifiche, che svolgono attività nell'ambito del sistema di emergenza sanitaria, cura il rapporto con gli organismi stessi ed esercita la vigilanza sulle relative attività; d) attiva procedure per l'eventuale utilizzazione dei mezzi di soccorso autorizzati al funzionamento, gestiti dagli organismi di cui alla lettera c) e dagli altri enti ed organismi pubblici e privati, ivi compresa l'Associazione italiana della Croce rossa, accreditati ai sensi della normativa vigente; e) opera, se necessario, in raccordo funzionale con le altre Regioni e, nei casi di maxiemergenza, anche d'intesa con le amministrazioni centrali competenti in materia di protezione civile

Con il medesimo atto legislativo, la Regione Lazio ha definito il sistema informativo

dell'emergenza composto dal complesso dei flussi informativi tra l'ARES 118, l'ASP e le strutture sanitarie e non sanitarie. Tale sistema è supportato da un sistema informatico e radio telecomunicativo integrato e viene organizzato e gestito in conformità agli indirizzi determinati dalla Giunta regionale
In particolare nella legge regionale si specifica che l'ARES 118, ai sensi della legge regionale 1 settembre 1999, n. 16, assicura all'Agenzia di sanità pubblica della Regione Lazio (ASP) i flussi informativi sulle attività di propria competenza con le modalità definite d'intesa con la stessa ASP e può avvalersi di quest'ultima anche per la definizione di specifici indicatori atti a valutare la qualità del servizio e delle prestazioni erogate e la percezione della qualità stessa da parte degli utenti. Può avvalersi altresì dell'Agenzia regionale per la protezione ambientale del Lazio (ARPA) e dell'Istituto zooprofilattico sperimentale delle Regioni Lazio e Toscana, secondo le disposizioni previste dalle leggi regionali 6 ottobre 1998, n. 45 e successive modifiche e 6 agosto 1999, n. 11, nonché, mediante apposite convenzioni, degli altri enti, istituzioni ed organismi aventi finalità di studio, formazione e ricerca nell'ambito del sistema sanitario

Finalità del documento e impegno dell'Azienda

Il Trattamento di Dati personali e soprattutto sanitari, costituisce elemento essenziale per l'attività dell'A.R.E.S. 118 e costitutivo della sua missione.

Il presente documento ha lo scopo di fornire un quadro di riferimento delle misure di sicurezza idonee adottate in conseguenza delle particolarità dei Trattamenti svolti, e di indicare i programmi futuri di miglioramento delle stesse che l'A.R.E.S. 118 intende perseguire a tutela dei soggetti i cui dati personali vengono trattati.

La descrizione complessiva e dettagliata della gestione dei dati personali può essere ricavata dall'insieme del sistema documentale che oltre al DPS prevede un Regolamento, specifiche procedure, istruzioni e documenti informativi.

La rilevazione puntuale della situazione corrente dei Trattamenti e degli strumenti informatici con cui gli stessi sono eseguiti è resa particolarmente complessa dalla evoluzione organizzativa tuttora in atto sia per quanto riguarda i processi dell'Azienda, sia per le architetture adottate per i sistemi informatici.

Definizioni e responsabilità

AMMINISTRATORE DI SISTEMA: il soggetto cui Ë conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.
Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui Ë conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a

un interessato identificato o identificabile.

DATI PERSONALI: 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.

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

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.

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 D.P.R. 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.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile Ë facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile Ë facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

TRATTAMENTO: qualunque operazione o complesso di operazioni, effettuate 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 dati .

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS): documento che definisce, sulla base dell'analisi dei rischi, le misure di sicurezza da adottare e che deve contenere le idonee informazioni previste dal p. 19.1 al p. 19.8 dell' Allegato B al Codice per la Privacy.

TITOLARE: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le

decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali, ivi compreso il profilo della sicurezza.

RESPONSABILE: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali.

INCARICATI: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

INTERESSATO: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

COMUNICAZIONE: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

DIFFUSIONE: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

DATO ANONIMO: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

BLOCCO: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

BANCA DI DATI: un complesso organizzato di dati personali, diviso in una o più unità dislocate in uno o più siti.

GARANTE: L'autorità di cui all'articolo 153 del Codice, istituita dalla legge 31 dicembre 1996, n. 675.

COMUNICAZIONE ELETTRONICA: la informazione scambiata/trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

CHIAMATA: la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

RETI DI COMUNICAZIONE ELTTRONICA: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse idonee a trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, reti utilizzate per diffusione circolare dei programmi sonori e televisivi, sistemi per trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

RETE DI COMUNICAZIONE PUBBLICA: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

SERVIZIO DI COMUNICAZIONE ELETTRONICA: i servizi consistenti solo o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

ABBONATO: qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura ditali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

UTENTE: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

DATI RELATIVI AL TRAFFICO: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

DATI RELATIVI ALL'UBICAZIONE: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

SERVIZIO A VALORE AGGIUNTO: il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

POSTA ELETTRONICA: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;

MISURE MINIME: Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31 del Codice.

STRUMENTI ELETTRONICI: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

AUTENTICAZIONE INFORMATICA: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

CREDENZIALI DI AUTENTICAZIONE: I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

PAROLA CHIAVE (Password): componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica

PROFILI DI AUTORIZZAZIONE: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

SISTEMA DI AUTORIZZAZIONE: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alla modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

SCOPI STORICI: Le finalità di studio,indagine, ricerca e documentazione di figure, fatti e circostanze del passato.

SCOPI STATISTICI: Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici.

SCOPI SCIENTIFICI: Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Modalità di aggiornamento e revisione

Il Documento Programmatico Sulla Sicurezza, viene revisionato annualmente entro il 31 marzo dell'anno in corso ed eventualmente sottoposto ad integrazioni e/o modifiche.

I Responsabili delle varie U.O. possono nel corso dell'anno aggiornare le schede di rilevazione in su supporto informatico che verrà trasmesso al Gruppo Privacy.

L'acquisizione di ulteriori elementi conoscitivi, il monitoraggio nell'adozione delle misure pianificate, l'evoluzione tecnologica e l'incremento della consapevolezza degli operatori e del coinvolgimento dei responsabili si auspica che portino ad un aggiornamento di tale documento prima della scadenza prevista del 31 marzo.

La distribuzione dei compiti e delle responsabilità
I soggetti

L'elenco completo dei soggetti individuati e copia dell'atto formale con cui sono stati nominati è reperibile presso l'Unità Operativa Affari Generali e Legali.

I Responsabili del trattamento sono individuati fra i soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Il Responsabile del trattamento dei dati personali e delle banche dati, designato con atto scritto dal Titolare, coincide, di norma, con il responsabile della struttura nell'ambito della quale i dati personali o le banche dati sono gestiti per le finalità istituzionali della rispettiva unità organizzativa
All'interno dell'Azienda i responsabili possono coincidere con coloro che ricoprono posizioni organizzative e funzionali ed in particolare :

- Direttore Sanitario;
- Direttore Amministrativo;
- Direttori Centrale Operativa e altri Direttori di struttura complessa;
- Responsabili di struttura semplice, o altri funzionari, per i quali si rende opportuna la designazione di Responsabili del trattamento in virtù delle particolarità organizzative e funzionali delle attività di competenza.

Nel caso degli incaricati si ritiene opportuno evidenziare alcune peculiarità.

1. L'ARES 118 si caratterizza per la capillare diffusione territoriale, per lo svolgimento delle attività per piccoli gruppi, per il trattamento di dati idonei a rilevare lo stato di salute anche da parte di operatori non legati a norme deontologiche di specifici albi professionali.
2. In accordo con lo specifico provvedimento del Garante, il titolare del trattamento deve designare quali incaricati o, eventualmente, responsabili del trattamento i soggetti che possono accedere ai dati personali trattati nell'erogazione delle prestazioni e dei servizi per svolgere le attività di prevenzione, diagnosi, cura e riabilitazione, nonché quelle amministrative correlate (artt. 30 e 29 del Codice).
3. Fermi restando, in quanto applicabili, gli obblighi in materia di segreto d'ufficio, deve essere previsto che, al pari del personale medico ed infermieristico, già tenuto al segreto professionale (art. 9 del codice di deontologia medica del 3 ottobre 1998; art. 4 del codice deontologico per gli infermieri del maggio del 1999), gli altri soggetti che non sono tenuti per legge al segreto professionale (ad es., personale tecnico e ausiliario) siano sottoposti a regole di condotta analoghe (cfr. anche art. 10 del codice di deontologia medica).

Alla luce del modello organizzativo e delle peculiarità dell'azienda ARES 118 tutti i dipendenti sono ritenuti incaricati del trattamento di dati personali. Agli operatori che svolgono funzioni specifiche o hanno compiti particolari, inoltre, possono essere esplicitati per iscritto specifici ulteriori obblighi dal Responsabile del trattamento

Utilizzo e trasmissione dei dati all'interno dell'Azienda ARES 118

L'accesso ai dati personali da parte delle strutture amministrative, di servizio e dei dipendenti dell'Azienda è limitato ai casi in cui sia finalizzato al perseguimento di scopi istituzionali, ed è ispirato al principio della libera circolazione delle informazioni.

Ogni richiesta d'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Azienda è collegata con lo svolgimento dell'attività inerente alla specifica funzione e viene valutata in via diretta e senza formalità nella misura necessaria al perseguimento dell'interesse istituzionale.

Qualora invece la richiesta d'accesso sia giustificata per un utilizzo diverso dei dati, i soggetti già indicati devono comunicarlo in maniera esplicita e formale nella richiesta; quest'ultima viene esaminata dal Responsabile del trattamento dei dati, e l'autorizzazione viene concessa o negata a seconda che il fine della richiesta rientri o meno nell'attività istituzionale dell'Azienda.

Il richiedente adotta tutte le misure necessarie a garantire la sicurezza dei dati a lui trasmessi.

Il trattamento dei dati personali / sensibili avviene, all'interno dell'Azienda, nelle sue varie articolazioni solo per l'adempimento delle competenze e per fini istituzionali e nel rispetto dei diritti della dignità personale e della riservatezza.

In particolare, per gli uffici che hanno rapporti con il pubblico, il Dirigente di competenza, anche nella sua qualità di Responsabile, ai fini del presente DPS, adotta ogni misura idonea a garantire la dignità delle persone e la riservatezza dei dati trattati, come da Art. 83 del Codice

Durante il trattamento il preposto incaricato salvaguardia la riservatezza dei dati anche nei confronti di altri dipendenti e colleghi impedendo ogni sproposita visione e consultazione

Ai fini dell'accesso ai dati sono equiparati alle strutture dell'Azienda il Collegio Sindacale, il l'organismo indipendente di Valutazione ed il Comitato Etico, nei limiti rigorosi di quanto necessario per il perseguimento delle rispettive finalità istituzionali

Analisi dei rischi

L'analisi dei rischi consente di acquisire consapevolezza e visibilità‡ sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.
L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;
- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
  - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
  - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
  - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

Individuazione delle risorse da proteggere

Le risorse da proteggere sono:

- personale;
- dati/informazioni;
- documenti cartacei;
- hardware;
- software;

Per ulteriori dettagli vedere gli Allegati 1 e 3.

Individuazione delle minacce

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse.

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Inondazione	X	X	X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi		X	
Danno volontario	X		
Interruzione di corrente		X	
Interruzione di acqua		X	
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura e umidità eccessive			X
Polvere			X
Radiazioni elettromagnetiche		X	
Scariche elettrostatiche		X	
Furto	X		
Uso non autorizzato dei supporti di memoria	X		
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Masquerading dell'identificativo dell'utente	X		
Uso illegale di software	X	X	
Software dannoso		X	
Esportazione/importazione illegale di software	X		
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		
Guasto tecnico di provider di rete		X	
Danni sulle linee	X	X	
Errore di trasmissione		X	
Sovraccarico di traffico	X	X	
Intercettazione (Eavesdropping)	X		
Infiltrazione nelle comunicazioni	X		
Analisi del traffico		X	
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Ripudio	X		

Rischi	Deliberato	Accidentale	Ambientale
Guasto dei servizi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Guasto software	X	X	
Uso di software da parte di utenti non autorizzati	X	X	
Uso di software in situazioni non autorizzate	X	X	

Per ulteriori dettagli delle minacce relative all'aspetto informatico vedere l'Allegato 2

Individuazione delle vulnerabilità

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nell'articolo 6.

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Locazione suscettibile ad allagamenti	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto
		Gestione inadeguata della rete
		Connessioni a linea pubblica non protette

Documenti cartacei	Software	Personale
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza del registro delle attività(log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

Individuazione delle contromisure

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico;
- contromisure di carattere procedurale;
- contromisure di carattere elettronico/informatico.

Contromisure di carattere fisico

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
- i locali ad accesso controllato sono all'interno di aree sotto la responsabilità del Responsabile UOS informatica
- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti;
- i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite a cura di ;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'ente di sicurezza interna Interpol.;
- i locali sono provvisti di sistema di allarme e di estintore;
- sono programmati interventi atti a dotare i locali ad accesso controllato di porte blindate, armadi ignifughi, impianti elettrici dedicati, sistemi di condizionamento, apparecchiature di continuità elettrica.

Contromisure di carattere procedurale

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, che è periodicamente controllata dal responsabile del trattamento o da un suo delegato;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- per l'ingresso ai locali ad accesso controllato è necessaria preventiva autorizzazione da parte del Responsabile del trattamento e successiva registrazione su apposito registro;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli allarmi e degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'incaricato del trattamento di tali dati;
- i registri, contenenti dati comuni e particolari, durante l'orario di lavoro devono essere tenuti in e affidati al responsabile di turno. Al termine dell'orario di lavoro vengono depositati e successivamente raccolti da un incaricato del trattamento e conservati in luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio dell'orario di lavoro.
- il responsabile del trattamento dei dati è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del responsabile del trattamento dei dati che Ë chiuso a chiave, una chiave di riserva Ë mantenuta con le dovute cautele dalla ditta ;
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è

conservato all'interno della stanza Protocollo informatico sita al piano terra e con accesso controllato

Adozione di misure tecnologiche di Sicurezza Informatica, la cui realizzazione è programmata nel corso dell'anno 2011

Tenuto conto dell'attuale disponibilità di idonee tecnologie informatiche, in grado di rispondere a queste esigenze, la U.O.S. Informatica provvederà entro l'anno 2011 alla realizzazione delle seguenti misure tecnologiche di Sicurezza Informatica :

Misura 1 : protezione e adeguamento tecnologico degli apparati
Le principali sottomisure di protezione, da adottare entro l'anno 2011 in parallelo all'adeguamento tecnologico delle apparecchiature informatiche aziendali, sono :

- Completamento del rafforzamento della protezione fisica dalla manomissione dell'HW degli apparati server e d'utente
- Maggiori limitazioni d'accesso con identificazione sicura dell'utente e degli apparati in rete

Misura 2 : protezione della rete informatica e delle informazioni aziendali
Le principali realizzazioni, che miglioreranno il livello di protezione della rete informatica aziendale entro l'anno 2011, sono indicate nelle seguenti sottomisure :

2.1 Integrazione delle protezioni antivirus, firewall, antispia e IDS (intrusion detection)
2.2 Gestione centralizzata dei backup sulla rete aziendale
2.3 Estensione del monitoraggio del traffico di rete e creazione di sottoreti aziendali superprotette
2.4 Sistemi d'accesso informatico e di firma digitale per l'invio di documenti in modalità telematica, gestito mediante "smart card"

Misura 3 : Aggiornamento delle politiche della sicurezza informatica

3.1 Politica per l'accesso fisico alle aree riservate agli apparati server (CED) aziendali
3.2 Politica per l'accesso agli uffici e alle relative apparecchiature informatiche d'utente
3.3 Integrazione e completamento della politica per l'utilizzo di apparecchiature informatiche portatili in azienda e in modalità "telelavoro", con accesso remoto dei dipendenti e dei collaboratori alla rete aziendale
3.4 Politica per la modifica periodica delle "username" e "password" sulla rete aziendale
3.5 Politica di "audit" per la verifica periodica delle misure di sicurezza informatica Politica di graduale bonifica delle procedure utilizzate sui PC aziendali.

Contromisure di carattere elettronico/informatico

Vedere l'Allegato 3.

Norme per il personale

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete (Allegato 4).

Incident response e ripristino

Vedere l'Allegato 3

Criteri per la cifratura o per la separazione dei dati sanitari dagli altri dati personali dell'interessato

Il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche dati è effettuato con le modalità di cui all'art. 22, comma 6 del Codice anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. (punto 24 all. B disciplinare tecnico 196/2003).
Prima che possa essere effettuata la separazione o dove questa non è possibile i dati sono opportunamente cifrati al fine di garantirne la sicurezza

Trattamento dei dati senza strumenti elettronici

Il trattamento dei dati personali effettuato senza strumenti elettronici è consentito con la adozione delle seguenti misure minime:

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Per ogni archivio i Responsabili del trattamento dei dati debbono definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso degli archivi.

Agli Incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico, con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione. (punto 27 all. B disciplinare tecnico d.lgs. 196/2003).

E' opportuno ritornare su quanto descritto precedentemente nella distribuzione dei compiti e delle responsabilità. A titolo esemplificativo tutti i dipendenti dell'aziende sono da considerarsi incaricati nel trattamento nel momento in cui fanno un soccorso, acquisiscono i dati, conservano le schede di accedendo all'archivio di postazione; chi svolge le funzioni di coordinatore ha ulteriori e specifici obblighi connessi al suo ruolo aziendale sulla tenute e gestione dell'archivio delle schede di soccorso.

E' in corso una revisione delle modalità di gestione delle schede di soccorso nelle postazioni con l'obiettivo di garantirne meglio la sicurezza e dell'interfaccia con le società che ne curano la successiva archiviazione, identificati con responsabili esterni del trattamento.

Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termini delle operazioni affidate. (punto 28 all. B disciplinare tecnico d.lgs. 196/2003)

L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Quando gli archivi non sono

dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate. (punto 29 all. B disciplinare tecnico d.lgs. 196/2003)

Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.
Qualora i documenti contengano dati sensibili e giudiziari gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura

La previsione di interventi formativi degli incaricati del trattamento

In considerazione del continuo contatto con gli utenti della maggioranza del personale dipendente dell'A.R.E.S. 118, la informazione e sensibilizzazione dei propri collaboratori assume un ruolo decisivo per garantire, non solo la corretta applicazione dei sistemi di sicurezza adottati, ma anche, e soprattutto la correttezza della informazione fornita agli utenti; ciò verrà ottenuto tramite momenti formativi che approfondiscano anche temi concreti e specifici, con l'intento di sensibilizzare ciascun operatore circa la necessità di adottare i comportamenti più adeguati, nonché di migliorare la conoscenza degli obblighi, dei rischi e delle sanzioni che la legge pone a carico dei trasgressori

Trattamenti di dati personali affidati all'esterno della struttura del titolare

Il Titolare del trattamento può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, nominandoli Responsabili del trattamento. Come previsto dal Regolamento in alcuni casi all'incarico di responsabile del trattamento si affiancherà quello di responsabile del sistema.

Il soggetto affidatario deve specificare il modello organizzativo, le modalità, gli strumenti i luoghi dove fisicamente avviene il trattamento dei dati stessi.

Con esclusione dei soggetti esterni che operano per dell'A.R.E.S. 118 in modo occasionale, ai Responsabili Esterni viene richiesto con periodicità almeno annuale, o comunque ogni qualvolta siano riscontrate significative carenze sul piano della sicurezza, una Relazione sulla Sicurezza che include informazioni atte ad assicurare la vigilanza sul piano organizzativo, logico e fisico.

Nel caso in cui questi non vengano espressamente nominati, i Responsabili del trattamento ai sensi della vigente normativa devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

Criteri per la scelta dei terzi a cui affidare il trattamento dei dati e modalità di affidamento

Il Titolare del trattamento può nominare Responsabile del trattamento quei soggetti terzi che abbiano i requisiti individuati all'art. 29 del Codice (esperienza, capacità, affidabilità).

Il Responsabile del trattamento dei dati deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti in particolare che sono state adottate le misure idonee di sicurezza per il trattamento dei dati secondo quanto disposto dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B del Codice. In allegato alla lettera di accettazione i soggetti interessati dovranno esplicitare le modalità di trattamento dei dati e i luoghi in cui fisicamente avviene tale trattamento.

Per ogni trattamento affidato ad un soggetto terzo nominato Responsabile del trattamento, il Titolare del trattamento attraverso le funzioni aziendali competenti si assicura che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

La nomina del Responsabile del trattamento dei dati del soggetto terzo deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

La U.O.C. Acquisizione Beni e Servizi, La UOC Affari Generali e le altre UU.OO. adibite alla definizioni di contratti e/o convenzioni sono tenute ad inserire nei capitolati speciali, nelle lettere di invito ovvero nel testo delle convenzioni uno specifico riferimento in cui si evidenzi che il soggetto esterno risulterà Responsabile del Trattamento dei dati ai sensi del D.Lg.vo 196/2003

Sviluppo applicazioni informatiche

In caso lo sviluppo di nuove applicazioni informatiche, o revisione di applicazioni preesistenti, sia affidato a società esterne, queste devono provvedere alla certificazione in accordo con quanto previsto dall'Art. 25 del Disciplinare Tecnico.

In particolare viene verificata, sotto la responsabilità del Responsabile Organizzativo la presenza delle seguenti caratteristiche:

- sono definite e realizzate le funzionalità atte a garantire l'esercizio da parte degli interessati dei diritti di cui all'art. 7 del Codice;
- sono previsti gli opportuni controlli per escludere dal trattamento dati soggetti a blocco o ad altre forme di restrizione d'uso;
- è verificata la conformità alle disposizioni normative e di legge che disciplinano il trattamento servito dalla applicazione, nel caso in cui la finalità del Trattamento sia l'ottemperanza ad un obbligo previsto da Legge o normativa;
- nel caso in cui vengano realizzati trattamenti di dati particolari avvalendosi delle autorizzazioni generali del Garante, deve essere verificata la applicabilità di detta Autorizzazione in relazione alle finalità e modalità del Trattamento stesso;
- i dati personali utilizzati sono pertinenti e non eccedenti rispetto alle finalità per cui viene realizzata la applicazione.

U.O.S. Sistema Informatico
Via Portuense, 240
00149 – Roma
Tel 06 45482304 - Fax 06 5593560
E-mail : lmarro@ares118.it

Aggiornamento del piano

Il presente piano Ë soggetto a revisione annua obbligatoria con scadenza entro il 31 marzo, ai sensi dell'art. 19 allegato B del D.L.vo 30/06/2003 Num. 196. Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- modifiche all'assetto organizzativo della ditta ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- danneggiamento o attacchi al patrimonio informativo della ditta tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

Elenco Allegati costituenti parte integrante di questo documento

- Allegato 1 - elenco trattamenti dei dati
- Allegato 2 - minacce hardware, minacce rete, minacce dati trattati, minacce supporti
- Allegato 3 - misure di carattere elettronico/informatico, politiche di sicurezza, incident response e ripristino
- Allegato 4 - regolamento per l'utilizzo della rete
- Allegato 5 – uso del proxy
- Allegato 6 – attività di videosorveglianza
- Lettere di incarico per il trattamento dei dati
- Lettera di incarico per il responsabile del trattamento
- Lettera di incarico per il custode delle password
- Lettera di incarico per l'amministratore di sistema

Il presente Documento Programmatico sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati.

Il redattore del documento

_____
(firma leggibile)

Nota: Fonti di documentazione
Il modello di documento programmatico sulla sicurezza Ë stato predisposto consultando le seguenti fonti:

- **http://www.garanteprivacy.it**
- *"Sicurezza informatica" ECDL IT Administrator - Modulo 5 Testo di riferimento per la certificazione EUCIP - McGraw Hill ISBN 88-3864333-4 Tabelle Minacce e vulnerabilità Cap. 1*
- *Il regolamento per l'utilizzo della rete Ë stato derivato dal documento CISEL 0203G286 - CISEL Centro Studi per gli Enti Locali - Maggioli*

U.O.S. Sistema Informatico
Via Portuense, 240
00149 – Roma
Tel 06 45482304 - Fax 06 5593560
E-mail : lmarro@ares118.it

ALLEGATO 1 – Elenco trattamenti dei dati

Tabella 1 - Elenco dei trattamenti dei dati

Finalità perseguita o attività svolta	Categorie di interessati	Natura dei dati trattati	Struttura di riferimento	Altre strutture che concorrono al trattamento	Descrizione degli strumenti utilizzati
Gestione collaboratori gestione dei fornitori	collaboratori e fornitori	Dati Personali sensibili / giudiziari	UOS Informatica	UOS Informatica	Sw e hw specifico al tracciamento del flusso interno dei dati

Descrizione sintetica: menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es. gestione del personale , gestione collaboratori, gestioni clienti, gestioni fornitori, ecc.) e delle categorie di persone cui i dati si riferiscono (personale, collaboratori, clienti, fornitori, ecc.).

Natura dei dati trattati: indicare la classe di rischio dei dati trattati tenendo presente la seguente classificazione:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI
  - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio;
  - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio
  - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

Struttura di riferimento: indicare la struttura (segreteria amministrativa, direzione, funzione svolta, ecc.) all'interno della quale viene effettuato il trattamento.

Altre strutture che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture È opportuno indicare, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.

Descrizione degli strumenti utilizzati: va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi) e altre tipologie di contenitori (es. armadi, schedario).

Tabella 2 - Descrizione della struttura organizzativa

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
UOS Informatica	Responsabile dati e fonia Responsabile sicurezza ed inviolabilità del dato interno Ares Responsabile della parte radio	Supervisore e coordinatore della parte radio e telecomunicazione, responsabile della sicurezza informatica interna

Struttura: riportare le indicazioni delle strutture menzionate nella Tabella 1.

Trattamenti effettuati dalla struttura: indicare i trattamenti di competenza di ciascuna struttura.

Compiti e responsabilità della struttura: descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.

Tabella 3 - Elenco del personale incaricato del trattamento in ogni struttura e delle dotazioni informatiche.

Cognome e Nome	Struttura di riferimento	Strumenti utilizzati	Responsabilità aggiuntive
Dott Marro Luca	UOS Informatica	Dati: Firewalling, proxy, antivirus Fonia: controllo della fatturazione e del corretto uso della componente fissa/mobile Radio: determinazione mancata copertura rete e sostituzione e ripristino apparecchiatura	Supervisore per la componente dati emergenza urgenza Responsabile del procedimento del nuovo sistema informativo Ares118

Nome e cognome: riportare le indicazioni per ogni incaricato del trattamento.

Struttura di riferimento: riportare l'indicazione della struttura di appartenenza di ogni incaricato.

Strumenti utilizzati: per ogni incaricato riportare le informazioni relative allo strumento utilizzato (p.e. numero di inventario del PC).

Responsabilità aggiuntive: indicare le eventuali responsabilità aggiuntive rispetto all' incarico per il trattamento dei dati, ad esempio responsabile del trattamento, responsabile delle copie di backup, custode delle chiavi di un contenitore o armadio, custode delle password, ecc.

Nota: *parte delle indicazioni sono tratte dalla ìGuida operativa per redigere il documento programmatico sulla sicurezza (DPS)î pubblicate dal garante*

ALLEGATO 2 – Minacce

Minacce a cui sono sottoposte le risorse hardware

Le principali minacce alle risorse hardware sono:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;

Minacce a cui sono sottoposte le risorse connesse in rete

Le principali minacce alle risorse connesse in rete possono provenire dall'interno, dall'esterno o da una combinazione interno/esterno e sono relative:
all'utilizzo della LAN/Intranet (interne);
ai punti di contatto con il mondo esterno attraverso Internet (esterne);

- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

In dettaglio si evidenziano le seguenti tecniche:

IP spoofing
L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

Packet sniffing
Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso È possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

Port scanning
Serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.

Highjacking
Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione È complessa e richiede elevate capacità e rapidità d'azione.

Social engineering
Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.

Buffer overflow
Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

Spamming
Saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.

Password cracking
Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.

Trojan
Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.

Worm
Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).

Logic bomb
Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.

Malware e MMC (Malicious Mobile Code)
Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.

DOS (Denial of Service)
Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.

DDOS (Distributed Denial of Service)
Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete

L'utilizzo di programmi di sniffing e port scanning È riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete locale LAN, tali programmi non sono in nessun caso utilizzati su reti esterne a quella della rete loca LAN.
La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dalla Autorità Giudiziaria.

Minacce a cui sono sottoposti i dati trattati

Le principali minacce ai dati trattati sono:

- accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

Minacce a cui sono sottoposti i supporti di memorizzazione

Le principali minacce ai supporti di memorizzazione sono:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

ALLEGATO 3 – Misure, incident response, ripristino

Tabella 1 - Connettività internet

Connettività	Apparecchiature di comunicazione	Provider
SPC	Router attraverso il servizio di connettività pubblico SPC	Telecom

Connettività: collegamenti tramite HDSL o ADSL alla Servizio Pubblico di Connettività

Apparecchiature di comunicazione: Apparecchiature utilizzate router

Provider: Telecom Italia.

Tabella 2 - Descrizione Personal Computer

Identificatico del PC	Tipo PC	Sistema operativo	Software utilizzato	Rete
pc001	PC 2 gb ram 250 hd 2,33 mhz	Windwos	S.O. Office antivirus proxy	

Identificativo del PC: confrontare schede inventario ufficio tecnico

Tipo PC:

Sistema operativo: Microsoft Windows.

Software utilizzato: Office Microsoft.

Rete: SPC.

U.O.S. Sistema Informatico
Via Portuense, 240
00149 – Roma
Tel 06 45482304 - Fax 06 5593560
E-mail : lmarro@ares118.it

Misure di carattere elettronico/informatico

Le misure di carattere elettronico/informatico adottate sono:

- utilizzo di server con configurazioni di ridondanza
- presenza di gruppi di continuità elettrica per il server
- attivazione di un sistema di backup de centralizzato e semi automatizzato con periodicità settimanale e storico di un mese a cura del personale interno
- Alla data di questo documento i responsabili delle copie sono indicati nell'Allegato 1 relativo al censimento dei trattamenti dei dati;
- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet (indicare se la misura Ë attiva o entro quando sarà adottata);
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows 2000 e XP, di seguito specificate (indicare se la misura Ë attiva o entro quando sarà adottata);
- divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro con sistemi operativi Windows 9x e Windows Me;
- installazione di un sistema antivirus su tutte le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria (indicare se la misura Ë attiva e quale prodotto Ë utilizzato o entro quando sarà adottata);
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate

Regole per la gestione delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale.
User-id e password iniziali sono assegnati, dal custode delle password.
User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.
La User-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.
La password Ë composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.
Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale Ë indicato il proprio user-id e al cui interno Ë contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.
Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.
Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema Ë autorizzato a intervenire sui personal computer.
In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:
le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
per la definizione/gestione della password devono essere rispettate le seguenti regole:

- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere più di due caratteri identici consecutivi;
- non deve contenere lo user-id come parte della password;
- al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
- la nuova password non deve essere simile alla password precedente;
- la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
- la password termina dopo sei mesi di inattività;
- la password Ë segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;
- l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia

Regole per la gestione di strumenti elettronico/informatico

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup realizzate su dispositivo, CD, cassetta, ecc. sono conservate in armadio chiuso a chiave, all'interno del locale CED in un apposito armadio blindato
- divieto di utilizzare floppy disk come mezzo per il backup;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.
- Il fax si trova in locale ad accesso controllato (specificare dove) e l'utilizzo è consentito unicamente agli incaricati del trattamento (specificare chi)

Il controllo dei documenti stampati Ë responsabilità degli incaricati al trattamento.
La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, Ë autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;
- disattivare gli ActiveX e il download dei file per gli utenti del browser Internet Explorer;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);

- attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- non attivare le condivisioni dell'HD in scrittura.
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiedere di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

- formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
- installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

Incident response e ripristino

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente(vedi tabella 3).
   Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso;
4. documentare tutte le operazioni.

Se l'incidente Ë dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi Ë frode, danno, abuso e non Ë configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.
Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

- eseguire una copia bit to bit degli hard disk del sistema compromesso;
- se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
- se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC (vedere Allegato 2) il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

Tabella 3 - Procedure di spegnimento

Sistema operativo	Azione
MS DOS	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.
UNIX/Linux	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Se la password di root è disponibile eseguire il comando su e poi i comandi sync e halt. 3. Se la password di root non è disponibile staccare la spina dalla presa di corrente.
Mac	4. Fotografare lo schermo e documentare i programmi che sono attivi. 5. Cliccare Special. 6. Cliccare Shutdown. 7. Una finestra indicherò che è possibile spegnere il sistema. 8. Staccare la spina dalla presa di corrente.
Windows 98/NT/2000/XP	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.

Nota: *(fonte U.S. Departement of Energy)*

ALLEGATO 4 – Regolamento per l'utilizzo della rete

Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica e dei servizi che, tramite la stessa rete, Ë possibile ricevere o offrire.
Con riferimento alle Figura 1 e Figura 2, si riportano i componenti passivi delle due reti presso le sedi ARES 118:

- **Centrale Operativa Roma:**
  - RETE Telecom ARES118 (Amministrativa)
    - 1 switch da 24 porte ENTERASYS A2H124-24 Ethernet - Tutte le porte sono occupate.
    - Firewall FortiGate 300 A ridondato.
  - RETE Fastweb RUPAR
    - 2 switch da 48 porte Cisco Layer 3 Ethernet interconnessi. Ci sono porte disponibili.
    - 1 Firewall FortiGate 60
    - Una linea RTG con modem 56K per assistenza remota.
  - RETE Fastweb RUPAR (Amministrativa)
    - 1 switch da 48 porte HP Procurve 5304xL Ethernet. Poche porte disponibili.
- **Centrali Operative di Rieti Frosinone Latina Viterbo**:
  - RETE Telecom ARES118 (Amministrativa)
    - 1 switch TP-LINK 10/100 da 8 porte Ethernet. Poche porte disponibili.
  - RETE Fastweb RUPAR per ciascuna provincia
    - 2 switch da 24 porte Cisco Layer 3 Ethernet interconnessi. Ci sono porte disponibili.
    - 1 Firewall FortiGate 60
    - Una linea RTG con modem 56K per assistenza remota.
- **Uffici Amministrativi di Via Portuense 240.**
  - RETE Telecom ARES118 (Amministrativa)
    - 2 switch da 48 porte Cisco Catalyst 2960. Ci sono porte disponibili.
- **Uffici Amministrativi di Via Portuense 332.**
  - RETE Telecom ARES118 (Amministrativa)
    - 1 Switch da 24 porte Cisco Catalyst 2960. Tutte le porte sono occupate.
    - 1 Switch da 16 porte 3com Baseline 2016. Poche porte disponibili.
- **N. 19 Postazioni 118 + Autoparco.**
  - Router Cisco 877 Telecom collegato direttamente al Computer.

Rete di accesso geografico (WAN)

La Rete ARES 118 Telecom e la rete RUPAR Fastweb sono interconnesse. Dalle sedi di Via Portuense 240, Via Portuense 332 e dalla Centrale Operativa di Roma, è possibile raggiungere l'IP 10.2.1.100 della RUPAR (portale della Sanità) per attività istituzionali.

Attraverso la RUPAR dalla Centrale Operativa di Roma la Soc. Capodarco ha attivato una postazione di lavoro per la "Gestione dei Posti Letto".

Non esistono connessioni con altre Reti o con banche dati esterne e/o Presidi Ospedalieri.

In Figura 1 se ne riporta lo schema che racchiude anche le tipologie dei collegamenti.

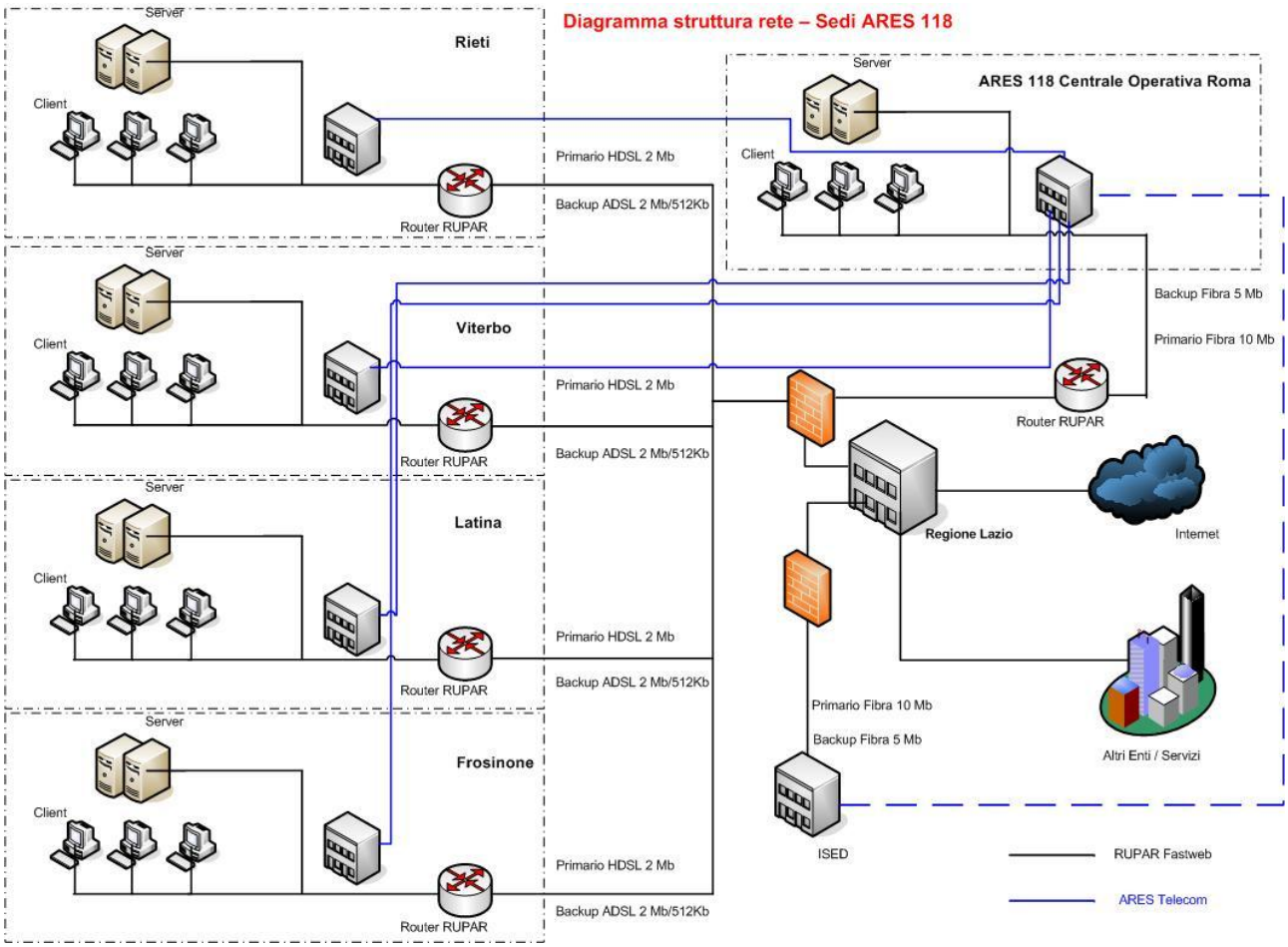

Figura 1: Diagramma struttura rete sedi ARES118 Lazio

Nel dettaglio, troviamo:

- C.O. Roma, 10 Mb ridondata, partizionata in 6 Mb Internet e 4 Mb Intranet
- Portuense 240, 4 Mb ridondata

- Portuense 332, 4 Mb ridondata
- C.O. FR - LT - VT - RI 2Mb ridondata
- 19 Postazioni, 600 Kb non ridondati
- Autoparco 600 Kb

Tutte le tratte ridondate sono anche bilanciate (down/up).

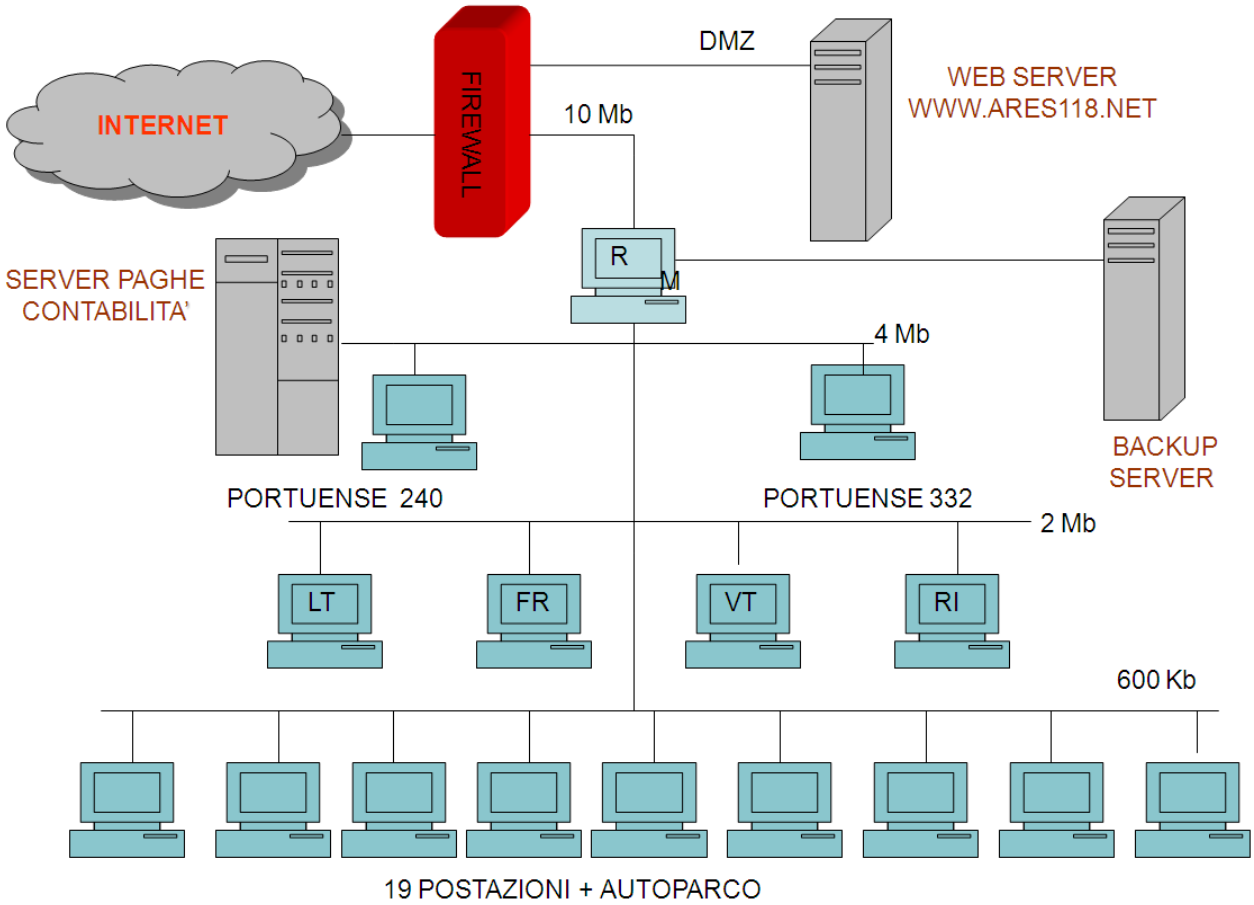

Figura 2: Dettaglio connettività rete ARES118 Lazio

Elenco degli applicativi SW e Fornitori

- Gestione Scheda Soccorso - fornitore ISED
- Sistema di registrazione chiamate di emergenza – fornitore Vitrociset
- Gestione Paghe e Presenze – fornitore Engineering
- Gestione Contabilità Economica – fornitore Data Ufficio
- Geolocalizzazione Nuove Ambulanze – fornitore ETHERIA
- Gestione Magazzino Logistico – fornitore ARES 118
- Gestione nuova influenza AH1N1 – fornitore ARES 118
- Gestione Telefonia – fornitore ARES 118

Tipologia e configurazione server dipartimentali

In gestione diretta dell'ARES 118 ci sono due Server IBM in Raid 5 dotati di Windows Server 2003 solo il server della Contabilità Economica e protetto da un gruppo di continuità, l'altro server contiene gli applicativi "Magazzino" "Influenza AH1N1" e "Telefonia" , gli applicativi sono stati sviluppati in Azienda. Entrambe i server sono dotati di antivirus aggiornati costantemente. Non vengono eseguiti backup su supporti esterni ai due server. L'accesso al server e alle procedure è protetto da Login e Password.

Principi generali - diritti e responsabilità

ARES 118 promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.
Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.
Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti s'impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.
Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo Ë tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

Abusi e attività vietate

E' vietato ogni tipo di abuso. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile, come specificato nell'allegato 3.

Attività consentite

E' consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di

manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore dare comunicazione dell'avvenuta modifica all'utente che provvedere ad informare il custode delle password come da procedura descritta nell'allegato 3;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.
L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.
L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.
Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili, l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.
L'accesso agli applicativi Ë consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Modalit‡ di accesso alla rete e agli applicativi

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.
L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.
L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.
Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password e rispettare le norme indicate nell'allegato 3.

Sanzioni

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di

natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti interni.

U.O.S. Sistema Informatico
Via Portuense, 240
00149 – Roma
Tel 06 45482304 - Fax 06 5593560
E-mail : lmarro@ares118.it

ALLEGATO 5 – Utilizzo del proxy

Utilizzo del proxy

L'utilizzo del proxy riguarda le misure procedurali relative all'identificazione e all'autenticazione degli utenti, le regole di utilizzo delle risorse hardware e software, le norme comportamentali e le responsabilità di ciascuno. Rientrano in questo aspetto le norme di comportamento interno per limitare l'uso privato di e-mail o Internet, in quanto i controlli sono possibili solo a determinate condizioni e con l'accordo delle rappresentanze sindacali unitarie. Si ricorda che il D.L.vo 196/03 (Codice in materia di protezione dei dati personali) ribadisce quanto dettato dall'art. 4 dello Statuto dei Lavoratori, ovvero il "... *divieto di utilizzo da parte del datore di lavoro di apparecchiature atte al controllo a distanza dell'attività del lavoratore, salvo che esigenze organizzative, produttive o di sicurezza non abbiano determinato, previo accordo con le rappresentanze sindacali, la lecita introduzione in azienda*". D'altro canto la consultazione di siti web da parte del lavoratore o l'utilizzo di posta elettronica durante il normale orario di lavoro non è consentita quando tale attività non sia pertinente con le mansioni affidate, come l'art. 1024 del codice civile prevede nel principio generale di diligenza del lavoratore. Per trovare un punto di equilibrio dei diritti del lavoratore Ë opportuno introdurre una policy trasparente e codificata con l'apporto dei lavoratori, dando anche la possibilità al datore di lavoro di prevedere meccanismi sanzionatori, sempre che la policy sia resa accessibile a tutti i lavoratori, come previsto dall'art. 7 dello Statuto dei Lavoratori. Sempre tra le politiche di sicurezza si può fare riferimento alle responsabilità civili e penali per i danni cagionati con il trattamento dei dati personali. A titolo di esempio si possono elencare:

- la responsabilità civile disciplinata dall'art. 2050 del Codice Civile e art. 15 D.Lgs. 196/03 "chi cagiona danno ad altri per effetto del trattamento dei dati personali Ë tenuto a risarcire il danno, a meno che non provi di aver adottato tutte le misure idonee per evitarlo";
- la sanzione penale che colpisce chi, essendovi tenuto, omette di adottare le misure di sicurezza (art. 169 del D.Lgs. 196/03), pari all'arresto fino a due anni o ad ammenda da 10mila a 50mila euro, ma con estinzione del reato in caso di regolarizzazione entro 6 mesi dall'accertamento del reato e pagamento di somma determinata dal Garante.

Le informazioni e le attività eseguite sulla rete informatica e telematica relative agli utilizzatori, sono registrate e conservate su file (registro elettronico delle attività o file di log).

Tali file possono essere soggetti ad indagini, nel rispetto di quanto sancito dal D.L.vo 30 giugno 2003, n. 196. Inoltre, il responsabile per la sicurezza può accedere ai file degli utilizzatori per proteggere l'integrità dei sistemi informatici.

Per il regolamento d'uso della rete (policy) vedere l'Allegato 4.

U.O.S. Sistema Informatico
Via Portuense, 240
00149 – Roma
Tel 06 45482304 - Fax 06 5593560
E-mail : lmarro@ares118.it

ALLEGATO 6 – Videosorveglianza

Videosorveglianza

Nell'esercitare attività di videosorveglianza, viene rispettato il principio di proporzionalità tra i mezzi impiegati ed i fini perseguiti, in particolare si precisa che:

- il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi;
- l'attività è svolta per la prevenzione di un pericolo concreto o di specifici reati, solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte.

Inoltre l'attività di videosorveglianza Ë esercitata osservando le seguenti indicazioni:

- sono fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
- Ë scrupolosamente rispettato il divieto di controllo a distanza dei lavoratori;
- sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;
- il periodo di conservazione dei dati Ë limitato allo stretto necessario e non eccede mai i 5 giorni;

la conservazione dei dati oltre il termine previsto alla lettera d), è possibile solo in relazioni al verificarsi di illeciti o quando siano in corso indagini giudiziarie;
i dati raccolti per fini determinati non sono utilizzati per finalità diverse o ulteriori, fatte salve le esigenze di polizia o di giustizia e non sono diffusi o comunicati a terzi.