Regione Basilicata

AZIENDA SANITARIA LOCALE DI POTENZA

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Edizione 2011

Redatto ai sensi del punto 19 del Disciplinare Tecnico allegato B al D Lgs. N. 196/2003

Marzo 2011

0 – SCOPO

Il presente Documento Programmatico Sulla Sicurezza è adottato, ai sensi del punto 19 del Disciplinare Tecnico (allegato B al D. Lgs. n. 196/2003) per inquadrare lo stato dell'arte della sicurezza informatica dell'Ente in materia di trattamento di dati personali, definire le politiche di sicurezza ed i criteri organizzativi per la loro attuazione.
In particolare nel Documento Programmatico Sulla Sicurezza vengono definiti i criteri tecnici e organizzativi per:

1. **Identificazione delle risorse da proteggere** (Elenco dei trattamenti dei dati personali presenti in azienda)
2. **La distribuzione dei compiti e delle responsabilità** nell'ambito delle strutture preposte al trattamento dei dati
3. **L'analisi dei rischi** che incombono sui dati
4. **Le misure esistenti e 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
5. **La descrizione dei criteri e delle modalità per il ripristino delle disponibilità dei** dati in seguito a distruzione o danneggiamento.
6. **La previsione dei interventi formativi degli incarichi del trattamento**, per renderli edotti dei rischi che incombono sui dati, e delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime addotte da titolare. La formazione programmate già dal momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali
7. **La descrizione dei criteri** da adottare per garantire l'adozione delle misure minime di sicurezza **in caso di trattamenti all'esterno** della struttura del titolare
8. Individuazione dei criteri da adottare per la **cifratura o per la separazione dei dati sanitari e di vita sessuale** dagli altri dati personali degli interessati**.**

0.1 CAMPO DI APPLICAZIONE

Il Documento Programmatico Sulla Sicurezza, che va predisposto in presenza di dati sensibili o giudiziari trattati con l'ausilio di strumenti elettronici, viene però esteso alla totalità degli strumenti elettronici, a prescindere dalla tipologia di dati contenuti su ciascuno; naturalmente parte delle misure da adottare si differenzieranno a seconda della tipologia dei dati contenuti.

0.2 RIFERIMENTI NORMATIVI

D. Lgs n. 196/2003
Disciplinare Tecnico (allegato B)
Direttive Comunitarie 95/46/Ce e 2202/58/Ce
Provvedimenti emanati dal Garante per la Protezione dei Dati Personali

0.3 INQUADRAMENTO DEL CONTESTO OPERATIVO

L'ASP (Azienda Sanitaria di Potenza) - Titolare dei trattamenti – nata dall'accorpamento di 3 distinte Aziende Sanitarie, ha ormai avviato il processo di unificazione aziendale, che vede una strutturazione funzionale assai diversa da quella delle aziende preesistenti.

Il processo di unificazione – che resta il principale obiettivo 'a tendere' – è da tempo in corso di realizzazione tramite una rete che ricopra l'intero territorio Aziendale, sia pur ricorrendo a risorse variabili a seconda della infrastrutturazione locale dei vari territori costituenti l'Azienda: nei paragrafi a seguire vengono riportati sinteticamente lo stato dell'arte del percorso di evoluzione della rete informatica.

1 . ELENCO DEI TRATTAMENTI DI DATI PERSONALI (REGOLA 19.1)

La ASP – in quanto Azienda Sanitaria Locale – tratta i dati personali tipici di questo genere di Titolare di Trattamenti; l'elenco è il seguente:

TRATTAMENTO	SERVIZIO/UNITÀ OPERATIVA
Gestione ed amministrazione delle attività relative alla Segreteria Generale. Protocollo generale posta in entrata ed in uscita;Collegio Sindacale; gestione deliberazioni; determinazioni ed ordinanze.	**Segreteria Direzionale**
Gestione ed archivio del Contenzioso, provvedimenti disciplinari. Ricevimento atti giudiziari; registrazione; partecipazione alle Commissioni di conciliazione; archiviazione delle cause; predisposizione e tenuta archivio cause; consulenza di supporto all'attività della Direzione Generale, Amministrativa e Sanitaria; gestione Ufficio disciplinare.	**Ufficio legale e contenzioso**
Gestione dell'acquisto di beni e pagamento ditte e professionisti; gestione del patrimonio mobiliare ed immobiliare; gestione dei fornitori; servizi di controllo interno; progettazione; affidamento o esecuzione di opere pubbliche; gare per forniture; autorizzazioni; concessioni; permessi; licenze; nulla osta.	**Attività Tecniche**

Gestione del personale dipendente. *T*rattamento giuridico ed economico del personale; presenze; gestione, reclutamento, selezione, valutazione, monitoraggio degli aspiranti all'assunzione; concorsi interni; adempimento obblighi fiscali e contabili; adempimento obblighi connessi al versamento delle quote di iscrizione a sindacati; attività informativa di supporto alla gestione del contenzioso (commissioni di conciliazione); tenuta e aggiornamento registri del personale; liquidazione pensioni e liquidazioni ai sensi della L. 336/70; cessioni del quinto dello stipendio ai creditori.	**Amministrazione del Personale**
Appalti, forniture, gare, gestione inventario, manutenzione apparecchi sanitari, locazioni, gestione fatture. Gestione dei fornitori; gestione locazioni; gestione manutenzione apparecchiature sanitarie e tecniche; gestione fatture; gestione e progettazione bandi di gare di appalto, per forniture tecniche e sanitarie.	**Economato Provveditorato**
Gestione della contabilità e documentazione fiscale. Pagamenti; tenuta registri fiscali e contabili; rapporti con il tesoriere; pagamento dei bonifici relativi alla L 336/70; pignoramento del quinto dello stipendio; commissione concorsi; fornitori.	**Economico Finanziaria**
Attività connesse al Controllo di Gestione.	**Centro di Controllo Direzionale/Controllo di Gestione**
Gestione dell'attività di formazione.	**Innovazione Ricerca e Formazione**
Attività di accoglienza, informazione ed analisi dei Bisogni; relazioni con il pubblico; informazioni, pubblica tutela; qualità percepita.	**Comunicazione e relazioni esterne**
Dichiarazioni di volontà alla donazione di organi e tessuti; prelievo di organi. Ricerche epidemiologiche; diagnosi, cura e terapia; interventi in caso di calamità, epidemie, malattie infettive; ricerche biomediche; informazione scientifica; gestione flussi informativi.	**Osservatorio Epidemiologico e pianificazione strategica**

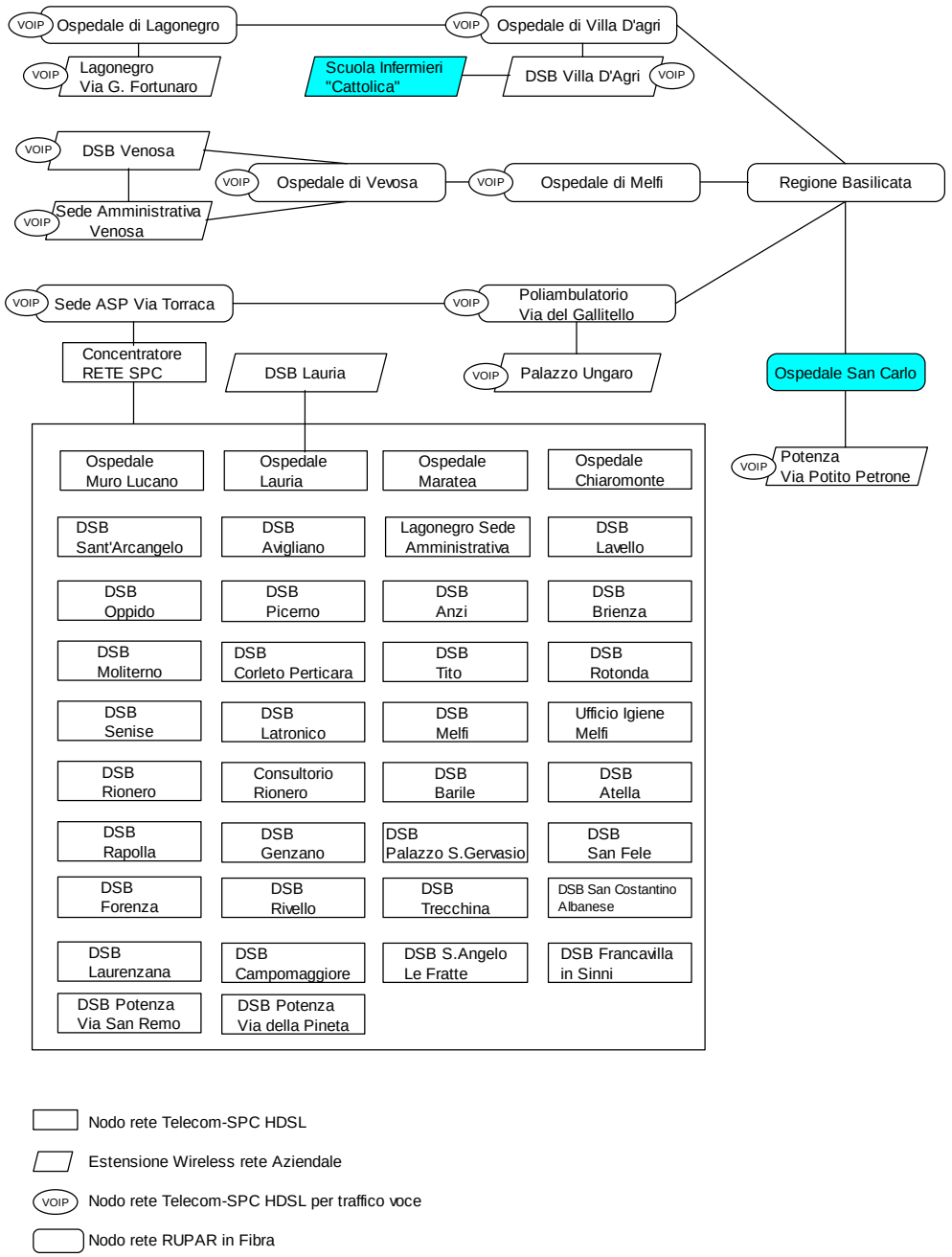
Prevenzione infortuni nell'ambiente di lavoro dell' AS di Potenza; controlli ed ispezioni su igiene e sicurezza del lavoro, verifiche sugli ambienti di lavoro; gestione normativa TU n 81/2008.	**Sicurezza, prevenzione, protezione e conformità strutturale**
Esame richieste, autorizzazioni accreditamento e gestione dell'attività relative	**Autorizzazione, accreditamento e gestione strutture accreditate**
Gestione computers e software; gestione banche dati dati ; sistemi e flussi informativi	**Sistema informativo automatizzato e tecnologia dell'informazione**
Gestione dati relativi a farmacisti ed acquisizione dati delle ricette; farmacovigilanza; autorizzazioni; concessioni; permessi; certificazioni; licenze; nulla-osta e distribuzione farmaci; assistenza integrativa; assistenza diretta agli utenti; monitoraggio della spesa sanitaria; lettura ottica delle ricette.	**Assistenza farmaceutica ospedaliera e territoriale**
Prestazioni ambulatoriali, diagnosi, cura e terapia dei tossicodipendenti e degli alcooldipendenti, registrazione e gestione amministrativa degli utenti, monitoraggio dei gruppi a rischio, sistemi di prevenzione delle malattie correlate alla tossicodipendenza; analisi statistiche e psicosomatiche, ricerche epidemiologiche, programmazione dei servizi, anche alternativi alla detenzione, inserimento lavorativo ed assistenza; vigilanza sugli enti ausiliari(Comunità Terapeutiche).	**Assistenza alle dipendenze patologiche/Ser.T.**
Diagnosi, cura e terapia degli utenti; prestazioni relative alla L 104/92; adozioni; presa in carico delle famiglie con problematiche socio-psicologiche; registrazione e gestione amministrativa degli assistiti; monitoraggio dei gruppi a rischio; analisi statistiche e psicosomatiche; ricerche epidemiologiche; programmazione dei servizi ed assistenza in materia di educazione sanitaria; di prestazioni sanitarie anche ambulatoriali (ginecologiche, infermieristiche, ostetriche, psicologiche, di assistenza sociale); ricerche sociologiche ed indagini di opinione. Raccolta, organizzazione, elaborazione, selezione, raffronto, interconnessione in forma anonima, comunicazione (nei limiti di legge), registrazione, conservazione, modificazione, estrazione, utilizzo dei dati relativi alla programmazione delle attività. Registrazione e gestione, anche amministrativa, dei dati relativi alle donne che abbiano subito violenza.	**Area Materno Infantile/ Consultori/Coordinamento Attività Consultoriali G.O.I.A.M.**
Gestione indagini strumentali, per diagnostica radiografica, per immagini fotografiche e per filmati. Registrazioni pazienti e gestione amministrativa.	**Dipartimento Diagnostica per Immagini/Radiologia**

Registrazione utenti e gestione amministrativa; diagnosi cura e terapia; monitoraggio dei gruppi a rischio; ricerche epidemiologiche ed analisi statistiche.	**Pneumologia Territoriale**
Trattamento dei dati relativi alle persone affette da disabilità mentali. Diagnosi, cura, terapia e riabilitazione degli utenti; attività ambulatoriali, domiciliari e delle strutture residenziali e semiresidenziali; attività di programmazione e di filtro ai ricoveri nelle case di cura neuropsichiatriche(accreditate e convenzionate) ed alle comunità terapeutiche psichiatriche; registro degli utenti e gestione amministrativa; monitoraggio dei gruppi a rischio; assistenza sanitaria.	**Dipartimento di Salute Mentale**
118- servizio di Emergenza-Urgenza.	**Dipartimento Interaziendale**
Gestione e Archivio delle Attività Ospedaliere. Gestione: delle ammissioni, dimissioni e trasferimenti degli utenti, del triage; della banca dati delle degenze; dell'attività di ricovero e/o di servizi, anche in regime di day hospital, day surgery ed altro; dell'attività di emergenza-urgenza e di denuncia di malattie infettive; della registrazione degli utenti, in entrata ed in uscita, e dei dati; dell' attività amministrativa; dei servizi di prenotazione; della redazione e gestione delle cartelle cliniche ed infermieristiche; degli interventi in caso di calamità; dell'accesso degli interessati; del monitoraggio dei gruppi a rischio; delle ricerche epidemiologiche, dell'analisi e della reportistica delle s.d.o.; della diagnosi, cura e terapia degli utenti. Archivio: registro ed archivio amministrativo degli utenti; registro dei donatori; registro degli esami citologici; registro della sala operatoria; registro delle prestazioni effettuate, con valutazione dei trattamenti eseguiti e/o da eseguire, della diagnosi, della programmazione dell'attività e dei servizi di controllo.	**Unità Operative di Ricovero/ Sevizi/ Aree/ Centri/ dei Presidi Ospedalieri**
Registro esami istologici; banche dati degenze; archivio cartelle cliniche; archivio sdo.	**Direzione Sanitaria dei PP OO**
Attività amministrative correlate alla gestione tecnico-amministrativa del PO	**Direzione Amministrativa dei PP OO**
Gestione Attività dei Distretti di II livello: riabilitazione; assistenza integrativa ed analisi per incontinenza; controllo e verifiche sui flussi informativi; convenzionamento per la medicina generale e la continuità assistenziale; ADI; assistenza protesica e riabilitativa; convenzionamento e scelta medico-pediatrica; gestione scelta medica; esenzioni dal pagamento ticket; assistenza emigrati; gestione dell'attività specialistica convenzionata interna; comitato zonale; centro di riferimento regionale per i ricoveri all'estero, gestione continuità assistenziale, pediatria,	**Distretti Sanitari/USIB/Aree dellAssistenza sanitaria di base**

medicina generale, specialistica ambulatoriale (ex Sumaisti); prestazioni FKT; AIAS; verifiche sulle autocertificazioni; gestione ambulatori, coordinamento e direzione Distretti di I livello; verifiche veridicità autocertificazioni; accesso all'anagrafe tributaria.	
Coordinamento delle attività del settore operativo "Handicap".	**Distretti Sanitari/Aree dell'assistenza sanitaria di base: Nucleo Handicap**
Gestione, registrazione dichiarazioni e certificazioni di tipo sanitario; prestazione di servizi sanitari; gestione dati relativi alle visite specialistiche; gestione attività dei laboratori di analisi; autorizzazioni e prenotazioni; diagnosi, cura e terapia; monitoraggio gruppi a rischio; ricerche epidemiologiche; analisi statistiche e psicometriche; interventi in caso di calamità, epidemie o malattie infettive; scelta e revoca medica, pagamento tickets; tenuta registro anagrafe sanitaria; esenzioni; assistenza emigrati; assistenza sanitaria all'estero.	**Distretti Sanitari/ Aree dell'assistenza sanitaria di base: Attività Poliambulatoriali**
Gestione e registrazione utenti, per i quali il medico curante richieda l'attivazione del servizio di Assistenza Domiciliare Integrata.	**Distretti Sanitari/ Aree dell'assistenza sanitaria di base: ADI**
Ispezioni, controlli e vigilanza sui prodotti alimentari di origine animale e rilascio della relativa certificazione; pareri sanitari per autorizzazioni allo svolgimento di attività di preparazione di alimenti; pareri per il rilascio di autorizzazioni sanitarie (requisiti strutturali e funzionali); verifiche preliminari e rilascio di conseguenti pareri; controllo ufficiale sui prodotti alimentari, ivi compresi i dietetici e quelli per la prima infanzia; controllo dei casi presunti o accertati di infezioni, intossicazioni, tossinfezioni di origine alimentare e relative indagini epidemiologiche; vigilanza e controllo acque minerali.	**Dipartimento Prevenzione collettiva e della salute umana: Igiene degli Alimenti/SIAN**
Indagini epidemiologiche; rilascio di autorizzazioni, permessi, pareri; attività di prevenzione in materia di igiene e sanità pubblica; igiene e sicurezza del lavoro; diagnosi, cura e terapia di malattie infettive e diffusive; monitoraggio gruppi a rischio; visite mediche fiscali; attività di polizia mortuaria e vigilanza cimiteriale; autorizzazioni, concessioni, licenze e nulla osta in materia di patenti, emissioni in atmosfera, bonifica amianto, vaccinazioni obbligatorie e facoltative; accertamenti preventivi di idoneità per liste di collocamento; porto d'armi; patenti; cause di servizio; personale della scuola; accertamenti di igienicità, agibilità ed abitabilità di edifici o parti di essi; accertamento invalidità civile;	**Dipartimento Prevenzione collettiva e della salute umana: Igiene Epidemiologica e Sanità Pubblica**
Consulenza, controlli ed ispezioni su igiene e sicurezza del lavoro, verifiche di impianti ed apparecchiature; vidimazione registri infortuni; pareri preventivi; verifica dell'applicazione della normativa vigente di settore; rilascio libretti di tirocinio, per esami di abilitazione alla conduzione di generatori di vapore; raccolta	**Dipartimento Prevenzione collettiva e della salute umana: Prevenzione e Protezione Impiantistica nei Luoghi di Lavoro/ SSPPLL**

certificazioni di collaudo e verifiche di attrezzature ed impianti.	
Attività di prevenzione delle malattie professionali e sicurezza nei luoghi di lavoro; diagnosi e cura di soggetti affetti da patologie legate all'attività ed all'ambiente di lavoro; giudizi di idoneità alle mansioni, su richiesta del lavoratore ricorrente, avverso il giudizio espresso dal medico competente; verifica dello stato di salute finalizzata al rilascio della dichiarazione di idoneità al lavoro; indagini epidemiologiche in ambito lavorativo.	**Dipartimento Prevenzione: Medicina del Lavoro**
Anagrafe del bestiame; interventi in caso di calamità, epidemie o malattie infettive; ricerche epidemiologiche.	**Dipartimento Prevenzione della sanità e benessere animale: Veterinaria Area "A" Sanità Animale**
Trattamento dei dati relativi alle aziende allevatrici ed alle patologie riscontrate sugli animali. Sanità, controlli e verifiche sullo stato di salute degli animali all'atto della macellazione, trasformazione e commercializzazione.	**Dipartimento Prevenzione della sanità e benessere animale Area "B" Igiene degli Alimenti di Origine Animale**
Anagrafe canina; attività di controllo dei farmaci; igiene degli alimenti e delle produzioni zootecniche; igiene del trasporto degli alimenti di origine animale.	**Dipartimento Prevenzione della sanità e benessere animale Area "C" Igiene delle Produzioni Zootecniche**
Gestione Centro Disturbi Alimentari	**DCA Chiaromonte**
Gestione Attività Riabilitazione Alcologica	**CRA Chiaromonte**
Gestione RSA/Hospice	**RSA/Hospice**
Gestione Centro Riabilitazione Traumi dello Sport	**Centro riabilitazione Traumi dello sport - Maratea**

1 . 1 EVOLUZIONE DELLA RETE DATI AZIENDALE, DELLA SICUREZZA PERIMETRALE E DELLE POSTAZIONI DI LAVORO.



La rete dati della ASP ha seguito, nella prima fase, una genesi analoga a quella della azienda che serve. Infatti, come quest'ultima, è nata come l'unione delle tre reti wan preesistenti che gestivano le ASL N.1 di Venosa, N.2 di Potenza e N.3 di Lagonegro confluite nella ASP senza alcun processo di razionalizzazione e omogeneizzazione.
Successivamente le UU.OO. S.I.A. degli attuali ambiti territoriali di Venosa, Potenza e Lagonegro, di concerto con il CTR e la Telecom, hanno rivisto l'insieme dei fabbisogni

aziendali, analizzando l'esistente, verificando quanto offerto dalla convenzione SPC-CNIPA, disegnando la nuova rete WAN esposta sinteticamente nello schema precedente.
La configurazione prevede di sfruttare come dorsale la rete RUPAR presente negli ospedali con collegamenti in fibra ottica a 2 Gbit ed i due nodi della MAN di Potenza di via Torraca e via del Gallitello con collegameti in fibra ottica ad 1 Gbit.
A questi si collegheranno varie estensioni realizzate o con sistemi Wireless o, per la maggior parte, con collegamenti XDLS.
Come risulta evidente dallo schema esposto il dimensionamento ed il posizionamento dei flussi ha tenuto conto anche della volontà aziendale di realizzare un sistema telefonico VOIP per la comunicazione tra le varie strutture.
Elemento fondamentale nella costituzione della rete e della sua successiva messa in sicurezza è stata la decisione di costituire un unico CED aziendale nei locali di via torraca a Potenza. In origine le tre aziende avevano ciascuno un proprio CED, l'accorpamento delle basi dati unito al notevole aumento di utenti collegati per singola procedura oltre che alla necessità di gestire in sicurezza un numero di accessi alla rete triplicato rispetto al precedente, ha consigliato di dismettere i vecchi CED e di concentrare tutti i server in un locale idoneo e meglio presidiato.
Per ciò che attiene alla gestione della rete, sarà creato un unico dominio, con server dedicati all'autenticazione, alla distribuzione delle patch ed all'aggiornamento dell'antivirus; sarà rivisto il piano degli indirizzamenti aziendali, modificate le tabelle di routing e installati firewall configurati con opportune policy di accesso. L'intera rete aziendale, pur sfruttando come dorsale la RUPAR ed inglobando 6 suoi nodi, sarà completamente isolata e sarà consentito l'accesso dall'esterno solo a chi sarà autorizzato.
Per ciò che attiene le postazioni client, saranno riconfigurate per l'accesso al dominio, verrà installato su di esse il nuovo antivirus di fornitura regionale ed il software "AxCrypt" per la cifratura e la protezione dei dati sensibili presenti sul singolo pc.
Per ciò che attiene il controllo degli accesso ai dati del client, per i pc con sistema operativo Windows NT, 2000, XP o successivo verrà utilizzato quanto già messo a disposizione dal software di base registrando gli utenti, proteggendoli con password adeguate e screen sever con password; per i sistemi operativi Windows millennium o precedenti verrà installato in software "Access Denied".
Per queste ultime considerazioni si ritiene inopportuno produrre in questa fase l'elenco dei client e delle relative configurazioni.

Tutto quanto suddetto sarà presumibilmente terminato nel corso dell'anno.

1.1.1 INDIVIDUAZIONE ARCHIVI E BANCHE DATI OGGETTO DI TRATTAMENTO

Vecchia contabilità Ambito territoriale Venosa – HP netserver e60

Fornitrore Procedura	Intema Enco
Nome Procedura	Enco
Nome server	
Gruppo di Lavoro	
Ram	128
CPU	Pentium III 350
UPS	Si
Sistema Operativo	SCO Open Server
DBMS	Informix
Antivirus	No
Controllo Remoto	telnet
IP Address	172.16.41.27
Backup	Sì (Nastro)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	No
Valutazione Rischio	Basso

Vecchie Paghe Ambito territoriale Venosa – Siemens Nixdorf RM 300

Fornitrore Procedura	Publisys
Nome Procedura	Urbe Lire – Specialisti Ambulatoriali Lire
Nome server	
Gruppo di Lavoro	
Ram	128
CPU	RISC
UPS	Sì
Sistema Operativo	Sinix
DBMS	C-Isam
Antivirus	No
Controllo Remoto	telnet
IP Address	172.16.41.200
Backup	Sì (Nastro)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	No
Valutazione Rischio	Basso

Personale Gestione liquidatoria Ambito territoriale Venosa – HP Netserver LC 2000 U3

Fornitrore Procedura	Publisys – Traccia
Nome Procedura	Urbe Lire – Specialisti Ambulatoriali Lire Urbe Euro – Specialisti Ambulatoriali Euro Rilevazione delle Presenze
Nome server	Server – URBE
Gruppo di Lavoro	Paghe
Ram	1 GB
CPU	2 xeon 700 MHz
UPS	Sì
Sistema Operativo	Windows 2000 server SP3
DBMS	Oracle 8.5
Antivirus	Sì
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.41.201
Backup	Sì (Nastro)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Personale Gestione liquidatoria Ambito territoriale Venosa – HP Netserver LC 2000 U3

Fornitrore Procedura	Publisys - Traccia
Nome Procedura	Urbe Lire – Specialisti Ambulatoriali Lire Urbe Euro – Specialisti Ambulatoriali Euro Rilevazione delle Presenze
Nome server	Server – URBE
Gruppo di Lavoro	Paghe
Ram	1 GB
CPU	2 xeon 700 MHz
UPS	Sì
Sistema Operativo	Windows 2000 server SP3
DBMS	Oracle 8.5
Antivirus	Sì
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.41.201
Backup	Sì (Nastro)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Personale DB

Fornitrore Procedura	Publisys - Traccia
Nome Procedura	Urbe Euro Rilevazione delle Presenze
Nome server	Svr – database – Intel SR2500 ALLX
Gruppo di Lavoro	workgroup
Ram	2 GB
CPU	xeon E5420 2,5 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP1
DBMS	Oracle 10
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.16.41.10
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Paghe Application

Fornitrore Procedura	Publisys
Nome Procedura	Urbe Euro
Nome server	Svr – APP Intel SR2500 ALLX
Gruppo di Lavoro	workgroup
Ram	4 GB
CPU	2 xeon E5420 2,5 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP1
DBMS	Oracle 10
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.16.41.11
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Rilevazione delle presenze application – Supermicro

Fornitrore Procedura	Traccia
Nome Procedura	Rilevazione delle Presenze
Nome server	Rilpres-web
Gruppo di Lavoro	workgroup
Ram	4 GB
CPU	2 xeon 3 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP2
DBMS	Oracle 10
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.16.41.8
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Vecchia Anagrafe sanitaria Ambito Territoriale Venosa – IBM Netfinity 7100

Fornitrore Procedura	Intema
Nome Procedura	Anagrafe Sanitaria
Nome server	s-anagrafe
Gruppo di Lavoro	workgroup
Ram	4 GB
CPU	2 xeon 700 MHz
UPS	Sì
Sistema Operativo	Windows 2000 SE SP4
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.41.2
Backup	Sì (Nastro)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

“Gestione Centro Trasfusionale” – Server Terra	
Fornitore Procedura	Menarini
Nome Procedura	CETRAPLUS WEB
Nome server	ASL1
Gruppo di Lavoro	WORKGROUP
Ram	3 GB
CPU	2 xeon 700 MHz
UPS	No
Sistema Operativo	Windows 2003 Server Servoce Pack 2
DBMS	Oracle
Antivirus	Si
Controllo Remoto	VNC, terminal server
IP Address	172.16.43.70
Backup	Sì (Disco)
Ubicazione	Locale centro trasfusionale Ospedale Melfi
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Controllo di Gestione, Protesica e Invalidi Civili - Ambito Territoriale di Venosa
– HP Proliant ML370

Fornitrore Procedura	Intema
Nome Procedura	Controllo di Gestione - Protesica - Invalidi Civili
Nome server	asl1servercup
Gruppo di Lavoro	Workgroup
Ram	4 GB
CPU	2 xeon 3 GHz
UPS	Sì
Sistema Operativo	Windows 2000 SE SP4
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.41.3
Backup	Sì (Nastro)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Protocollo – Magazzino e Contabilità Gestione liquidatoria - Ambito Territoriale di Venosa IBM Xserver 346

Fornitrore Procedura	Intema
Nome Procedura	Protocollo – Magazzino – Cont€nti
Nome server	nlb1-asl1
Gruppo di Lavoro	Workgroup
Ram	4 GB
CPU	2 xeon 3,2 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP1
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.41.7
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Magazzino e Contabilità (DB 1) - Ambito Territoriale di Venosa - IBM Xserver 346

Fornitrore Procedura	Intema
Nome Procedura	Magazzino – Contabilità
Nome server	dcasl1-sql1.asl1.int
Gruppo di Lavoro	asl1.int
Ram	4 GB
CPU	2 xeon 3,2 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP2
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.1
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore + cluster con dcasl1-sql2.asl1.int
Valutazione Rischio	Basso

Magazzino e Contabilità (DB 2) - Ambito Territoriale di Venosa - IBM Xserver 346

Fornitrore Procedura	Intema
Nome Procedura	Magazzino – Contabilità
Nome server	dcasl1-sql2.asl1.int
Gruppo di Lavoro	asl1.int
Ram	4 GB
CPU	2 xeon 3,2 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP2
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.2
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore + cluster con dcasl1-sql2.asl1.int
Valutazione Rischio	Basso

Magazzino e Contabilità (Application 1) - Ambito Territoriale di Venosa - IBM Xserver 346

Fornitrore Procedura	Intema
Nome Procedura	Magazzino – Cont€nti
Nome server	web1-asl1.asl1.int
Gruppo di Lavoro	asl1.int
Ram	4 GB
CPU	2 xeon 3,2 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP2
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.11
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore + NLB con web2-asl1.asl1.int
Valutazione Rischio	Basso

Magazzino e Contabilità (Application 2) - Ambito Territoriale di Venosa - IBM Xserver 346

Fornitrore Procedura	Intema
Nome Procedura	Magazzino – Contabilità
Nome server	Web2-asl1.asl1.int
Gruppo di Lavoro	asl1.int
Ram	4 GB
CPU	2 xeon 3,2 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP2
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.11
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	Dischi e alimentatore + NLB con web1-asl1.asl1.int
Valutazione Rischio	Basso

Anagrafe Vaccinale - Ambito territoriale di Venosa - IBM Xserver 3550

Fornitrore Procedura	Sincon
Nome Procedura	Giava 4.0
Nome server	
Gruppo di Lavoro	
Ram	
CPU	
UPS	Si
Sistema Operativo	
DBMS	
Antivirus	
Controllo Remoto	
IP Address	172.18.94.30
Backup	
Ubicazione	CED sede amministrativa Venosa
Fault Tollerance	
Valutazione Rischio	

AREA SANITA' – ASP : "Airo e Cup" (Application 1) – Ambito territoriale di Lagonegro - SERVER RACK: IBM XSERIES 346	
Fornitore Procedura	INTEMA SANITA' S.r.l.
Nome Procedura	AIRO – CUP – GSO – ARCA
Nome server	Web1-ASL3
Gruppo di Lavoro	asl3.int
Ram	4,00 GB
CPU	Nr. 2 Intel Xeon – 3,20 GHz
UPS	Sì
Sistema Operativo	Microsoft Windows Server 2003 Standard Edition – SP2
DBMS	Microsoft SQL Server 2500
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.139
Backup	Sì (NAS)
Ubicazione	Locale CED – P.O. Lagonegro – Sede Nodo RUPAR
Fault Tollerance	Dischi e alimentatore + NLB con web2-ASL3.asl3.int
Valutazione Rischio	Basso

AREA SANITA' – ASP : "Airo e Cup" (Application 2) – Ambito territoriale di Lagonegro - SERVER RACK: IBM XSERIES 346	
Fornitore Procedura	INTEMA SANITA' S.r.l.
Nome Procedura	AIRO – CUP – GSO – ARCA
Nome server	Web2-ASL3
Gruppo di Lavoro	asl3.int
Ram	4,00 GB
CPU	Nr. 2 Intel Xeon - 3,20 GHz
UPS	Sì
Sistema Operativo	Microsoft Windows Server 2003 Standard Edition – SP2
DBMS	Microsoft SQL Server 2500
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.140 / 141
Backup	Sì (NAS)
Ubicazione	Locale CED – P.O. Lagonegro – Sede Nodo RUPAR
Fault Tollerance	Dischi e alimentatore + NLB con web1-ASL3.asl3.int
Valutazione Rischio	Basso

AREA SANITA' – ASP : "Airo e Cup" (DB1) – Ambito territoriale di Lagonegro - SERVER RACK: IBM XSERIES 346	
Fornitore Procedura	INTEMA SANITA' S.r.l.
Nome Procedura	AIRO – CUP – GSO – ARCA
Nome server	DCASL3-SQL1
Gruppo di Lavoro	asl3.int
Ram	4,00 GB
CPU	Nr. 2 Intel Xeon - 3,20 GHz
UPS	Sì
Sistema Operativo	Microsoft Windows Server 2003 Standard Edition – SP2
DBMS	Microsoft SQL Server 2500
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.129
Backup	Sì (NAS)
Ubicazione	Locale CED – P.O. Lagonegro – Sede Nodo RUPAR
Fault Tollerance	Dischi e alimentatore + Cluster con DCASL3-SQL2.asl3.int
Valutazione Rischio	Basso

AREA SANITA' – ASP : Airo e Cup (DB 2) – Ambito territoriale di Lagonegro - SERVER RACK: IBM XSERIES 346	
Fornitore Procedura	INTEMA SANITA' S.r.l.
Nome Procedura	AIRO – CUP – GSO – ARCA
Nome server	DCASL3-SQL2
Gruppo di Lavoro	asl3.int
Ram	4,00 GB
CPU	Nr. 2 Intel Xeon - 3,20 GHz
UPS	Sì
Sistema Operativo	Microsoft Windows Server 2003 Standard Edition – SP2
DBMS	Microsoft SQL Server 2500
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.132
Backup	Sì (NAS)
Ubicazione	Locale CED – P.O. Lagonegro – Sede Nodo RUPAR
Fault Tollerance	Dischi e alimentatore + Cluster con DCASL3-SQL1.asl3.int
Valutazione Rischio	Basso

AREA SANITA' - "Anagrafe Vaccinale" – Ambito territoriale di Lagonegro - SERVER RACK: IBM XSERIES 3550	
Fornitore Procedura	Sincon
Nome Procedura	GIAVAWEB - Gestione Anagrafi Vaccinali
Nome server	
Gruppo di Lavoro	
Ram	2,00 GB
CPU	Intel Xeon - 3,20 GHz
UPS	Sì
Sistema Operativo	Microsoft Windows Server 2003 Standard Edition – SP2
DBMS	Microsoft SQL Server 2005
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.160
Backup	Sì (NAS)
Ubicazione	Locale CED – P.O. Lagonegro – Sede Nodo RUPAR
Fault Tollerance	Dischi e alimentatore + NLB con web1-ASL3.asl3.int
Valutazione Rischio	Basso

AREA SANITA' – ASP : "Anagrafe Sanitaria" – Ambito territoriale di Lagonegro - SERVER RACK: Fujitsu Siemens PRIMERGY RX300 S3	
Fornitore Procedura	INTEMA SANITA' S.r.l.
Nome Procedura	ANAG_SANI
Nome server	INT2K3R2X64
Gruppo di Lavoro	MYUSERGROUP
Ram	8,00 GB
CPU	Nr. 2 Intel Xeon 5120 @ 1,86 GHz
UPS	Sì
Sistema Operativo	Microsoft Windows Server 2003 Enterprise X64 Edition – SP2
DBMS	Microsoft SQL Server 2000
Antivirus	Eset Nod32 – Vers. 3.0
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.132.3
Backup	Sì (NAS)
Ubicazione	Locale CED – P.O. Lagonegro – Sede Nodo RUPAR
Fault Tollerance	
Valutazione Rischio	Basso

GESTIONE LIQUIDATORIA "Contabilità" (FE) – Ambito territoriale di Lagonegro - SERVER DESK: IBM XSERIES 346 MSI 9151	
Fornitore Procedura	INTEMA SANITA' S.r.l.
Nome Procedura	CONTENTI
Nome server	ASL3-NLB1
Gruppo di Lavoro	ASL3
Ram	4,00 GB
CPU	Nr. 2 Intel Xeon 3,20 GHz
UPS	Sì
Sistema Operativo	Microsoft Windows Server 2003 Standard Edition – SP2
DBMS	Microsoft SQL Server 2000
Antivirus	Eset Nod32 – Vers. 3.0
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.132.201
Backup	Sì (NAS)
Ubicazione	Locale CED – P.O. Lagonegro – Sede Nodo RUPAR
Fault Tollerance	
Valutazione Rischio	Basso

GESTIONE LIQUIDATORIA – "Contabilità" (DB) – Ambito territoriale di Lagonegro - SERVER DESK: IBM XSERIES 346 MSI 9151	
Fornitore Procedura	INTEMA SANITA' S.r.l.
Nome Procedura	CONTENTI
Nome server	ASL3-DB
Gruppo di Lavoro	ASL3
Ram	4,00 GB
CPU	Nr. 2 Intel Xeon 3,20 GHz
UPS	Sì
Sistema Operativo	Microsoft Windows Server 2003 Standard Edition – SP2
DBMS	Microsoft SQL Server 2000
Antivirus	Eset Nod32 – Vers. 3.0
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.132.200
Backup	Sì (NAS)
Ubicazione	Locale CED – P.O. Lagonegro – Sede Nodo RUPAR
Fault Tollerance	
Valutazione Rischio	Basso

AREA AMMINISTRATIVA Rilevazione Presenze – Ambito territoriale di Lagonegro - SERVER DESK: HP Proliant ML350	
Fornitore Procedura	COOP. LA TRACCIA
Nome Procedura	RilPres - Rilevazione delle Presenze
Nome server	RILPRES – “HEWLETT PACKARD”
Gruppo di Lavoro	
Ram	2,00 GB
CPU	Intel Xeon E5410 2,33 GHz
UPS	Sì
Sistema Operativo	Microsoft Windows Server 2003 Standard Edition – SP2
DBMS	Oracle 10
Antivirus	Eset Nod32 – Vers. 3.0
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.131.40
Backup	Sì
Ubicazione	CED – UO SIA – Sede amministrativa di Lagonegro
Fault Tollerance	
Valutazione Rischio	Basso

GESTIONE LIQUIDATORIA “Personale” – Ambito territoriale di Lagonegro - SERVER DESK: IBM XSERIES 266 MSI 9151	
Fornitore Procedura	PUBLISYS
Nome Procedura	GIURIDICO / PAGHE
Nome server	SERVER_PAGHE01
Gruppo di Lavoro	Workgroup
Ram	1,00 GB
CPU	Intel Xeon 3,00 GHz
UPS	
Sistema Operativo	Microsoft Windows Server 2000 – SP4
DBMS	Oracle 8.0
Antivirus	Eset Nod32 – Vers. 3.0
Controllo Remoto	VNC e Terminal Server
IP Address	172.16.131.42
Backup	Sì (Cassette)
Ubicazione	CED – UO SIA – Sede amministrativa di Lagonegro
Fault Tollerance	
Valutazione Rischio	Basso

AREA AMMINISTRATIVA “Protocollo – Gestione Delibere” – Ambito territoriale di Lagonegro - SERVER DESK: MAXDATA	
Fornitore Procedura	INTEMA SANITA’ S.r.l.
Nome Procedura	GUPAR
Nome server	TEST
Gruppo di Lavoro	PROTOCOLLO
Ram	2,00 GB
CPU	Intel Xeon 2,40 GHz
UPS	No
Sistema Operativo	Microsoft Windows Server 2003 Standard Edition – SP2
DBMS	Microsoft SQL Server 2000
Antivirus	Eset Nod32 – Vers. 3.0
Controllo Remoto	VNC
IP Address	172.16.131.80
Backup	Sì (Disco Esterno)
Ubicazione	CED – UO SIA – Sede amministrativa di Lagonegro
Fault Tollerance	No
Valutazione Rischio	Basso

AREA AMMINISTRATIVA “Gestione Centro Trasfusionale” - Ambito territoriale di Lagonegro - PC DESK: HP COMPAQ DC 7700	
Fornitore Procedura	
Nome Procedura	CETRAPLUS WEB
Nome server	CENTRAPLUS
Gruppo di Lavoro	WORKGROUP
Ram	488,00 MB
CPU	Intel(R) Pentium(R) 4 – 3,20GHz
UPS	No
Sistema Operativo	Microsoft Windows XP Professional – SP3
DBMS	Oracle
Antivirus	Eset Nod32 – Vers. 3.0
Controllo Remoto	VNC
IP Address	172.16.132.239
Backup	Sì (Disco)
Ubicazione	Locale CED – P.O. Lagonegro – Sede Nodo RUPAR
Fault Tollerance	No
Valutazione Rischio	Basso

AREA SANITARIA “Gestione Presa in Carico del Paziente” – Ambito territoriale di Lagonegro - PC DESK: PC ASSEMBLATO	
Fornitore Procedura	IT CONSULT
Nome Procedura	SICOD I-CARE
Nome server	I CARE (Web Application)
Gruppo di Lavoro	
Ram	2,00 GB
CPU	Intel Pentium Dual Core E2180 – 2,00 GHz
UPS	No
Sistema Operativo	Linux – (Ubuntu)
DBMS	MY – SQL
Antivirus	ClamWin
Controllo Remoto	Putty
IP Address	172.16.131.40
Backup	Sì (Disco Interno)
Ubicazione	CED – UO SIA – Sede amministrativa di Lagonegro
Fault Tollerance	No
Valutazione Rischio	Basso

Magazzino e Contabilità gestione Liquidatoria Ambito territoriale Potenza – Server Intel SC5400

Fornitrore Procedura	Intema
Nome Procedura	Magazzino – Cont€nti
Nome server	ASL2PZGESTIONAL
Gruppo di Lavoro	WORKGRUOP
Ram	1 Gb
CPU	2 x Intel Xeon 2,4 Ghz
UPS	Si
Sistema Operativo	Windows 2000 Server Service Pack 4
DBMS	MSSql
Antivirus	Si
Controllo Remoto	Desktop Remoto
IP Address	172.16.61.6
Backup	Sì su disco
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Server XFB Ambito territoriale Potenza – Server Intel SC5400

Fornitrore Procedura	Intema
Nome Procedura	XFB
Nome server	svr-isa.
Gruppo di Lavoro	WORKGRUOP
Ram	1 Gb
CPU	2 x Intel Xeon 2,4 Ghz
UPS	Si
Sistema Operativo	Windows 2003 Server
DBMS	
Antivirus	Si
Controllo Remoto	Desktop Remoto
IP Address	172.16.61.3
Backup	Sì su disco
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Server Paghe Gestione Liquidatoria e RILPRES Ambito territoriale Potenza – Server DELL

Fornitrore Procedura	Publisys – Traccia
Nome Procedura	Urbe – Rilpres
Nome server	
Gruppo di Lavoro	WORKGRUOP
Ram	2 Gb
CPU	2 x Intel Xeon 2,8 Ghz
UPS	Si
Sistema Operativo	Windows 2003 Server Service Pack 1
DBMS	Oracle 8.5
Antivirus	Si
Controllo Remoto	Desktop Remoto
IP Address	172.16.61.9
Backup	Sì su disco
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Server Vecchio Protocollo Ambito territoriale Potenza – Server Intel SC5400

Fornitrore Procedura	Intema
Nome Procedura	Gupar
Nome server	
Gruppo di Lavoro	WORKGRUOP
Ram	1 Gb
CPU	2 x Intel Xeon 2,4 Ghz
UPS	Si
Sistema Operativo	Windows 2000 Professional Service Pack 4
DBMS	MSSQL
Antivirus	Si
Controllo Remoto	Desktop Remoto
IP Address	172.16.61.3
Backup	Sì su disco
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Server Vecchia Anagrafe Ambito territoriale Potenza – Server Intel SC5400

Fornitrore Procedura	Intema
Nome Procedura	Anagrafe Sanitaria
Nome server	Server-net.
Gruppo di Lavoro	WORKGRUOP
Ram	1 Gb
CPU	2 x Intel Xeon 2,4 Ghz
UPS	Si
Sistema Operativo	Windows 2000 Professional Service Pack 4
DBMS	MSSQL
Antivirus	Si
Controllo Remoto	Desktop Remoto
IP Address	172.16.61.2
Backup	Sì su disco
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Server Script collegamento CUP - Lab Analisi – Protocollo Ambito territoriale Potenza – Server Intel SR2400

Fornitrore Procedura	Intema
Nome Procedura	Gupar
Nome server	NUOVOCUP
Gruppo di Lavoro	WORKGRUOP
Ram	2 Gb
CPU	2 x Intel Xeon 2,4 Ghz
UPS	Si
Sistema Operativo	Windows 2003 Server Service Pack 1
DBMS	MSSQL
Antivirus	Si
Controllo Remoto	Desktop Remoto
IP Address	172.16.61.10
Backup	Sì su disco
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Server Laboratorio analisi - Ambito territoriale Potenza – Server

Fornitrore Procedura	Software Team
Nome Procedura	Magellano
Nome server	asl2-250ad1800c.
Gruppo di Lavoro	WORKGRUOP
Ram	4 Gb
CPU	2 x Intel Xeon 2 Ghz
UPS	Si
Sistema Operativo	Windows 2003 Server R2 Service Pack 1
DBMS	Oracle
Antivirus	Si
Controllo Remoto	Desktop Remoto
IP Address	172.16.61.16
Backup	Sì su disco
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Server Protesica e Gazzette Ufficiali - Ambito territoriale Potenza – Server DELL

Fornitore Procedura	Datasoftware
Nome Procedura	Sigao
Nome server	INVALIDI
Gruppo di Lavoro	WORKGRUOP
Ram	2 Gb
CPU	2 x Intel Xeon 2,8 Ghz
UPS	Si
Sistema Operativo	Windows 2003 SE Service Pack 1
DBMS	MSSql
Antivirus	Si
Controllo Remoto	Desktop Remoto
IP Address	172.16.61.12
Backup	Sì su disco
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore
Valutazione Rischio	Basso

Vecchio Cup (DB 1) – Ambito territoriale Potenza - IBM Xserver 346

Fornitrore Procedura	Intema
Nome Procedura	Magazzino – Contabilità
Nome server	dcasl2-sql1.asl2.int
Gruppo di Lavoro	Asl2.int
Ram	4 GB
CPU	2 xeon 3,2 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP2
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.65
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore + cluster con dcasl1-sql2.asl1.int
Valutazione Rischio	Basso

Vecchio Cup (DB 2) – Ambito territoriale Potenza - IBM Xserver 346

Fornitrore Procedura	Intema
Nome Procedura	Magazzino – Contabilità
Nome server	Dcasl2-sql2.asl2.int
Gruppo di Lavoro	Asl2.int
Ram	4 GB
CPU	2 xeon 3,2 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP2
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.66
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore + cluster con dcasl1-sql2.asl1.int
Valutazione Rischio	Basso

Vecchio Cup (Front-end 1) – Ambito territoriale Potenza - IBM Xserver 346

Fornitrore Procedura	Intema
Nome Procedura	CUP
Nome server	Web2-asl2.asl2.int
Gruppo di Lavoro	Asl2.int
Ram	4 GB
CPU	2 xeon 3,2 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP2
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.75
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore + NLB con web2-asl1.asl1.int
Valutazione Rischio	Basso

Vecchio Cup (Front-end 2) – Ambito territoriale Potenza - IBM Xserver 346

Fornitrore Procedura	Intema
Nome Procedura	Cup
Nome server	Web2-asl2.asl2.int
Gruppo di Lavoro	Asl2.int
Ram	4 GB
CPU	2 xeon 3,2 GHz
UPS	Sì
Sistema Operativo	Windows 2003 SE SP2
DBMS	MS SQL server
Antivirus	Sì
Controllo Remoto	Terminal Server
IP Address	172.18.94.76
Backup	Sì (Nas)
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	Dischi e alimentatore + NLB con web1-asl1.asl1.int
Valutazione Rischio	Basso

Vecchie Paghe Ambito territoriale Potenza – Siemens Nixdorf RM 300

Fornitrore Procedura	Publisys
Nome Procedura	Urbe Lire – Specialisti Ambulatoriali Lire
Nome server	
Gruppo di Lavoro	
Ram	128
CPU	RISC
UPS	Sì
Sistema Operativo	Sinix
DBMS	C-Isam
Antivirus	No
Controllo Remoto	telnet
IP Address	
Backup	Sì (Nastro)
Ubicazione	CED sede amministrativa Potenza
Fault Tollerance	No
Valutazione Rischio	Basso

“Gestione Centro Trasfusionale” - Ambito territoriale di Potenza - PC DESK: HP COMPAQ DC 7700	
Fornitore Procedura	
Nome Procedura	CETRAPLUS WEB
Nome server	CENTRAPLUS
Gruppo di Lavoro	WORKGROUP
Ram	488,00 MB
CPU	Intel(R) Pentium(R) 4 – 3,20GHz
UPS	No
Sistema Operativo	Microsoft Windows XP Professional – SP3
DBMS	Oracle
Antivirus	Eset Nod32 – Vers. 3.0
Controllo Remoto	VNC
IP Address	
Backup	Sì (Disco)
Ubicazione	Locale Centro trasfusionale Ospedale di Villa d’Agri – Sede Nodo RUPAR
Fault Tollerance	No
Valutazione Rischio	Basso

1.2 SEDI ED UFFICI PRESSO CUI VENGONO TRATTATI I DATI

1) <u>AMBITO TERRITORIALE VENOSA</u>

OSPEDALI

-Presidio Ospedaliero di Melfi;
-Presidio Ospedaliero di Venosa;

TERRITORIO

-U.S.I.B. di Melfi
-Sub distretto di Rionero
-Sub distretto di Pescopagano

- U.S.I.B. di Venosa
-Sub distretto di Lavello
- Sub distretto di Palazzo

-Consultori Familiari di Venosa, Melfi, Lavello, Rionero, Rapone.

- SerT di Melfi

-Centro di Salute Mentale di Lavello
Nuclei operativi territoriali di Melfi, Rionero, Venosa, Palazzo;

-n. 4 Case Alloggio di Genzano (n. 2), Ginestra, Maschito.

Punti salute di: Atella, Barile, Genzano, Palazzo S. Gervasio, Rapolla, Rapone, Rionero, San Fele, Lavello

DIPARTIMENTO DI PREVENZIONE

-Sede Centrale Via P. Di Chirico Venosa; sul territorio l'attività si svolge presso i Distretti e Punti Salute.

STRUTTURA TECNICO AMMINISTRATIVA

Via Roma 187 Venosa (ex sede centrale della ASL 1).

2) **AMBITO TERRITORIALE POTENZA**

OSPEDALI

Presidio Ospedaliero dI Villa D'Agri (Marsicovetere).

TERRITORIO

- U.S.I.B. di Potenza
- U.S.I.B. di Villa D'Agri (Marsicovetere)

-Sub distretto di Avigliano
-Sub distretto di Muro Lucano
-Sub distretto di Picerno
-Sub distretto di Oppido Lucano
-Sub distretto di Anzi
-Sub distretto di Brienza
-Sub distretto di Sant'Arcangelo

Poliambulatori di Potenza e Villa D'Agri;

Ambulatori: Corleto Perticara, Moliterno;

Farmaceutica Territoriale a Potenza;

Consultori Familiari di Laurenzana, Oppido Lucano, Avigliano, Campomaggiore, Muro Lucano, Picerno, S. Angelo Le Fratte, Potenza (Corso Umberto I e Via P. Petrone), Corleto Perticara, Sant'Arcangelo, Marsiconuovo, Villa D'Agri (Marsicovetere);

SerT di Potenza;

Dipartimento di Salute Mentale Potenza;

SPDC c/o AO San Carlo (Potenza);

Centro Riabilitazione Psichiatrica di Avigliano;

3 Gruppi Appartamento ad Avigliano;

3 Case Alloggio a Potenza;

Casa Alloggio a Villa D'Agri (Marsicovetere);

Casa Alloggio a Tramutola.

DIPARTIMENTO DI PREVENZIONE

Sede Centrale Via P. Petrone Potenza; sul territorio l'attività si svolge presso i Distretti e Ambulatori Comunali;

STRUTTURA TECNICO AMMINISTRATIVA

Via Torraca 2 Potenza (ex sede centrale della ASL 2)

3) **AMBITO TERRITORIALE LAGONEGRO**

OSPEDALI

-Presidio Ospedaliero di Lagonegro;
-Presidio Ospedaliero di Lauria;
-Presidio Ospedaliero di Maratea;
-Presidio Ospedaliero di Chiaromonte;

TERRITORIO

- U.S.I.B. di Lauria

-Sub- Distretto di Lagonegro;
-Sub-Distretto di Latronico;
-Sub- Distretto di Maratea;
-Sub-Distretto di Rotonda;

- U.S.I.B. di Senise
-Sub-Distretto di San Costantino Albanese;

-Consultori Familiari di Lagonegro, Lauria, Latronico, Rotonda, Maratea e Senise.

-SerT di Lagonegro

-Centro di Salute Mentale di Lauria ;
- Case Alloggio di Trecchina, Lauria e Vallina di Calvera.
-Gruppo appartamento Pecorone - Lauria

In tutti gli altri Comuni vi sono gli Ambulatori Comunali

STRUTTURE RESIDENZIALI

-Residenza Sanitaria Assistenziale di Maratea;
-Residenza Sanitaria Assistenziale di Chiaromonte;

-Centro per la Cura dei Disturbi alimentari di Chiaromonte;

-Centro per la riabilitazione Alcologica di Chiaromonte

DIPARTIMENTO DI PREVENZIONE

-Sede Centrale Via Piano dei Lippi Lagonegro; sul territorio l'attività si svolge presso i Distretti e Ambulatori Comunali;

STRUTTURA TECNICO AMMINISTRATIVA

Via Piano dei Lippi Lagonegro (ex sede centrale della ASL 3)

2 . DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ (REGOLA 19.2)

2.1 IL TITOLARE DEI TRATTAMENTO

Il Titolare del trattamento è individuato nell'Amministrazione stessa, cioè l'Azienda Sanitaria Locale di Potenza (ASP).

2.2 I RESPONSABILI DEL TRATTAMENTO

La specificità dell'Ente ha suggerito al Titolare l'individuazione di più Responsabili, sia interni sia esterni all'Ente.
In particolare, per quanto riguarda gli interni, si è ritenuto opportuno far coincidere il Dirigente di ciascuna UO con il Responsabile dei Trattamenti, così come deliberato con Provvedimento DG n. 10 del 17 gennaio 2011 e successiva integrazione deliberata con Provvedimento DG n. ___ del _____ 2011 .
Per quanto riguarda partners esterni, invece, l'Ente ha previsto l'eventualità di nominarli Responsabili, di volta in volta, su richiesta del Dirigente referente dell'attività in partenariato.

Si riporta di seguito l'elenco dei Responsabili interni, specificando l'ambito territoriale di competenza qualora l'Unità Operativa non svolga la propria attività a livello aziendale:

Attività Amministrative			
Nominativo		***Unità Operativa***	***Ambito territoriale***
Claps	Nicola	Segreteria Direzionale	
Pennacchio	Antonio	Economato, Proveditorato e Tecnico	
Chiarelli	Giacomo	Affari Generali	
De Franchi	Gabriella	Ufficio Legale e Contenzioso	
Savino	Francesco	Economico-Finanaziaria	
Berardi	Maddalena	Gestione del Personale	

Tecnostrutture di Staff			
Nominativo		***Unità Operativa***	***Ambito territoriale***
Cascini	Giuseppe	Comunicazione e Relazioni Esterne	
Nolè	Beatrice	Centro di Controllo Direzionale	Potenza
Chiarelli	Giovanni B.	Controllo di Gestione	Lagonegro
Ammirati	Giuseppina	Osservatorio Epidemiologico Pianificazione Strategica e Verifica degli Obiettivi	
Mazzeo	Nicola	Sistema Informativo Automatizzato e Tecnologie dell' Informazione	
Verrastro	Pietro	Gestione Strutture Accreditate	
Perrotta	Rocco B.	Autorizzazione e Accreditamento	
Chiarelli	Agostino	Innovazione, Ricerca e Formazione	

Area dell'Assistenza Territoriale – Distretti della Salute			
Nominativo		***Unità Operativa***	***Ambito territoriale***
Cellini	Roland	Assistenza Primaria	Lagonegro
Trabace	Rosa	CDA 'Fondazione Stella Maris Mediterraneo' Chiaromonte (UOSD)	Lagonegro
Dattola	Alberto	Assistenza alle Dipendenze Patologiche CRA Fondazione "Stella Maris Mediterraneo" Chiaromonte (UOSD)	Lagonegro
Bacchini	Anna	Assistenza Primaria	Venosa
Ciriello	Grazia Maria	USIB – Melfi	Venosa
Frangione	Maria	USIB- Venosa	Venosa
Fundone	Pietro	Assistenza alle Dipendenze Patologiche	Venosa
De Fino	Massimo	USIB – Lauria	Lagonegro
Petruzzelli	Raffaella	USIB – Senise	Lagonegro
Molinari	Sergio	USIB - Potenza	Potenza
Agriesti	Giuseppina	Ser T Potenza (UOSD)	Potenza
Donnoli	Donato	Ser T Villa D'Agri (UOSD)	Potenza
Corona	Giovanni Vito	Oncologia Critica Territoriale e Cure Palliative PO Melfi	Venosa
Amorosi	Antonio	Ostetricia e Ginecologia Territoriale	Lagonegro
Di Noia	Maddalena	Servizio Territoriale di Ostetricia e Ginecologia (UOSD)	Lagonegro

Assistenza Farmaceutica			
Nominativo		***Unità Operativa***	***Ambito territoriale***
De Michele	Anna Maria	Assistenza Farmaceutica Articolazione Ospedaliera	
Carretta	Antonio	Assistenza Farmaceutica Articolazione Territoriale	

Area Assistenza Ospedaliera			
Nominativo		***Unità Operativa***	***Ambito territoriale***
Alfieri	Salvatore	Ortopedia e Traumatologia PO Lagonegro	Lagonegro
Di Lascio	Nicola	Pediatria PO Lagonegro	Lagonegro
Falcone	Giuseppe	Chirurgia Generale, DS, Ambulatoriale e Domiciliare - PO Chiaromonte	Lagonegro
Labanchi	Riccardo	Ostetricia e Ginecologia PO Lagonegro	Lagonegro
Mileti	Libero	Anestesia e Rianimazione PO Lagonegro	Lagonegro
Mileti	Libero	Responsabile pro tempore DIRES	

Frittella	Giacomo	Coordinamento Sanitario dei Protocolli Operativi della Centrale Operativa (UOSD)	
La Rocca	Michele	Pronto Soccorso PO Lagonegro (UOSD)	Lagonegro
Scaldaferri	Gino	Laboratorio Analisi PP OO del Lagonegrese e del PO di Chiaromonte	Lagonegro
Motola	Domenico	Resp.le Tecnico - Amm.vo dei PP OO Unificati del Lagonegrese	Lagonegro
D'Angola	Luigi	Direzione Sanitaria POU Melfi-Venosa	Venosa
Gonnella	Giovanni	Pneumologia PO Melfi	Venosa
Capogrosso	Vincenzo	UTIC e Cardiologia POU Venosa-Melfi	Venosa
Bonifacio	Mario	Anestesia e Rianimazione POU Melfi-Venosa	Venosa
Padula	Giuseppe	Ostetricia e Ginecologia PO Melfi	Venosa
Soligno	Ornella	Pediatria PO Melfi	Venosa
Curzio	Francesco	Percorsi Integrati di Ostetricia e Ginecologia PO Lagonegro	Lagonegro
Iadanza	Domenico	Servizio Territoriale di Pediatria Sociale	Lagonegro
Lapadula	Giuseppe	Neonatologia PO Melfi	Venosa
De Rosa	Nicola	Medicina Fisica e Riabilitazione PO Venosa	Venosa
Mascolo	Vito	Ortopedia e Traumatologia PO Melfi	Venosa
Araneo	Antonio A	Medicina Generale Specialistica POU Melfi-Venosa	Venosa
Araneo	Antonio A	Cardiologia e Diabetologia PO Maratea	Lagonegro
Bombini	Antonio	Attività di Nefrologia e Dialisi (UOSD) Muro Lucano e Villa D'Agri	Potenza
Mitidieri	Pasquale	Day Hospital Internistico (UOSD) PO Lagonegro	Lagonegro
Sansone	Gennaro	Nefrologia e Dialisi PO Lauria e Maratea (UOSD)	Lagonegro
Gaudiano	Giuseppe	Nefrologia e Dialisi PO Chiaromonte (UOSD)	Lagonegro
Lauletta	Rinaldo	Cardiologia e UTIC (UOSD) PO Lagonegro	Lagonegro
Caruso	Enzo	Percorsi Integrati di Cura delle Patologie Endocrine e Metaboliche (UOSD)	Lagonegro
Lavitola	Pasquale	Attività Internistica del CDA di Chiaromonte Fondazione "Stella Maris Mediterraneo"	Lagonegro
Masino	Bruno	Direzione Sanitaria PO Villa D'Agri	Potenza
Di Salvo	Donato	Medicina Generale PO Villa D'Agri	Potenza
Martini	M. Cristina	Pneumologia PO Villa D'Agri	Potenza
ff Martini	M. Cristina	Pneumologia Territoriale (ex ASL n 2)	
Mazzeo Cicchetti	Agostino	Cardiologia e UTIC PO Villa D'Agri	Potenza
Mormando	Fedele	Ortopedia Traumatologia PO Villa D'Agri	Potenza
Sagone	Vincenzo	Anestesia e Rianimazione PO Villa D'Agri	Potenza

Serica	Ubaldo	Ostetricia e Ginecologia PO Villa D'Agri	Potenza
Loffredo	Domenico	Chirurgia Generale PO Villa D'Agri	Potenza
Toscano	C. Pompeo	Accettazione e PS – OBI PO Villa D'Agri	Potenza
Cavaliere	Domenico	Laboratorio Analisi PO Villa D'Agri	Potenza
Borgia	Michele	Centro Trasfusionale (UOSD)	Venosa
Perrone	Carmela	Centro Trasfusionale (UOSD)	Potenza
Volonnino	Canio	Centro Trasfusionale (UOSD)	Lagonegro
Barile	Vincenzo	Radiologia	Potenza
Camaldo	Giuseppe	Ecografia Territoriale (UOSD)	Lagonegro
Cantisani	Rosario	Neuroradiologia (UOSD)	Potenza
Lacerenza	Domenico	Oculistica PO Venosa	Venosa
Buccino	Vincenzo	Endoscopia Digestiva (UOSD) PO Venosa	Venosa
Arenella	Antonio	Chirurgia d'Urgenza e Vascolare (UOSD)PO Lagonegro	Lagonegro
Fulco	Rocco	Chirurgia Laparoscopica e Day Surgery (UOSD) PO Lagonegro	Lagonegro
Vassallo	Fiorentino	Urologia (UOSD) PO Lagonegro	Lagonegro
Alagia	Luigi	Percorsi Integrati di Ortopedia(UOSD) PO Lagonegro	Lagonegro
Colarusso	Diodoro	Medicina di Urgenza PO Lagonegro	Lagonegro
Gagliardi	Antonio	Direzione Sanitaria dei PP.OO. Lagonegrese	Lagonegro
Magno	Giuseppe	Area Medica di Assistenza Post - Acuzie PO Lauria	Lagonegro
Mandarino	Bruno	Medicina dell'Invecchiamento - Geriatria PO Maratea	Lagonegro
Palo	Vincenzo	Malattie dell'Apparato Respiratorio PO Maratea	Lagonegro
Salsano	Gaetano	Radiologia PP OO del Lagonegrese	Lagonegro
Maglione	Francesco	Laboratorio Analisi POU Melfi-Venosa	Venosa
Stabile	Fernando	Radiologia POU Melfi - Venosa	Venosa
ff Arenella	Antonio	Chirurgia PO Lagonegro	Lagonegro
ff Cancellara	Francesca	Medicina Interna Distrettuale e Residenziale PO Chiaromonte	Lagonegro

Salute Mentale			
Nominativo		***Unità Operativa***	***Ambito territoriale***
Guarino	Alfonsina	Centro di Salute Mentale Lauria	Lagonegro
Sgarra Carta	Marta	Strutture Residenziali e Semiresidenziali (UOSD)	Potenza
Giannone	Rosa	Strutture Residenziali e Semiresidenziali (UOSD)	Venosa
Masessa De Dovitiis	Giovanni	CSM (UOSD)	Potenza
Laieta	Angelo	Centro Riabilitativo di Avigliano, Psico-Sociale e Psico-Diagnostica di Potenza (UOSD)	Potenza

Romano	Maria Ippolita	Servizio Psichiatrico di Diagnosi Cura PO Chiaromonte	Lagonegro

Prevenzione Collettiva della Salute Umana			
Nominativo		***Unità Operativa***	***Ambito territoriale***
Negrone	Francesco Saverio	Igiene Epidemiologia e Sanità Pubblica	Potenza
Di Nubila	Vincenzo	Medicina dello Sport (UOSD)	
Marandola	Francesco	Referenza Aziendale Politiche	
Marina	Saverio	Vaccinali (UOSD)	
Via	Michele Angelo	Medicina del Lavoro e Sicurezza degli Ambienti di Lavoro	Potenza
Caputo	Angelo	Igiene degli Alimenti e della Nutrizione (SIAN)	Lagonegro
Romaniello	Antonio	Igiene degli Alimenti e della Nutrizione (SIAN)	Potenza
Fortunato	Antonio	Igiene Epidemiologia e Sanità Pubblica	Venosa
Schettino	Biagio	Medicina del Lavoro e Sicurezza degli Ambienti di Lavoro	Lagonegro
Focaraccio	Caterina	Igiene, Epidemiologia e Sanità Pubblica	Lagonegro
Romanelli	Salvatore	Prevenzione, Protezione e Impiantistica nei Luoghi di Lavoro	Potenza

Prevenzione della Sanità e Benessere Animale			
Nominativo		***Unità Operativa***	***Ambito territoriale***
Bochicchio	Vito	Sanità Animale	Venosa
Bochicchio	Angelo	Igiene degli Allevamenti e delle Produzioni Zootecniche	Venosa
Iacoviello	Mauro	Igiene della Produzione, Trasformazione, Commercializzazione, Cons. e Trasp. dei Prodotti di Origine Animale e loro derivati	Venosa
Chiarelli	Agostino	Igiene Allevamenti e delle Produzioni Zootecniche	Lagonegro
Marranchiello	Egidio	Sanità Animale	Lagonegro
Raimondi	Paolo	Sanità Animale	Potenza
Perrotta	Rocco Berardino	Igiene della Produzione, Trasformazione, Commercializzazione, Cons. e Trasp. dei Prodotti di Origine Animale e loro Derivati	Potenza
Rosa	Pietro	Igiene degli Allevamenti e Produzioni Zootecniche	Potenza
ff Chiarelli	Giacomantonio	Igiene della Produzione, Trasformazione, Commercializzazione, Cons. e Trasp. dei Prodotti di Origine Animale e loro derivati	Lagonegro

Nominativo		Attività Tecniche Unità Operativa	Ambito territoriale
ff Nolè	Giuseppe	Attività Tecniche e Gestione del Patrimonio	Venosa
ff Cicale	Franca	Attività Tecniche e Gestione del Patrimonio	Lagonegro e Potenza

2.3 GLI INCARICATI DEL TRATTAMENTO

Tutti i soggetti che trattano dati personali vengono nominati 'Incaricati' da parte del relativo responsabile; naturalmente la nomina non è limitata ai dipendenti di ruolo, ma si estende anche agli 'irregolari' di vario tipo, come stagisti, interinali, tirocinanti, collaboratori a vario titolo, qualora la funzione comporti necessariamente il trattamento dei dati personali.

2.4 GLI AMMINISTRATORI DI SISTEMA

In ossequio al Provvedimento Generale del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e s.m.i. l'Azienda ha provveduto a censire i soggetti che svolgono il ruolo di Amministratori di Sistema, secondo le indicazioni del Provvedimento succitato, e con Delibera DG n. 1208 del 15 dicembre 2009 ha provveduto a formalizzarne il ruolo, effettuando le nomine di rito.
L'elenco degli Amministratori di sistema interni è il seguente:
Nicola Mazzeo Responsabile SIA ambito territoriale Venosa
Rocco Primucci Coadiutore ambito territoriale Venosa)
Donato Macchia Operatore Tecnico ambito territoriale Venosa
Lucio Fonzeca Operatore Tecnico ambito territoriale Venosa
Claudio Granieri Componente SIA (ambito territoriale Potenza)
Giuseppe Guarino Assistente Tecnico ambito territoriale Potenza
Angelo Raffaele Dalia Responsabile SIA ambito territoriale Lagonegro
Gulfo Nicola Assistente ambito territoriale Lagonegro
Calabria Antonio Operatore Tecnico ambito territoriale Lagonegro

Per quanto concerne le società esterne che svolgono il ruolo in outsourcing, si è provveduto ad invitarli a tenere elenco aggiornato delle persone fisiche preposte alle operazioni di amministrazione di sistemi, comunicandone copia alla ASP.

3 . ANALISI DEI RISCHI (REGOLA 19.3)

Individuare le risorse a rischio e le possibili minacce costituisce un fondamentale passo per la definizione di un sistema sicuro.
Atteso che un sistema informativo è costituito da un insieme di risorse hardware e software in relazione tra loro, tale continua relazione espone il sistema ad una grande quantità di possibili minacce o incidenti involontari.
E' possibile catalogare il livello di rischio in tre soglie:
a) bassa (rischio remoto e comunque rapidamente reversibile)
b) media (rischio remoto ma con effetti non facilmente ovviabili) pertanto occorre prevedere accorgimenti per prevenire e contenere il rischio;
c) alta (rischio inaccettabile) pertanto occorre porre in essere tutte le contromisure di natura fisica e logica per cercare di abbattere il rischio o almeno contenerlo in un ambito accettabile.

3.1 RISCHIO HARDWARE

Vi sono diverse categorie di dispositivi hardware che sono passibili di malfunzionamenti dovuti a guasti o manomissioni sia tra i dispositivi di gestione della rete che tra i server ed i pc che vengono utilizzati nelle nostre strutture. La nostra Asl ha una rete geografica e quindi ha apparecchiature di tipo diverso a seconda della loro funzione: essenzialmente abbiamo dei router per il collegamento tra le varie strutture e degli swithc o Hub per la gestione delle singole LAN. Per i dispositivi di rete la loro sicurezza è data, per quanto attiene all'aspetto fisico, dalla loro inaccessibilità, infatti devono essere sistemati in ambienti al sicuro da accessi indiscriminati: l'accesso è consentito ad utenti autorizzati. Le attrezzature utilizzate nelle varie strutture della nostra Azienda sono poste per la gran parte in armadi di rete chiusi a chiave o, in alternativa in luoghi accessibili solo al personale autorizzato. L'altro dispositivo di sicurezza è dato dalla password; per le apparecchiature più esposte è necessario che questa venga cambiata più frequentemente. La minaccia più comune e pericolosa per la risorsa hardware è rappresentata dal malfunzionamento che può essere accidentale o intenzionale. E' accidentale ciò che non avviene per la volontà di qualche soggetto, anche quelli causati da operatori per disattenzione o uso non corretto. Per ridurre al minimo tali rischi si allocano le macchine in ambienti sicuri nei quali è difficile azionarle accidentalmente; a tali ambienti può accedere solo il personale qualificato e per ragioni di servizio. Se vi fosse la necessità di far accedere altre persone, anche fuori dell’orario d’ufficio, queste ultime debbono essere accompagnate da un utente autorizzato, inoltre detti accessi debbono essere registrati, e la registrazione sarà effettuata a cura del personale che custodisce le chiavi d’accesso. Altre minacce riguardano l'utilizzo improprio delle risorse (un esempio consiste nell'utilizzare la memoria di massa per memorizzare informazioni d'interesse dell'incursore, che seppure non producano danno e non compromettano il sistema. ne riducono di fatto le risorse limitandone il tempo di disponibilità . Per ridurre al minimo tali tipologie di rischio, i server sono posti in ambienti protetti da (firewall che assolvono a compiti di patting, filtering).

TABELLA DI ANALISI DEI RISCHI SULLE RISORSE HARDWARE

Risorsa	Elemento di Rischio	Soglia Individuata	Motivazione
Tutte	Uso non autorizzato	Bassa	L'utilizzo è soggetto all'uso di password
Tutte	Manomissione/Sabotaggio	Bassa	Alle risorse non accede personale non autorizzato. La manutenzione è effettuata da tecnici di fiducia.
Tutte	Probabilità/Frequenza di guasto	Bassa	L'hardware acquistato è qualità ed è sottoposto garanzia pluriennale.
Tutte	Rischi connessi all'elettricità	Bassa	I dispositivi critici sono protetti da sistemi di continuità.

3.2 RISCHIO SOFTWARE

Nel sistema Informativo dell'Asl esistono vari tipi software:
• sistemi operativi: Windows 95/98/ME, Windows NT/2000/XP, Sco Unix, Sinix;
• DBMS: Oracle, Informix, C-ISAM;
• Tutti i software utilizzati sono di tipo commerciale e, tranne per quelli di tipo generale quale Office, l'Azienda ha in essere un contratto di manutenzione con le softwarehouse fornitrici.

La presenza di varie tipologie ha diversi riflessi sulla sicurezza atteso che richiede allo staff tecnico una competenza che oltre ad essere approfondita deve risultare abbastanza ampia (per rispondere alle possibili minacce) I sistemi software sono soggetti a due tipologie di minacce: il malfunzionamento e la disattivazione, che possono dipendere entrambe da cause accidentali o intenzionali. Il malfunzionamento è un funzionamento non corrispondente a quello desiderato dovuto a motivi accidentali (bugs, sezioni di codice errate) . La minimizzazione di questo problema sta in una adeguata politica di intercettazione di virus e simili. La disattivazione consiste nella mancata operatività in seguito ad eventi accidentali (eccessivo numero di richieste per un server) o intenzionali (denial of service attack) . Generalmente il software commerciale garantisce maggiore sicurezza sia per il controllo più elevato in fase di distribuzione, che per il supporto garantito dal produttore. Per i software autoprodotti la valutazione della sicurezza dipende esclusivamente dall'attenzione prestata alla sicurezza in fase di progettazione e sviluppo degli stessi.

TABELLA DI ANALISI DEI RISCHI SULLE RISORSE SOFTWARE

Risorsa	Elemento di Rischio	Soglia Individuata	Motivazione
Tutte	Accesso non autorizzato alle basi dati connesse	Bassa	I software che trattano i dati controllano l'accesso tramite una finestra di autenticazione(finestra di login)
Tutte	Errori software che minacciano l'integrità dei dati	Bassa	I software sono utilizzati da parecchi anni e non hanno causato la perdita o il danneggiamento dei dati trattati

Tutte	Presenza di codice non conforme alle specifiche del programma	Bassa	I programmi sono forniti da produttori che operano nel settore da tempo con serietà.

3.3 RISCHIO DATI

I dati possono essere catalogati in base alla tipologia:
a) dati di configurazione (stabiliscono la modalità di funzionamento)
b) dati di archivio (oggetto di elaborazione)
c) dati di log (registrano informazioni sul funzionamento del sistema)
d) dati informativi (per la consultazione)
e) dati storici (copie di back up)
Le minacce per i dati si possono ricondurre a: accesso non autorizzato (violazione della riservatezza) e modifica non autorizzata (violazione dell'integrità). Entrambe le minacce possono essere accidentali (un utente senza intenzionalità accede e modifica dati non di sua competenza) ed intenzionali (un utente deliberatamente accede a dati riservati e li modifica per scopi precisi dolosi alterazione documenti di archivio, cancellazione prove intrusione).
Le minacce derivanti da virus rientrano nelle due categorie precedentemente descritte in quanto i virus si introducono nel sistema in modo fraudolento causando danni quali cancellazione o alterazione, quindi sostanzialmente violando l'integrità dei dati.

TABELLA DI ANALISI DEI RISCHI SULLE RISORSE DATI

Risorsa	Elemento di rischio	Soglia individuata	Motivazione
Tutte	Accesso non autorizzato	Bassa	L’accesso ai dati avviene solo attraverso l’utilizzo di password. All’archivio cartaceo possono accedere solo i diretti incaricati in possesso delle chiavi.
Tutte	Cancellazione o Manomissione di dati	Bassa	L’accesso ai server avviene solo attraverso l’utilizzo di password. All’archivio cartaceo possono accedere solo i diretti incaricati in possesso delle chiavi.
Tutte	Perdita di dati	Bassa	I dati sono conservati in dischi con tecnologia RAID 0 o 5 al fine di prevenire anche rotture fisiche degli stessi. Vengono effettuate periodicamente copie di Backup sia su disco che su nastro.
Tutte	Incapacità di ripristinare backup	Bassa	I backup da nastro non hanno mai dato problemi di ripristino, inoltre abbiamo quello su disco di scorta.
Tutte	Minacce da Virus	Media	Abbiamo un antivirus con aggiornamento automatico tramite rete. Sono vietati i collegamenti Dial-up.

3.4 RISCHIO RISORSE PROFESSIONALI

Le risorse professionali sono costituite da tutti coloro che interagiscono con il sistema informativo e sono in possesso di informazioni utili relative al funzionamento dello stesso. Rientrano tra le risorse professionali sia il personale interno che svolge funzioni di amministrazione e gestione di risorse hardware e software, che il personale esterno che in virtù di rapporti convenzionali o di fornitura in essere con l'Azienda, accede ad una o più risorse del S.I.A per attività di manutenzione, gestione e installazione. I sistemi di sicurezza più che alle persone fisiche debbono riguardare le postazioni di lavoro ed ad una maggiore sicurezza da implementare sulle macchine in dotazione alle postazioni.

TABELLA DI ANALISI DEI RISCHI SULLE RISORSE PROFESSIONALI

Risorsa	Elemento di Rischio	Soglia Individuata	Motivazione
Interna	Rivelazione di informazioni all'esterno	Bassa	Il personale interno è stato formato ed è a conoscenza delle misure minime da adottare.
Esterna	Acquisizione di privilegi ed informazioni inerenti l'accesso alle risorse	Bassa	L’azienda ha responsabilizzato con un accordo le ditte fornitrici

La documentazione cartacea che riguarda il funzionamento del sistema nel suo complesso (software, hardware) sia a livello tecnico che di gestione, può subire danneggiamento a causa di eventi naturali e per azioni accidentali o intenzionali. Il sistema di sicurezza consiste nel custodirla in appositi armadi di sicurezza che proteggano gli stessi sia da incendi che da campi magnetici, individuando una persona quale responsabile della custodia.

4 . MISURE ADOTTATE, DA ADOTTARE ED ADEGUAMENTO DELLE MISURE PRESENTI (REGOLA 19.4)

4.1 PREMESSA

Le misure di sicurezza costituiscono il complesso delle misure tecniche, informatiche, organizzative, logiche e procedurali, atte a garantire il livello minimo di protezione richiesto dal decreto legislativo n. 196/03, al fine di tutelare i dati personali e sensibili dai rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Attivare dei servizi di sicurezza è quindi necessario, ma da soli non possono essere sufficienti a garantire la sicurezza dell'intero sistema e quindi debbono essere integrate anche da aspetti organizzativi e gestionali per il mantenimento di un buon livello di sicurezza.
I Servizi di sicurezza di base sono:

- l'identificazione dell'utente che richiede l'accesso ad un servizio tramite ***user e password***;
- il controllo degli accessi tramite verifica dell'autorizzazione all'accesso da parte di utente autenticato con specifico profilo di autenticazione;
- la possibilità di verificare l'integrità dei dati;
- la gestione degli incidenti;

I meccanismi di sicurezza, cioè le modalità tecniche attraverso le quali si realizzano i servizi di sicurezza, si possono riassumere in:

- identificazione degli utenti con la possibilità di controllare e monitorare gli accessi da parte degli utenti;
- backup: possibilità di tenere copia dei dati di grande importanza al fine di garantire un ripristino della funzionalità eventualmente compromessa;
- antivirus: possibilità di rimuovere codice potenzialmente pericoloso;
- firewall: permettendo la creazione automatica delle regole per il filtraggio, controllo dei pacchetti nelle trasmissioni, archiviazione log delle attività.

4.2 MISURE DI SICUREZZA DI TIPO FISICO ADOTTATE

Le misure poste in essere hanno lo scopo di mantenere un ambiente di lavoro protetto che impedisca perdite di informazioni e di patrimonio intellettuale di proprietà dell'Azienda:

- L'accesso ai locali in cui sono presenti uno o più sistemi server o postazioni di lavoro è protetto tramite porte munite di serratura;
- L'accesso è normato in modo che è impedito l'accesso a soggetti non autorizzati, al fine di garantire che i dati personali o sensibili presenti nel locale, siano utilizzati solo da quanti ne hanno titolo, in qualità di responsabili o incaricati del trattamento, nei soli limiti in cui ciò sia funzionale allo svolgimento dei propri compiti;
- Fuori dell'orario di lavoro tutti gli accessi debbono essere registrati;
- L'accesso sia del personale interno che di quello esterno ai locali ove sono custoditi dati personali e/o sensibili, è filtrato dalla conoscenza personale da parte degli operatori-amministratori dei sistemi/ufficio;
- I fascicoli delle pratiche non devono essere lasciati in posizione visibile sulla propria scrivania. Inoltre, non devono essere lasciati incustoditi sulle scrivanie o su altri ripiani

di lavoro atti, documenti e fascicoli, che devono essere conservati negli schedari e prelevati solamente per il tempo necessario allo studio della pratica, per poi esservi riposti al termine del trattamento della stessa.

- I locali/uffici sono, alla fine dell'orario di lavoro, chiusi a chiave;
- La chiave è custodita dall'operatore;
- I locali server della sede di Potenza verranno dotati di telecamera IP con registrazione degli accessi, naturalmente nel rispetto della normativa in materia di videosorveglianza;
- Gli uffici e locali delle strutture centrali dei tre ambiti territoriali dell'Azienda sono vigilati durante la notte da personale dedicato;
- I corridoi di disimpegno per i vari uffici sono tutti dotati di estintori per la soppressione di focolai di incendio;
- La linea elettrica che serve i locali che ospitano i CED aziendali è servita da un gruppo di continuità opportunamente dimensionato;
- I locali che ospitano i CED aziendali sono tenuti a temperatura idonea al funzionamento dei server in essi collocati tramite condizionatori ed, inoltre, hanno estintori per la soppressione di focolai di incendio;
- Gli ambienti adibiti ad archivio sono anch'essi dotati di estintori;
- Gli archivi ed uffici amministrativi ospitati pressi i presidi ospedalieri sono chiusi a chiave a cura del personale addetto;
- L'accesso dall'esterno è filtrato, specie di notte, dal portiere che per agevolare l'ingresso deve azionare la sbarra che vieta l'accesso;
- Presso l'ospedale di Melfi, in aggiunta al portiere, nelle ore notturne, sosta in portineria un vigilante che effettua periodici controlli sia degli spazi esterni che di quelli interni.

4.3 MISURE DI SICUREZZA DI TIPO LOGICO ADOTTATE

Sono misure software che sfruttano sistemi di protezione messi a disposizione o dai sistemi operativi adottati o dagli applicativi al fine di controllare, discriminare e rendere sicuri gli accessi ai dati:

- Identificazione: ad ogni utente collegato alla rete viene assegnato un UserId che lo identifica univocamente e con la quale chiede l’accesso alla rete aziendale;
- Assegnazione Password di Rete: viene data in maniera univoca all’utente attraverso le restrizioni esposte in precedenza;
- Assegnazione Password di Bios: agli utenti che hanno un sistema operativo di tipo 9X viene data questa ulteriore protezione, al fine di salvaguardare l’accesso ai dati custoditi localmente;
- Revoca di UserId: nel caso di mancato utilizzo della stessa per più di 60 giorni, si procede ad una sospensione cautelativa degli accessi alla rete;
- Conservazione delle Password di Rete: avviene in un database cifrato incomprensibile anche all’amministratore del sistema;
- Ripristino Password: in caso di dimenticanza l’utente può chiedere all’amministratore di sistema il ripristino della stessa; l’amministratore ne fornirà una temporanea che scadrà al primo accesso dell’utente alla rete e lo obbligherà a cambiarla;
- Richieste di UserId: le richieste, sia per l’accesso alla rete che per l’accesso alle procedure, devono essere effettuate dal responsabile del trattamento indicando l’incaricato interessato e quali sono le funzioni a cui deve essere abilitato;

- Aggiornamento Antivirus: Presso l'Asl è in uso l'E-trust della C.A., fornitoci dalla Regione, che provvede ad aggiornare giornalmente le postazioni collegate alla rete.

4.4 MANUTENZIONE DEI SISTEMI OPERATIVI ED APPLICAZIONI SOFTWARE

I servizi di manutenzione software saranno avviati su iniziativa dell'impresa che sviluppa il software applicativo, la quale garantisce un perfetto funzionamento del sistema informatico.
Il servizio di manutenzione del sistema di elaborazione e comunicazione dovrà articolarsi su:

- manutenzione del software di base;
- manutenzione del software d'ambiente;
- manutenzione del software applicativo.

La Manutenzione del software di base comprende:

- l'ggiornamento dei programmi con installazione di moduli software correttivi (service pack, hot fix, ecc.);
- la reinstallazione e personalizzazione del software a fronte di problemi tecnici accertati;

La manutenzione del software d'ambiente prevede che il servizio sarà effettuato per eliminare i difetti che potrebbero riscontrarsi nell'utilizzo del software d'ambiente, costituito dal prodotto per la gestione delle basi di dati relazionale e per l'installazione di eventuali release successive.
L'assistenza e la manutenzione del software applicativo viene effettuata dall'Impresa partner con proprio personale di elevata competenza tecnica e professionale, che provvede alla formazione del personale dell'Amministrazione.
1. Il servizio di manutenzione ordinaria dei Programmi Applicativi comprende:
    a) La manutenzione *correttiva* che consiste nella rimozione di eventuali errori o malfunzionamenti da effettuarsi anche con intervento presso la sede dell'Amministrazione.
    b) La manutenzione *adeguativa* che riguarda adeguamenti derivanti da nuove disposizioni legislative, sempre che non comportino sostanziali modifiche alla logica dei programmi e/o alla struttura dei dati, da consegnarsi entro termini utili per consentirne l'applicazione. Gli interventi che comportano sostanziali modifiche rientreranno nel servizio di manutenzione straordinaria.
    c) Interventi *on-site* che consistono nella fornitura di prestazioni in loco di personale specializzato richieste dall'Amministrazione per effettuare le operazioni richieste dall'assistenza correttiva e/o adeguativa.
2. Il servizio di manutenzione straordinaria dei Programmi Applicativi dovrà comprende:
    a) La manutenzione migliorativa relativa al mantenimento dell'efficienza delle procedure e dei programmi al variare delle condizioni e dei carichi di lavoro.
    b) La manutenzione innovativa per la creazione di nuovi elaborati, personalizzati o generalizzati utili al soddisfacimento di nuove esigenze dell'Amministrazione.

Inoltre, in Azienda sono tuttora attivi numerosi PC con sistema operativo Windows 98 o precedenti, per i quali il sistema non consente un'adeguata politica di autenticazione dell'utente, e pertanto al momento tale misura (obbligatoria) resta inapplicata; s'intende porre rimedio attraverso uno dei seguenti intervento:

a) sostituzione dei computer più obsoleti;
b) implementazione del sistema operativo per i computers meno obsoleti, per i quali l'intervento valga la spesa;

c) istallando su tutti gli altri apposito software di gestione dell'autenticazione (es. Access Denied o SafeGate).

Poiché in tutti e 3 i casi è necessario un cospicuo impiego di risorse sia economiche sia umane (nei casi b e c), l'intervento è subordinato alla disponibilità economica da parte della Direzione Generale.

4.5 REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE

In ossequio al Provvedimento Generale dal Garante per la Protezione dei Dati Personali del 01.03.2007 pubblicato sulla G.U. del 10.03.2007, n. 58 (Linee guida per posta elettronica e internet), da considerarsi elemento certamente non residuale delle Misure di Sicurezza, con Provvedimento del Direttore Generale n. 570 del 28.05.2010 è stato adottato il Regolamento Aziendale per l'utilizzo delle Risorse Informatiche e Telematiche aziendali; il regolamento, è pubblicato sul canale telematico 'Privacy' del sito aziendale. Naturalmente è stato consumato il passaggio del confronto con le Organizzazioni dei Lavoratori sia a livello dirigenziale sia di comparto, tanto nel rispetto di quanto prescritto dall'art. 4 della Legge n. 300 del 1970 (Statuto dei Lavoratori) .

4.6 MISURE DI SICUREZZA PER TRATTAMENTO DATI SENZA COMPUTERS

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.

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 (artt. 22 e 24 del Disciplinare Tecnico Allegato B del D.Lgs. n. 196/2003.) gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

Tutto ciò va applicato anche a qualunque tipo di copia effettuata sui documenti contenenti dati personali.

4.7 PROTEZIONE AREE E LOCALI DI CRUCIALE IMPORTANZA

Tutti i locali ove sono o saranno ubicati servers o più in generale attrezzature rilevanti ai fini della custodia e della disponibilità dei dati personali saranno protetti (oltre che con misure di tipo logico-informatiche di cui si è già detto) contro il rischio di intrusione fisica da parte di persone non autorizzate. La protezione dovrà riguardare sia le porte di accesso sia le aperture verso l'esterno da dove è possibile intrusione di estranei.

5 . CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI (REGOLA 19.5)

Il piano di ripristino della disponibilità dei dati è finalizzato alla definizione delle idonee misure da adottare per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
Attualmente l'Ente sta predisponendo un piano di disaster recovery che tenga conto della nuova realizzazione della rete dati e del nuovo CED di via Torraca a Potenza. L'opportunità di avere un sito quale l'ex CED di Lagonegro, collegato in fibra a quello di via Torraca e configurato per l'allocazione in sicurezza di server e non più utilizzato, rende immediatamente disponibile un locale dove realizzare il "sito di disaster recovery". In questa struttura, una volta ultimata la realizzazione del CED di via Torraca, sarà installato un server blade su cui virtualizzare repliche dei server presenti nel CED principale, pronte ad entrare in funzione ove gli accorgimenti installati sui server di Potenza non fossero sufficienti ad evitarne il blocco.
Infatti i server attualmente in uso hanno diversi accorgimenti che ne prevengono il fault a secondo della configurazione realizzata:

- Alta affidabilità: configurazione con 1 storage, 2 server in NLB per la parte application e 2 server in cluster per la parte DB. I server hanno dischi in modalità RAID 5 ed hot swap, con alimentatori ridondati. Questa configurazione consente il funzionamento anche con un solo server funzionante per tipologia (1 application e 1 DB) su cui funzioni almeno un alimentatore e 2 dei tre dischi, per altro sostituibili senza spegnere il server.
- Media affidabilità: server con doppio alimentatore e RAID 5 per i dischi, consente il funzionamento con un solo alimentatore e 2 dei 3 dischi funzionanti, sostituibili a caldo.

In attesa di realizzare quanto esposto il disaster recovery è affidato alle sole caratteristiche dei server, con eventualità remota di blocco nel caso della configurazione in alta affidabilità, difficile per quella in media.
Vengono comunque programmate copie di Backup su NAS, su cassetta o su HD appartenenti ad altri server per consebtire il ripristino dei dati in caso di completa perdita della base dati. A riguardo, appena i server saranno dislocati nel CED di via Torraca, sarà realizzato un piano di schedulazione dell'attività definente anche regole comuni per l'ubicazione e l'etichettatura delle copie su CD o su Nastro; in particolare, vanno definiti:

- modalità di backup (automatico, manuale, frequenza, supporto, ecc.);
- l'ubicazione delle copie;
- eventuali convenzioni nella applicazione di etichette o contrassegni per CD e Nastri;
- la frequenza di rotazione dei supporti;
- i metodi per il trasporto dei salvataggi dal luogo di archiviazione verso l'esterno e le procedure di ritorno dei salvataggi in caso di situazione di disaster.

6 . PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI (REGOLA 19.6)

6.1 PREMESSA

L'importanza sostanziale attribuita dalla ASP alla normativa privacy trova un riscontro inconfutabile nell'oneroso programma formativo voluto dall'Azienda, messo in atto avvalendosi di un soggetto esterno selezionato attraverso una procedura ad evidenza pubblica, allo scopo di introdurre le prescrizioni e le tutele previste dal Codice Privacy in relazione alle procedure ed alle attività normalmente messe in atto nell'Ente, senza ignorare, ma anzi valorizzando tutto quanto già sperimentato da ciascuna delle Aziende di provenienza, verificando al contempo lo stato di attuazione degli adempimenti esplicitamente previsti, come ad esempio la Notifica, l'adozione delle Misure Minime di Sicurezza (comprendenti il presente Documento Programmatico sulla Sicurezza) e così via; il progetto è stato avviato nel Settembre 2010 e proseguirà fino a marzo 2012.

Il progetto contiene i seguenti canali formativi:

A. Attività formativa frontale generica;
B. Attività formativa frontale in ECM;
C. Attivazione di Laboratori sperimentali formativi interattivi;
D. Attività di formazione online (basato su piattaforma e-learning).

6.2 FINALITÀ

Se da un punto di vista formale il processo di formazione ha lo scopo di adempiere ad una precisa previsione normativa, da un punto di vista più sostanziale tale processo ha la finalità di migliorare le 'prestazioni' degli addetti, rendendoli maggiormente consapevoli delle potenzialità – ma anche dei limiti e dei rischi – connessi con l'utilizzo dello strumento informatico e della rete telematica, e, in aggiunta a questo, sensibilizzare gli operatori sui contenuti più vasti di questa delicata materia.

6.3.1 PIANO DI FORMAZIONE CON ATTIVITÀ DI AULA

Ad oggi circa il 70% del totale degli addetti ha già fruito di moduli formativi frontali presso le Aziende di provenienza, anche attraverso moduli in 'ECM' (previo accreditamento presso il Ministero della Salute) per i soggetti tenuti a tale tipo di formazione.

a) **IL PRIMO IMPIANTO**: è stato erogato tra il 2006 ed il 2008, anche in ECM, per circa il 70% degli addetti; ai restanti addetti si estende a tappeto, per gruppi volutamente non omogenei, con l'obiettivo di rendere tutti consapevoli delle problematiche connesse con la normativa privacy in generale e con l'utilizzo dello strumento informatico e della rete telematica in particolare, in relazione ai trattamenti di dati personali. Questa fase è iniziata nel settembre 2010 e verrà conclusa a marzo 2012, replicata per tutti i nuovi assunti, a valere come base formativa minima indispensabile affinché gli incaricati dei trattamenti possano svolgere in maniera consapevole e responsabile le funzioni

connesse con il loro ruolo.

Gli argomenti principali da trattare in aula sono i seguenti:
MODULO 1: I FONDAMENTALI
- Le definizioni: “interessato”, “dato personale”, “banca dati”, “trattamento”, “comunicazione” e “diffusione”.
- Gli adempimenti: Notifica, Sicurezza, Regolamenti.
- Le tipologie di dati: comune, particolare, sensibile, sanitario.
- La struttura a presidio della *privacy*: titolare, responsabile, incaricato.
- Il regime sanzionatorio.
- La comunicabilità dei dati personali.
- L’interessato e le misure di tutela: accesso, informativa, consenso.
- i Partners: come disciplinare i trattamenti di dati in regime di partenariato.
- Conservazione dei dati: modalità e durata della conservazione.
- Contemperamento della normativa sull’accesso con la normativa sulla privacy in particolare negli atti a rilevanza esterna: tecniche di redazione.
- Come rispondere al telefono o a richieste fatte a voce, di persona.

MODULO 2: LA SICUREZZA INFORMATICA

- Definizione di un Sistema Sicuro
- Minacce alla sicurezza
- Origini delle minacce
- Calamità naturali
- Utenti interni all'organizzazione
- Aggressori esterni (hacker)
- Obiettivi delle minacce
- Norme comportamentali:
- utilizzo delle postazioni di lavoro
- accesso ad internet
- utilizzo della posta elettronica
- utilizzo delle password e altre misure di sicurezza

b) ULTERIORI INTERVENTI FORMATIVI SUCCESSIVI.

Successivamente al primo impianto si sono messi in atto interventi formativi maggiormente ‘mirati’ nei confronti di addetti a servizi che necessitavano di particolari ulteriori nozioni formative: in tal caso sono stati gli stessi servizi a rappresentare tale esigenza, che l’Azienda, tramite consulente esterno, ha provveduto a soddisfare.

6.3.2 PIANO DI FORMAZIONE CON LABORATORI FORMATIVI

Questa attività - particolarmente utile per uniformare il lavoro degli addetti provenienti dalle diverse realtà aziendali, confrontando soluzioni precedentemente adottate - sarà il luogo ove capitalizzare quanto di positivo vi è stato nelle esperienze fatte ed evidenziare i punti deboli eventuali nel ‘sistema-privacy’. I temi oggetto di laboratorio sono:

	DENOMINAZIONE	OGGETTO	PARTECIPANTI	N.ro SEDUTE
	La Struttura di presidio, Norme, Individuazione e Modalità dei Trattamenti	• Una ricognizione delle norme Statali, Regionali, Aziendali vigenti; individuazione di ulteriori norme aziendali necessarie e predisposizione dei relativi atti di adozione. • Verifica degli adempimenti adottati • Verifica della rispondenza del modello di struttura di presidio all'organizzazione aziendale • I trattamenti in azienda • Le regole generali • Le regole in presenza di soli dati comuni; le regole in presenza di dati sensibili (non sanitari) e giudiziari; le regole in presenza di dati sanitari; • La redazione degli atti a rilevanza esterna	Gruppo Aziendale Privacy di riferimento Referenti privacy delle preesistenti Aziende Sanitarie Strutture che predispongono atti a rilevanza esterna	5
	La sicurezza dei dati	• Le misure minime di sicurezza, con particolare riferimento al **Documento Programmatico sulla Sicurezza** • Gli amministratori di sistema, alla luce dei recenti Provvedimenti Generali del Garante	Gruppo Aziendale Privacy di riferimento Referenti informatici di riferimento	3
	Le procedure amministrative	• Gestione rapporto di lavoro in ambito pubblico; la corretta tenuta dei fascicoli del personale; • le tutele dell'attività contrattualistica, dal bando al contratto; • autotutela privacy verso i fornitori di servizi; • contemperamento privacy / diritto d'accesso;	Gruppo Aziendale Privacy di riferimento Strutture amministrative: risorse umane, provveditorato, economato	5

	Le regole nella sanità; la sanità elettronica	• le regole generali indicate dal Codice Privacy nel Titolo V della Parte II (artt. 75-94) e dala prescrizione del Garante del 9 novembre 2005 (Strutture sanitarie: rispetto della dignità) • le regole specifiche in tema di: • dati genetici • sanità elettronica: Fascicolo sanitario elettronico, Dossier sanitario, Referti ondine • acquisizione consenso al trattamento dei dati	Gruppo Aziendale Privacy di riferimento Direzioni sanitarie ospedaliere, Distretti sanitari, Servizi territoriali Uffici tecnici (occasionalmente) Referenti informatici (occasionalmente) CUP (occasionalmente) Cure primarie (occasionalmente) Servizi ospedalieri coinvolti (occasionalmente)	5
	I servizi territoriali Dipendenza e Salute Mentale	• Problematicità utenti, spesso minorenni o in stato di detenzione o di libertà vigilata • Presenza di associazioni di volontariato ed altri contraenti • Le famiglie, risorsa / problema • I rapporti con Uffici giudiziari e Forze dell'Ordine • Presenza di tirocinanti	Gruppo Aziendale Privacy di riferimento Servizi per le Dipendenze Salute mentale	2
	Macchine e strumenti elettronici sul posto di lavoro	• Fotocopiatrice e stampanti • Fax e telefono • computer internet e posta elettronica • videosorveglianza, impianti di localizzazione geografica (GPS)	Gruppo Aziendale Privacy di riferimento Amministratori di sistema Risorse umane, Provveditorato. Economato, Tecnico Servizi ospedalieri coinvolti (occasionalmente)	5
	Follow up	**Manuale pratico privacy**	Gruppo Aziendale Privacy di riferimento	---

6.3.3 PIANO DI FORMAZIONE IN E-LEARNING

La piattaforma progettata si basa sul noto modello Moodle, mettendo a disposizione degli utenti le seguenti risorse:

* lezioni on-line
* forum
* gestione di contenuti
* glossari

* manuale privacy

RISORSA	OGGETTO	PARTECIPANTI
lezioni on-line	Sarà costituito dalle presentazioni oggetto di moduli in aula, che verranno pubblicate sulla piattaforma; è un modo per 'rinfrescare' saltuariamente i contenuti dei moduli formativi.	Chiunque
Il forum	È la comunità virtuale in cui gli addetti dell'Azienda potranno 'incontrarsi' sul tema della privacy. Il forum verrà utilizzato come strumento di supporto on-line dell'attività privacy che man mano verrà messa in campo con gli altri canali formativi e metterà in comunicazione i dipendenti per un confronto sul tema privacy.	Chiunque
La gestione dei contenuti	É lo spazio ove verrà inserita la documentazione rilevante, come ad esempio la normativa (statale, regionale, aziendale) le modulistiche (informative, nomine di incaricato, acquisizione di consenso e così via); si pubblicheranno anche casi tipici che man mano verranno evidenziati nel forum.	Chiunque
Glossario	Conterrà le definizioni principali dei termini in uso sia in campo privacy sia in campo informatico (per le parti rilevanti sulla normativa privacy).	Chiunque
Manuale pratico privacy	Il forum aziendale alimenterà in maniera significativa la costruzione del manuale pratico, proprio perché sarà il luogo in cui si evidenzieranno i problemi quotidianamente afrontati in tema privacy, ai quali deve esser data una 'risposta' nell'ambito del Manuale	Chiunque in lettura Gruppo Aziendale Privacy di riferimento in modalità 'modifica' e 'scrittura

7 . TRATTAMENTI EFFETTUATI IN COLLABORAZIONE CON PARTNERS ESTERNI (REGOLA 19.7)

7.1 PREMESSA

Sono molto numerose le attività svolte in collaborazione con terzi che comportano il trattamento di dati personali; talvolta si tratta di esternalizzazioni strettamente connesse con l'ordinamento stesso dell'Ente (vedasi il caso della Tesoreria), altre volte si tratta di servizi affidati all'esterno attraverso procedure ad evidenza pubblica, altre volte, infine, vi sono progetti precisi che vengono condotti in collaborazione con altre pubbliche amministrazioni o con soggetti privati. Talvolta i partner effettuano l'attività presso le proprie sedi, altre volte i soggetti dipendenti dai partner effettuano l'attività presso gli uffici dell'Ente, altre volte ancora possono verificarsi entrambe le possibilità.

7.2 ATTIVITÀ RICOMPRENDENTI TRATTAMENTI DI DATI PERSONALI AFFIDATE A SOGGETTI ESTERNI

Numerose sono le attività esternalizzate che comportanto una cospicua mole di dati personali trattati; nella tabella seguente si elencano i trattamenti censiti in cui sono coinvolti partenr esterni con indicazione della tipologia di dati trattati nonché gli estremi dei partner esterni.

7.3 MISURE DI AUTOTUTELA PER GARANTIRE L'ADOZIONE DELLE MMS DA PARTE DEI SOGGETTI ESTERNI.

Rispetto a tale problematica, l'Ente retiene di tutelarsi adeguatamente perseguendo alternativamente una delle seguenti strade:

- Nominando Responsabile dei trattamenti il soggetto partner
- Sottoscrivendo col partner un apposito protocollo d'intesa inerente la gestione e lo scambio di dati personali per la realizzazione delle finalita' istituzionali attuate in partenariato.

Nel primo caso – restando in carico all'Ente la Titolarità dei Trattamenti – il soggetto partner nominato Responsabile dei Trattamenti dovrà necessariamente adeguarsi alle policies dell'Ente stesso, a partire dal presente Documento Programmatico, e, naturalmente, il Titolare ha in ogni momento la posibilita di verificare l'adeguatezza dei Trattamenti effettuati, alla stessa stregua che nei confronti dei Responsabili interni all'Ente.
Nel secondo caso, invece, venendo a mancare lo specifico rapporto Titolare/Responsabile, le garanzie sotto il profilo 'privacy' verranno reciprocamente sottoscritte nel suddetto Protocollo d'intesa, che comprende, tra l'altro, prescrizioni circa le modalità di trattamento, le misure di sicurezza, le indicazioni sulla struttura di presidio dei Trattamenti, la facoltà dell'Ente di verificare in qualsiasi momento le attività di trattamento messe in essere dal partner.

Ai Responsabili dei Trattamenti spetterà verificare - ove ricorra - l’opportunità di nominare i partners responsabili dei Trattamenti ovvero considerarli come autonomi Titolari; nel primo caso essi segnaleranno al Titolare i partner da nominare, completi di tutti i dati necessari a circoscrivere la nomina stessa; nel secondo caso i Responsabili provvederanno alla sottoscrizione del protocollo d’intesa con i soggetti partner, avendo adottato gli schemi-tipo di protocollo.

8 . CRITERI E MODALITÀ PER LA CIFRATURA O LA SEPARAZIONE DEI DATI SANITARI E DI VITA SESSUALE DAGLI ALTRI DATI IDENTIFICATIVI (REGOLA 19.8)

Per la protezione dei dati sensibili presenti sulla singola postazione, è stato installato su ogni client il software **"AxCrypt"**

L'applicativo studiato per la difesa tramite crittografia estrema, permette di rendere inaccessibili files e cartelle presenti su hard disk, rete locale o dischi removibili.
Le operazioni basilari sono semplici e tutti gli utenti di Windows possono farne uso senza alcuno sforzo.

Alcuni utilizzi generici:

1. Rendere impossibile l'accesso ai files conteneti dati sanitari sul proprio PC, si tratti di immagini, documenti, email, archivi, programmi o qualsiasi altro formato rappresentabile con un file.
2. Proteggere singoli files prelevati da posizioni diverse su hard disk o rete locale, con un solo click.
3. Trasportare files importanti senza il timore che la perdita o il furto del supporto fisico, sia esso un disco magnetico, ottico o un notebook.
4. Comunicazione tra due o più sedi con la certezza che il passaggio via Internet di un'email contenente informazioni o programmi non possa essere usata in caso di intercettazione.
5. Distruzione di files in modo che non siano recuperabili con gli appositi software.

INDICE