REGIONE BASILICATA

UFFICIO S. I. R. S.

Misure di Sicurezza Adottate

Sistema Informativo per la Formazione e l'Orientamento Professionale

SIRFO < Ver. 2.8.5>

REGIONE BASILICATA

DIPARTIMENTO PRESIDENZA DELLA GIUNTA REGIONALE
UFFICIO SISTEMA INFORMATIVO REGIONALE E STATISTICA

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Controllo del documento

Identificazione documento

Titolo	Tipo	Identificatore	Nome *file*
<Titolo dell'intervento>	Misure di Sicurezza Adottate	<MSXXXXX1.0>	<71AM_XXXXX_Misure di Sicurezza Adottate_061109>

Approvazioni

	Nome	Data	Firma
Redatto da:			
Revisionato da:			
Approvato da:			

Variazioni

Versione	Data	Autore	Paragrafi modificati

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Distribuzione

Copia No.	Nome	Locazione
1		
2		
3		
4		
5		
6		

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Indice

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

1. Introduzione

Il presente documento si prefigge l'obiettivo di individuare e gestire i rischi correlati alla gestione e utilizzo del Sistema Informativo "SIRFO" di proprietà dell'Ente, al fine di assicurarne l'affidabilità determinando opportune azioni che abbiano la capacità di garantire disponibilità, integrità e riservatezza delle informazioni trattate, nonché l'autenticità dei dati presenti sul sistema.

Il presente documento è stato redatto in accordo con le linee guida stabilite dal CNIPA in materia di sicurezza dei sistemi informativi automatizzati presenti nella Pubblica Amministrazione e in conformità alle direttive emanate dalle norme ISO/IEC 27001:2005 ed ISO/IEC 17799:2005 in materia di "sistemi di gestione per la sicurezza delle informazioni", e alle norme previste dal Decreto Legislativo 30 giugno 2003, n.196.

1.1 Scopo del Documento

Obiettivo primario del presente documento è quello di specificare le misure adottate, o da adottare, per assicurare che il Sistema Informativo "SIRFO" in dotazione all'Ente sia munito di appropriati controlli di sicurezza atti a fornirne adeguata protezione, secondo le linee guida sopra indicate.

A tale scopo si procederà :

- all'identificazione delle risorse da proteggere
- all'analisi dei rischi a cui possono essere soggette dette risorse
- alla indicazione di un piano operativo che comprenda misure di sicurezza fisica e logica.

1.2 Definizioni ed Acronimi

Lista e descrizione delle definizioni e degli acronimi.

Acronimo	Significato
SIA	Sistema Informativo Automatizzato
PA	Pubblica Amministrazione

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

1.3 Riferimenti

Il presente documento è stato redatto seguendo le linee guida emanate dal CNIPA (Linee guida per la sicurezza ICT delle Pubbliche Amministrazioni - Marzo 2006) le quali fanno riferimento a differenti leggi, decreti ministeriali e direttive fra le quali il D.lgs. n° 196 del 2003 (art. 31-36) che disciplina il trattamento dei dati personali.
Inoltre, come già detto, il presente documento segue anche le direttive emanate dalle norme ISO/IEC 27001:2005 ed ISO/IEC 17799:2005 in materia di "sistemi di gestione per la sicurezza delle informazioni".

1.4 Overview

Il presente documento riporterà la politica di sicurezza adottata per la protezione dell'applicativo "SIRFO", ed una serie di indicazioni per la protezione o risoluzione dei problemi generati da minacce relative ai rischi possibili.

Il documento è suddiviso in sezioni, corrispondenti alle varie risorse prese in esame, e alle tipologie di rischio da contrastare.

Le varie sezioni del documento comprenderanno una parte generale in forma descrittiva e una serie di tabelle in cui sono riportate le informazioni più in dettaglio.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

2. Identificazione Risorse da Proteggere

Per un dato Sistema Informativo, e in particolare per il "SIRFO", le risorse da esaminare e mettere in sicurezza sono essenzialmente:

- hardware (computer, supporti magnetici, apparecchiature in genere)
- software (Sistemi Operativi, Database, Applicazioni)
- dati gestiti dal sistema
- personale dell'Ente o esterno

La necessaria fase propedeutica ad ogni possibile scelta di un'adeguata politica di security consiste in un censimento dei beni da proteggere, e nell' individuazione delle possibili cause di rischio e delle vulnerabilità e minacce cui potrebbero essere soggetti.

2.1 Identificazione Risorse Hardware

Il Sistema Informativo "SIRFO" è realizzato secondo uno schema di tipo client-server, nel quale i dati sono memorizzati nel Database che si trova nel server localizzato nel Data Center al P.T. del Palazzo della Giunta, e gli utenti vi accedono collegandosi dai propri computer tramite l'applicativo appositamente realizzato. Questa struttura è stata realizzata per rendere più veloci le operazioni di elaborazione da parte di utenti di vari uffici distribuiti sul territorio regionale.

In questo documento si tratterà delle problematiche di sicurezza delle apparecchiature poste nel Data Center, sulle quali si trovano i dati oggetto dei trattamenti, ai quali accedono gli utenti opportunamente autorizzati. Per i client dei vari uffici si rimanda alle procedure di sicurezza adottate localmente.

In questa sezione saranno riportate accurate informazioni riguardanti le caratteristiche delle macchine censite. A tal fine sono state predisposte due distinte tabelle. Nella prima saranno inserite informazioni relative all'hardware, alla tipologia e alla connessione in rete della macchina censita; nella seconda, invece, saranno riportate informazioni inerenti i dispositivi di protezione attivati sulla macchina.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Scheda Risorsa Hw n. 01 - Dati Generali	
Serial Number Hardware	
Descrizione Macchina	Etichetta: SIRFO Nome macchina: SSIRFO Contatti: ing. Nicola Scandiffio (Lucana Sistemi) d.ssa Enza Lionetti (Regione Basilicata)
Produttore	generico
Modello	IBM compatibile - (minitower)
Quantità	1
Caratteristiche Tecniche	N. 2 alimentatori
Ubicazione	Locale Data Center – Palazzo Giunta – P.T. – Collocato su scaffale in ferro
Indirizzo IP	172.16.30.13 / 255.255.255.0 172.17.1.101 / 255.255.240.0 (non utilizzato) Gateway: 172.16.30.64 DNS: 172.16.1.1 / 172.16.1.2
Descrizione Servizi Forniti	Database Server per Procedura SIRFO

Configurazione Hardware		
Ram Mb	1GB	
Processori	4 Processori Xeon da 500 Mhz	
Hardisk Gb	N. 3 HD	Capacità 1° disco 10GB
		Capacità 2° disco 10GB
		Capacità 3° disco 10GB
Livello RAID	RAID5	
Device	Floppy / CD-rom	

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

(dat/floppy/cd-rom)	
Tipologia Sistema	Singolo
Tipo File System	NTFS
Sistema Operativo	Windows NT Server 4.0 S.P. 6a

Tipologia			Note-Descrizione
Server	SI		
Client		NO	
Altro		NO	

Connessione in Rete			Note-Descrizione
Pubblica		NO	
Privata	SI		
Assente		NO	

Dispositivi di Protezione Attivati			
Dispositivi	Presenti		Note-Descrizione
Password	SI		L'accesso è controllato tramite UserID e pw
Antivirus	SI		Installato e aggiornato automaticamente dal CTR
Altro Dispositivo	SI		Doppio Alimentatore

Componenti di Rilievo Presenti ai fini della Sicurezza dei Dati	
Componente	Descrizione

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Scheda Risorsa Hw n. 02 - Dati Generali	
Serial Number Hardware	generico
Descrizione Macchina	Client SIRFO
Produttore	generico
Modello	Classe PENTIUM IV
Quantità	
Caratteristiche Tecniche	generiche
Ubicazione	Generica
Indirizzo IP	Indirizzo Classe RUPAR
Descrizione Servizi Forniti	Accesso a Database SIRFO

Configurazione Hardware		
Ram Mb	512Mb	
Processori	1 Processore da 1,4 Ghz	
Hardisk Gb		Capacità 1° disco
		Capacità 2° disco
Livello RAID	Non richiesto	
Device (dat/floppy/cd-rom)	Floppy / cd-rom	
Tipologia Sistema	Singolo	
Tipo File System	NTFS	
Sistema Operativo	Windows 2000 / XP	

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Tipologia			Note-Descrizione
Server		NO	
Client	SI		
Altro		NO	

Connessione in Rete			Note-Descrizione
Pubblica		NO	
Privata	SI		
Assente		NO	

Dispositivi di Protezione Attivati			
Dispositivi	Presenti		Note-Descrizione
Password	SI		
Antivirus	SI		
Altro Dispositivo		NO	

Componenti di Rilievo Presenti ai fini della Sicurezza dei Dati	
Componente	Descrizione

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

2.2 Identificazione Software

I software utilizzati comprendono sistemi operativi, gestori di database e applicazioni. In particolare sono presenti:

Server Data Center:

- Sistema Operativo: Windows NT Server 4.0 S.P. 6a
- Database: RDBMS Oracle 8

Client:

- Sistemi Operativi: Windows 2000 / XP
- Applicativo: Procedura SIRFO ver.2.8.5
- Client ORACLE per eseguire l'Applicazione

Scheda Risorse Sw : SIRFO (Base)	
Id Software	01
Descrizione Software	Sistema Operativo Windows NT Server 4.0 S.P. 6a
Number Licenza d'Uso	
Responsabile della Procedura	ing. Nicola Scandiffio (Lucana Sistemi) ing. Francesco D'Ercole (Lucana Sistemi) CTR
Serial Number Hardware	

Tipologia Software			Note-Descrizione
Base	SI		
Ambiente		NO	
Applicativo		NO	

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Scheda Risorse Sw : SIRFO (Ambiente)	
Id Software	02
Descrizione Software	RDBMS Oracle 8
Number Licenza d'Uso	
Responsabile della Procedura	ing. Francesco D'Ercole (Lucana Sistemi) ing. Nicola Scandiffio (Lucana Sistemi) d.ssa Cristina Mangia (Lucana Sistemi)
Serial Number Hardware	

Tipologia Software			Note-Descrizione
Base		NO	
Ambiente	SI		
Applicativo		NO	

Scheda Risorse Sw : SIRFO (Applicativo)	
Id Software	03
Descrizione Software	Procedura SIRFO – Sistema Informativo del Dipartimento Formazione della Regione Basilicata – ver.2.8.5
Number Licenza d'Uso	
Responsabile della Procedura	ing. Francesco D'Ercole (Lucana Sistemi) ing. Nicola Scandiffio (Lucana Sistemi) d.ssa Cristina Mangia (Lucana Sistemi) d.ssa Enza Lionetti (Regione Basilicata)
Serial Number Hardware	vari

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Tipologia Software			Note-Descrizione
Base		NO	
Ambiente		NO	
Applicativo	SI		ver.2.8.5

2.3 Identificazione Dati

Questa sezione sarà dedicata al rilevamento dei dati trattati dal sistema informativo in oggetto, con riferimento anche alla presenza di dati personali. A tale scopo è stata predisposta la tabella "Natura dei Dati Personali Presenti in Archivio", in cui sarà specificata la natura dei suddetti dati.

Questa sezione sarà completata da una tabella atta a contenere informazioni relative agli strumenti di backup e alle politiche di backup connesse.

I dati gestiti all'interno del "SIRFO" riguardano le informazioni inserite dagli utenti relative a Gestione e Monitoraggio di Corsi di Formazione per progetti a finanziamento regionale, nazionale, e comunitario. Tali informazioni sono di carattere anagrafico, economico, fisico e procedurale utili per effettuare il monitoraggio da parte della Regione Basilicata e del Ministero dell'Economia e delle Finanze e la rendicontazione all'Unione Europea.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Scheda Risorsa Dati n. 01	
Identificativo Data Base	SIRFO
Denominazione Data Base	SIRFO
Descrizione Data Base	Sistema Informativo per la Formazione e l'Orientamento Professionale
Riferimento Normativo	POR 2000-2006
Finalità Istituzionale	Gestione e Monitoraggio di Corsi di Formazione – Rendicontazione per la Regione, il Ministero dell'Economia e delle Finanze, l'Unione Europea
Serial Number Hardware	
Condivisione Data Base	Condivisione tramite rete locale Intranet per inserimento, modifica, cancellazione, e trattamento in genere da parte di personale autorizzato interno ed esterno all'Ente (Dipendenti Regionali, della Provincia ed Agenzie provinciali – Ageforma, Apof) - Le Società che organizzano i corsi possono inserire dati presso la propria sede, inviandoli via e-mail al sistema centrale, consultare via Internet i datigenerali (ciascuna quelli che la riguardano), ma non agire direttamente sul DB.
Livello di Criticità dei Dati	Alto (**N.B.:** indicativo del valore che l'Ente attribuisce ai dati.)
DBA	Marcello Ugliano – Dip. Presidenza della Giunta Regione Basilicata

Tipologia Data Base			Note-Descrizione
Archivio Cartaceo	SI		Fatture, Registri Presenze, Rendiconti finali
Archivio Elettronico	SI		Dati per Gestione e Monitoraggio Corsi Formazione

Dati Personali			Note-Descrizione
Persone Fisiche	SI		Dati anagrafici, e in parte anche dati sensibili/giudiziari
Persone Giuridiche	SI		Dati generali
Enti	SI		Dati generali

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Associazioni	SI		Dati generali

Natura dei Dati Personali Presenti in Archivio	
Dati	Natura dei Dati
Origine Razziale ed Etnica	Sensibili
Convinzioni Religiose-Appartenenza ad organizzazioni di carattere religioso	Assenti
Opinioni Politiche-Adesione a Partiti o Organizzazioni a Carattere Politico	Assenti
Adesione a Sindacati o Organizzazioni a Carattere Sindacale	Assenti
Dati di Identificazione Personale: Codice Fiscale, Nominativo, Indirizzo	Comuni
Dati Relativi a Famiglia e Situazioni Particolari	Comuni
Istruzione e Cultura	Comuni
Beni, Proprietà, Possessi	Assenti
Stato di Salute	Sensibili
Informazioni Relative a Provvedimenti Giudiziari di cui all'Art. 686 del Codice di Procedura Penale	Giudiziari

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Strumenti e Politiche di Backup			
Dispositivo di Backup: Tape Library			
Presente		Modello	Frequenza del Backup
SI		IBM-3582 (Sw IBM Tivoli TSM)	Giornalmente si effettuano in modo automatico 2 export di ORACLE; - uno viene memorizzato su un HD di un altro server localizzato anch'esso nel Data Center (Server Borse); viene conservato un export per ogni giorno della settimana, e poi viene man mano sovrascritto nella settimana seguente. - L'altro è trasferito via ftp in una cartella appositamente creata su un Disco (da 300 Gb) del server MngBackup, al quale è collegata la libreria automatizzata, e sul quale è installato il Sw IBM Tivoli Storage Manager che gestisce i Backup. In questa cartella ogni giorno il nuovo export sostituisce il precedente. I Backup eseguiti con questo Sw sono schedulati, in modo che venga effettuato automaticamente un backup ogni giorno. Dei Backup eseguiti da Tivoli si conservano inoltre due versioni, una attiva ed una inattiva, in modo da conservare i dati completi di due giorni. Un altro Backup viene effettuato mensilmente, ed anche di questo si conservano due versioni.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Incaricati del Backup	
Ente/Società	Nominativi
Regione Basilicata	Marcello Ugliano
Lucana Sistemi s.r.l.	Ing. Viti – Ing. Scandiffio

Supporti di Backup		
Numero di Supporti	Dicitura Etichetta-Descrizione	Note
2 HD da 300Gb Fino a 24 nastri da 200/400Gb		Tutti i Backup sono memorizzati sia sui 2 dischi da 300Gb installati sullo stesso server, che in copia sui nastri nella libreria ad esso collegata. La libreria contiene fino a 24 nastri da 200/400Gb. La gestione dei dati nei dischi e nei nastri viene effettuata dallo stesso Sw Tivoli, che ne memorizza la collocazione in un suo database, del quale viene effettuato un apposito salvataggio due volte al giorno.

]

2.4 Identificazione Risorse Professionali

Appartengono a questa categoria quanti a diverso titolo interagiscono con il Sistema Informativo durante l'arco di vita dello stesso.

E' importante identificare le strutture interne ed esterne, e relative figure professionali interagenti con il S.I.

I dati dovranno essere organizzati nelle tabelle predisposte a contenerli, in modo che ad ogni ufficio sia associata la lista delle risorse interne e ad ogni società esterna risulti associata la lista delle risorse esterne che a vario titolo si occupano del S.I.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Gli utilizzatori dell'applicativo "SIRFO" si possono suddividere in categorie di cui segue la descrizione:

- Amministratore: utenti che hanno la possibilità di agire sull'intera base dati, inoltre sono gli unici abilitati alla creazione di nuove utenze applicative;
- Autorità di Controllo II° Livello: utenti che possono effettuare controlli a campione sulla base dati per effettuare eventuali comunicazioni di irregolarità compiute sui progetti alla Comunità Europea;
- Autorità di Pagamento: utenti che attingono i dati economici della base dati per effettuare le richieste di importi di finanziamento alla Comunità Europea (domande di pagamento);
- Responsabile di Misura: utenti responsabili della validazione dei dati inseriti dagli utenti di base;
- Utente Base: utenti che inseriscono le informazioni riferite all'istruzione della pratica di progetto;
- Utente Ente Esterno: utenti che istruiscono le pratiche di progetto all'interno degli enti periferici di appartenenza come le province, o le agenzie provinciali

Le categorie sopraindicate si distribuiscono in tre aree fisicamente distinte:

- Regione Basilicata: utenti presenti all'interno delle costruzioni ubicate in Potenza, presso gli edifici in via Anzio, nonché presso le sedi di Melfi, Lagonegro, Matera, Metaponto
- Territorio Regionale: utenti presenti all'interno degli enti periferici come le province, o le agenzie provinciali
- Lucana Sistemi s.r.l.: utenti che si occupano della manutenzione correttiva ed evolutiva dell'applicativo presenti nella sede della società fornitrice.

Gli utenti Amministratori interni ed esterni, che provvedono alla gestione del Sistema, stabilendo incarichi e profili per il trattamento dei dati, effettuando operazioni di controllo e monitoraggio, o che provvedono alla manutenzione correttiva ed evolutiva dell'Applicativo, sono riportati nelle tabelle seguenti.

Per le altre categorie di utenti esistono appositi elenchi gestiti e conservati dalla D.ssa Lionetti, in qualità di Amministratore del S.I., presso gli uffici del Dipartimento Formazione della Regione Basilicata.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Identificazione Risorse Professionali Interne						
Struttura di Appartenenza 1	Ente	Dip.	Ufficio	Servizio	Struttura	Funzione
	Regione Basilicata	Presidenza della Giunta	Ufficio Sistema Informativo Regionale e Statistica			
Risorse	Matricola		Cognome	Nome		Funzione Svolta
			Ugliano	Marcello		DBA
.						
.						
Struttura di Appartenenza 2	Ente	Dip.	Ufficio	Servizio	Struttura	Funzione
	Regione Basilicata	Formazione				
Risorse	Matricola		Cognome	Nome		Funzione Svolta
			Lionetti	Enza		Amministratore
			Giorgio	Francesco		Amministratore

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Identificazione Risorse Professionali Esterne						
Società di Appartenenza 1	Denom. o Rag. Sociale	Indirizzo Sede Legale	Rappresentante Legale	Rif. Contratto n. rep	Data	Funzione
	Lucana Sistemi s.r.l.	Via Cicerone 13 Matera	D'Ercole Cosimo			Assistenza SIRS

Risorse	Cognome	Nome	Funzione Svolta
	D'Ercole	Francesco	Responsabile Progetto
	Scandiffio	Nicola	Analista - Sviluppatore
	Mangia	Cristina	Analista - Sviluppatore

.

.

Società di Appartenenza n	Denom. o Rag. Sociale	Indirizzo Sede Legale	Rappresentante Legale	Rif. Contratto n. rep	Data	Funzione

Risorse	Cognome	Nome	Funzione Svolta

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

2.5 Identificazione Documentazione Cartacea

Questa sezione riguarda tutta la documentazione relativa all'hw, ai programmi, ai sistemi, alle procedure di gestione ecc.
Tali beni sono sottoposti a minacce quali la loro alterazione e/o distruzione ad opera di eventi naturali, di azioni accidentali e di comportamenti intenzionali.
Vanno quindi conservati in luoghi sicuri.

Identificazione Documentazione Cartacea									
Riferimenti Document.	Cod.Uff	Ufficio	Identificatore Doc.	Titolo Doc.	Autori	Creazione	Ultimo Agg	Paragrafi Modificati	Num. Copie

Distibuzione	Copia Num.	Assegnatario	Locazione

N.B. La Versione del documento è contenuta nell'Identificatore del documento

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

2.6 Identificazione Supporti di Memorizzazione

In questa sezione, invece, si provvederà ad identificare i supporti di backup, relativi al S.I. preso in esame, i responsabili dell'operazione di backup, e gli incaricati della custodia del supporto.

Identificazione Supporti di Memorizzazione								
Riferimenti Supporto	Cod.Uff.	Ufficio	Identificatore Supp.	Etichetta	Tipo Supporto	Data Salvataggio	Responsabile Salvataggio	Num. Copie
Custodia	Incaricato		Ubicazione Conservazione Copia		Altra Localizzazione Esterna			

Come già descritto in precedenza, tutti i Backup sono memorizzati sia su 2 dischi da 300Gb installati sullo stesso server ove si trova il Sw IBM Tivoli Storage Manager che li esegue, che in copia sui nastri nella libreria ad esso collegata.
La libreria contiene fino a 24 nastri da 200/400Gb.
La gestione dei dati nei dischi e nei nastri viene effettuata dallo stesso Sw Tivoli, che ne memorizza la collocazione in un suo database, del quale viene effettuato un apposito salvataggio due volte al giorno.
Non esiste quindi un supporto specifico legato ad un dato Backup, individuabile con una sua etichetta, ma è possibile solo individuare, in un file di testo, l'etichetta dei nastri utilizzati per il backup del database interno ove sono memorizzate le informazioni sulla localizzazione dei dati salvati. Anche questo file viene a sua volta salvato due volte al giorno.
Poiché sia il server che gestisce i Backup, che contiene una copia dei dati salvati, che la libreria con i nastri, che contiene la seconda copia, sono localizzati nel Data Center dove sono anche buona parte dei server con i dati originali, in caso di danneggiamento che colpisca tutto l'armadio in cui sono allocati, o l'intero locale, potrebbero essere danneggiati anche i Backup. Sarebbe consigliabile spostare dette apparecchiature dedicate al Backup in un altro ambiente opportunamente protetto ed isolato dai dati originali.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

3. Analisi dei Rischi

Dopo aver effettuato il censimento dei beni, si procederà ad individuare minacce e vulnerabilità a cui sono sottoposte le risorse.

Le tre macrocategorie sulle quali sarà effettuata l'analisi sono quelle relative a risorse hardware, software, dati.

I livelli di rischio sono fissati mediante una scala qualitativa a tre valori i cui significati sono riportati nella tabella sottostante.

Rischio:	
Livello	**Significato**
Basso	Rischio basso, minaccia remota e facilmente reversibile
Medio	Rischio superiore al precedente, associato anch'esso ad una minaccia remota, il cui verificarsi, però, ha effetti non facilmente reversibili ed eliminabili. E' auspicabile predisporre opportune ed adeguate misure di sicurezza atte a contenere il rischio.
Alto	Rischio elevato, inaccettabile pensare di correrlo. Dovrà essere pensato ed attivato un insieme di contromisure, capace di abbattere il rischio al fine di contenerlo entro livelli ritenuti accettabili

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

3.1 Risorse Hardware

Fine della sicurezza fisica è quello di proteggere persone ed hardware coinvolti nel funzionamento del sistema informativo. In particolare occorre definire le politiche di salvaguardia dei computer, server e client, e degli impianti di supporto quali rete, alimentazione e condizionamento.

Analisi Rischi: Risorse Hardware		
Risorsa	Server SIRFO	
Elemento di Rischio	Livello di Rischio	Note-Motivazione
Uso non Autorizzato	Basso	L'accesso al server è protetto per mezzo di UserID e password gestiti dal CTR in quanto il server fa parte del Dominio regionale; L'applicativo SIRFO inoltre ha una propria gestione degli accessi sia per l'amministrazione che per le utenze.
Manomissione/Sabotaggio	Basso	L'accesso al locale Data Center è consentito solo al personale interno ed esterno autorizzato e presente in una apposita lista
Frequenza/Probabilità di Guasto	Medio	Pc IBM Compatibile non recente
Deterioramento Supporti di Memoria	Medio	Presenza di 3 HD in RAID5, con buona possibilità di ricostruzione dei dati eventualmenta danneggiati, ma non di tipo HOT-SWAP, e quindi non immediatamente sostituibili in caso di guasti senza interruzione del servizio

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Intercettazione della Trasmissione	Basso	La trasmissione dei dati di backup avviene solo tra la zona DMZ in cui si trova il server SIRFO e quella MZ in cui è invece il server di Backup. I dati gestiti dal Sistema nel DataBase sono trasmessi comunque solo sulla rete interna (CAMPUS/VPN), e non via INTERNET.
Rischi Connessi all'Elettricità	Medio	Il server Sirfo non è inserito in un armadio Rack, ma su uno degli scaffali metallici, per cui la sua alimentazione è fornita da una sola linea, protetta dal generatore generale; perciò, pur essendo dotato di alimentatori ridondanti, non è sufficientemente protetto in caso di interruzione della linea.
Furto	Basso	Il locale del Data Center in cui si trova il server SIRFO, pur non avendo porte blindate o inferriate alle finestre, può essere considerato abbastanza sicuro, per la sua posizione controllata con facilità dalla Vigilanza, e comunque ha accessi chiusi e muniti di serrature di sicurezza ed elettriche con Badge.
Rischi Connessi a Variazioni di Temperatura (Guasto Climatizzatore/Umidità Eccessiva)	Basso	Il server SIRFO è in un ambiente il cui condizionamento è assicurato da due condizionatori, e controllato da opportuni sensori che rilevano eventuali anomalie, allertando se necessario la Vigilanza
Azione di Virus Informatici (Codici Maligni)	Basso	Presenza di Antivirus installato dal CTR e aggiornato automaticamente

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

3.2 Risorse Software

In questa sezione si esamineranno gli elementi di rischio e i relativi livelli di rischio a cui sono sottoposte le risorse software

Analisi Rischi: Risorse Software		
Risorsa	Sw Applicativo SIRFO	
Elemento di Rischio	Livello di Rischio	Note-Motivazione
Accesso non Autorizzato alle Basi Dati Connesse	Basso	Il software che tratta i dati controlla l'accesso tramite una finestra di autenticazione (finestra di Login). L'accesso è consentito solo ad Utenti autorizzati con UserID e password specifici assegnati a ciascuno
Errori Software che Minacciano l'Integrità dei Dati	Basso	L'applicativo SIRFO viene rilasciato, dopo opportuni test, in versioni consistenti. Eventuali malfunzionamenti di cui si venga a conoscenza sono immediatamente corretti da nuove versioni del sw, oppure mediante patch.
Presenza di Codice non Conforme alle Specifiche del Programma	Basso	Tutte le funzionalità che compongono l'applicativo sono state analizzate, progettate e realizzate secondo le specifiche.
Mancanza Autenticazione Utente	Basso	Gli utenti autorizzati, quando accedono all'Applicativo, lo fanno dopo essersi autenticati, con un proprio identificativo e password.
Mancanza Logging degli Accessi	Basso	Una registrazione degli accessi non avviene nel momento in cui si accede, ma in seguito alla effettuazione di qualche operazione sui dati. In questo caso si memorizza data, ora, utente, operazione

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

		effettuata.
Errori Software Noti	Basso	Il software è in continua evoluzione e manutenzione, per ovviare ad eventuali problemi e/o segnalazioni
Cattiva Gestione Password	Medio	Inizialmente viene fornita ai nuovi utenti una password di default, che deve essere obbligatoriamente cambiata dagli stessi utenti al primo accesso. Non vi sono vincoli particolari di lunghezza, complessità, durata per la creazione delle password. Gli utenti dovrebbero essere istruiti su come creare e/o modificare le password in base ai criteri di sicurezza.
Diritti di Accesso Scorretti	Basso	Gli utenti autorizzati, quando accedono all'Applicativo assumono dei ruoli predefiniti, assegnati e /o modificati secondo la necessità dall'Amministratore del Sistema Informativo, e per ciascuno dei quali sono consentite operazioni specifiche sui dati (lettura, modifica, cancellazione, ..)
Uso del Software Incontrollato		
Sessioni Aperte senza Presenza Utente	Medio	Al software presente sul server si accede soltanto per motivi di manutenzione, e inoltre il server è in un ambiente protetto, con salvaschermo automatico a tempo, disattivabile con password. Non esistono particolari precauzioni sui client in caso di allontanamento

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

		dell'utilizzatore a sessione aperta, a meno che non siano impostate dall'utente stesso per il proprio PC. Tutti gli utenti devono essere adeguatamente formati sulle procedure di lavoro in sicurezza.
Assenza di Backup	Alto	L'assenza dei backup del database comprometterebbe la possibilità di utilizzo dell'applicativo dopo un danneggiamento. Vengono pertanto adottate le seguenti contromisure: - Server: Export di Oracle e Backup regolarmente effettuati ogni giorno in più copie su supporti diversi (dischi e nastri), anche se localizzati negli stessi locali del Data Center. - Client: E' sufficiente la reinstallazione del software da parte dell'azienda fornitrice
Carenza nella Dismissione dei Supporti	Medio	Il personale che effettua l'assistenza deve essere istruito affinchè i supporti magnetici contenenti i dati siano resi del tutto inutilizzabili prima di dismetterli.
Uso Illegale di Password	Basso	Le password sono memorizzate nel database in forma non leggibile. Le password sono personali, impostate direttamente dai singoli utenti (eccetto che per l'amministrazione del DataBase), e non dovrebbero essere portate a conoscenza di altri, o conservate in luoghi facilmente accessibili.
Installazione/Copia Illegale del Software	Basso	L'applicazione necessita di un particolare ambiente (Oracle)

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

		che di per sé ha una notevole complessità e sistemi di sicurezza (utenti e password). Non è quindi utilizzabile per semplice copia, e necessita di specifiche conoscenze per l'installazione, e UserID e password per la gestione dei dati.
Furto di Credenziali di Autenticazione	Medio	Gli utenti devono essere opportunamente istruiti per diminuire questo rischio. La sottrazione delle credenziali di qualsiasi utente consente al malintenzionato di conoscere, modificare o eliminare i dati di competenza di quella particolare utenza. In caso di emergenza si possono ripristinare i dati utilizzando i backup, controllare i log delle operazioni effettuate, e modificare le credenziali sottratte.
Comportamenti Sleali o Fraudolenti	Basso	Il personale che si occupa della gestione ed amministrazione e gli utilizzatori fanno parte di dipartimenti ed uffici regionali, o di società esterne ben note all'Ente e considerate affidabili. In ogni caso sono inclusi negli appositi elenchi delle persone autorizzate, perciò sono tutti univocamente identificabili e inoltre tutte le operazioni effettuate sono rintracciabili.
Errore Umano nella Gestione della Sicurezza Fisica	Medio	Questo tipo di rischio è sempre possibile, ma si cerca di minimizzarlo con opportuna formazione del personale autorizzato.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

3.3 Risorse Dati

In questa sezione si esamineranno gli elementi di rischio e i relativi livelli di rischio a cui sono sottoposte le risorse dati

Analisi Rischi: Risorse Dati		
Risorsa	Banca Dati SIRFO	
Elemento di Rischio	Livello di Rischio	Note-Motivazione
Accesso non Autorizzato	Basso	Il software che tratta i dati controlla l'accesso tramite una finestra di autenticazione (finestra di Login). L'accesso è consentito solo ad Utenti autorizzati con UserID e password specifici assegnati a ciascuno
Cancellazione o Modifica non Autorizzata dei Dati	Basso	Gli utenti autorizzati, quando accedono all'Applicativo assumono dei ruoli predefiniti per ciascuno dei quali sono consentite operazioni specifiche sui dati (lettura, modifica, cancellazione, ..)
Perdita di Dati	Basso	Esecuzione di Copie giornaliere di salvataggio dei dati (export di Oracle) e Backup automatizzati, collocati su HD di server diversi da quello ove si trovano i dati originali, e su nastri (nello stesso locale).
Assenza di Backup	Basso	Il Backup dei dati viene effettuato giornalmente e mensilmente in duplice copia su dischi e nastri per mezzo del Sw IBM Tivoli, e vengono

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

		conservati i dati di due backup consecutivi. Gli export di Oracle conservano i dati di una settimana.
Impossibilità di Ripristinare Copie di Backup	Medio	Non sono pianificati test di ripristino dei dati, ma i salvataggi sono effettuati su supporti diversi, sia HD che nastri.
Grant/Ruoli Assegnati in Maniera Impropria	Basso	Gli utenti autorizzati, quando accedono all'Applicativo assumono dei ruoli predefiniti, assegnati e /o modificati secondo la necessità dall'Amministratore del Sistema Informativo
Furto Supporti	Basso	I server che contengono i dati originali e di Backup, e la libreria automatizzata che contiene i nastri di Backup, sono collocati in locali chiusi ad accesso limitato a personale autorizzato, e controllati dalla vigilanza.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

4. Piano Operativo

Definite quali sono le risorse da proteggere si può procedere con la stesura di un piano operativo che evidenzia tutte le azioni e le misure in essere e da adottare (policy di sicurezza) per garantire la sicurezza del Sistema Informativo.

Tale piano operativo consente di determinare l'insieme delle contromisure di natura fisica e logica ed organizzativa più idonee per il conseguimento dell'obiettivo prefissato.

4.1 Sicurezza Fisica

Fine della sicurezza fisica è quello di proteggere persone ed hardware coinvolti nel funzionamento del sistema informativo. In particolare occorre definire le politiche di salvaguardia dei computer, server e client, e degli impianti di supporto quali la rete.

Sicurezza Fisica: Misure Adottate	
Descrizione Misura	Note per la Corretta Applicazione
Custodia/Accesso Archivi Cartacei	Non vi sono documenti cartacei contenenti dati personali. La Documentazione tecnica relativa all'Applicativo "SIRFO" è conservata presso la Lucana Sistemi s.r.l. ed è stata consegnata in copia agli amministratori del sistema presso il Dipartimento Formazione della Regione Basilicata.
Custodia/Accesso Supporti Magnetici	I supporti utilizzati per l'attività di backup sono HD collocati nel server che gestisce detta attività, e nastri posti nella libreria automatizzata IBM-3582 ad esso collegata, nei locali del Data Center. Per ottenere una maggiore sicurezza sia il server che la libreria dovrebbero essere collocati in un altro ambiente, anch'esso ben protetto. Tale intervento sarebbe in linea con i requisiti della ISO/IEC 27001:2005 (A.10.5.1) in materia di "sistemi di gestione per la sicurezza delle informazioni".
Accesso Fisico ai Locali	Il personale autorizzato interno ed esterno accede al Data Center principalmente attraverso i locali del CTR, quindi utilizzando un Badge magnetico per aprire una porta dotata di serratuta elettrica. Per le pulizie e situazioni particolari o di emergenza è possibile accedere tramite una porta sul corridoio con chiavi in possesso della vigilanza.
Dispositivi Antincendio	I locali della sede sono dotati di allarme antincendio che allerta la vigilanza in caso di necessità.
Continuità Alimentazione Elettrica	Il Server è dotato di alimentatori ridondanti, collegati ad una stessa linea di alimentazione proveniente dal gruppo di continuità generale dell'edificio. Per maggiore sicurezza

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	occorrerebbe avere linee di alimentazione separate.
Verifica leggibilità supporti di Backup	Non si effettuano test di leggibilità dei supporti di backup a scadenze prestabilite. Detti test dovrebbero essere effettuati ogni due o tre mesi

Le tabelle riportate di seguito servono a particolareggiare aspetti rilevanti inerenti le policy intraprese dall'Ente a garanzia della sicurezza fisica.

Sicurezza Fisica: Gestione Backup

Organizzazione dei Job di Backup - Alternanza e Periodicità dei Salvataggi

Giorno (della Settimana)	Job Name	Server	Tipo Backup	Cadenza Temporale	Posizione Copia 1	Posizione Copia 2	Start	Periodo Conservazione
Dal Lunedì al Sabato	BACKUP _GIORN_ FTP	MNGBAC KUP	Full, con Sw Tivoli	Giornaliero	n.2 HD da 300Gb sullo stesso server	Nastri nella libreria IBM3582 collegata al server di Backup	Ore 6:00	Due giorni
Domenica	BACKUP _MENS_ FTP	MNGBAC KUP	Full, con Sw Tivoli	Mensile	n.2 HD da 300Gb sullo stesso server	Nastri nella libreria IBM3582 collegata al server di Backup	Ore 5:00	Due mesi
Dal Lunedì al Sabato		SIRFO	Export Oracle	Giornaliero	HD su Server Borse		Ore 23:00	Sette giorni

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Sicurezza Fisica: Accesso ai Locali	
Personale Esterno	
	Procedura d'Accesso
Server	1)Si effettua il Riconoscimento e l'iscrizione nell'elenco del personale autorizzato 2) Il Badge consegnato è personale e va custodito con cura per tutta la durata dell'autorizzazione 3)E' consentito accedere ai locali soltanto per il tempo necessario allo svolgimento della propria attività 4) Il Badge va restituito al termine del periodo contrattuale 5) I permessi di accesso alle aree sicure dovrebbero essere regolarmente rivisti e aggiornati, e revocati quando necessario o non più utili.
Postazioni di Lavoro	
Personale Interno	
	Procedura d'Accesso
Server	1) Iscrizione nell'elenco del personale autorizzato 2) Accesso ai locali tramite badge/chiavi forniti per lo svolgimento dell'attività autorizzata 3) Eliminazione dall'elenco e restituzione di badge/chiavi in caso di cambiamento delle mansioni
Postazioni di Lavoro	

Sicurezza Fisica: Accesso Archivi Cartacei
Procedure/Credenziali di Autenticazione
Non vi sono documenti cartacei contenenti dati personali, ma solo documentazione tecnica. Non sono necessarie procedure particolari di autenticazione

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Sicurezza Fisica: Accesso Supporti Magnetici
Procedure/Credenziali di Autenticazione
1) A ciascun utente autorizzato è assegnato un identificativo univoco (UserID/Password) al quale corrisponde un profilo con i necessari permessi per l'effettuazione delle operazioni di controllo, gestione, manutenzione, ecc.. 2) Gli incaricati, dopo il login, potranno effettuare le operazioni loro consentite. 3) Dovranno comunque prestare la massima attenzione a non lasciare incustodita la postazione di lavoro con sessioni aperte o visibili da parte di altri. 4) Al termine delle attività dovranno disconnettersi dal server effettuando le procedure di logout previste dal sistema 5) I supporti magnetici che fanno parte integrante del sistema di backup sono gestiti dal Sw TIVOLI. Questi è installato su un server presente all'interno dell'area di sicurezza e l'accesso al sistema è controllato dallo stesso mediante una procedura di autenticazione specifica.

In linea con i requisiti della ISO/IEC 27001:2005, la protezione della intranet da accessi non autorizzati ai servizi forniti via rete implica due aspetti principali:

1. Il primo riguarda il controllo degli accessi fisici alla rete, per cui occorre che siano applicati appropriati meccanismi di autenticazione per gli utenti e le apparecchiature, e la cui sorveglianza dovrebbe essere sempre garantita dagli utenti autorizzati al loro utilizzo. Tale pratica contribuisce a preservare la rete da accessi non autorizzati che possono avvenire localmente.
2. Per quanto riguarda il secondo aspetto, occorre assicurarsi che siano interposte appropriate interfacce fra la rete interna e le reti di altre organizzazioni, o le reti pubbliche per mezzodi "Firewall", software o hardware, che garantiscono la protezione al passaggio di dati nei punti di interconnessione tra rete privata e rete esterna (es. una Intranet ed una Internet) e controllano il traffico di rete interno ed esterno, consentendo solo quello autorizzato tramite regole appositamente definite.

Sicurezza Fisica: Sistemi in Rete	
Politiche di Sicurezza dell'Ente	
Server	
Controllo Accessi Fisici	
Sistemi Autorizzazioni e Identificazione per l'Accesso Locale e alla Rete Aziendale	
Ridondanza Dati	
Ridondanza Sistema	

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Sicurezza Impianti	
Protezione Intranet da Accessi non Autorizzati (potrebbe essere inclusiva delle tre righe sottostanti)	
Postazioni Fisiche di Accesso alla Rete	
Strumenti Hardware per la Protezione della Rete	
Strumenti Software per la Protezione della Rete	
Utilizzo di IDS (Intrusion Detection System)	

4.2 Sicurezza Logica

La sicurezza logica impatta sull'integrità, disponibilità, e riservatezza delle informazioni gestite, ed è pertanto una componente estremamente critica della sicurezza di un sistema informativo.

Inoltre, relativamente alla perdita di dati, con conseguente indisponibilità dell'informazione, vanno definiti criteri e procedure per il salvataggio di dati, e per il ripristino della disponibilità dei dati. Le due tabelle successive sono state predisposte per accogliere queste informazioni.

Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di elementi che concorrono nella realizzazione del livello di sicurezza da raggiungere. In generale la normativa ISO individua i seguenti macro-servizi di sicurezza:

1. controllo accessi;
2. antivirus;
3. controllo software;
4. riservatezza;
5. integrità.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Sicurezza Logica: Misure Adottate	
Descrizione Misura	Note per la Corretta Applicazione
Assegnazione di Codici Identificativi Univoci agli Incaricati	1) A ciascun utente autorizzato è assegnato a livello di Sistema un identificativo univoco (UserID/Password) al quale corrisponde un profilo con i necessari permessi per l'effettuazione delle operazioni di controllo, gestione, manutenzione, ecc.. 2) Analoga procedura è implementata a livello dell'applicativo SIRFO, per gli incaricati della gestione dei dati
Predisposizione ed Aggiornamento Antivirus	L'Ente ha adottato le necessarie contromisure alla diffusione dei virus informatici dotando tutte le postazioni di lavoro presenti sulla LAN regionale oppure sulla RUPAR di software antivirus (Unicenter TNG – Advanced Antivirus). L'installazione di programmi Antivirus è effettuata direttamente dal CTR (Centro Tecnico Regionale), che provvede anche all'aggiornamento.
Richieste Fatte ai Produttori di Software	Gestione Password. Suddivisione degli utenti in base a ruoli specifici con assegnazione di permessi per l'effettuazione di particolari operazioni (inserimento, modifica, cancellazione, …)
Controllo degli Accessi ai Sistemi Informativi	Il sistema informativo SIRFO è in grado di fare il logging delle operazioni effettuate. Una registrazione degli accessi non avviene nel momento in cui si accede, ma in seguito alla effettuazione di qualche operazione sui dati. In questo caso si memorizza data, ora, utente, operazione effettuata.
Controllo Software	- Aggiornamento S.O. effettuato ove ritenuto necessario dal CTR – Verifica e manutenzione dei programmi che compongono l'Applicativo eseguita dalla Società fornitrice del Sw, sia direttamente che in seguito ad eventuali segnalazioni provenienti dagli utenti.
Riservatezza (Accesso Autorizzato)	Rischi per la riservatezza dei dati possono verificarsi mediante l'accesso in locale e la trasmissione in rete. Il database della Oracle garantisce la totale riservatezza dei dati, sia in locale che in rete, mediante algoritmi di cifratura certificati. Non è inoltre possibile visualizzare i dati direttamente sul server senza la conoscenza di opportuni UserID e Password di amministrazione

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Integrità (Modifica Autorizzata)	Oracle garantisce l'integrità dei dati. Infatti, oltre alla cifratura, e' garantito l'aspetto che se vengono modificati i dati sulla rete nel colloquio tra client e server del Database, il prodotto è in grado di rilevare i pacchetti corrotti.
Disponibità dei Dati	Backup Automatici giornalieri e mensili eseguiti sia come export di Oracle che tramite l'uso del Sw IBM Tivoli Storage Manager
Password: Policy Assegnazione-modifica	Allo stato attuale non vi sono particolari policy di assegnazione e modifica delle password di accesso al SIRFO.
Profilazione Utenti	L'applicativo SIRFO permette di gestire i profili per singoli utenti o gruppi, concedendo o negando autorizzazioni secondo quanto stabilito dall'Amministratore.
Sicurezza Reti di Telecomunicazione (Intranet dell'Ente /Internet)	La gestione della sicurezza della Intranet dell'Ente viene effettuata direttamente da Uffici e personale ad essa preposti.

Sicurezza Logica: Password	
Regole di Definizione	Non sono impostate regole di definizione della password
Assegnazione	Inizialmente la password viene impostata dall'amministratore in modo standard, in seguito l'utente è obbligato a modificarla a proprio piacimento al primo accesso.
Modalità di Modifica	La modifica della password è consentita a ciascun utente all'interno dell'applicativo
Modalità Registrazione Password	Memorizzata su Database in modalità criptata
Policy Trasmissione Password in Rete	Non sono definite policy per la trasmissione in rete della password

Oltre alle informazioni sintetiche riportate in precedenza, può essere utile compilare una scheda analitica contenente le informazioni utili alla gestione operativa della sicurezza, ed in particolare alle attività di verifica e di controllo.

Procedure Attive per il Salvataggio		
Data Base	Criteri Individuati per il Salvataggio (Procedure Operative in Essere)	Struttura Operativa Incaricata del Salvataggio
SIRFO	Back-up quotidiano e mensile della base dati	SIRS/Lucana Sistemi

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	(Export di Oracle e Backup con Sw IBM Tivoli)	

Ripristino Data Base: <Nome del Data Base>	
Criteri e Procedure per il Ripristino dei Dati (Scheda Operativa)	Pianificazione delle prove di ripristino
	Nessuna pianificazione di ripristino in Regione per assenza di risorse hardware.

Nella tabella di seguito riportata devono essere inserite informazioni in relazione alle modalità di protezione adottate per i dati per cui è richiesta la cifratura o la separazione fra dati identificativi e dati personali (dati di tipo sanitario), nonché criteri e modalità con le quali viene tutelata la sicurezza di tali trattamenti.

Non vi sono dati per cui sia richiesta specificamente la cifratura o la separazione dai dati identificativi

Cifratura				
Dato	Protezione Scelta (Cifratura/Separazione)	Data di Effettività	Tecnica Adottate	
			Descrizione	Informazioni Utili

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

4.3 Sicurezza Organizzativa

Oltre all'adozione delle opportune misure tecnologiche precedentemente illustrate, devono essere definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi.

L'aspetto organizzativo principale riguarda la definizione di ruoli, compiti e responsabilità per la gestione del processo di Sicurezza.

In Regione Basilicata, in particolare per il Sistema Informativo "SIRFO", è stata identificata nell'Amministratore del sistema la figura responsabile del processo di sicurezza dell'applicativo.
Altre figure importanti per la sicurezza e il corretto funzionamento del Sistema sono il DBA (DataBase Administrator) e il Responsabile Elaborazione Dati.

La tabella successiva individua competenze e responsabilità correlate.

Sicurezza Organizzativa: Misure Adottate	
Descrizione Misura	Note per la Corretta Applicazione/Responsabilità correlate alla figura
Formazione Incaricati	
Custodia Documenti Cartacei	
Responsabile Gestione Processo Sicurezza SI	
Identificazione Incaricati Preposti alle Attività di Trattamento	
Assegnazione di Codici Identificativi Univoci agli Incaricati	
Identificazione Custode Password	
Identificazione Amministratore Sistema	Tale figura si occupa della gestione del sistema compiendo una serie di attività: • autorizza i nuovi utenti all'accesso nel sistema fornendo user-id e password, nonché il corretto profilo di lavoro, quindi, l'accesso a dati e funzioni mediante una funzionalità di sua sola competenza;

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	• si preoccupa di sensibilizzare e formare gli utenti al trattamento di dati "sensibili", affinché non vengano divulgati per scopi non espressamente previsti dal corretto utilizzo sistema • verifica che gli utenti utilizzino le funzioni messe a disposizione secondo i riferimenti normativi aggiornati; • fa conoscere la documentazione tecnica e di supporto all'utilizzo dell'applicativo solo agli utenti autorizzati;
Identificazione DBA	Tale figura si preoccupa di verificare che la base dati sia sempre disponibile ed interviene in caso di mancato accesso dell'applicativo alla base dati. Controlla inoltre che i back-up vengano effettuati regolarmente verificando l'esistenza dei file salvati sul server corrispondente all'indirizzo IP 172.18.18.50.
Identificazione Responsabile Elaborazione Dati	Tale figura si preoccupa di verificare che l'Applicazione sia sempre disponibile per l'accesso da parte degli utenti, ed interviene in caso di mancato funzionamento dell'applicativo.

N.B.: Le misure diversificate per il colore carattere rosso, per la loro natura generale, qualificante il processo di sicurezza dell'intero Ente e non del singolo Sistema Informativo, possono ritenersi campi opzionali.]