REGIONE BASILICATA
UFFICIO S. I. R. S.

Misure di Sicurezza Adottate

Centrale Bandi e Avvisi Pubblici Regione Basilicata

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:	Dott. Gianni Emilio Esposito	27/10/2010	
Revisionato da:			
Approvato da:			

Variazioni

Versione	Data	Autore	Paragrafi modificati

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

Distribuzione

Copia No.	Nome	Locazione
1		
2		
3		
4		
5		
6		

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

Indice

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

1. Introduzione

Questo documento si prefigge l'obiettivo di individuare e gestire i rischi sul sistema informativo Centrale Bandi della Regione Basilicata, 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.

1.1 Scopo del Documento

Obiettivo primario del presente documento è quello di specificare le misure adottate per assicurare che il sistema informativo Centrale Bandi della Regione Basilicata sia munito di appropriati e proporzionati controlli di sicurezza atti a fornirne adeguata protezione.

1.2 Definizioni ed Acronimi

[Lista e descrizione delle definizioni e degli acronimi.

Acronimo	Significato
SIA	Sistema Informativo Automatizzato
PA	Pubblica Amministrazione

]

1.3 Riferimenti

[Riferimenti bibliografici, documenti, articoli, siti web di riferimento.]

1.4 Overview

Per quanto riguarda la gestione della sicurezza, relativamente alle applicazioni che verranno fornite con il presente progetto, si pone particolarmente attenzione al contesto infrastrutturale nel quale tali applicazioni sono immmerse. La gestione degli accessi e delle autorizzazioni è infatti gestito dall' IMS in uso presso l'ente. Le applicazioni che svilupperemo,

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

per rendere ancora più sicuro il canale di comunicazione con i client, forniranno un canale protetto di comunicazione basato su protocollo HTTPS. In questo modo la connessione con i Client, già filtrata da altri strati applicativi, sarà resa inattaccabile dall'esterno grazie all'approccio SSL. Inoltre l'accesso alle applicazioni sarà garantito dalla creazione di Policy XACML molto restrittive che in accordo con i moduli di Policy (PEP e PDP) gestiti dall'infrastruttura regionale non permetteranno nessun accesso non consentito alle applicazioni.

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

2. Identificazione Risorse da Proteggere

2.1 Identificazione Risorse Hardware

[In questa sezione saranno riportate accurate informazioni riguardanti le caratteristiche delle macchine censite. La sezione sarà virtualmente divisa in due sottosezioni, in cui saranno inserite rispettivamente informazioni relative alle caratteristiche hardware delle macchine censite, e ai dispositivi di protezione presenti sulle macchine. 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 e i componenti di rilievo finalizzati alla sicurezza dei dati. Per ogni distinta macchina censita devono essere predisposte una scheda risorsa hardware, ed una scheda dispositivi di protezione attivati; il raggruppamento di piu' macchine in un'unica scheda è consentito esclusivamente per macchine aventi caratteristiche identiche e prossimità di ubicazione.

La scheda successiva va caricata sul sistema di assessment della server farm.]

- DATABASE SERVER

CPU	Intel Xeon 3 GHz (o equivalente)
Memoria RAM	2 GB/ consigliato 4 GB RAM
Hard Disk	
Disco di Sistema	10 GB
Disco Dati	60 GB Hard Disk/ consigliato 70 GB in Raid 5

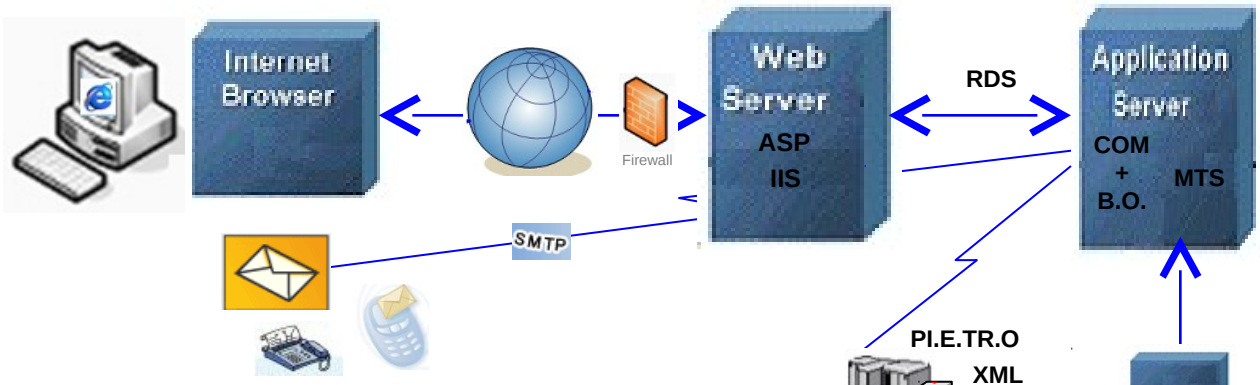
- APPLICATION SERVER

CPU	Intel Xeon 3 GHz (o equivalente)
Memoria RAM	1 GB/ consigliato 2 GB
Hard Disk	
Disco di Sistema	10 GB
Disco Dati	60 GB Hard Disk/ consigliato 70 GB in Raid 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



Legenda
IIS Internet Information Services
ASP Active Server Pages
MTS Microsoft Transaction Server
COM+ Component Services & B.O. Business Object
DTC Distributed Transaction Coordinator
RDS Remote Data Services
PI.E.TR.O Piattaforma EAI Transazionale Online

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

2.2 Identificazione Software

- DATABASE SERVER

Sistema Operativo Windows 2000 Server (SP4 o superiore)
o Windows 2003 Server (SP1 o superiore)

Software di Base SQL Server 2000 Standard Edition SP4 o superiore (consigliata Enterprise Edition)
SQL Server 2005 Express Edition SP2 o superiore.

MS DTC (Microsoft Distributed Transaction Coordinator). Se è presente un firewall tra il Database Server e l'Application Server è necessario seguire le indicazioni di Microsoft (http://support.microsoft.com/?scid=kb;en-us;306843&x=9&y=16) per configurare correttamente il firewall stesso per l'utilizzo di MS DTC.

La versione Standard Edition di SQL Server 2000 è consigliata per computer con una RAM fino a 2 GB; la versione Enterprise Edition è consigliata per computer con una RAM superiore a 2 GB. SQL Server 2005 Standard Edition gestisce tutta la ram presente sul server.

- APPLICATION SERVER/WEB SERVER

Sistema Operativo Windows 2000 Server o Advanced Server SP4 o superiore
o Windows 2003 Server SP1 o superiore

Software di Base IIS – Internet Information Services 5.0 o superiore
COM+ Services
MDAC 2.6 SP1 o superiore
SMTP Service
Internet Explorer 6.0 o superiore

MS DTC (Microsoft Distributed Transaction Coordinator). Se è presente un firewall tra il Database Server e l'Application Server è necessario seguire le indicazioni di Microsoft (http://support.microsoft.com/?scid=kb;en-us;306843&x=9&y=16) per configurare correttamente il firewall stesso per l'utilizzo di MS DTC.

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

- WEB CLIENT

Sistema Operativo Windows 98/2000 SP2 o superiore, Windows NT 4.0 SP6 o superiore, Windows XP/2003, Windows Vista;

2.3 Identificazione Dati

[Questa sezione sarà dedicata al rilevamento dei dati trattati dal sistema informativo in oggetto. Particolare rilievo sarà dato 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.

]

2.4 Identificazione Risorse Professionali

2.5 Identificazione Documentazione Cartacea

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

2.6 Identificazione Supporti di Memorizzazione

[

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

3. Analisi dei Rischi

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

3.1 Risorse Hardware

[Fine della sicurezza fisica è quello di proteggere persone ed hardware coinvolti nel

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	Elemento di Rischio	Livello di Rischio	Note-Motivazione
	Accesso non Autorizzato alle Basi Dati Connesse		
	Errori Software che Minacciano l'Integrità dei Dati		
	Presenza di Codice non Conforme alle Specifiche del Programma		
	Mancanza Autenticazione Utente		
	Mancanza Logging degli Accessi		
	Errori Software Noti		
	Cattiva Gestione Password		
	Diritto di Accesso Scorretti		
	Uso del Software Incontrollato		
	Sessioni Aperte senza Presenza Utente		
	Assenza di Backup		
	Carenza nella Dismissione dei Supporti		

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

	Uso Illegale di Password		
	Installazione/Copia Illegale del Software		
	Furto di Credenziali di Autenticazione		
	Comportamenti Sleali o Fraudolenti		
	Errore Umano nella Gestione della Sicurezza Fisica		

]

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	Elemento di Rischio	Livello di Rischio	Note-Motivazione
	Accesso non Autorizzato		
	Cancellazione o Modifica non Autorizzata dei Dati		
	Perdita di Dati		
	Assenza di Backup		
	Impossibilità di Ripristinare Copie di Backup		
	Grant/Ruoli Assegnati in Maniera Impropria		
	Furto Supporti		

]

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

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 passo 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	Es: I documenti cartacei contenenti dati personali sono conservati in armadio ignifugo dotato di serratura, nel locale ..... adibito ad archivio.....
Custodia/Accesso Supporti Magnetici	Es: I supporti utilizzati per l'attività di backup sono conservati in armadi ignifughi dotati di serratura, nel locale adibito ad archivio interno alla sede, ed in una sede distaccata individuata
Accesso Fisico ai Locali	
Dispositivi Antincendio	Es: I locali della sede sono dotati di estintori.....
Continuità Alimentazione Elettrica	Es: Server collegato ad un gruppo di continuità
Verifica leggibilità supporti di Backup	Es: I supporti di backup si testano e verificano con cadenza mensile (bimestrale)

Le

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.

Vanno considerate e qui riportate adeguate policy di autenticazione ai sistemi, che garantiscano riservatezza ed integrità dei dati.

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

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.

4.3 Sicurezza Organizzativa

[Oltre all'adozione delle opportune misure tecnologiche precedentemente illustrate, devono essere