tronici e va esteso alla totalità degli strumenti elettronici, anche se non contengono dati sensibili e giudiziari;

Considerato che lo stesso deve contenere idonee informazioni in relazione ai punti di cui all'art. 19 dell'allegato B del codice in materia di protezione dei dati personali;

Considerato, altresì, che, con nota presidenziale prot. n. 92 dell'11 gennaio 2008, è stato dato incarico all'ufficio del Sovrintendente di Palazzo d'Orléans e dei siti presidenziali, di provvedere, con specifico riferimento alla gestione informatizzata dei dati, per il sito di Palazzo d'Orléans e per gli altri siti presidenziali;

Atteso che, con nota prot. n. 3382 del 28 marzo 2008, il servizio IV dell'ufficio del Sovrintendente di Palazzo d'Orléans e dei siti presidenziali ha trasmesso il piano di sicurezza dipartimentale, relativo all'ufficio di Palazzo d'Orléans e dei siti presidenziali, finalizzato all'aggiornamento del documento programmatico di sicurezza;

Ritenuto di dovere conseguentemente provvedere;

Decreta:

Art. 1

Per quanto in premessa specificato, è approvato, ai sensi dell'art. 34 e del disciplinare tecnico (allegato B) del decreto legislativo 30 giugno 2003, n. 196, l'allegato documento programmatico in materia di misure minime di sicurezza con riferimento agli uffici e dipartimenti riconducibili al Presidente della Regione.

Art. 2

Il presente decreto sarà pubblicato nella *Gazzetta Ufficiale* della Regione siciliana.

Palermo, 31 marzo 2008.

Il Vicepresidente: LEANZA

Allegato

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA - ART. 34 E DISCIPLINARE TECNICO

(Allegato B), decreto legislativo 30 giugno 2003, n. 196

O - SCOPO

Il presente documento programmatico in materia di misure minime di sicurezza è adottato, ai sensi del punto 19 del disciplinare tecnico (allegato B al decreto legislativo n. 196/2003) per regolamentare il trattamento dei dati personali, le politiche di sicurezza ed i criteri organizzativi per la loro attuazione.

Come previsto dal succitato punto 19 dell'allegato B del codice privacy, il documento programmatico sulla sicurezza deve contenere:

A) elenco dei trattamenti dei dati personali;

B) la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

C) l'analisi dei rischi che incombono sui dati;

D) 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;

E) la descrizione dei criteri e delle modalità per il ripristino delle disponibilità dei dati in seguito a distruzione o danneggiamento;

F) la previsione degli interventi formativi degli incaricati 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 adottate dal titolare. La formazione programmata già al 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;

G) le descrizioni dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti all'esterno della struttura del titolare.

O.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, anche se non contengono dati sensibili o giudiziari; naturalmente parte delle misure da adottare si differenziano a seconda della tipologia dei dati.

O.2 - **Riferimenti normativi**

— decreto legislativo n. 196/2003;

— disciplinare tecnico (allegato B);

— direttive comunitarie nn. 95/46/CE e 2202/58/CE.

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

1.1 - **Premessa**

Atteso che i trattamenti sono comuni alle strutture regionali facenti capo al Presidente della Regione ed operanti presso i siti presidenziali di cui alla delibera della Giunta regionale n. 57 del 27 febbraio 2007 si è ritenuto di dover riportare in maniera unitaria l'elenco dei trattamenti dei dati personali.

1.2 - **Elenco dei trattamenti**

Denominazione del trattamento di dati personali	Presenza dati sensibili/giudiziari
Nomine e designazioni da parte della Regione	Si
Gestione del rapporto di lavoro del personale inserito a vario titolo presso l'ente	Si
Attività sanzionatoria e di tutela amministrativa e giudiziaria	Si
Anagrafe patrimoniale dei titolari di cariche elettive di cariche direttive	Si
Assicurazione rischi di morte, invalidità permanente e temporanea, dipendenti da infortunio o infermità e assicurazione invalidità dei consiglieri e Assessori regionali e dei consiglieri degli enti strumentali in carica	Si
Attività ispettiva	Si
Concessioni, autorizzazioni, iscrizioni, agevolazioni, finanziamenti ed altri benefici a persone fisiche e giuridiche e organizzazioni sociali	Si
Documentazione dell'attività istituzionale della Giunta regionale e degli altri organi della Giunta o di altri enti pubblici regionali o vigilati dalla Regione	Si
Attività del Comitato regionale per le comunicazioni	Si
Gestione archivio, gestione protocollo	Si
Gestione atti amministrativi (delibere, determine, disposizioni, decreti)	Si
Commissariamenti ad acta	No
Registro persone giuridiche	Si
URP	Si
Gestione eventi ed attività di rappresentanza organizzati dalla Presidenza	No
Attività contrattuale	Si
Gestione capitoli del bilancio e contabilità	No
Istituzione e tenuta registro infortuni sul lavoro	Si
Tenuta elenco lavoratori sottoposti a sorveglianza sanitaria ai sensi della legge n. 626/94	Si
Attività gestionali Batteria del Presidente	No
Gestione albo ditte cottimo	No
Gestione incentivi e spese per la progettazione	No
Gestione del personale in servizio	No
Gestione albo ditte forniture di beni e servizi	No
Gestione visitatori	No
Attività gestione consegnatari	No
Attività gestione cassieri	No
Gestione sistemi informativi e informatici per i siti presidenziali	Si
Protocollo ufficio Sovrintendente	Si
Contratti dirigenti	Si

2 - (REGOLA 19.2) - DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

2.1 - **Il titolare del trattamento**

Il titolare del trattamento è individuato nell'Amministrazione stessa, cioè gli uffici ed i dipartimenti di riferimento del Presidente, rappresentata dal Presidente della Regione.

2.2 - **I responsabili del trattamento**

La specificità dell'ente ha suggerito l'individuazione di più responsabili, sia interni sia esterni all'ente.

In particolare, per quanto riguarda gli interni, si è ritenuto attribuire il ruolo di responsabile dei trattamenti ai dirigenti di area, servizio, unità operativa, nonché ai preposti degli uffici di diretta collaborazione, alle dirette dipendenze ed agli uffici speciali riferibili al Presidente della Regione.

Per qunto riguarda partners esterni, invece, l'ente ha previsto l'eventualità di nominarli responsabili, di volta in volta, su richiesta del dirigente referente dell'attività di partenariato.

L'individuazione delle figure suddette viene effettuata tramite apposito atto presidenziale; ciascun responsabile viene espressamente nominato con apposita nota.

2.3 - **Gli incaricati del trattamento**

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

2.4 - **Altri incarichi rilevanti ai fini della privacy**

Palazzo d'Orleans e siti presidenziali ad esclusione di via Caltanissetta

Responsabile della sicurezza informatica: Cirrito Rosario.
Amministratore della rete: Cirrito Rosario.
Custode delle passwords: Cirrito Rosario.

Via Caltanissetta

Responsabile della sicurezza informatica: Fontana Francesco.
Amministratore della rete: Fontana Francesco.
Custode delle passwords: Fontana Francesco.

3 - (REGOLA 19.3) - ANALISI DEI RISCHI

3.1 - **Premessa**

La totalità dei dati trattati è conservata, alternativamente o contemporaneamente, in fascicoli riposti in schedari dotati di chiusura, archiviati al termine della pratica, e tramite personal computer connessi in rete.

E' stata compiuta l'analisi dei rischi, avendo attenzione alla tipologia degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali, nonché all'impatto sulla sicurezza dei dati, in relazione a ciascun evento e alla gravità e probabilità stimata dell'evento stesso. Per ciascun evento probabile si è ipotizzata naturalmente la contromisura adottata o da adottare.

3.2 - **Livelli di rischio**

Basso

— rischio basso o indeterminato: rischio non sufficientemente sotto controllo, ma generalmente modesto sia sotto il profilo della probabilità d'accadimento che della gravità dei danni che ne potrebbero derivare;
— inadempimenti formali a norme di legge che comunque non determinano situazioni di rischio di rilievo;

Medio

— rischi non sufficientemente sotto controllo, generalmente medio quanto a probabilità d'accadimento e gravità delle conseguenze;
— rischio con elevata probabilità d'accadimento di eventi dannosi oppure con possibili forti conseguenze in termini di entità del danno, ma non l'uno e l'altro aspetto congiunti;

Alto

— inadempimenti formali a norme di legge che possono determinare situazioni di rischio di rilievo;
— rischio non sufficientemente sotto controllo, con elevata probabilità d'accadimento di eventi dannosi associata a possibili gravi conseguenze in termini di entità del danno;

Analisi dei rischi che incombono sui dati

Il presente paragrafo è stato redatto in conformità a quanto disposto dal punto 19.3 del disciplinare tecnico in materia di misure minime di sicurezza (allegato B del decreto legislativo n. 196 del 30 giugno 2003).

I rischi ai quali possono essere soggetti i dati trattati dal personale nell'ambito dell'esercizio della propria normale attività possono essere tutti quelli indicati nell'art. 31 del decreto legislativo n. 196/2003, vale a dire: la distruzione o la perdita, anche accidentale; l'accesso non autorizzato; il trattamento non consentito; il trattamento non conforme alle finalità per le quali è avvenuta la raccolta dei dati personali.

Si prende in considerazione la lista dei seguenti eventi:

Categoria: comportamenti degli operatori

— sottrazione di credenziali di autenticazione;
— carenza di consapevolezza, disattenzione o incuria;
— comportamenti sleali o fraudolenti;
— errore materiale;

Categoria: eventi relativi agli strumenti

— azione di virus informatici o di programmi suscettibili di recare danno;
— spamming o tecniche di sabotaggio;
— malfunzionamento, indisponibilità o degrado degli strumenti;
— accessi esterni non autorizzati;
— intercettazione di informazioni in rete;

Categoria: eventi relativi al contesto fisico-ambientale

— ingressi non autorizzati a locali/aree ad accesso ristretto;
— sottrazione di strumenti contenenti dati;
— eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria;
— guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.);
— errori umani nella gestione della sicurezza fisica.

Rischi	Categoria	Descrizione dell'impatto sulla sicurezza (probabilità: alta/media/bassa) (gravità: alta/media/bassa)
Sottrazione di credenziali di autenticazione	Comportamenti degli operatori	Non vi è vantaggio personale a sottrarre le credenziali (probabilità: bassa - gravità: bassa)
Carenza di consapevolezza, disattenzione o incuria	Comportamenti degli operatori	Può capitare di lasciare il computer non presidiato ma in genere il profilo di "login" si disconnette automaticamente (probabilità: media - gravità: bassa)
Comportamenti sleali o fraudolenti	Comportamenti degli operatori	Non si hanno notizie storiche dell'evenienza di tali comportamenti (probabilità: bassa - gravità: bassa)
Errore materiale	Comportamenti degli operatori	Non sussistono catene di errori che possano causare danni irreversibili o comunque non facilmente riparabili (probabilità: bassa - gravità: bassa)

Rischi	Categoria	Descrizione dell'impatto sulla sicurezza (probabilità: alta/media/bassa) (gravità: alta/media/bassa)
Azione di virus informatici o di programmi suscettibili di recare danno	Eventi relativi agli strumenti	I PC sono protetti da antivirus e firewall aziendali (probabilità: bassa - gravità: media)
Spamming o tecniche di sabotaggio	Eventi relativi agli strumenti	Il server di posta evidenzia lo "spamming" (probabilità: media - gravità: bassa)
Malfunzionamento, indisponibilità o degrado degli strumenti	Eventi relativi agli strumenti	Il parco macchine aziendale è mantenuto costantemente in efficienza e prontamente sostituito ove obsoleto (probabilità: bassa - gravità: bassa)
Accessi esterni non autorizzati	Eventi relativi agli strumenti	La sottorete è protetta dal firewall della VPN regionale (probabilità: bassa - gravità: bassa)
Intercettazione di informazioni in rete	Eventi relativi agli strumenti	La VPN utilizza fibra ottica per le interconnessioni di fonia e dati (probabilità: bassa - gravità: bassa)
Ingressi non autorizzati a locali/aree ad accesso ristretto	Eventi relativi al contesto fisico-ambientale	L'accesso all'immobile è sorvegliato dalla P.S. Il server di rete è ubicato in locale sottochiave (centrale telefonica) (probabilità: bassa - gravità: bassa)
Sottrazione di documenti contenenti dati	Eventi relativi al contesto fisico-ambientale	Non si hanno notizie storiche dell'evenienza di tali comportamenti (probabilità: bassa - gravità: media)
Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali dovuti ad incuria	Eventi relativi al contesto fisico-ambientale	Non si hanno notizie storiche di danni prodotti da tali eventi e le banche dati sono logicamente distribuite oltre che con backup periodici (probabilità: bassa - gravità: bassa)
Guasto a sistemi complementari	Eventi relativi al contesto fisico-ambientale	I PC utilizzati non necessitano di CDZ (probabilità: media - gravità: bassa)
Errori umani nella gestione della sicurezza fisica	Eventi relativi al contesto fisico-ambientale	L'eventuale errore umano (cancellazione archivi) è comunque rimediabile (probabilità: bassa - gravità: media)

4 - (REGOLA 19.4) - MISURE IN ESSERE E DA ADOTTARE

4.1 Per evitare o ridurre al minimo tutti questi rischi sono state adottate una serie di misure di sicurezza, di carattere organizzativo, fisico e logico, che riguardano le varie operazioni di trattamento che vengono effettuate e, in particolare, la custodia dei dati personali ed il controllo della loro integrità.

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura adottata (dal gg/mm/aaaa) o da adottare	Tempi previsti	Struttura o addetti all'adozione	Descrizione sintetica
1	Sottrazione, distruzione	Tenuta registro infortuni	Dal 24 luglio 2003	—		Conservazione sotto chiave
2	Memorizzazione difettosa/cancellazione	Banca dati sorveglianza sanitaria lavoratori ex legge n. 626/94	Dalla data di istituzione banca dati	—	*	Copia cartacea e su server
3	Memorizzazione difettosa/cancellazione	Rubrica e contatti telefonici della Batteria del Presidente	Dalla data di istituzione banca dati	—	*	Copia su file server
4	Memorizzazione difettosa/cancellazione	Gestione albo ditte cottimo (art. 24, testo coordinato, legge n. 109/94)	Dalla data di istituzione banca dati	—	*	Copia su file server
5	Memorizzazione difettosa/cancellazione	Gestione incentivi e spese per la progettazione (art. 17, testo coordinato, legge n. 109/94	Dalla data di istituzione banca dati	—	*	Copia su file server
6	Memorizzazione difettosa/cancellazione	Gestione del personale in servizio	Dalla data di istituzione banca dati	—	*	Copia su file server
7	Memorizzazione difettosa/cancellazione	Gestione albo ditte fornitori di beni e servizi	Dalla data di istituzione banca dati	—	*	Copia su file server
8	Memorizzazione difettosa/cancellazione	Gestione visitatori	Dalla data di istituzione banca dati	—	*	Copia su file server
9	Memorizzazione difettosa/cancellazione	Attività gestione consegnatari	Dalla data di istituzione banca dati	—	*	Copia su file server
10	Memorizzazione difettosa/cancellazione	Attività gestione cassiere	Dalla data di istituzione banca dati	—	*	Copia su file server

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura adottata (dal gg/mm/aaaa) o da adottare	Tempi previsti	Struttura o addetti all'adozione	Descrizione sintetica
11	Memorizzazione difettosa/cancellazione	Gestione informatica protocollo informatizzato	Dalla data di istituzione banca dati	—	*	Originale su CD settimanali (area 1) e copia sicurezza banca dati da server dedicato a file server (servizio 4)
12	Memorizzazione difettosa/cancellazione	Gestione informatica del personale e visite	Dalla data di istituzione banca dati	—	*	Copia sicurezza banca dati da server dedicato a file server (servizio 4)
13	Memorizzazione difettosa/cancellazione	Gestione file server	Dalla data di istituzione banca dati	—	*	Conservazione dati ridondante con ripristino automatica errore (RAID 5)
14	Memorizzazione difettosa/cancellazione	Gestione delibere della Giunta regionale	Dalla data di istituzione banca dati	—	*	Copia su CD

(*) Struttura o addetti all'adozione: aree, servizi e unità operative di base cui compete il trattamento dei dati in base alle competenze risultanti dai vigenti funzionigrammi.

4.2 - **Regole per la gestione delle passwords**

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito User-id) e password personale.

User-id e password iniziale sono assegnati dal custode delle passwords.

User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.

La User-id è costituita da 8 caratteri che corrispondono alle prime 8 lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.

La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà elementi facilmenti ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle passwords, il quale provvede a metterla nella cassaforte in un plico sigillato.

Ogni 6 mesi (3 nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle passwords una busta chiusa sulla quale è indicato il proprio User-id, al cui interno è contenuta la nuova password; il custode delle passwords provvederà a sostituire la precedente busta con quest'ultima. Le passwords verranno automaticamente disattivate dopo 3 mesi di non utilizzo. Le passwords di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di manutenzione straordinaria possono esere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione, l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione da custodire in cassaforte.

Le disposizioni di seguito elencate sono vincolanti per tutti i posti di lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:

— le passwords assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo.

Per la definizione – gestione della password devono essere rispettate le seguenti regole:

— la password deve essere costituita da una sequenza di minimo 8 caratteri alfanumerici e non deve essere facilmente individuabile; deve contenere almeno un carattere alfabetico ed uno numerico; non deve contenere più di 2 caratteri identici consecutivi; non deve contenere lo User-id come parte della password; al primo accesso la password ottenuta dal custode delle password deve essere cambiata; la nuova password non deve essere simile alla password precedente; la password deve essere cambiata almeno ogni 6 mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari; la password termina dopo 6 mesi di inattività; la password è segreta e non deve essere comunicata ad altri, va custodita con diligenza e riservatezza; l'utente deve sostituire la password, nel caso ne accertasse la perdita.

4.3 - **Misure di sicurezza per trattamenti effettuati con strumenti non automatizzati**

Per ogni archivio i responsabili del trattamento dei dati debbono definire l'elenco degli incaricati autorizzati ad accedervi ed impartire istruzioni tese a garantire un controllo costante nell'accesso degli archivi. Gli incaricati che trattano atti, documenti e dati personali sono tenuti a conservarli e restituirli al termine delle operazioni. Qualora i documenti contengano dati sensibili e giudiziari, gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

4.4 - **Protezione aree e locali di cruciale importanza**

Tutti i locali ove sono ubicati servers o più in generale attrezzature rilevanti ai fini della custodia e della disponibilità dei dati personali devono essere protetti, oltre che con misure di tipo logiche 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 laddove fosse possibile l'intrusione di estranei.

5. - (REGOLA 19.5) - CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI

Il presente paragrafo è stato redatto in conformità a quanto disposto dal punto 18, dal punto 19.4, dal punto 19.5 e dal punto 23 del disciplinare tecnico in materia di misure minime di sicurezza (allegato B del decreto legislativo n. 196 del 30 giugno 2003).

Di seguito, sono elencati i criteri, le modalità e le procedure per il ripristino della disponibilità dei dati e gli incaricati alla custodia delle copie ed al salvataggio dei dati.

In conformità al punto 23 del disciplinare tecnico, sono adottate idonee misure 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 7 giorni.

Ripristino banche dati

Banca dati/database/archivio	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino
Banca dati sorveglianza sanitaria lavoratori ex legge n. 626/94	Copia sicurezza su CD	Semestrale
Riepiloghi annuali congedi dipendenti	Copia sicurezza su CD e su server	Semestrale
Gestione albo ditte cottimo (art. 24, testo coordinato, legge n. 109/94)	Copia sicurezza su CD e su server	Semestrale
Gestione incentivi e spese per la progettazione (art. 17, testo coordinato, legge n. 109/94	Copia sicurezza su CD e su server	Semestrale
Gestione del personale in servizio	Copia sicurezza su CD e su server	Semestrale
Gestione albo ditte fornitori di beni e servizi	Copia sicurezza su CD e su server	Semestrale
Rubrica e contatti telefonici della Batteria del presidente	Copia sicurezza su CD e su server	Semestrale
Gestione visitatori	Copia sicurezza su CD e su server	Semestrale
Gestione consegnatari	Copia sicurezza su CD e su server	Semestrale
Gestione cassiere	Copia sicurezza su CD e su server	Semestrale
Protocollo informatizzato	Copia sicurezza su CD e su server	Semestrale
Gestione file server	Copia sicurezza su CD e su server	Semestrale
Gestione delle delibere della Giunta regionale	Copia sicurezza su CD e su server	semestrale

Sono impartite istruzioni orgnizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Salvataggio e backup banche dati

Banca dati	Procedure per il salvataggio	Frequenza	Luogo di custodia delle copie
Banca dati sorveglianza sanitaria lavoratori ex legge n. 626/94	Copia sicurezza su CD	☐ giornaliera ☒ settimanale	Armadio chiuso
Batteria del Presidente	Copia sicurezza su file server	☐ giornaliera ☒ settimanale	San server IBM
Gestione albo ditte cottimo (art. 24, testo coordinato, legge n. 109/94)	Copia sicurezza su CD	☐ giornaliera ☒ settimanale	Armadio chiuso
Gestione incentivi e spese per la progettazione (art. 17, testo coordinato, legge n. 109/94	Copia sicurezza su CD	☐ giornaliera ☒ settimanale	Armadio chiuso
Gestione del personale in servizio	Copia sicurezza su file server	☐ giornaliera ☒ settimanale	San server IBM
Gestione elenco ditte fornitori di beni e servizi	Copia sicurezza su CD	☐ giornaliera ☒ settimanale	Armadio chiuso
Gestione visitatori	Copia sicurezza su file server	☐ giornaliera ☒ settimanale	San server IBM
Gestione consegnatari (PDO/MAG)	Copia sicurezza su CD	☐ giornaliera ☒ settimanale	Armadio chiuso
Gestione cassiere	Copia sicurezza su CD	☐ giornaliera ☒ settimanale	Armadio chiuso
Gestione informatica protocollo informatizzato	Copia sicurezza su file server	☐ giornaliera ☒ settimanale	San server IBM
Gestione file server	Copia sicurezza su file server	☐ giornaliera ☒ settimanale	San server IBM
Gestione delle delibere della Giunta regionale	Copia sicurezza su file server	☐ giornaliera ☒ settimanale	San server IBM

6 - (REGOLA 19.6) - PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

Il presente paragrafo è stato redatto in conformità a quanto disposto dal punto 19.6 del disciplinare tecnico in materia di misure minime di sicurezza (allegato B del decreto legislativo n. 196 del 30 giugno 2003).

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Non sono previsti nuovi interventi formativi		

(2008.15.1134)008