REGIONE EMILIA-ROMAGNA
Atti amministrativi

GIUNTA REGIONALE

Atto del Dirigente:	DETERMINAZIONE n° 597 del 23/01/2012
Proposta:	DPG/2012/462 del 13/01/2012
Struttura proponente:	DIREZIONE GENERALE CENTRALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA
Oggetto:	DISCIPLINARE TECNICO PER AMMINISTRATORI DI SISTEMA DELLA GIUNTA E DELL'ASSEMBLEA LEGISLATIVA DELLA REGIONE EMILIA-ROMAGNA
Autorità emanante:	IL DIRETTORE - DIREZIONE GENERALE CENTRALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA
Firmatario:	LORENZO BROCCOLI in qualità di Direttore generale
Luogo di adozione:	BOLOGNA data: 23/01/2012

DIREZIONE GENERALE CENTRALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA
IL DIRETTORE

Visto il Decreto Legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione di dati personali” e in particolare gli articoli 31 ss. e 154 comma 1, lett. c) e h), nonché il disciplinare tecnico in materia di misure minime di sicurezza di cui all’Allegato B del Codice stesso;

Viste le deliberazioni della Giunta regionale:

- n. 2416/2008 del 29/12/2008 “Indirizzi in ordine alle relazioni organizzative e funzionali tra le strutture e sull'esercizio delle funzioni dirigenziali. Adempimenti conseguenti alla delibera 999/2008. Adeguamento e aggiornamento della delibera 450/2007.” e in particolare l’Appendice 5 “Direttiva in materia di trattamento di dati personali con particolare riferimento alla ripartizione di competenze tra i soggetti che effettuano il trattamento”;
- n. 1264 del 01/08/2005 avente ad oggetto “Linee guida della Giunta della Regione Emilia-Romagna in materia di protezione dei dati personali”;
- n. 2199 del 19/12/2005 “Adozione del Codice di comportamento della Regione Emilia-Romagna, ai sensi dell'art. 25 della l.r. 26 novembre 2001, n. 43”;
- n. 1465 del 19/10/2011 avente ad oggetto “Disciplinare per l’assegnazione e l’utilizzo di utenze di telefonia fissa e mobile della Giunta della Regione Emilia-Romagna;

Viste le proprie determinazioni:

- n. 6928/2009 “Disciplinare tecnico su modalità e procedure relative alle verifiche di sicurezza sul sistema informativo, ai controlli sull’utilizzo dei beni messi a disposizione dall’Ente per l’attività lavorativa con particolare riferimento alle strumentazioni informatiche e telefoniche ed esemplificazioni di comportamenti per il corretto utilizzo di tali beni, da applicare nella Giunta e nell’Assemblea Legislativa della Regione Emilia-Romagna”;
- n. 1703/2009 “Disciplinare Tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna”;
- n. 4856/2008 “Disciplinare Tecnico in materia di videosorveglianza nella Giunta e nell'Assemblea legislativa della Regione Emilia-Romagna”;
- n. 2649/2007 “Disciplinare Tecnico relativo al controllo degli accessi ai locali

della Giunta della Regione Emilia-Romagna";

- n. 2651/2007 "Disciplinare Tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta della Regione Emilia-Romagna";
- n. 14852/2011 "Disciplinare Tecnico per utenti sull'utilizzo dei sistemi informativi della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna";
- n. 4213/2009 "Linee guida per la *governance* del sistema informatico regionale;

Viste le deliberazioni dell'Ufficio di Presidenza dell'Assemblea legislativa regionale:

- n. 197 del 18 ottobre 2006 "Direttiva e Linee guida dell'Assemblea legislativa della Regione Emilia-Romagna in materia di protezione dei dati personali, con particolare riferimento alla ripartizione di competenze tra i soggetti che effettuano il trattamento. - Modifica ed integrazione della deliberazione n. 45/2003 e n. 1/2005";

- n. 43 del 29 marzo 2011 "Modifiche ed integrazioni alla delibera n. 197/2006 concernente le direttive e linee guida dell'Assemblea legislativa in materia di protezione dei dati personali e alla delibera n. 10 del 2011, recante "Aggiornamento dei Responsabili ai sensi del D.Lgs. 30 giugno 2003, n. 196 in materia di trattamento dei dati personali - anno 2011";

- n. 173 del 24 luglio 2007 "Parziali modifiche e integrazioni agli indirizzi in ordine alle relazioni organizzative e funzionali tra le Strutture e sull'esercizio delle funzioni dirigenziali approvati con deliberazione n. 45/2003";

- n. 183/2005 di approvazione del Codice di comportamento;

Viste le determinazioni:

- n. 33 del 11/02/2008 "Disciplinare Tecnico relativo al controllo degli accessi ai locali della Assemblea legislativa della Regione Emilia-Romagna";
- n. 120 del 29/03/2011 "Parziali modifiche al "Disciplinare tecnico relativo al controllo degli accessi ai locali dell'Assemblea legislativa della Regione Emilia-Romagna" approvato con Determinazione n. 33 del 06/02/2008";
- n. 480 del 28/11/2007 "Disciplinare Tecnico in materia di sicurezza delle applicazioni informatiche nella Assemblea legislativa della Regione Emilia-Romagna";

Visti i provvedimenti e le schede del Garante per la protezione dei dati personali di seguito riportati:

- Provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari

dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema." pubblicato sulla G.U. n. 300 del 24-12-2008;

- Provvedimento del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento" pubblicato sulla G.U. n. 149 del 30-06-2009
- Provvedimento del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" pubblicato sulla G.U. n. 287 del 9 dicembre 2008;
- Scheda informativa - 12 dicembre 2008 "Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori";

Vista inoltre la propria determinazione n. 1416 del 2 marzo 2009 " Disciplinare tecnico per amministratori di sistema della Giunta e dell'Assemblea legislativa della Regione Emilia-Romagna ", che definiva il carattere sperimentale delle prescrizioni in esso contenute;

Vista, inoltre, la propria determinazione n. 2564/2010 "Proroga del periodo di sperimentazione previsto dalle determinazioni nn. 1416/2009 (disciplinare tecnico per amministratori di sistema della Giunta e dell'Assemblea Legislativa) e 1703/2009 (disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna)" con la quale si è provveduto a prorogare il periodo di sperimentazione fino al 31 marzo 2011;

Rilevato che:

- la tutela del patrimonio delle informazioni riveste importanza strategica per la Giunta e per l'Assemblea legislativa della Regione Emilia-Romagna, oltre che essere soggetta a precisi vincoli di legge imposti dal Codice;
- il sistema informativo regionale è costituito da un'infrastruttura tecnologica molto articolata e complessa, costituita da sistemi di elaborazione dati di varia natura, basi dati, apparati di rete e di sicurezza, sistemi software anche complessi per cui si rende necessario assicurare maggiore organicità e coordinamento all'attività del personale informatico incaricato di gestire e amministrare i sistemi informatici e telematici;
- la gestione tecnica e la manutenzione degli impianti di elaborazione o di sue componenti comportano in molti casi attività che vanno considerate a tutti gli effetti alla stregua di trattamenti di dati personali;

Rilevata la necessità di:

- intraprendere una specifica azione rivolta ai soggetti preposti alla gestione e manutenzione di sistemi di elaborazione dati, banche dati, apparati di rete e di sicurezza, sistemi software (c.d. amministratori di sistema), per sensibilizzarli

rispetto alla rilevanza delle loro operazioni sui trattamenti di dati personali ma anche rispetto alla peculiarità e ai rischi ad esse associate;

- promuovere l'adozione di specifiche cautele nello svolgimento delle mansioni svolte dagli amministratori di sistema, unitamente ad accorgimenti e misure tecniche, procedurali ed organizzative volte ad agevolare le attività di verifiche da parte del titolare o dei responsabili da esso designati;
- informare dell'esistenza di tali figure o di ruoli analoghi all'interno dell'Ente, svolti in relazione anche a talune fasi dei trattamenti di dati personali;
- rendere nota l'identità degli amministratori di sistema qualora la loro attività riguardi anche indirettamente servizi o sistemi che permettono il trattamento di informazioni di carattere personale di lavoratori;

Ritenuto quindi per tutti i motivi sopraesposti di dover esplicitare e disciplinare le attività svolte dai c.d. "amministratori di sistema" al fine di facilitare l'attribuzione dei compiti agli stessi, sensibilizzarli rispetto alla peculiarità e ai rischi associati alle loro attività, dare trasparenza della loro esistenza e dei loro compiti, assicurare organicità e coerenza nello svolgimento delle loro attività;

Considerato che, a seguito della sperimentazione prevista dalle già citate determinazioni nn. 1416/2009 e 2564/2010, si è rilevata l'opportunità di modificare ed integrare alcune disposizioni, con particolare riferimento:

- alla gestione amministrativa degli amministratori di sistema, con la finalità di semplificare e rendere più efficace ed efficiente la gestione stessa, sostituendo l'atto amministrativo annuale di aggiornamento con la gestione di un Registro digitale;
- alla specificazione relativa ai log degli amministratori;
- alla descrizione delle modalità con cui è effettuata la verifica annuale dell'attività degli amministratori, verifica prevista dalle disposizioni del Garante per la protezione dei dati personali;

Valutato, pertanto, di approvare, a conclusione del periodo di sperimentazione, il disciplinare allegato con le modifiche sopra sinteticamente richiamate;

Acquisito il parere favorevole espresso dal Direttore Generale dell'Assemblea legislativa, dott. Luigi Benedetti, come da lettera prot. n. 943 del 11 gennaio 2012;

Sentito il parere del Comitato di Direzione nella seduta del 28/11/2011 ;

Dato atto di aver rispettato le vigenti disposizioni in materia di relazioni sindacali;

Dato atto del parere allegato;

DETERMINA

1. di approvare l'allegato "Disciplinare tecnico per amministratori di sistema della

Giunta e dell'Assemblea legislativa della Regione Emilia-Romagna", parte integrante della presente determinazione che sostituisce integralmente il precedente Disciplinare Tecnico approvato con determinazione n. 1416 del 2 marzo 2009;

2. di delegare il Responsabile del Servizio Sistema Informativo-Informatico regionale della Giunta al mantenimento dell'elenco aggiornato dei nominativi degli amministratori di sistema della Giunta e degli ambiti di operatività degli stessi, in funzione dei profili autorizzativi assegnati;

3. di dare atto che il Direttore Generale dell'Assemblea Legislativa provvederà a delegare il Responsabile del Servizio Sistemi informativi - informatici e innovazione al mantenimento dell'elenco aggiornato dei nominativi degli amministratori di sistema e degli ambiti di operatività degli stessi, in funzione dei profili autorizzativi assegnati;

4. di disporre che qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano di informazioni di carattere personale dei lavoratori, l'identità degli stessi sia resa nota attraverso il portale di comunicazione interna Internos;

5. di portare a conoscenza di tutti gli amministratori di sistema l'allegato "Disciplinare tecnico per amministratori di sistema della Giunta e dell'Assemblea legislativa della Regione Emilia-Romagna" con mezzi che attestino la certezza dell'avvenuta ricezione, a partire dalla data di adozione del presente atto;

6. di dare idonea informazione a tutti i soggetti interessati dell'allegato Disciplinare tramite apposita sezione sul portale di comunicazione interna Internos e con ogni altro mezzo di comunicazione ritenuto necessario o utile a tal fine.

Lorenzo Broccoli

Allegato

Disciplinare tecnico per amministratori di sistema della Giunta e dell'Assemblea legislativa della Regione Emilia-Romagna

Sommario

1 Premessa

Il presente disciplinare tecnico descrive le regole tecniche ed organizzative che gli amministratori di sistema devono applicare per garantire la sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche nella Giunta e nell'Assemblea legislativa della Regione Emilia-Romagna (di seguito denominate "Ente").

Tenendo conto di quanto esplicitato nel Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" pubblicato sulla G.U. n. 300 del 24-12-2008, così come modificato dal Provvedimento del 25 giugno 2009 dello stesso Garante, la definizione di "amministratori di sistema", ai fini dell'applicazione del presente disciplinare, è la seguente:

> **«amministratori di sistema»** sono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (quali ad es. gli amministratori di dominio e di server), nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente «responsabili» di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti «in chiaro» le informazioni medesime.

Pertanto, considerata la delicatezza di tali peculiari mansioni e i rischi ad esse associati, la designazione di un amministratore di sistema non può prescindere da alcune considerazioni e accorgimenti:

a) *valutazione delle caratteristiche soggettive*: l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

b) *designazioni individuali*: la designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

c) *elenco degli amministratori di sistema*: gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere conservate in un apposito registro. Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono

il trattamento di informazioni di carattere personale dei lavoratori, l'Ente rende nota o conoscibile l'identità degli amministratori di sistema con comunicazione effettuata nell'ambito del portale di comunicazione interna Internos;

d) *servizi in outsourcing*: nel caso di servizi di amministrazione di sistema affidati in outsourcing il Responsabile esterno formalmente designato conserva direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;

e) *verifica delle attività*: l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei Responsabili della sicurezza della Giunta e dell'Assemblea legislativa ognuno per la parte di propria competenza, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;

f) *registrazione degli accessi*: devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Ai fini del presente disciplinare, si intende per sistema informativo il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni. Esempi di sistemi informativi sono server (file, database, web, mail, ecc.), applicazioni , apparati di rete (router, switch, ecc.), strumenti di sicurezza (firewall, IDS, ecc.).

2 Obiettivo

La presente policy ha l'obiettivo di definire i principi generali e le regole dirette a disciplinare le attività poste in essere dagli Amministratori di Sistema preposti alla gestione e manutenzione del sistema informatico aziendale in attuazione a quanto richiesto dal Provvedimento a carattere generale dell'Autorità Garante per la protezione dei dati personali. Scopo della formalizzazione delle seguenti regole è altresì quello di assicurare la sicurezza logica delle informazioni dell'Ente e delle risorse ICT, al fine di garantirne l'integrità, la disponibilità, la riservatezza e l'affidabilità, nel pieno rispetto delle politiche di sicurezza aziendali.

3 Riferimenti normativi

Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) e, in particolare, gli artt. 31 ss. e 154, comma 1, lett. c) e h), nonché il disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B al medesimo Codice;

Provvedimento del Garante per la protezione dei dati personali "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" del 27 novembre 2008, così come modificato dal provvedimento del 25 giugno 2009.

4 Ambito d'applicazione

Le regole illustrate nel disciplinare tecnico si applicano a tutti i dipendenti appartenenti all'organico dell'Ente e a tutti coloro che a vario titolo (lavoratori subordinati, collaborazioni coordinate e continuative, tirocinanti, consulenti, ecc.) svolgono attività, compiti, mansioni come amministratori di sistema. Tali regole integrano quelle descritte nel *"Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta e nell'Assemblea legislativa della Regione Emilia-Romagna"*, ,e nel "*Disciplinare tecnico su modalità e procedure per verifiche di sicurezza su sistemi informativi, per controlli sull'utilizzo dei beni messi a disposizione dall'ente per attività lavorativa con riferimento alle strumentazioni informatiche e telefoniche ed esempi di comportamenti per il corretto utilizzo dei beni, da applicare nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna"* ,con particolare riferimento a quanto contenuto nell'Allegato A).

5 Registro digitale degli amministratori di sistema

Il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" richiede che sia mantenuto costantemente e tempestivamente aggiornato un elenco nominativo degli amministratori di sistema e che lo stesso sia reso disponibile, ad esempio in caso di accertamenti da parte del Garante stesso. Tale elenco deve specificare per ciascun nominativo l'ambito di operatività in funzione dei profili autorizzativi assegnati.

A tale scopo è istituito, il Registro digitale degli amministratori di sistema che contiene le seguenti macro categorie di sistemi amministrati.

- *Amministratori di dominio;* si tratta degli amministratori dei domini Active Directory interno ed esterno; rientrano in questa categoria i componenti dei gruppi "Domain Admins" e tutti coloro che attraverso un meccanismo di delega hanno la possibilità di agire su un sottoinsieme degli oggetti dei domini.
- *Amministratori di server;* si tratta degli utenti che hanno diritti amministrativi su uno o più server; a titolo esemplificativo rientrano in questa categoria gli utenti appartenenti al gruppo "Administrators" di uno o più server Windows o gli utenti di uno o più server Linux che attraverso il comando "sudo" possono impersonare l'utente "root".
- *Amministratori di basi di dati;* rientrano in questa categoria gli utenti che hanno la possibilità di manipolare la struttura di uno o più database attraverso comandi di "Data Definition Language".
- *Amministratori di apparati di rete;* rientrano in questa categoria gli utenti che hanno la possibilità di accedere ad apparati di rete layer 2 o layer 3 e modificarne le configurazioni.

- *Amministratori di apparati di sicurezza;* rientrano in questa categoria gli utenti che possono modificare le configurazioni di sistemi hardware o software dedicati alla sicurezza, quali ad esempio firewall, sistemi di intrusion prevention, web proxy e sistemi antivirus.
- *Amministratori di postazioni di lavoro individuale;* rientrano in questa categoria gli utenti appartenenti al gruppo "Administrators" di una o più postazione di lavoro.
- *Amministratori di sistemi software complessi;* rientrano in questa categoria gli amministratori di sistemi software applicativi o infrastrutturali che contengono diverse componenti hardware e software che interagiscono tra loro; esempi di sistemi software complessi sono i sistemi ERP, i sistemi di data warehouse, i sistemi di posta elettronica e i sistemi middleware.
- *Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori;* rientrano in questa categoria gli amministratori di sistema appartenenti ad una delle categorie sopra elencate che permettono il trattamento di informazioni personali riguardanti i lavoratori.

I nominativi degli amministratori che appartengono a quest'ultima categoria, come richiesto dal provvedimento del Garante per la protezione dei dati personali sopra citato, vengono comunicati attraverso il portale di comunicazione interna Internos.

All'interno del registro digitale degli amministratori di sistema, le macro categorie elencate sono ulteriormente dettagliate in ulteriori sottolivelli. In ogni categoria così specificata vengono descritte le funzioni svolte dagli amministratori e gli identificativi degli amministratori che svolgono tali funzioni.

La creazione e la tenuta del Registro digitale degli amministratori di sistema è in capo al Servizio Sistema informativo-informatico regionale che individua gli strumenti tecnologici più idonei per la gestione, la conservazione e l'aggiornamento.

La designazione dell'Amministratore di sistema è effettuata dal Responsabile della struttura a cui lo stesso è assegnato.

Le funzioni di amministrazione di sistema effettuate in modalità *outsourcing* non comportano né obblighi di inserimento nel Registro digitale degli amministratori di sistema né di designazione individuale da parte dell'Ente: tali compiti spettano al soggetto esterno che fornisce il servizio di *amministrazione di sistema in outsourcing* per l'Ente (cfr. par. 2 lett. d) del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008).

Le funzioni di amministrazione di sistema effettuate in modalità i*nsourcing* comportano invece obblighi di inserimento nel Registro digitale degli amministratori di sistema a seguito della designazione individuale da parte del soggetto esterno a cui sono affidati compiti di amministratore di sistema per l'Ente:

La gestione dell'elenco degli amministratori di sistema, così come descritta nel presente paragrafo, sostituisce gli adempimenti stabiliti al punto 5 del dispositivo della Determinazione del Responsabile del Servizio Sistema Informativo-Informatico regionale n. 6169/2009 avente ad oggetto "*Designazione degli amministratori di sistema della Giunta Regionale ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modifiche*", nonché al punto 5 del

dispositivo della determinazione della Responsabile del Servizio Gestione e Sviluppo n. 518/2009 avente ad oggetto “Designazione degli amministratori di sistema della Assemblea legislativa della Regione Emilia-Romagna ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modifiche”.

6 Procedura designazione degli amministratori di sistema

Per la Giunta, la lettera di designazione e incarico ad amministratore di sistema deve essere inviata al Servizio Sistema Informativo-Informatico regionale per l’aggiornamento del Registro digitale degli amministratori di sistema di cui al paragrafo 3. In alternativa, qualora fossero attivi meccanismi di delega per permettere l’accesso al Registro digitale degli amministratori di sistema da parte della struttura a cui l’amministratore è assegnato, potrà essere un delegato della struttura di appartenenza ad aggiornare il Registro.

Per l’Assemblea legislativa la designazione e l’ incarico di amministratore di sistema verrà comunicata dal Responsabile del Servizio Sistemi Informativi – informatici e innovazione all’amministratore di sistema nominato di cui precedentemente sono state attestate dal suo Responsabile di Struttura o dall’ Azienda esterna di appartenenza, le caratteristiche di esperienza, capacità e affidabilità.

La lettera di designazione per i dipendenti della Giunta verrà inviata anche per conoscenza al Servizio Organizzazione e Sviluppo per l’aggiornamento dell’Osservatorio delle competenze.

La lettera di designazione per i dipendenti dell’Assemblea legislativa verrà inviata anche per conoscenza al Servizio Organizzazione, bilancio e attività contrattuale per l’aggiornamento dell’Osservatorio delle competenze.

L’aggiornamento del Registro digitale degli amministratori di sistema di cui al paragrafo 3 sarà, per l’Assemblea legislativa, a carico del Servizio Sistemi informativi – informatici e innovazione.

Tutti i facsimili di designazione degli amministratori di sistema sono pubblicati nella sezione Privacy di Internos.

6.1 Amministratore di sistema “Interno”

Per amministratore di sistema “interno” si intende il personale alle dirette dipendenze dell’Ente a cui sono attribuite funzioni di amministratore di sistema.

L’attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto che si intende designare, il quale deve, quindi, fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza (cfr. par. 2 lett. a) del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008).

La valutazione è effettuata dal Responsabile della struttura a cui il soggetto da designare è assegnato.

A ciascuna singola persona fisica cui siano attribuite funzioni di amministratore di sistema è inviata una lettera di incarico, con l’elencazione degli ambiti di operatività in funzione dei

profili autorizzativi assegnati (cfr. Allegato 1 “Lettera di incarico ad amministratore di sistema di un dipendente/collaboratore regionale della Giunta” e Allegato 1a “Lettera di incarico ad amministratore di sistema di un dipendente/collaboratore regionale dell’Assemblea Legislativa”).

Qualora fosse necessario integrare le funzioni di un amministratore di sistema interno già designato, occorre inviare una lettera di integrazione dell’incarico (cfr. Allegato 2 “Lettera di integrazione/modifica delle funzioni di un amministratore di sistema dipendente/collaboratore della Giunta già designato” e Allegato 2a “Lettera di integrazione/modifica delle funzioni di un amministratore di sistema dipendente/collaboratore dell’Assemblea Legislativa già designato”)

6.2 Amministratori di sistema in “Insourcing”

Per amministratore di sistema in “i*nsourcing*” si intende il personale alle dipendenze di società esterne che svolge funzioni di amministratore di sistema presso l’Ente.

L’attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto che si intende designare, il quale deve, quindi, fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza (cfr. par. 2 lett. a) del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008).

La valutazione deve essere effettuata dall’Azienda di appartenenza del soggetto da designare amministratore di sistema; l’Azienda stessa deve essere preventivamente designata quale Responsabile esterno dei trattamenti di dati personali rispetto ai quali è chiamata a svolgere funzioni di amministratore di sistema.

Il Responsabile della struttura a cui fa capo il contratto con l’Azienda esterna deve richiedere che questa attesti l’effettuata valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto a cui sono attribuite funzione di amministratore di sistema.

A ciascuna singola persona fisica, cui siano attribuite funzioni di amministratore di sistema, deve essere inviata una lettera di incarico, con l’elencazione degli ambiti di operatività in funzione dei profili autorizzativi assegnati (cfr. Allegato 3 “Lettera di incarico ad amministratore di sistema *insourcing* di un soggetto dipendente da Fornitore esterno della Giunta” e Allegato 3a “Lettera di incarico ad amministratore di sistema *insourcing* di un soggetto dipendente da Fornitore esterno dell’Assemblea Legislativa”).

Qualora fosse necessario integrare le funzioni di un amministratore di sistema in *insourcing* già designato, occorre inviare lettera di integrazione dell’incarico (cfr. Allegato 4 “Lettera di integrazione/modifica delle funzioni di un amministratore di sistema *insourcing* già designato dipendente da Fornitore esterno della Giunta” e Allegato 4a “Lettera di integrazione/modifica delle funzioni di un amministratore di sistema *insourcing* già designato dipendente da Fornitore esterno dell’Assemblea Legislativa”).

6.3 Amministratori di sistema in “Outsourcing”

Nel caso di servizi affidati all’esterno, in modalità *outsourcing*, la designazione degli amministratori di sistema è effettuata dai soggetti che erogano i servizi stessi, i quali,

designati quali Responsabili esterni per i servizi affidati, hanno l'obbligo di conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

6.4 Amministratori di sistema delle "Postazioni di lavoro"

Tutti gli utenti che sono amministratori di postazione/i di lavoro devono essere designati amministratori di sistema.

In questi casi, prima dell'invio della lettera di incarico, il referente informatico oppure il Responsabile della struttura di appartenenza dell'amministratore di sistema che si intende designare, invia alle caselle email dedicate alla gestione e controllo della sicurezza (securityadmin@regione.emilia-romagna.it) e all'assistenza utenti (mailutenti@regione.emilia-romagna.it per la Giunta e cedcons@regione.emilia-romagna.it per l'Assemblea Legislativa) una richiesta di assegnazione di privilegi di amministratore della postazione di lavoro, corredata delle precise e circostanziate motivazioni poste a base della richiesta; valutate le motivazioni espresse, la struttura informatica centrale fornirà nulla osta alla designazione ad amministratore di sistema oppure, in alternativa, proporrà soluzioni alternative alla concessione dei privilegi richiesti. La valutazione delle caratteristiche soggettive del soggetto da designare amministratore di sistema segue quanto disposto dai parr. 6.1 e 6.2.

7 Sistema di Access Log

Il Garante per la protezione dei dati personali, nel provvedimento del 27 novembre 2008, prevede che venga tenuta traccia degli accessi logici degli amministratori di sistema ai sistemi da essi amministrati. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo di tempo, non inferiore a sei mesi.

A tale scopo è predisposto un sistema centralizzato di raccolta dei log dei sistemi, che garantisce le caratteristiche di completezza e inalterabilità richieste. Il sistema centralizzato di gestione dei log (*log management*) raccoglie i log di tutti gli accessi logici degli utenti (amministratori di sistema e non) dei sistemi sui quali siano stati designati amministratori di sistema e per i quali la tracciatura degli accessi sia tecnicamente possibile. Tale sistema è utilizzato inoltre per raccogliere e gestire i log di sicurezza di tutti i differenti sistemi che fanno parte del sistema informatico regionale (vedi capitolo 15).

La gestione del sistema di Access Log è in capo al Servizio Sistema informativo-Informatico regionale per la Giunta e al Servizio Sistemi informativi - informatici e innovazione per l'Assemblea legislativa: pertanto, ogni qualvolta venga attivato un sistema su cui è necessario autorizzare funzioni di "amministratore di sistema", occorre concordare col suddetto Servizio le modalità di integrazione ai fini della raccolta dei log. Allo stesso modo, una volta che il sistema viene dismesso, deve essere comunicata la dismissione al suddetto Servizio.

8 Verifica annuale delle attività degli amministratori di sistema

Il Garante per la protezione dei dati personali, nel provvedimento del 27 novembre 2008 sull'amministratore di sistema, fa previsione di un "due diligence" in capo al Titolare relativamente agli "accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare" sulle mansioni svolte dagli amministratori di sistema designati.

Nell'ambito delle funzioni di controllo sulla gestione dei rischi e, quindi, dell'internal audit, con "due diligence" si intende il processo di accertamento che viene messo in atto per verificare la compliance normativa, ovvero il rispetto di specifiche disposizioni impartite dal legislatore, da autorità di settore, da organismi di certificazione e da policy interne.

Tale attività è espletata in seno alle procedure previste nel Disciplinare Tecnico in materia di verifiche di sicurezza e controllo delle strumentazioni. Difatti, secondo quanto stabilito in tale Disciplinare, il Responsabile della Sicurezza effettua le cosiddette "Verifiche periodiche con cadenza superiore a 15 giorni", con le quali effettua una serie di verifiche di sicurezza volte a monitorare la conformità dei sistemi informativi e dei comportamenti dei soggetti utenti del sistema informativo regionale, alle prescrizioni di legge e alle regole stabilite dall'Ente nelle policy regionali adottate.

In tali casi , si verifica la corretta designazione da parte delle Strutture degli amministratori di sistema e, inoltre, la sussistenza dei requisiti di capacità e di affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. A tale scopo sono previste apposite verifiche atte a misurare la reale sussistenza dei profili di conoscenza e di capacità dei soggetti designati amministratori di sistema.

Inoltre dal sistema centralizzato di raccolta dei log sono estratti, relativamente alle macro categorie di sistemi amministrati di cui al par. 5 del presente Disciplinare, specifici report che contengono riferimenti a:

- Sistema amministrato
- Nome utente dell'amministratore
- Monte accessi al sistema un relativo ad un determinato periodo temporale
- Login riusciti
- Login falliti

In adempimento alle prescrizioni di legge, tali report sono conservati agli atti del Responsabile della Sicurezza della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna.

9 Sicurezza fisica

L'accesso ai locali della Giunta è regolato dall'apposito disciplinare tecnico regionale in materia ("*Disciplinare tecnico relativo al controllo degli accessi ai locali della Giunta della Regione Emilia-Romagna*" Determinazione n. 2649/2007 e sue eventuali modificazioni) mentre quello dell'Assemblea legislativa dal "Disciplinare tecnico relativo al controllo degli

accessi ai locali dell'Assemblea legislativa della Regione Emilia-Romagna" Determinazione n. 33 del 11 febbraio 2008, così come modificato dalla Determinazione n. 120 del 29 marzo 2011.

La scelta dei locali in cui installare, conservare o utilizzare sistemi informatici deve essere fatta tenendo in considerazione i potenziali rischi di sicurezza sui dati causati tanto da eventi accidentali quanto da dolo. In funzione dell'analisi dei rischi devono essere valutate e adottate idonee misure di protezione, quali sistemi di anti intrusione, sistemi anti incendio, sistemi di rilevazione fumi, sistemi antiallagamento.

La scelta delle misure di sicurezza dei locali deve in ogni caso tenere conto dei vincoli imposti dalla normativa in materia di tutela della salute e di sicurezza dei lavoratori (D.Lgs. 81/2008, "Testo Unico sulla Sicurezza e Salute delle Lavoratrici e dei Lavoratori").

La protezione dei server e degli apparati di rete considerati critici per il funzionamento e la disponibilità dei sistemi informativi deve prevedere sistemi di protezione elettrica quali stabilizzatori di corrente ed apparecchiature UPS, e di sistemi di condizionamento dell'aria nei locali per garantire il mantenimento di una costante ed adeguata temperatura di esercizio.

La definizione dei cablaggi deve prevedere la predisposizione di tracce dedicate.

La scelta dei locali per gli armadi (es. per contenere switch) deve essere fatta individuando ambienti idonei, possibilmente dedicati e ad accesso limitato (solo agli amministratori di sistema e ad eventuali altri soggetti autorizzati). Gli armadi medesimi devono essere chiusi a chiave e le relative chiavi devono essere in possesso del solo personale interno e/ o esterno autorizzato ed incaricato. Le chiavi di accesso a locali o armadi possono essere conservate presso le portinerie dell'Ente. In tal caso devono essere osservate le disposizioni previste nel "Disciplinare tecnico relativo al controllo degli accessi ai locali della Giunta della Regione Emilia-Romagna" adottato con determinazione n. 2649/2007 e nel "Disciplinare tecnico relativo al controllo degli accessi ai locali dell'Assemblea legislativa della Regione Emilia-Romagna" Determinazione n. 33 del 11 febbraio 2008, così come modificato dalla Determinazione n. 120 del 29 marzo 2011.

10 Controllo dell'accesso ai dati

L'accesso ai dati ed alle strumentazioni informatiche utilizzate per trattarli deve essere concesso al solo personale espressamente autorizzato (nel caso di dati personali i c.d. incaricati del trattamento). L'elenco del personale incaricato deve essere aggiornato con le modalità individuate nella deliberazione di Giunta n. 2416/2008 Appendice 5 e nella deliberazione dell'Ufficio di Presidenza n. 197 del 18/10/2006.

In nessun modo devono essere concessi permessi di accesso ai sistemi senza preventiva autorizzazione formale del responsabile funzionale o del referente regionale di progetto. Le modalità con cui viene formulata tale autorizzazione possono variare a seconda del tipo di trattamento (per esempio email, lettera protocollata, Determinazione).

10.1 Autenticazione informatica

L'accesso ai dati trattati con strumentazioni informatiche deve essere concesso esclusivamente previa opportuna autenticazione.

Gli strumenti di autenticazione devono essere progettati in funzione del valore dei dati trattati. Deve essere prevista l'ipotesi di utilizzo di sistemi di autenticazione forte ove necessario (smart card, token hardware, dispositivi one-time password, sistemi biometrici).

Devono essere previsti meccanismi di separazione dei privilegi (vedasi anche paragrafo 10.2), sia a livello di sistema operativo che a livello applicativo, per consentire l'accesso ai dati e le operazioni effettuate sugli stessi, in misura corrispondente ai diversi profili degli utenti.

10.2 Autorizzazione

È necessario introdurre dei criteri generali di definizione dei ruoli amministrativi e di gestione delle autorizzazioni, pur nel pieno rispetto dei principi di delega e di autonomia dei referenti di applicazioni e sistemi che gestiscono porzioni del sistema informativo.

Il principio generale a cui attenersi è che i ruoli amministrativi critici non si devono sovrapporre. Ad esempio gli sviluppatori non devono essere anche sistemisti, gli amministratori della sicurezza non devono essere sistemisti o sviluppatori e così via. Qualora non fosse possibile dal punto di vista organizzativo mantenere o adottare questa separazione di ruoli, devono essere introdotti controlli compensativi che permettano di tracciare puntualmente le operazioni eseguite (ad esempio tramite l'utilizzo di strumenti evoluti di monitoraggio, audit puntuali, notifiche via email).

10.3 Gestione delle credenziali

Le credenziali consentono all'utente di accedere ai dati e pertanto è necessario che la loro assegnazione segua procedure codificate e condivise. Tali procedure possono essere diverse in funzione sia del valore dei dati da trattare che dei sistemi coinvolti.

In generale, le richieste delle credenziali di autenticazione devono essere fatte dai responsabili funzionali o referenti regionali di progetto. In ogni caso, deve essere tenuta traccia della richiesta che ha generato la creazione di una credenziale di autenticazione sul sistema. Le modalità con cui sono formulate le richieste variano in funzione della criticità dei dati o dei sistemi (per esempio: email, lettera protocollata, Determinazione).

Ogni credenziale di autenticazione deve riferirsi ad un singolo utente. Non è consentito l'utilizzo di credenziali condivise. Fanno al momento eccezione a questa regola le credenziali amministrative di accesso ai sistemi (es. root, administrator), che devono comunque essere assegnate ad un numero limitato di incaricati e devono essere utilizzate solo nel caso di interventi particolari sui sistemi. Ove possibile, bisogna privilegiare sempre l'utilizzo di credenziali nominative anche nel caso di operazione di amministrazione dei sistemi.

La gestione delle credenziali deve seguire le procedure documentate per i vari sistemi di autenticazione. La policy di scadenza delle credenziali non utilizzate è normalmente di 180 giorni. Fa eccezione a questa regola il dominio applicativo esterno per la peculiarità di alcune applicazioni che sono utilizzate dagli utenti con periodicità annuale: in questo caso le credenziali non utilizzate sono disabilitate dopo un anno. Le policy di gestione delle password devono essere allineate sui diversi sistemi e comunque conformi ai dettami del Dlgs 196/03: lunghezza minima 8 caratteri, scadenza 90 giorni, modifica al primo accesso, blocco dopo 5 tentativi errati.

Le credenziali amministrative non nominative di gestione dei sistemi non sono vincolate alle stesse regole delle credenziali nominative, non scadono dopo un periodo di inutilizzo, non vengono bloccate dopo un certo numero di tentativi errati, non hanno la password che scade e non ne viene richiesta la modifica al primo accesso. Perciò gli amministratori dei sistemi sono tenuti ad adottare politiche di modifica manuale delle password dei loro sistemi e a monitorare gli eventuali tentativi di accesso non autorizzato.

Le credenziali amministrative non nominative create al solo scopo di avviare servizi sui server non devono poter effettuare l'accesso interattivo sui sistemi stessi o, ove ciò non fosse tecnologicamente possibile, deve essere comunque monitorato il loro utilizzo per scopi diversi rispetto all'ambito per cui sono state create.

Le credenziali di autenticazione con privilegi amministrativi non devono essere inviate via email: in tali casi, è necessario convocare l'utente e fornirgli le credenziali verbalmente, oppure mediante un sistema di scambio informazioni sicuro.

Gli amministratori dei sistemi sono tenuti a rispettare le procedure adottate e a non creare particolarità o eccezioni nella gestione delle credenziali utente.

La gestione delle credenziali amministrative deve seguire regole molto rigide e stringenti: devono essere identificate le persone autorizzate a richiedere l'aggiunta o la modifica di amministratori dei sistemi o delle applicazioni e deve essere previsto un sistema di notifica che avvisi gli altri amministratori del cambiamento.

In generale una procedura di gestione delle credenziali deve prevedere:

a. l'identificazione di chi può chiedere la creazione, la modifica, la disabilitazione, la cancellazione di un'utenza, le operazioni di sblocco dell'utente o il reset della password; tale identificazione, qualora avvenga tramite telefono, deve essere fatta chiedendo alcuni dati personali al richiedente;
b. la modalità di inoltro della richiesta: alcune operazioni quali la creazione o la modifica dovranno essere fatte via email o fax, altre quali il reset della password potranno anche essere fatte verbalmente dall'utente interessato tramite telefono previa la verifica da parte degli amministratori dell'identità dell'interessato (es. tramite richiesta di alcuni dati personali); per il reset della password privilegiare comunque modalità di self-service, in cui sia l'utente stesso, in seguito alla risposta ad alcune domande da lui stesso precedentemente impostate, ad avere la possibilità di azzerare la password;
c. l'elenco dei destinatari della richiesta: ad esempio i referenti dell'applicazione, gli amministratori dei sistemi, il servizio di help desk;
d. la tempistica di evasione della richiesta;
e. l'archiviazione e il backup delle richieste pervenute via email e delle risposte relative all'attività svolta. Se la richiesta è in formato cartaceo deve essere acquisita agli atti;
f. la modalità di risposta al richiedente per comunicare l'avvenuta attivazione dell'utenza, il nome utente e la password (a tale proposito valutare se sia opportuno crittografarla, ovvero comunicarla verbalmente all'utente, ove possibile).

10.4 Gestione delle password

La lunghezza minima consentita per le password deve essere impostata ad almeno otto

caratteri. Ove la tecnologia non lo consenta, la lunghezza delle password deve essere impostata al massimo consentito dal sistema.

La durata della password dovrebbe essere impostata in base al grado di criticità di sistemi e basi dati. Inoltre, una eventuale password di “single sign on” è opportuno abbia una durata inferiore a quella delle password che sostituisce.

Per contrastare attacchi alle password di tipo “bruteforce” i sistemi informatici devono prevedere opportuni meccanismi per la disabilitazione di un account dopo un intervallo finito di tentativi di accesso non riusciti. Devono comunque essere previsti meccanismi di difesa da attacchi di tipo *denial of service* causati dal blocco volontario di account legittimi. Un esempio di tali meccanismi di difesa è di consentire per un account un limite massimo di cinque tentativi di accesso non riusciti, prevedendo il blocco dell'account per un periodo di trenta minuti nel caso in cui tale limite venga superato.

Ove tecnologicamente possibile, deve essere data agli utenti la possibilità di modificare la propria password senza l’intervento degli amministratori.

Devono essere previsti meccanismi di implementazione dei sistemi tali da garantire all'utente la modifica della propria password al primo accesso al sistema.

Le password non devono essere conservate in chiaro, né trasmesse su canali non cifrati. Utilizzare adeguati meccanismi di cifratura anche in funzione del valore dei dati. Per esempio, utilizzare hash calcolati con funzioni irreversibili per la conservazione su disco e protocolli di comunicazione cifrati come SSL.

In caso di trattamento di dati sensibili e/o giudiziari o comunque di rilevanza strategica, devono essere previsti sistemi di controllo delle password per consentire il solo utilizzo di password “resistenti” ad attacchi “bruteforce”. Per esempio, password formate con valori alfanumerici maiuscoli e minuscoli, simboli e caratteri speciali.

Al momento dell'installazione, su tutti i sistemi devono essere modificate le password di default utilizzate dal produttore/installatore.

11 Protezione dei dati

11.1 Backup dei dati

Per garantire la disponibilità dei dati devono essere previste idonee procedure di backup in funzione del valore dei dati trattati. Tali procedure devono essere formalizzate per iscritto e tenute aggiornate con cadenza almeno annuale.

Con cadenza periodica (perlomeno annuale) devono essere effettuati controlli a campione (su un campione opportunamente numeroso: es. una copia per ogni mese) sulle copie di backup per verificarne la disponibilità e l'integrità.

A fronte di cambiamenti intervenuti nel sistema di backup o nei sistemi che devono essere archiviati devono essere fatti dei test di backup e restore per verificare la consistenza dei dati salvati.

Tutti i test vanno documentati in un “diario di bordo” che riporti la data del test, il sistema coinvolto, la persona che ha eseguito il test e l’esito delle operazioni effettuate.

Le copie di backup devono essere conservate in locali fisicamente separati da quelli dei sistemi origine dei dati, per garantire la disponibilità delle copie in caso di eventi accidentali quali incendi o disastri naturali. Le copie dei backup devono essere riposte, possibilmente, in casseforti le cui chiavi sono conservate da personale identificato. L'elenco del personale autorizzato deve essere regolarmente mantenuto aggiornato.

Gli amministratori devono censire e tenere aggiornate le informazioni sul backup dei sistemi da loro gestiti. In particolare devono richiedere alla struttura competente l'attivazione del backup per i nuovi sistemi e applicazioni e devono segnalare esigenze particolari di backup che esulino dalle politiche in essere di backup centralizzato.

Gli amministratori del sistema di backup devono monitorare l'esito dei task eseguiti e, qualora rilevassero problemi, darne pronta segnalazione agli amministratori dei sistemi coinvolti.

Il sistema di backup, sia per quanto riguarda il software di base che il software applicativo, deve essere mantenuto aggiornato, in particolare relativamente alle patch/hot-fixes di sicurezza. Qualora venissero rilasciate patch/hot-fixes di sicurezza per la parte client, gli aggiornamenti sui singoli sistemi devono essere pianificati in accordo con gli amministratori degli stessi.

Le politiche di backup debbono essere documentate, mantenute aggiornate, e messe a disposizione in apposita sezione di Internos ad accesso riservato per la consultazione sia da parte degli amministratori di sistema sia da parte dei soggetti incaricati per quanto di propria competenza.

11.2 Procedure di dismissione dei sistemi: protezione dei dati

Ogni qualvolta si dismette un dispositivo elettronico o informatico che contiene dati personali, è necessario adottare idonei accorgimenti e misure, anche attraverso soggetti terzi, tecnicamente qualificati, che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Chi procede al riutilizzo di dispositivi elettronici o informatici è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo ove possibile, l'autorizzazione a cancellarli o a renderli non intellegibili.

Il processo di rimozione dei dati dai dischi dei computer è denominato *disk sanitizing*, *cleaning*, *purging*, o *wiping*. Il metodo scelto per "disinfettare" un disco dipende dalla criticità dei dati in esso contenuti.

Cancellare un file comporta in effetti la sola rimozione del puntatore al file. Esistono strumenti software in grado di recuperare file cancellati e quindi i dati in essi contenuti. Pertanto, per garantire la cancellazione sicura delle informazioni le tecniche possibili sono:

- sovrascrittura: consiste nella sostituzione dei dati precedentemente memorizzati con nuove informazioni, procedendo alla scrittura byte a byte del disco utilizzando una sequenza regolare oppure una sequenza casuale di valori;

- formattazione “a basso livello” (LLF) dei dispositivi di tipo hard disk, laddove possibile, attenendosi alle istruzioni fornite dal produttore e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
- smagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici, in grado di garantire la cancellazione rapida delle informazione anche su dispositivi non più funzionanti sui quali potrebbero non essere applicabili le procedure di cancellazione software;
- distruzione fisica dei dispositivi.

La sovrascrittura è in genere sufficiente a garantire che i dati prima presenti non siano più recuperabili e dunque leggibili.

Smagnetizzare o distruggere fisicamente il disco garantisce l’inutilizzabilità futura del disco medesimo e dunque previene qualsiasi tentativo di recupero dei dati.

Le procedure utilizzate in caso di reimpiego o di smaltimento dei dispositivi e degli strumenti informatici debbono essere documentate, mantenute aggiornate, e messe a disposizione in apposita sezione di Internos ad accesso riservato per la consultazione sia da parte degli amministratori di sistema sia dei soggetti incaricati per quanto di propria competenza.

12 Protezione delle applicazioni

12.1 Design e sviluppo

Valgono le regole descritte nel documento *"Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta della Regione Emilia-Romagna" Determinazione n 2651/2007 e sue eventuali modificazioni* e nel “Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nell’Assemblea legislativa della Regione Emilia-Romagna” Determinazione n. 480/2007 e sue eventuali modificazioni.

12.2 Deployment e gestione

Le decisioni in merito alla richiesta, lo sviluppo o l'acquisizione, l'installazione e l'utilizzo di un'applicazione devono essere documentate per iscritto ed opportunamente autorizzate dal responsabile funzionale o referente di progetto. Analoga documentazione deve essere prevista per le modifiche da effettuare su applicazioni già esistenti.

L'installazione di hardware o software deve sempre essere effettuata da personale autorizzato e comunque seguendo quanto prescritto nel presente disciplinare tecnico.

Nel caso di sistemi utilizzati per l'adozione delle misure minime di sicurezza previste dalla normativa vigente, deve essere richiesta al fornitore una descrizione scritta dell'intervento che ne attesta la conformità alle disposizioni previste dalla legge.

Valgono le regole descritte nel documento *“Linee guida per la governance del sistema informatico regionale”* Determinazione n. 4213/2009 *e sue successive modificazioni*.

13 Protezione dei sistemi

È compito di ogni amministratore mantenere un elenco aggiornato e completo delle risorse gestite.

Precedentemente alla progettazione, implementazione, installazione o gestione di un sistema, deve essere effettuata un'analisi dei rischi per determinare le misure di sicurezza da adottare.

Tutti gli interventi tecnici che coinvolgono la creazione, modifica o eliminazione di uno dei meccanismi di sicurezza indicati nel disciplinare tecnico, devono essere opportunamente documentati ed autorizzati da parte del proprio referente funzionale.

13.1 Workstation

Gli amministratori dei client devono tener conto delle policy generali relative alle workstation.

Policy generale

a. Gli utenti finali non devono avere privilegi amministrativi sulle workstation: per eventuali eccezioni a questa regola attenersi a quanto prescritto al paragrafo 6.4;

b. il software utilizzato sulle workstation deve essere associato, qualora fosse necessario, ad una licenza, in accordo con le specifiche del fornitore/produttore;

c. le workstation assegnate al personale dell'Ente devono essere utilizzate solo per gli scopi designati;

d. è vietato installare hardware addizionale senza autorizzazione da parte del Servizio Sistema Informativo - Informatico Regionale o del Servizio Sistemi informativi - informatici e innovazione, ognuno per la parte di propria competenza;

e. è vietato installare software su una workstation dell'Ente senza autorizzazione da parte del Servizio Sistema Informativo - Informatico Regionale o del Servizio Sistemi informativi - informatici e innovazione, ognuno per la parte di propria competenza;

f. è vietato alterare o cancellare software o modificare configurazioni su una workstation dell'Ente senza autorizzazione da parte del Responsabile del Servizio Sistema Informativo - Informatico Regionale o del Servizio Sistemi informativi - informatici e innovazione, ognuno per la parte di propria competenza;

Per quanto concerne le prescrizioni di dettaglio, vedere la *Tabella A Installazione Windows client*.

13.2 Server

Gli amministratori dei sistemi server devono tener conto delle seguenti policy generali e devono documentare qualsiasi eccezione a queste regole.

Policy generale

a. L'elenco dei server è contenuto all'interno del CMDB dell'Ente. Per ognuno di essi sono indicati:

   - i riferimenti fisici e logici del server (nome e indirizzo di rete) e la sua ubicazione;
   - le versioni dell'hardware e del sistema operativo;
   - le funzioni e applicazioni principali oppure il ruolo all'interno dell'infrastruttura regionale.

b. Hardware, sistemi operativi, servizi ed applicazioni installati devono essere approvati dal Servizio Sistema Informativo - Informatico Regionale o dal Servizio Sistemi informativi - informatici e innovazione per l'Assemblea legislativa, ognuno per la parte di propria competenza. Fare riferimento al documento "Linee guida per la governance del sistema informatico regionale" Determinazione n. 451/2008.

c. Tutte le patch/hot-fixes di sicurezza rilasciate dai fornitori devono essere installate nel minor tempo possibile e comunque non dopo i 90 giorni dal loro rilascio, valutando a priori in base al rischio la verifica in ambiente di pre-produzione. Sono ammesse eccezioni basate su specifiche esigenze di servizio dell'Ente, adeguatamente giustificate, documentate e riportate dagli amministratori al Responsabile del Servizio Sistema Informativo - Informatico Regionale o dal Responsabile del Servizio Sistemi informativi - informatici e innovazione dell'Assemblea legislativa, ognuno per la parte di propria competenza. Questa direttiva si applica a tutti i servizi installati, anche qualora tali servizi possano essere temporaneamente o definitivamente disabilitati. È compito degli amministratori mantenersi costantemente aggiornati sulle patches/hotfixes da installare.

d. Servizi non necessari ad esigenze di servizio dell'Ente devono essere disabilitati.

e. Servizi ad accesso non anonimo devono essere protetti da apposite ACL (Access Control Lists).

f. Servizi non sicuri devono essere sostituiti da equivalenti oggetti sicuri, ove ciò sia possibile. Per esempio servizi con traffico in chiaro (FTP, telnet, HTTP) devono essere sostituiti da servizi con traffico cifrato (S-FTP, SSH, HTTPS).

g. Relazioni di fiducia tra sistemi possono essere configurate solo per specifiche esigenze di servizio. Devono essere documentate dagli amministratori di sistema e portate a conoscenza dei Responsabile della Sicurezza della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna

h. Qualsiasi attività di amministrazione remota deve essere effettuata utilizzando canali sicuri (es. connessioni di rete con crittografia, che utilizzino SSH o IPSEC). Qualora non sia disponibile una modalità di accesso remoto sicuro, dovrebbero essere utilizzate "one-time" password per tutti i livelli di accesso.

i. I server di produzione devono essere fisicamente localizzati in un ambiente ad accesso controllato, con un impianto di condizionamento adeguato alle esigenze, ovvero in grado di mantenere la temperatura e l'umidità entro i limiti che consentono la normale operatività dei server.

j. E' vietata l'installazione di hardware e software non autorizzato. Tutte le attività di modifica di hardware o software devono essere preventivamente autorizzate, preferibilmente mediante definizione e schedulazione delle attività di aggiornamento (upgrade sistema operativo, modifica hardware, ecc.).

k. Tutti i server di produzione devono essere collegati ad un sistema di UPS (Uninterruptible Power Supplies); se possible tale sistema dovrebbe permettere la disconnessione (shutdown) automatica dei server oppure l'attivazione di un sistema di alimentazione di emergenza prima dell'esaurimento delle batterie.

Per quanto concerne le prescrizioni di dettaglio, vedere la *Tabella B Installazione Server:generalità*, la *Tabella C Installazione Windows Server* e la *Tabella D Installazione Unix Server*.

13.3 Apparati di rete

Gli amministratori di rete nell'attività di configurazione e gestione degli apparati di rete di produzione devono basarsi sulle seguenti regole generali e documentare le eventuali deroghe o eccezioni.

Policy generale

a. Tutti i router dovrebbero usare TACACS+ oppure RADIUS per autenticare gli utenti. L'accesso con account locali è consentito solo in situazioni d'emergenza ovvero quando non fosse disponibile il sistema centralizzato di autenticazione.

b. La password di enable deve essere configurata utilizzando il meccanismo di "enable secret" che ne permette la cifratura sicura.

c. Disabilitare le seguenti funzioni (alcuni termini inglesi non sono stati tradotti perché così sono conosciuti in ambito tecnico):
    - IP directed broadcast
    - pacchetti in ingresso con indirizzi non validi come da RFC1918
    - TCP small services
    - UDP small services
    - tutti i source routing
    - tutti i servizi web

d. Utilizzare il protocollo SNMP v3. In caso non fosse possibile, usare la community SNMP adottata dall'Ente e comunque diversa da *public* o *private*, oppure limitare l'accesso agli apparati impostando opportuni filtri.

e. Le regole di accesso devono essere aggiunte o modificate aderendo alle necessità dell'Ente.

f. I router devono avere un banner di login che notifichi a chi accede che l'apparato è proprietà dell'Ente e che l'accesso è consentito al solo personale autorizzato.

g. Gli apparati di rete devono essere elencati nel sistema CMDB dell'Ente e quindi censiti riportando i riferimenti dei responsabili tecnici, i riferimenti fisici e logici.

h. Il protocollo Telnet non dovrebbe essere usato per gestire i router se non utilizzando un canale sicuro di trasmissione. In ogni caso è preferibile utilizzare il protocollo SSH.

Per quanto concerne le prescrizioni di dettaglio, vedere la *Tabella E Installazione apparato di rete*.

13.4 Dispositivi portatili

I dispositivi portatili seguono le stesse policy indicate per le workstation con un'attenzione maggiore alla protezione dei dati personali e alla tutela rispetto ai possibili tentativi di furto.

Per i dispositivi PDA/Smartphone è necessario fare riferimento alle policy regionali in materia di telefonia mobile e alle *"Linee guida per la governance del sistema informatico regionale" (*Determinazione n. 4213/2009 *e sue successive modificazioni)*.

In caso di furto o smarrimento di un dispositivo smartphone che lo permetta, l'amministratore di tali dispositivi deve agire tempestivamente, anche su segnalazione verbale del possessore, previa verifica dell'identità dello stesso tramite, ad esempio, la richiesta di alcuni dati identificativi personali (es matricola, codice fiscale, ecc.). L'amministratore del sistema, verificata l'identità del possessore del dispositivo, dovrà tempestivamente cancellare i dati del dispositivo da remoto per evitare il furto o l'uso improprio da parte di soggetti non autorizzati di eventuali dati personali memorizzati sul dispositivo e assicurarsi che l'utente invii il prima possibile idonea documentazione di attestazione del furto o smarrimento.

Policy generale

a. I dispostivi portatili, ove tecnicamente possibile, devono essere protetti dai tentativi di furto: es. custoditi in ambienti chiusi a chiave, protetti tramite cavo di sicurezza con chiave o combinazione (nel caso di laptop).

b. Tutte le schede di rete (es. PC cards, Internet Key, schede WiFi) utilizzate su laptop o desktop di proprietà dell'Ente devono essere registrate. Tali schede non possono essere utilizzate mentre il laptop o desktop è collegato alla rete interna.

Per quanto concerne le prescrizioni di dettaglio, vedere la *Tabella A Installazione Windows client*.

14 Protezione delle reti e delle comunicazioni

Di seguito sono riportate le policy e le procedure relative alle connessioni Internet, alle comunicazioni, alla sicurezza perimetrale, alla Intranet, alla DMZ, alla VPN ed alle connessioni wireless.

I referenti informatici sono tenuti a rammentare a tutti gli utenti appartenenti alla struttura di loro competenza le disposizioni contenute nel Disciplinare Tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna, nello specifico la parte relativa alla Protezione delle rete e delle comunicazioni e nel "Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nell'Assemblea legislativa della Regione Emilia-

Romagna.

Protezione delle reti: connessione ad Internet

Policy generale

a. Le connessioni permanenti ad Internet, esclusi gli ambienti di test autorizzati per le prove ed il supporto agli utenti, devono passare esclusivamente attraverso il firewall regionale. I firewall devono essere utilizzati per rendere più sicure le connessioni ad Internet e ad altre reti. Gli utenti che si connettono dall'esterno alla rete regionale tramite VPN devono utilizzare personal firewall e/o "firewall appliances" per rendere più sicure le loro connessioni ad internet e ad un provider.

b. I firewall sono la "prima linea di difesa" da minacce esterne. La sicurezza interna non è garantita dalla presenza di un firewall perimetrale. I sistemi interni, gli apparati di rete e le applicazioni devono essere adeguatamente aggiornati e configurati a prescindere dalla presenza del firewall.

c. Tutti i sistemi di rete locali o globali (firewall, router, ecc.) che consentono una connessione simultanea alla rete dell'Ente e ad una qualsiasi rete "non-trusted" (Internet or terza parte) devono essere gestiti e aggiornati dagli amministratori di rete e di sicurezza centrali.

d. Le connessioni dirette ad Internet non sono consentite, se non dopo esplicita e formale approvazione da parte del Responsabile del Servizio Sistema Informativo - Informatico Regionale. In ogni caso non è consentito l'accesso diretto ad internet (es. via modem e via reti wireless: wi-fi, UMTS, etc) qualora si sia connessi alla rete locale.

e. Tutti i dispositivi che implementano la funzione di Network Address Translation (NAT) locali sulla rete dell'Ente che non siano gestiti da operatore autorizzato, devono essere gestiti dagli amministratori locali. Tali dispositivi possono essere installati solo previa approvazione del Responsabile del Servizio Sistema Informativo - Informatico Regionale.

f. Ogni firewall deve avere il proprio set di regole. Tali regole devono essere aggiornate e riviste periodicamente per verificarne la coerenza con le modifiche fatte nell'arco di tempo. Le regole devono essere aggiornate anche in seguito al sorgere di nuovi attacchi o vulnerabilità. Per rendere il processo di creazione del set di regole meno soggetto ad errori e più verificabile dovrebbe basarsi su una matrice, o elenco, di applicazioni di rete.

g. Le patch e hotfix per i firewall devono essere tempestivamente valutate, selezionate ed installate. Le regole del firewall devono essere aggiornate quando necessario anche a seguito di rilevazioni o segnalazioni di incidenti di sicurezza . A tale proposito, è necessario utilizzare un processo formale di gestione delle integrazioni e cancellazioni delle regole di configurazione del firewall: tale processo verrà dettagliato definendo e schedulando le attività di aggiornamento (upgrade sistema operativo, modifica hardware, ecc.).

h. I firewall devono essere testati nuovamente dopo ogni modifica della configurazione. Devono inoltre essere testati periodicamente tramite l'ausilio di personale tecnico specializzato.

i. Le Access Control Lists devono essere configurate specificando quale tipo di connettività sia permessa, con la specifica condizione che tutte le altre non sono permesse. Tutto il traffico di rete che non sia esplicitamente permesso, non deve essere consentito.

j. Qualsiasi protocollo e traffico che non sia necessario, ad esempio non utilizzato o non necessario e/o non consentito dalla policy, deve essere bloccato utilizzando un “border router” e la tecnologia “packet filtering”. Ciò consente di ridurre il rischio di attacco e riduce il traffico sulla rete, rendendola (e rendendolo) quindi più agevole da monitorare.

k. L’infrastruttura di rete deve essere configurata in modo da chiudere sessioni inattive dopo un’ora, con l’eccezione di specifiche necessità di servizio.

l. Tutte le porte non utilizzate sul proxy o sul firewall devono essere bloccate.

m. Occorre bloccare sul firewall i seguenti servizi e tipi di traffico applicativo in ingresso, con eccezioni dipendenti da necessità di servizio:

Applicazione	Numeri porta	Azione
Login services	telnet - 23/tcp	Bloccare sempre
	SSH - 22/tcp	Restringere a specifici sistemi
	FTP - 21/tcp	Restringere con “strong authentication”
	NetBIOS - 139/tcp	Bloccare sempre
	r services - 512/tcp - 514/tcp	Bloccare sempre
	Remote Desktop – 3389/tcp	Bloccare sempre
RPC ed NFS	Portmap/rpcbind - 111/tcp/udp	Bloccare sempre
	NFS – 2049/tcp/udp	Bloccare sempre
	lockd - 4045/tcp/udp	Bloccare sempre
NetBIOS in Windows NT	135/tcp/udp	Bloccare sempre
	137/udp	Bloccare sempre
	138/udp	Bloccare sempre
	139/tcp	Bloccare sempre
	445/tcp/udp in Windows 2000	Bloccare sempre
X Windows	6000/tcp - 6255/tcp	Bloccare sempre
Naming services	DNS - 53/udp	Restringere a server DNS esterni
	DNS zone transfers - 53/tcp	Bloccare a meno che non sia secondaria esterna
	LDAP . 389/tcp/udp	Bloccare sempre
Mail	SMTP – 25/tcp	Bloccare a meno di trasmissione di una mail dall’esterno
	POP - 109/tcp and 110/tcp	Bloccare sempre
	IMAP – 143/tcp	Bloccare sempre
Web	HTTP - 80/tcp and SSL 443/tcp	Bloccare tranne che per server Web pubblici
	Si può anche bloccare common high-order HTTP port choices – 8000/tcp, 8080/tcp, 8888/tcp, ecc.	
"Small Services"	Porte sotto 20/tcp/udp	Bloccare sempre
	Time - 37/tcp/udp	Bloccare sempre
Miscellaneous	TFTP - 69/udp	Bloccare sempre
	finger - 79/tcp	Bloccare sempre
	NNTP . 119/tcp	Bloccare sempre

	LPD - 515/tcp	Bloccare sempre
	syslog . 514/udp	Bloccare sempre
	SNMP - 161/tcp/udp, 162/tcp/udp	Bloccare sempre
	BGP - 179/tcp	Bloccare sempre
	SOCKS - 1080/tcp	Bloccare sempre
ICMP	Bloccare la richiesta in ingresso di “echo” (ping e Windows traceroute)	
	Bloccare riposte in uscita a “echo”, eccedenti il limite di tempo, e messaggi con destinazioni irraggiungibili eccetto messaggi "packet too big" (type 3, code 4). Ciò significa che si intende anticipare l’utilizzo legittimo di richieste “echo” ICMP per bloccare utilizzi malevoli noti.	

Quanto riportato in tabella è stato adattato da linee guida CERT/CC (Computer Emergency Response Team/Coordination Center) e SANS Institute.

n. E’ altresì necessario bloccare i seguenti tipi di traffico di rete su firewalll interfaccianti Internet o terze parti:

1) Traffico in ingresso da una fonte non autenticata, con un indirizzo di destinazione del firewall stesso. Questo tipo di pacchetto normalmente rappresenta un tipo di prova o attacco contro il firewall.

2) Traffico in ingresso con un indirizzo sorgente che indica come il pacchetto si sia originato su una rete dietro il firewall. Questo tipo di pacchetto, verosimilmente, indica un tentativo di “spoofing” in corso.

3) Traffico in ingresso contenente traffico ICMP (Internet Control Message Protocol). L’ ICMP può essere utilizzato per fare una mappatura delle reti interne.

4) Traffico in ingresso o in uscita da un sistema che utilizzi un indirizzo sorgente che ricade entro gli intervalli di indirizzi riservati in RFC 1918 come destinati a reti private. Come riferimento, RFC 1918 riserva i seguenti intervalli di indirizzi per le reti private:

   - Da 10.0.0.0 a 10.255.255.255 (Classe A, o “/8” in notazione CIDR)
   - Da 172.16.0.0 a 172.31.255.255 (Classe B, o “/12” in notazione CIDR)
   - Da 192.168.0.0 a 192.168.255.255 (Classe C, o “/16” in notazione CIDR)

   Il traffico in ingresso con questi indirizzi sorgente tipicamente indica l’inizio di un attacco “denial-of-service” che coinvolge il flag TCP SYN. Alcuni firewall sono dotati di funzionalità per contrastare tali attacchi, ma questo tipo particolare di traffico di rete deve ancora essere bloccato con apposite regole.

5) Traffico in ingresso, da una sorgente non autenticata, contenente traffico SNMP (Simple Network Management Protocol). Tali pacchetti possono essere indice che un intruso stia mettendo alla prova la rete, ma ci sono scarse motivazioni per cui l’Ente voglia permettere traffico SNMP in ingresso, e pertanto deve essere bloccato nella grande maggioranza dei casi.

6) Traffico in ingresso contenente informazione di tipo “IP Source Routing”. Source Routing è un meccanismo che permette ad un sistema di specificare i percorsi che il traffico di rete deve percorrere per viaggiare dalla sorgente alla destinazione. Da un punto di vista della sicurezza, il Source Routing può consentire ad un intruso (attacker) di costruire un pacchetto che aggiri i controlli del firewall. Nelle reti moderne, IP Source Routing viene raramente utilizzato, ed inoltre applicazioni valide sono ancora meno comuni su Internet.

7) Traffico di rete in ingresso o in uscita contenente un indirizzo sorgente o destinazione pari a 127.0.0.1 (localhost). Tale traffico rappresenta solitamente un tipo di attacco contro il firewall.

8) Traffico di rete in ingresso o in uscita contenente un indirizzo sorgente o destinazione pari a 0.0.0.0. Alcuni sistemi operativi interpretano tale indirizzo sia come localhost che come broadcast; pertanto tali pacchetti possono essere utilizzati per sferrare attacchi.

9) Traffico in ingresso o in uscita contenente un indirizzo di tipo “directed broadcast” (indirizzo che comprende tutti gli host di una rete). Un tale indirizzo viene spesso utilizzato per dare inizio ad un attacco massivo, quale lo SMURF. Gli indirizzi “directed broadcast” permettono ad un sistema di inviare un messaggio broadcast con un indirizzo sorgente diverso dal proprio. In altre parole, un sistema può inviare un messaggio con un indirizzo alterato. Qualsiasi sistema risponda al messaggio “directed broadcast”, quindi invia la propria risposta al sistema specificato nell’indirizzo sorgente, invece che al vero sistema sorgente. Tali pacchetti possono essere utilizzati per creare vaste “tempeste” di traffico di rete, già utilizzate in passato per rendere inservibili alcuni dei principali siti su Internet.

o. Solo il personale autorizzato deve avere accesso ai firewall, per mezzo di meccanismi di autenticazione “strong” e autorizzati.

p. I firewall e le loro configurazioni devono essere oggetto di regolari backup.

q. I firewall devono registrare sui log tutta l’attività significativa (come ad esempio modifiche di tipo amministrativo e tentativi di aggirare le regole di filtraggio).

r. Gli amministratori devono configurare il firewall per ricevere informazioni qualora fossero rilevati comportamenti sospetti quali tentativi di login falliti o di modifica delle regole.

s. La modifica alle regole deve essere chiesta esclusivamente da personale autorizzato tramite email da inviare alla casella di posta Securityadmin@regione.emilia-romagna.it e comunque in base a definizione e schedulazione dell’attività di aggiornamento (upgrade sistema operativo, modifica hardware, ecc.).

t. Tutti i firewall e le policy di sicurezza devono essere oggetto di audit e verifica almeno una volta l’anno.

u. Il piano di installazione e aggiornamento dei firewall deve essere consistente con le esigenze di servizio (es. con le finestre di servizio definite) e accuratamente pianificato.

v. Gli utenti devono ricevere in anticipo eventuali segnalazioni di disservizio causato da interventi sul firewall (es. per interventi di manutenzione e aggiornamento).

w. In caso di malfunzionamento bloccante del firewall devono essere avvisati tempestivamente anche il Responsabile del Servizio Sistema Informativo - Informatico Regionale e il Responsabile della Sicurezza della Giunta.

x. Nel caso di utilizzo di “modem pools” o server RAS, questi dovrebbero trovarsi dal lato non sicuro del firewall, oppure su un firewall “screened subnet”.

La protezione delle reti richiede che gli amministratori possano verificare che gli utenti non connettano alla rete interna dell'Ente strumenti elettronici personali o comunque non espressamente autorizzati, che non usino né strumenti “peer-to-peer” (per es. Skype, Emule, Limewire, Kazaa, Ares, BitTorrent, BitTornado, eDonkey, WinMX, Napster, Morpheus, Filetopia, SoulSeek, Shareaza, Azureus, ecc.), né strumenti di “sniffing”, “cracking” o “scanning”.

Utilizzare strumenti di IDS/IPS per l’analisi del traffico di rete e/o la prevenzione di eventuali intrusioni o dell’eventuale introduzione (anche involontaria) di programmi nocivi quali ad esempio virus, worm, spyware. Preferire soluzioni Network IDS rispetto a soluzioni Host IDS, in quanto consenteno due livelli di controllo: uno basato sulla verifica delle firme rispetto ad un database di riferimento e l’altro, basato sull’analisi del traffico di rete rilevato tramite sonde, per evidenziare eventuali anomalie grazie a funzioni ed algoritmi matematici.

Per gli strumenti IDS/IPS installati per la protezione della rete interna, Campus e sedi periferiche, DMZ e accesso verso Internet, valgono le stesse *Policy generale definite per i firewall.*

La protezione delle reti richiede inoltre che gli utenti non possano navigare in siti ritenuti malevoli rischiando di infettare le proprie stazioni di lavoro con malware. Gli amministratori possono attivare sistemi antivirus e di web filtering sulla navigazione Internet, per limitare questi rischi.

14.1 Protezione delle comunicazioni: posta elettronica

Gli amministratori dei sistemi di posta devono cercare di limitare i danni che la posta indesiderata, i malware, il phishing ed in genere i messaggi provenienti da internet possono procurare all’utente finale.

Policy generale

a. Impostare il filtro per posta indesiderata.

b. Impostare l’Elenco Mittenti bloccati che indirizza i mittenti bloccati nella posta indesiderata; questa funzione bloccherà anche allegati indesiderati e file di grandi dimensioni provenienti da contatti esclusi dall'elenco dei Mittenti attendibili.

c. Impostare, ove siano stati bloccati per errore dei mittenti attendibili, l’Elenco Mittenti attendibili che consente di accettare i messaggi provenienti dai mittenti designati.

d. Installare ed aggiornare (automaticamente) l’antivirus.

e. Bloccare gli allegati indesiderati o troppo grandi.

f. Impostare il Filtro antispam.

14.2 Sicurezza della rete interna

La rete interna (intranet) deve essere adeguatamente protetta da accessi non autorizzati e, al tempo stesso, dall'uso non consentito delle risorse informatiche da parte degli utenti.

Le informazioni relative alla topologia di rete, agli indirizzi intranet, alle configurazioni di rete devono essere mantenute riservate sia a livello procedurale che tecnico.

Salvo ove espressamente autorizzato, deve essere vietata la connessione ad Internet tramite modem o altri apparati di accesso remoto, anche wireless, di macchine collegate alla rete interna.

Connessioni con reti esterne devono essere effettuate tenendo conto dei rischi di sicurezza e delle opportune contromisure da implementare.

Policy generale

a. Tutte le connessioni LAN devono essere autorizzate dal Servizio Sistema Informativo - Informatico Regionale o dal Servizio Sistemi informativi - informatici e innovazione per l'Assemblea legislativa, ognuno per la parte di propria competenza. Gli utenti non devono utilizzare connessioni non autorizzate. In particolare, non deve esistere alcuna connessione diretta ad Internet non autorizzata da parte di un utente.

b. Tutti i componenti LAN devono essere registrati con un numero cespite univoco ed inoltre devono essere compiute ispezioni per assicurare che siano collegati alla rete esclusivamente componenti autorizzati.

c. I componenti LAN, gli hub, i bridge, i repeater, devono essere conservati in armadi chiusi a chiave e/o sale server sicure, per quanto possibile.

d. Al momento di acquistare componenti di rete, preferire gli switch agli hub.

e. Le sale server devono essere tenute sempre chiuse.

f. L'accesso alle sale server deve essere limitato al solo personale autorizzato dell'Ente. Altre figure, interne od esterne all'Ente, le quali richiedano accesso alle sale server, dovranno farne richiesta al Servizio Sistema Informativo - Informatico Regionale dell'Ente o al Servizio Gestione e Sviluppo per l'Assemblea legislativa.

g. Tutto il cablaggio di rete deve essere adeguatamente documentato.

h. Tutti gli accessi alla rete inutilizzati devono essere disattivati.

i. Gli utenti non devono collegare, posizionare alcun oggetto sui cavi e sulle prese di rete.

j. L'utilizzo di software di analisi della LAN è consentito al solo personale autorizzato dell'Ente o di terze parti.

k. Gli strumenti per l'analisi della LAN devono essere custoditi in modo sicuro quando non utilizzati.

l. E' opportuno che tutto il cablaggio della rete locale sia periodicamente revisionato e la revisione sia documentata a scopo di riferimento futuro.

m. E' opportuno che schemi di cablaggio che prevedano la ridondanza siano utilizzati ove possibile.

14.3 DMZ

La policy seguente stabilisce i requisiti di sicurezza per tutte le reti ed i componenti presenti nell'Ente, localizzati nella cosiddetta "De-Militarized Zone" (DMZ). Il rispetto di tali prescrizioni consente di minimizzare i rischi di immagine dovuti all'utilizzo non autorizzato delle proprie risorse IT ed i rischi dovuti alla perdita di dati sensibili/confidenziali.

Policy generale

a. La DMZ non deve essere connessa alla rete interna dell'Ente, né tramite connessione fisica né tramite wireless.

b. La DMZ deve trovarsi in un ambiente fisicamente separato da qualsiasi altra rete interna. Qualora ciò non sia possibile, i componenti devono essere posizionati in un rack chiuso, con accesso limitato. Inoltre, i gestori della DMZ devono aggiornare la lista di coloro i quali hanno accesso alla medesima.

c. Il firewall deve costituire l'unico punto di accesso tra la DMZ e la rete interna dell'Ente ed Internet. Qualsiasi forma di "cross-connection" che aggiri il firewall è vietata.

d. I sistemi operativi e le applicazioni della DMZ devono essere configurati secondo gli standard di installazione e configurazione previsti.

e. Tutte le patch/hot-fixes di sicurezza rilasciate dai fornitori devono essere installate nel minor tempo possibile e in ogni caso non dopo 30 giorni dalla data del rilascio. Questo vale per tutti i servizi installati, anche qualora tali servizi possano essere temporaneamente o definitivamente disabilitati. È compito degli amministratori mantenersi costantemente aggiornati sulle patches/hotfixes da installare.

f. Attività di amministrazione remota devono essere effettuate su canali sicuri (es. connessioni di rete con crittografia, che utilizzino SSH o IPSEC).

14.4 Accesso remoto e VPN da e verso la Intranet regionale

Gli accessi remoti o tramite VPN debbono essere concessi solo previa richiesta del responsabile di struttura o del responsabile funzionale.

Tutti gli accessi tramite connessione dial-in devono essere registrati e concessi al solo personale preventivamente riconosciuto ed autenticato e tutte le connessioni devono essere effettuate tramite meccanismi di call-back.

Gli accessi remoti o tramite VPN devono essere monitorati attraverso appositi strumenti di monitoraggio e reportistica al fine di poter avere un quadro aggiornato in qualsiasi momento si renda necessario.

Policy generale

a. La connessione VPN alle risorse regionali in modalità Office Mode è configurata solo su computer di proprietà dell'Ente e configurati dal proprio personale, o da personale esterno esplicitamente e formalmente autorizzato.

b. Altre modalità di connessione in VPN devono essere concordate con i tecnici regionali. L'utente abilitato potrà accedere ad un sottoinsieme di risorse consentite.

c. L'accesso VPN deve essere sotto il completo controllo degli amministratori che configurano e gestiscono i concentratori VPN. Gli utenti non devono poter creare punti di accesso VPN.

d. I concentratori VPN devono essere situati sul lato non sicuro del firewall, oppure in una sottorete dedicata.

e. L'utilizzo della VPN dovrebbe essere controllato tramite un meccanismo di autenticazione del tipo "two-factor", ad esempio SecurID.

f. Durante la connessione alla rete dell'Ente, una VPN deve convogliare tutto il traffico da e verso il pc sul tunnel VPN; qualsiasi altra modalità di traffico deve essere abbandonata.

g. Il "Dual (split) tunneling" non è consentito sui client; è permessa una sola connessione di rete.

h. Su tutti i computer collegati con la rete interna dell'Ente tramite VPN o altra tecnologia, devono essere installati i più recenti service pack e hot-fixes di sicurezza, nonché i più aggiornati software antivirus. Vedere in proposito il *"Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna"*

i. Gli utenti della VPN devono essere automaticamente disconnessi dalla rete dell'Ente dopo 30 minuti di inattività. L'utente, per ricollegarsi, deve autenticarsi nuovamente (logon).

j. E' consentito l'utilizzo di solo software client per VPN approvato dal Servizio Sistema Informativo - Informatico Regionale dell'Ente.

Gli accessi in VPN verso aziende esterne all'Ente Regione, le cui configurazioni sono gestite dai tecnici informatici dell'azienda stessa, necessarie per specifici progetti o per raggiungere la Intranet aziendale da parte di consulenti, devono essere richieste, verificate ed autorizzate dal Servizio Sistema Informativo - Informatico Regionale dell'Ente.

Tale VPN deve essere, comunque, configurata per convogliare tutto il traffico da e verso il pc sul tunnel VPN; qualsiasi altra modalità di traffico deve essere abbandonata. Il "Dual (split) tunneling" non deve essere consentito sui client; deve essere permessa una sola connessione di rete.

14.5 Wireless

Prima di procedere ad una implementazione wireless, occorre inviare una richiesta scritta ed adeguatamente motivata al Servizio Sistema Informativo - Informatico Regionale o al Servizio Sistemi informativi - informatici e innovazione dell'Assemblea Legislativa, ognuno per la parte di propria competenza.

Policy generale

a. Tutti gli accessi LAN wireless devono utilizzare prodotti e configurazioni di sicurezza approvati dal Servizio Sistema Informativo - Informatico Regionale.

b. Tutti i punti di accesso e le Base Stations connessi alla rete dell'Ente devono essere registrati e approvati dagli amministratori. Tali punti di accesso e Base Stations sono soggetti a periodici "penetration test" e audit da parte del Servizio Sistema Informativo - Informatico Regionale.

c. Tutte le schede di rete wireless (es. PC cards) utilizzate su laptop o desktop di proprietà dell'Ente devono essere registrate.

d. Per connettersi alla rete dell'Ente, tutti i computer degli uffici con connettività LAN wireless devono utilizzare il protocollo di autenticazione che il Servizio Sistema Informativo - Informatico Regionale ha deciso di adottare in base sia agli standard internazionali definiti per le connessioni wireless che alle caratteristiche di sicurezza nella trasmissione delle credenziali (es. PEAP)..

e. Le implementazioni wireless devono prevedere l'installazione di crittografia hardware WPA "point to point" almeno a 128 bit.

f. Tutte le implementazioni devono supportare indirizzi hardware che siano registrati e tracciati, cioè indirizzi MAC.

g. Il SSID (Service Set IDentifier) deve essere configurato in modo da non contenere alcuna informazione identificativa dell'Ente, come la ragione sociale, il nome dell'ufficio, il nome del dipendente, ecc...

h. L'accesso come amministratore, sia fisico che remoto, a punti di accesso wireless deve essere ristretto a figure individuate formalmente dal Responsabile del Servizio Sistema Informativo - Informatico Regionale o dal Responsabile del Servizio Gestione e Sviluppo per l'Assemblea legislativa, ognuno per la parte di propria competenza, per evitare rischi di "tampering", ad esempio resettando il punto di accesso per ritornare indietro alla configurazione di default di fabbrica (e dunque più vulnerabile). Tutte le password di default che consentono il login ai punti di accesso wireless devono essere opportunamente modificate.

15 Gestione dei log dei sistemi amministrati

È compito di ogni amministratore monitorare costantemente i sistemi gestiti per prevenire e limitare gli effetti di eventuali incidenti di sicurezza. Il metodo principale per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei file di log.

La definizione ed il rilevamento degli eventi di sistema deve essere effettuata in funzione del valore dei dati ed in modo tale da consentire la verifica dell'efficacia e dell'efficienza delle procedure di sicurezza. Ove possibile devono comunque essere rilevati:

- autenticazione (login e logout, riusciti e non);
- accesso ai dati classificati sensibili dal punto di vista sicurezza (lettura e scrittura);
- modifica di funzioni amministrative (es. la disabilitazione delle funzioni di logging, la gestione dei permessi, ecc.);
- connessioni di rete (in ingresso ed in uscita).

Ove possibile ogni voce di log deve contenere:

- data/ora dell'evento;
- luogo dell'evento (macchina, indirizzo IP, ecc.);
- identità dell'utente;
- identificativo del processo che ha generato l'evento;
- connessioni di rete (in ingresso ed in uscita) relative all'evento;
- descrizione dell'evento.

L'accesso ai log deve essere concesso al minor numero possibile di incaricati preventivamente individuati.

La frequenza di rotazione dei log è dipendente dalla frequenza di generazione degli eventi del sistema e da eventuali vincoli tecnici o legali. In ogni caso deve essere previsto un meccanismo che, successivamente al backup, sovrascriva i log esistenti ad intervalli regolari.

Ove possibile, gli amministratori devono mantenere on line i file di log contenenti gli eventi di sicurezza per almeno 1 mese.

Gli amministratori devono configurare i sistemi da essi amministrati in modo da far confluire tali log al sistema centralizzato di log management, nel quale i log, opportunamente aggregati, normalizzati e filtrati, vengono conservati in maniera tale da non poter essere modificati.

Al fine di prevenire e limitare gli effetti di eventuali incidenti di sicurezza, è consigliabile, attraverso appositi strumenti di correlazione che attingono ai log memorizzati sul sistema di log management, generare allarmi al verificarsi di eventi significativi dal punto di vista della sicurezza.

16 Gestione degli incidenti di sicurezza

Tutti gli amministratori devono reagire agli incidenti di sicurezza con prontezza e con spirito di cooperazione segnalando al proprio responsabile e al Responsabile della Sicurezza le violazioni di sicurezza interna o gli eventi che possono portare a credere che vi sia stata un'elusione delle misure di sicurezza previste.

Gli amministratori, dopo una prima verifica dell'accaduto, devono contattare l'Unità di Gestione degli Incidenti di Sicurezza della Giunta o dell'Assemblea Legislativa, a seconda che i sistemi coinvolti siano di competenza dell'una o dell'altra struttura.

Per gestire correttamente gli incidenti è indispensabile avere un elenco aggiornato dei beni (assets) che permetta di identificare i sistemi/applicazioni e il relativo livello di criticità.

Le macro fasi di gestione dell'incidente sono le seguenti:

- rilevazione incidente;
- identificazione e analisi dell'incidente;

- contenimento, Raccolta evidenze, Rimozione e Ripristino;
- chiusura dell'incidente.

Le procedure corrette e i relativi comportamenti sono specificatamente previsti nel "Disciplinare Tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna" al quale si rinvia.

17 Controlli di sicurezza

17.1 Analisi dei rischi

Nel rispetto delle *"Linee guida della Giunta della Regione Emilia-Romagna in materia di protezione dei dati personali"* Deliberazione di Giunta n.1264/2005 *e* di quelle dell'Assemblea legislativa adottate con Deliberazione dell'Ufficio di Presidenza n. 197 del 18/10/2006 e del presente disciplinare tecnico, è obbligo di ogni amministratore valutare i potenziali rischi di sicurezza derivanti dal design, l'installazione, l'utilizzo e la gestione dei sistemi informatici di competenza.

Ogni progetto che prevede l'installazione, l'utilizzo, la modifica, l'eliminazione di uno o più sistemi informatici, deve quindi essere preceduto da un'adeguata analisi dei rischi che tenga conto del valore delle risorse da proteggere, delle potenziali minacce di sicurezza, dei meccanismi di sicurezza.

17.2 Security audit

I sistemi informatici sono periodicamente valutati ed analizzati per identificare il livello di rischio cui le risorse sono esposte.

Opportune verifiche sono regolarmente effettuate per valutare l'efficacia e l'efficienza dei meccanismi di sicurezza utilizzati. Le modalità e procedure di esecuzione di tali verifiche sono contenute nel *"Disciplinare tecnico su modalità e procedure per verifiche di sicurezza su sistemi informativi, per controlli sull'utilizzo dei beni messi a disposizione dall'ente per attività lavorativa con riferimento alle strumentazioni informatiche e telefoniche ed esemplificazione di comportamenti per il corretto utilizzo dei beni, da applicare nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna"*

I security audit possono essere affidati a fornitori esterni di servizi. In tal caso è necessario farsi rilasciare da questi ultimi apposita attestazione di conformità del servizio fornito ai requisiti previsti dalla normativa vigente in materia di protezione dei dati personali.

18 Documentazione tecnica

Gli amministratori di sistema hanno il compito di provvedere alla documentazione e al tempestivo aggiornamento della stessa, in relazione a tutti i sistemi, banche dati, apparati di rete e sicurezza, applicazioni software di qualunque natura e complessità, nonché alle procedure operative di installazione, configurazione ed aggiornamento delle strumentazioni informatiche e telematiche di competenza. Gli amministratori di ciascuna

area possono utilizzare, per la realizzazione e gestione della documentazione di propria competenza, qualsiasi sistema di gestione documentale.

All'interno del Servizio Sistema Informativo – Informatico Regionale verrà avviato un processo di definizione e implementazione di un sistema documentale che possa permettere la gestione e la condivisione della documentazione utile fra amministratori di sistema ed altri eventuali soggetti incaricati. Al momento in cui il sistema documentale sarà operativo verranno impartite apposite disposizioni da parte del Responsabile del Servizio Informativo - Informatico Regionale agli amministratori di sistema, al fine di disciplinare le modalità con cui la documentazione dovrà essere creata e resa disponibile.

Gli amministratori di sistema hanno l'obbligo di collaborare, per quanto di propria competenza, alla predisposizione e all'aggiornamento di documentazione relativa alle procedure operative per la corretta sequenza di spegnimento e accensione dei diversi sistemi (hardware e software) presenti presso il CED regionale o eventualmente dislocati presso altre sedi regionali. Tale documentazione dovrà essere consultata in caso di spegnimento programmato o conseguente ad incidente che coinvolge tali sistemi; inoltre deve essere conservata sia in forma elettronica che cartacea, per permetterne la consultazione anche in caso di indisponibilità complessiva della infrastruttura tecnologica.

La Regione Emilia-Romagna dispone di un Configuration Management Database (CMDB) contenente le informazioni più significative relative alle componenti del sistema informatico. Tale database costituisce di fatto il sistema informativo del sistema informatico dell'ente e contiene i dettagli dei *configuration item* (CI) della infrastruttura IT, intesi come gli asset costituenti l'intero ambito informatico, sia materiali (hardware) che immateriali (software).

Il CMDB aiuta l'organizzazione nella comprensione delle relazioni tra le componenti censite e la loro configurazione e rappresenta un componente fondamentale nei processi di change management..

I dati contenuti in questo database sono strategici per il buon governo dell'infrastruttura e, al fine di garantire un elevato livello qualitativo del sistema, è fondamentale assicurare un costante aggiornamento delle informazioni in esso contenute. Tale obiettivo è perseguibile attraverso regolari attività di allineamento dei dati. Poiché l'implementazione attuale non dispone di automatismi in tal senso, è fondamentale l'apporto degli amministratori di sistema che, secondo il proprio ambito operativo di responsabilità, sono ritenuti garanti della qualità del dato del CMDB e come tali devono provvedere al suo aggiornamento costante e tempestivo.

Gli amministratori di dominio, di server, di rete, di database, di sicurezza delle postazioni di lavoro devono aggiornare costantemente i dati di propria competenza presenti sul CMDB. Tali tipologie di amministratori devono anche contribuire all'evoluzione del database, coordinandosi con i gestori per la modellazione dei dati di propria competenza.

Gli amministratori di software complesso, che non sono chiamati a gestire direttamente i propri dati sul database, devono essere disponibili a fornire tutte le informazioni relative ai software amministrati ogni qualvolta verranno loro richieste dai gestori del database.

Le informazioni registrate all'interno del CMDB sono rese accessibili agli amministratori di sistema, previa autorizzazione e profilazione dei medesimi ed in funzione del proprio ambito di competenza.

TABELLE

Tabella A: Installazione Windows Client

Id e nome attività	Descrizione	Note
CL001: Service Pack	Installare il più recente Service Pack	
CL002: patch di sicurezza	Installare le patch di sicurezza successive al Service Pack	
CL003: SP e patch per Office ed Explorer	Installare il più recente Service Pack e le patch di sicurezza anche per MS Office ed Internet Explorer	
CL004: Update software installato – non Microsoft	Installare le patch e gli aggiornamenti di sicurezza degli applicativi installati sul sistema	
CL005: antivirus	Installare il software antivirus e i relativi aggiornamenti, in accordo con la policy antivirus interna	
CL006: NTFS	Formattare tutte le partizioni disco con NTFS	
CL007: password Amministratore	Impostare per l'Amministratore una "strong password"	
CL008: Componenti superflui di Windows	Disinstallare componenti superflue di Windows	
CL009: servizi non necessari	Disabilitare i servizi non necessari	
CL010: account non necessari	Disabilitare o cancellare gli account non necessari e limitare gli amministratori locali: l'utente finale non deve avere privilegi amministrativi	
CL011: Account "Guest"	Disabilitare l'account "Guest"	
CL012: File e directory	Proteggere i file e directory critici	
CL013: Protezione registry	Proteggere il registry da accessi anonimi	
CL014: ACL registry	Applicare appropriate ACL (access control list) per il registry	
CL015: condivisioni	Rimuovere tutte le condivisioni di file non necessarie	
CL016: ACL condivisioni	Definire appropriate ACL su tutte le condivisioni di file necessarie	
CL017: policy password	Definire policy "forti" per le password degli account locali: composizione, cambio al primo accesso, periodicità ed automatismi per gli utenti	
CL018: policy blocco/sblocco account	Definire una policy per il blocco e lo sblocco di un account locale (es. n.ro massimo ammissibile tentativi di accesso falliti, tempo di sblocco automatico)	
CL019: Account Amministratore	Valutare l'opportunità di rinominare l'account dell'Amministratore per rendere più difficile un attacco	
CL020: Dominio e workgroup	Inserire la workstation nel dominio Windows dell'Ente anzichè in un workgroup	

Id e nome attività	Descrizione	Note
CL021: Null Session e Shares di Amministrazione	Fare, ove possibile, l'hardening delle shares di amministrazione ADMIN$, IPC$, C$, ed eliminare le Null Session	
CL022: Firewall	Attivare il personal firewall su ogni macchina	
CL023: MBSA	Controllare il sistema con il tool Microsoft Baseline Security Analyzer	
CL024: Warning logon	Definire il messaggio di warning che compare al logon	
CL025: Event Viewer	Abilitare l'auditing degli eventi di sicurezza	
CL026: diritti di debug	Revocare i diritti utente che consentono il debug di programmi	
CL027: SYSKEY	Abilitare la protezione SYSKEY	

Tabella B: Installazione Server (generale)

Id e nome attività	Descrizione	Note
SV001 – Sala server	Posizionare il server in una server room opportunamente protetta ed attrezzata (es. condizionamento, antincendio)	
SV002 – Gruppo di continuità	Collegare ogni nuovo server destinato alla produzione ad un gruppo di continuità, il quale consenta, in caso di emergenza, perlomeno di completare lo spegnimento della macchina	
SV003 – Hardware fault tolerant	Se, in base alla classificazione di criticità dei sistemi esistente, il server da portare in esercizio risulta critico, installare hardware in modalità "fault tolerant".	
SV004 – Backup	Attivare il backup dei dati e delle applicazioni operanti sul server	
SV005 – Restore	Attivare e verificare le procedure di restore dei dati e delle applicazioni operanti sul server.	
SV006 – Accessi	Limitare gli accessi ai listener delle basi dati ai soli sistemi server che le utilizzano	
SV007: Vulnerability Assessment	Effettuare prima di ogni passaggio in produzione di un nuovo server critico un Vulnerability Assessment, comprensivo di Penetration Test	
SV008: Orario interno macchine	Sincronizzare in tutte le macchine l'orario interno con un "time server" centralizzato dell'Ente o esterno (es. istituto G. Ferraris di Torino) con stratum basso	
SV009: Centralizzazione log	Centralizzare o salvare i log per la conservazione, correlazione ed analisi delle informazioni contenute	

Tabella C: Installazione Windows Server

Id e nome attività	Descrizione	Note
WS001: Service Pack	Installare i più recenti Service Pack rilasciati da Microsoft	
WS002: Patch di sicurezza	Installare le patch di sicurezza successive al Service Pack rilasciate da Microsoft	
WS003: Antivirus	Installare il software antivirus e i relativi aggiornamenti, in accordo con la policy antivirus interna	
WS004: NTFS	Formattare tutte le partizioni disco con NTFS	
WS005: Password Amministratore	Impostare per l'Amministratore locale una "strong password"	
WS006: Servizi	Disabilitare tutti i servizi non necessari	
WS007: Account	Disabilitare o cancellare gli account non necessari	
WS008: Guest	Disabilitare l'account "Guest"	
WS009: File e directory	Proteggere file e directory critici	
WS010: Protezione registry	Proteggere il registry da accessi anonimi	
WS011: ACL registry	Applicare appropriate ACL (access control list) per il registry	
WS012: Condivisioni	Rimuovere tutte le condivisioni di file non necessarie	
WS013: ACL condivisioni	Definire appropriate ACL su tutte le condivisioni di file necessarie	
WS014: Policy password	Definire policy "forti" per le password degli account locali: composizione, cambio al primo accesso, periodicità ed automatismi per gli utenti	
WS015: Policy blocco/sblocco account	Definire una policy per il blocco e lo sblocco di un account locale (es. numero massimo ammissibile tentativi di accesso falliti, tempo di sblocco automatico)	
WS016: Account Amministratore	Rinominare l'account dell'Amministratore per rendere più difficile un attacco	
WS017: debug	Revocare i diritti utente che consentono il debug di programmi	
WS018: Event Viewer	Abilitare l'auditing degli eventi di sicurezza	
WS019: Dominio e workgroup	Inserire i server in rete interna nel dominio Windows dell'Ente anzichè in un workgroup	Eccezione: la DMZ, le cui macchine fanno parte di un workgroup
WS020: Null Session e Shares di Amministrazione	Fare l'hardening delle shares di amministrazione ADMIN$, IPC$, C$, ed eliminare le Null Session	
WS021: Amministratori di dominio e locali	Restringere il numero degli amministratori di dominio e locali ai soli che gestiscono il dominio o il server in questione	

Id e nome attività	Descrizione	Note
WS022: Logon warning	Definire il messaggio di warning che compare al logon	
WS023: Patch del produttore e configurazioni dei servizi	Applicare le Patch critiche e le misure di sicurezza fornite dal produttore per il software ed i servizi installati sul sistema operativo (es. URLSCAN e lockdown per l'IIS web server). Per ulteriori dettagli, fare riferimento alle indicazioni di sicurezza riportate sul sito del fornitore	
WS024: MBSA	Effettuare la scansione del sistema con il tool Microsoft Baseline Security Analyzer	

Tabella D: Installazione Unix Server

Id e nome attività	Descrizione	Note
US001: Patch	Applicare le patch di sicurezza più recenti	
US002: Antivirus	Installare il software antivirus e relativi aggiornamenti, in accordo con la policy antivirus interna	
US003: Servizi non necessari	Disabilitare, rimuovere o proteggere con firewall locali tutti i servizi e le applicazioni non necessarie (es. sendmail)	
US004: Servizi R e servizio Telnet: disattivazione	Disattivare i servizi rlogin, srh, rcp, Telnet	
US005: Servizi richiesti	Attivare i soli servizi richiesti	
US006: Porte non necessarie	Verificare che siano disabilitate le porte di cui non si prevede l'utilizzo da parte di servizi o applicazioni che supportano le attività correnti	
US007: Utenze nominali amministratori	Permettere, ove possibile, l'accesso soltanto con utenze nominali e prevedere che gli amministratori debbano elevare i propri privilegi utilizzando gli strumenti forniti dal sistema (es. sudo, su –, etc.)	
US008: Cambio password	Impostare la policy di cambio password in accordo con la policy interna	
US009: Script di start-up	Disabilitare tutti gli script di start-up non necessari	
US010: Account e gruppi non necessari	Rimuovere tutti gli account ed i gruppi non più utilizzati o non necessari	
US011: File hosts.equiv	Rimuovere tutti gli host non necessari dal file hosts.equiv, oppure rimuovere il file se rsh o rlogin non sono richiesti	
US012: File .rhosts	Rimuovere tutti i file .rhosts non necessari	
US013: Permessi di accesso	Definire gli opportuni permessi di accesso a tutti i file e cartelle	
US014: Root password	Comunicare la "root password" solo al gruppo responsabile dell'amministrazione di sistema. Disabilitare l'accesso remoto per l'utente root	
US015: Logging servizi	Tracciare (logging) e/o proteggere l'accesso ai servizi per mezzo di metodi "access-control" (ad es. TCP Wrappers)	

Id e nome attività	Descrizione	Note
US016: Firewall “built-in”	Utilizzare un firewall “built-in”, se disponibile per Unix OS	
US017: PAM	Disabilitare servizi non necessari da Pluggable Authentication Modules (PAM) e garantire che PAM sia sicuro per default	
US018: FTP e SFTP	Impedire, se possibile, gli accessi mediante FTP, utilizzando come sostituto il più sicuro SFTP o FTPS	
US019: Server di stampa	Rimuovere oppure configurare opportunamente il supporto all’utilizzo del server come “print server”	
US020: Patch fornitore	Applicare le patch critiche e le misure di sicurezza fornite dal produttore a software e servizi installati sul sistema operativo (ad es. mod_security per il server web Apache).	

Tabella E: Installazione apparato di rete, firewall, IDS/IPS

Id e nome attività	Descrizione	Note
NT001: Analisi dei rischi	Effettuare un'analisi dei rischi a supporto della decisione circa il passaggio in produzione del nuovo apparato di rete	
NT002: Firewall e porte	Bloccare tramite i firewall installati le porte inutilizzate o di cui non si prevede l'utilizzo	
NT003: Policy firewall e IDS/IPS	Configurare i nuovi firewall e IPS/IDS basandosi su una specifica policy (ruleset) o gruppo	
NT004: Logging	Prevedere per componenti quali firewall, IDS/IPS e router il logging	
NT005: Configurazione router	Configurare ogni nuovo router in modo da rispettare uno standard predefinito: es. su autenticazione utente, su rimozione protocolli non necessari, su disattivazione servizi non necessari o potenzialmente pericolosi (nel caso di router connessi verso l'esterno)	
NT006: Proxy e Web filtering	Installare i proxy in modo che consentano l'accesso solo alle porte ed ai servizi indispensabili (es. http, ftp etc.) Configurare il Web filtering per la categorizzazione di siti e bloccare l'accesso a categorie non attinenti con l'attività lavorativa .	
NT007: Failover componenti critici	Configurare in failover i componenti critici: ridondanza e passaggio a componente di backup in caso di guasto del primo	
NT008: Sessioni inattive	Configurare l'infrastruttura di rete in modo da chiudere sessioni inattive dopo un certo periodo di tempo, salvo eccezioni da individuare e normare	
NT009: Salvataggio configurazioni	Attivare il salvataggio delle configurazioni per tutti gli apparati di rete per cui queste sono previste (es. firewall, router)	
NT010: Passaggio in produzione	Verificare che il piano di installazione e passaggio in produzione di uno o più firewall sia congruente con le esigenze di servizio dell'infrastruttura da proteggere (es. finestre di servizio) ed i relativi upgrade schedulati	
NT0011: Protezione apparati	Installare qualsiasi apparato di rete in alloggiamenti protetti (armadio chiuso a chiave, server room chiusa, traccia per cavi dedicata)	
NT012: Documentazione modifica	Documentare ogni modifica all'infrastruttura di rete in modo appropriato prima del passaggio in produzione	
NT013: Linea in dial-up	Installare e configurare ogni linea in dial-up in modo controllato e solo per esigenze specifiche (es. server RAS dedicati e protetti)	

1 Allegato 1 – Lettera di incarico ad amministratore di sistema di un dipendente collaboratore regionale della Giunta

Al dipendente regionale

_____

e p.c. Al Servizio Sistema Informativo-Informatico regionale
Al Servizio Organizzazione e Sviluppo

OGGETTO: Lettera di incarico ad amministratore di sistema di un dipendente/collaboratore regionale

Come previsto dal paragrafo 6.1 del Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa, la si designa amministratore di sistema, con le funzioni analiticamente individuate nell'Allegato 1) alla presente nota, in ragione delle valutate caratteristiche di esperienza, competenza e affidabilità, oggetto di valutazione da parte del sottoscritto/a Responsabile/Direttore.

Le regole tecniche ed organizzative in relazione alla sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche cui dovrà attenersi nell'espletamento dell'incarico attribuitole, sono descritte nel Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa reperibile in formato elettronico su Internos, Sezione "Privacy\Normativa sulla privacy".

Le si richiede di presentarsi entro il _____ presso la segreteria del/ della Servizio/Direzione scrivente per sottoscrivere l'avvenuta ricezione della presente e la presa visione del Disciplinare Tecnico suindicato.

Si invia infine la presente anche al Servizio Organizzazione e sviluppo per il concordato aggiornamento nell'Osservatorio delle competenze dei dati relativi al dipendente in indirizzo.

Cordiali saluti.

Il Direttore Generale/Il Responsabile di Servizio

Allegato 1)

Amministratori di dominio

Categoria	Amministratori - Cognome e nome
Domain Controller	
Delega Amministrativa RERSDM	
Delega Amministrativa Extrarer	

Amministratori di server

Categoria	Amministratori - Cognome e nome
Sistemi Linux	
Sistemi Windows fuori Dominio	
Sistemi Windows in Dominio	
Sistemi Windows Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
Sistemi Windows Servizio Informativo-Informatico Agricolo Regionale	
Sistemi Windows Servizio geologico, sismico e dei suoli	
Apparati layer 2 di infrastruttura server (blade)	
Ms SQL Server	
Oracle	
Oracle Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
MySQL e PostgreSQL	

Amministratori di apparati di rete

Categoria	Amministratori - Cognome e nome
Apparati layer 2 di infrastruttura server (blade)	

Amministratori di base di dati

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	
Oracle **Servizio Risanamento Atmosferico, Acustico, Elettromagnetico**	
MySQL e PostgreSQL	

Amministratori di postazioni di lavoro individuali

Categoria	Amministratori – Cognome e nome
Sistemi Windows	

Amministratori di sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
R/3 Agenzie e Regione e Agenzie Amministrazione landscape	
R/3 Agenzie e Regione e Agenzie Amministrazione strato applicativo	
BW 3.5 (Sap Netweaver 2004)	
CRM 4.0 Amministrazione landscape	
CRM 4.0 Amministrazione strato applicativo	
Mobile 7 (Sap Netweaver 2004s)	
Solution Manager (Sap Netweaver 2004s)	

SAS

Categoria	Amministratori – Cognome e nome
Server	
SAS v.9.1.3	

Servizi di rete

Categoria	Amministratori - Cognome e nome
DNS esterni (titolarità Lepida)	

Posta elettronica

Categoria	Amministratori - Cognome e nome
Sistemi di Posta	

Protocollo informatico

Categoria	Amministratori - Cognome e nome
Egrammata	

Servizio FTP sicuro

Categoria	Amministratori - Cognome e nome
FTPS	

Sistemi CMS

Categoria	Amministratori - Cognome e nome
Web@Work	
Plone	

VmWARE

Categoria	Amministratori - Cognome e nome
VmWare ESX 3.5	

CITRIX

Categoria	Amministratori - Cognome e nome
Citrix Metaframe 4.5	

SAN - Storage Centralizzato

Categoria	Amministratori - Cognome e nome
SAN HEWLETT PACKARD ITALIANA S.R.L	

SAN IBM	Balestrini Roberto Pierno Paolo

Sistema di Monitoraggio – ZABBIX

Categoria	Amministratori – Cognome e nome
Sistema di monitoring integrato	

Sistema di Middleware

Categoria	Amministratori – Cognome e nome
Application Server (WebSphere)	
Application Server (Tomcat/JBoss)	
Framework Microsoft .NET	
Web Server (Apache e IIS)	

Atti amministrativi

Categoria	Amministratori – Cognome e nome
Atti	

Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori

Sistemi Server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows in Dominio	

RDBMS

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	

Sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione landscape	

SAP HR ECC 6.0 **(Sap Netweaver 2004s)** Amministrazione strato applicativo	

Applicazioni

Categoria	Amministratori – Cognome e nome
Applicazioni su mainframe	
Applicazioni SqlServer – interfaccia Access	
Applicazione Web – DB Oracle	

2 Allegato 1a – Lettera di incarico ad amministratore di sistema di un dipendente collaboratore dell'Assemblea Legislativa

Al dipendente regionale

_____

e p.c. Al Servizio Sistema Informativo-Informatico regionale

Al Servizio Organizzazione e Sviluppo

OGGETTO: Lettera di incarico ad amministratore di sistema di un dipendente/collaboratore regionale

Come previsto dal paragrafo 6.1 del Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa, la si designa amministratore di sistema, con le funzioni analiticamente individuate nell'Allegato 1) alla presente nota, in ragione delle valutate caratteristiche di esperienza, competenza e affidabilità, oggetto di valutazione da parte del sottoscritto/a Responsabile/Direttore.

Le regole tecniche ed organizzative in relazione alla sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche cui dovrà attenersi nell'espletamento dell'incarico attribuitole, sono descritte nel Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa reperibile in formato elettronico su Internos, Sezione "Privacy\Normativa sulla privacy".

Le si richiede di presentarsi entro il _____ presso la segreteria del/ della Servizio/Direzione scrivente per sottoscrivere l'avvenuta ricezione della presente e la presa visione del Disciplinare Tecnico suindicato.

Si invia infine la presente anche al Servizio Organizzazione e sviluppo per il concordato aggiornamento nell'Osservatorio delle competenze dei dati relativi al dipendente in indirizzo.

Cordiali saluti.

Il Responsabile

Servizio Sistemi informativi-informatici e innovazione

Allegato 1)

Amministratori di dominio

Categoria	Amministratori – Cognome e nome
Domain Controller	
Delega Amministrativa RERSDM	
Delega Amministrativa Extrarer	

Amministratori di server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows fuori Dominio	
Sistemi Windows in Dominio	
Sistemi Windows Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
Sistemi Windows Servizio Informativo-Informatico Agricolo Regionale	
Sistemi Windows Servizio geologico, sismico e dei suoli	
Apparati layer 2 di infrastruttura server (blade)	
Ms SQL Server	
Oracle	
Oracle Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
MySQL e PostgreSQL	

Amministratori di apparati di rete

Categoria	Amministratori – Cognome e nome
Apparati layer 2 di infrastruttura server (blade)	

Amministratori di base di dati

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	
Oracle **Servizio Risanamento Atmosferico, Acustico, Elettromagnetico**	
MySQL e PostgreSQL	

Amministratori di postazioni di lavoro individuali

Categoria	Amministratori – Cognome e nome
Sistemi Windows	

SAP

Categoria	Amministratori – Cognome e nome
R/3 Agenzie e Regione e Agenzie Amministrazione landscape	
R/3 Agenzie e Regione e Agenzie Amministrazione strato applicativo	
BW 3.5 (Sap Netweaver 2004)	
CRM 4.0 Amministrazione landscape	
CRM 4.0 Amministrazione strato applicativo	
Mobile 7 (Sap Netweaver 2004s)	
Solution Manager (Sap Netweaver 2004s)	

SAS

Categoria	Amministratori – Cognome e nome
Server	
SAS v.9.1.3	

Servizi di rete

Categoria	Amministratori – Cognome e nome

DNS esterni (titolarità Lepida)	

Posta elettronica

Categoria	Amministratori - Cognome e nome
Sistemi di Posta	

Protocollo informatico

Categoria	Amministratori - Cognome e nome
Egrammata	

Servizio FTP sicuro

Categoria	Amministratori - Cognome e nome
FTPS	

Sistemi CMS

Categoria	Amministratori - Cognome e nome
Web@Work	
Plone	

VmWARE

Categoria	Amministratori - Cognome e nome
VmWare ESX 3.5	

CITRIX

Categoria	Amministratori - Cognome e nome
Citrix Metaframe 4.5	

SAN - Storage Centralizzato

Categoria	Amministratori - Cognome e nome
SAN HEWLETT PACKARD ITALIANA S.R.L	
SAN IBM	Balestrini Roberto Pierno Paolo

Sistema di Monitoraggio – ZABBIX

Categoria	Amministratori – Cognome e nome
Sistema di monitoring integrato	

Sistema di Middleware

Categoria	Amministratori – Cognome e nome
Application Server (WebSphere)	
Application Server (Tomcat/JBoss)	
Framework Microsoft .NET	
Web Server (Apache e IIS)	

Atti amministrativi

Categoria	Amministratori – Cognome e nome
Atti	

Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori

Sistemi Server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows in Dominio	

RDBMS

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	

Sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione landscape	
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione strato applicativo	

Applicazioni

Categoria	Amministratori – Cognome e nome
Applicazioni su mainframe	
Applicazioni SqlServer – interfaccia Access	
Applicazione Web – DB Oracle	

3 Allegato 2 – Lettera di integrazione-modifica delle funzioni di un amministratore di sistema della Giunta

Al dipendente regionale

_____

e p.c. Al Servizio Sistema Informativo-Informatico regionale
Al Servizio Organizzazione e Sviluppo

OGGETTO: Lettera di integrazione/modifica delle funzioni di un amministratore di sistema dipendente/collaboratore già designato

Come previsto dal paragrafo 6.1 del Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa,, la sua designazione ad amministratore di sistema è aggiornata, in ragione delle valutate caratteristiche di esperienza, competenza e affidabilità, con le funzioni analiticamente individuate nell'Allegato 1) alla presente nota.

Le regole tecniche ed organizzative in relazione alla sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche cui dovrà attenersi nell'espletamento dell'incarico attribuitole, sono descritte nel Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa reperibile in formato elettronico su Internos, Sezione "Privacy\Normativa sulla privacy".

Le si richiede di presentarsi entro il _____ presso la segreteria del/della Servizio/Direzione scrivente per sottoscrivere l'avvenuta ricezione della presente.

Si invia infine la presente anche al Servizio Organizzazione e sviluppo per il concordato aggiornamento nell'Osservatorio delle competenze dei dati relativi al dipendente in indirizzo.

Cordiali saluti.

Il Direttore Generale/Il Responsabile di Servizio

Allegato 1)

Amministratori di dominio

Categoria	Amministratori – Cognome e nome
Domain Controller	
Delega Amministrativa RERSDM	
Delega Amministrativa Extrarer	

Amministratori di server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows fuori Dominio	
Sistemi Windows in Dominio	
Sistemi Windows Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
Sistemi Windows Servizio Informativo-Informatico Agricolo Regionale	
Sistemi Windows Servizio geologico, sismico e dei suoli	
Apparati layer 2 di infrastruttura server (blade)	
Ms SQL Server	
Oracle	
Oracle Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
MySQL e PostgreSQL	

Amministratori di apparati di rete

Categoria	Amministratori – Cognome e nome
Apparati layer 2 di infrastruttura server (blade)	

Amministratori di base di dati

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	
Oracle **Servizio Risanamento Atmosferico, Acustico, Elettromagnetico**	
MySQL e PostgreSQL	

Amministratori di postazioni di lavoro individuali

Categoria	Amministratori – Cognome e nome
Sistemi Windows	

Amministratori di sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
R/3 Agenzie e Regione e Agenzie Amministrazione landscape	
R/3 Agenzie e Regione e Agenzie Amministrazione strato applicativo	
BW 3.5 (Sap Netweaver 2004)	
CRM 4.0 Amministrazione landscape	
CRM 4.0 Amministrazione strato applicativo	
Mobile 7 (Sap Netweaver 2004s)	
Solution Manager (Sap Netweaver 2004s)	

SAS

Categoria	Amministratori – Cognome e nome
Server	
SAS v.9.1.3	

Servizi di rete

Categoria	Amministratori - Cognome e nome
DNS esterni (titolarità Lepida)	

Posta elettronica

Categoria	Amministratori - Cognome e nome
Sistemi di Posta	

Protocollo informatico

Categoria	Amministratori - Cognome e nome
Egrammata	

Servizio FTP sicuro

Categoria	Amministratori - Cognome e nome
FTPS	

Sistemi CMS

Categoria	Amministratori - Cognome e nome
Web@Work	
Plone	

VmWARE

Categoria	Amministratori - Cognome e nome
VmWare ESX 3.5	

CITRIX

Categoria	Amministratori - Cognome e nome
Citrix Metaframe 4.5	

SAN - Storage Centralizzato

Categoria	Amministratori - Cognome e nome
SAN HEWLETT PACKARD ITALIANA S.R.L	

SAN IBM	Balestrini Roberto Pierno Paolo

Sistema di Monitoraggio – ZABBIX

Categoria	Amministratori – Cognome e nome
Sistema di monitoring integrato	

Sistema di Middleware

Categoria	Amministratori – Cognome e nome
Application Server (WebSphere)	
Application Server (Tomcat/JBoss)	
Framework Microsoft .NET	
Web Server (Apache e IIS)	

Atti amministrativi

Categoria	Amministratori – Cognome e nome
Atti	

Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori

Sistemi Server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows in Dominio	

RDBMS

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	

Sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione landscape	

SAP HR ECC 6.0 **(Sap Netweaver 2004s)** Amministrazione strato applicativo	

Applicazioni

Categoria	Amministratori – Cognome e nome
Applicazioni su mainframe	
Applicazioni SqlServer – interfaccia Access	
Applicazione Web – DB Oracle	

4 Allegato 2a – Lettera di integrazione-modifica delle funzioni di un amministratore di sistema dell'Assemblea Legislativa

Al dipendente regionale

_____

e p.c. Al Servizio organizzazione, bilancio e attività contrattuale

OGGETTO: Lettera di integrazione/modifica delle funzioni di un amministratore di sistema dipendente/collaboratore già designato

Come previsto dal paragrafo 6.1 del Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa,, la sua designazione ad amministratore di sistema è aggiornata, in ragione delle valutate caratteristiche di esperienza, competenza e affidabilità, con le funzioni analiticamente individuate nell'Allegato 1) alla presente nota da parte del Responsabile della Struttura _____ di cui alla nota con protocollo _____

Le regole tecniche ed organizzative in relazione alla sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche cui dovrà attenersi nell'espletamento dell'incarico attribuitole, sono descritte nel Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa reperibile in formato elettronico su Internos, Sezione "Privacy\Normativa sulla privacy".

Le si richiede di presentarsi entro il _____ presso la segreteria del/della Servizio/Direzione scrivente per sottoscrivere l'avvenuta ricezione della presente.

Si invia infine la presente anche al Servizio Organizzazione e sviluppo per il concordato aggiornamento nell'Osservatorio delle competenze dei dati relativi al dipendente in indirizzo.

Cordiali saluti.

Il Responsabile

Servizio Sistemi informativi-informatici e innovazione

Allegato 1)

Amministratori di dominio

Categoria	Amministratori – Cognome e nome
Domain Controller	
Delega Amministrativa RERSDM	
Delega Amministrativa Extrarer	

Amministratori di server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows fuori Dominio	
Sistemi Windows in Dominio	
Sistemi Windows Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
Sistemi Windows Servizio Informativo-Informatico Agricolo Regionale	
Sistemi Windows Servizio geologico, sismico e dei suoli	
Apparati layer 2 di infrastruttura server (blade)	
Ms SQL Server	
Oracle	
Oracle Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
MySQL e PostgreSQL	

Amministratori di apparati di rete

Categoria	Amministratori – Cognome e nome
Apparati layer 2 di infrastruttura server (blade)	

Amministratori di base di dati

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	
Oracle **Servizio Risanamento Atmosferico, Acustico, Elettromagnetico**	
MySQL e PostgreSQL	

Amministratori di postazioni di lavoro individuali

Categoria	Amministratori – Cognome e nome
Sistemi Windows	

Amministratori di sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
R/3 Agenzie e Regione e Agenzie Amministrazione landscape	
R/3 Agenzie e Regione e Agenzie Amministrazione strato applicativo	
BW 3.5 (Sap Netweaver 2004)	
CRM 4.0 Amministrazione landscape	
CRM 4.0 Amministrazione strato applicativo	
Mobile 7 (Sap Netweaver 2004s)	
Solution Manager (Sap Netweaver 2004s)	

SAS

Categoria	Amministratori – Cognome e nome
Server	
SAS v.9.1.3	

Servizi di rete

Categoria	Amministratori - Cognome e nome
DNS esterni (titolarità Lepida)	

Posta elettronica

Categoria	Amministratori - Cognome e nome
Sistemi di Posta	

Protocollo informatico

Categoria	Amministratori - Cognome e nome
Egrammata	

Servizio FTP sicuro

Categoria	Amministratori - Cognome e nome
FTPS	

Sistemi CMS

Categoria	Amministratori - Cognome e nome
Web@Work	
Plone	

VmWARE

Categoria	Amministratori - Cognome e nome
VmWare ESX 3.5	

CITRIX

Categoria	Amministratori - Cognome e nome
Citrix Metaframe 4.5	

SAN - Storage Centralizzato

Categoria	Amministratori - Cognome e nome
SAN HEWLETT PACKARD ITALIANA S.R.L	

SAN IBM	Balestrini Roberto Pierno Paolo

Sistema di Monitoraggio – ZABBIX

Categoria	Amministratori – Cognome e nome
Sistema di monitoring integrato	

Sistema di Middleware

Categoria	Amministratori – Cognome e nome
Application Server (WebSphere)	
Application Server (Tomcat/JBoss)	
Framework Microsoft .NET	
Web Server (Apache e IIS)	

Atti amministrativi

Categoria	Amministratori – Cognome e nome
Atti	

Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori

Sistemi Server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows in Dominio	

RDBMS

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	

Sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione landscape	

SAP HR ECC 6.0 **(Sap Netweaver 2004s)** Amministrazione strato applicativo	

Applicazioni

Categoria	Amministratori – Cognome e nome
Applicazioni su mainframe	
Applicazioni SqlServer – interfaccia Access	
Applicazione Web – DB Oracle	

5 Allegato 3 - Lettera di incarico ad amministratore di sistema insourcing di un soggetto dipendente da fornitore esterno della Giunta

All'amministratore di sistema

_____

e p.c. All'Azienda _____

Al Responsabile Servizio sistema informativo-informatico regionale

OGGETTO: Lettera di incarico ad amministratore di sistema insourcing di un soggetto dipendente da Fornitore esterno

Come previsto dal paragrafo 6.2 del Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa, Vi si designa amministratori di sistema, in ragione delle caratteristiche di esperienza, competenza e affidabilità attestate dall'Azienda_____ con lettera Prot. _____del _____, con particolare riferimento alle funzioni analiticamente individuate nell'Allegato 1) alla presente nota.

Le regole tecniche ed organizzative in relazione alla sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche cui dovrà attenersi nell'espletamento dell'incarico attribuitole, sono descritte nel Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa reperibile in formato elettronico su Internos, Sezione "Privacy\Normativa sulla privacy".

Le si richiede di presentarsi entro il _____ presso la segreteria del/della Servizio/Direzione scrivente per sottoscrivere l'avvenuta ricezione della presente e la presa visione del Disciplinare Tecnico suindicato.

Cordiali saluti.

Il Direttore Generale/Il Responsabile del Servizio

Allegato 1)

Amministratori di dominio

Categoria	Amministratori - Cognome e nome
Domain Controller	
Delega Amministrativa RERSDM	
Delega Amministrativa Extrarer	

Amministratori di server

Categoria	Amministratori - Cognome e nome
Sistemi Linux	
Sistemi Windows fuori Dominio	
Sistemi Windows in Dominio	
Sistemi Windows Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
Sistemi Windows Servizio Informativo-Informatico Agricolo Regionale	
Sistemi Windows Servizio geologico, sismico e dei suoli	
Apparati layer 2 di infrastruttura server (blade)	
Ms SQL Server	
Oracle	
Oracle Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
MySQL e PostgreSQL	

Amministratori di apparati di rete

Categoria	Amministratori - Cognome e nome
Apparati layer 2 di infrastruttura server (blade)	

Amministratori di base di dati

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	
Oracle **Servizio Risanamento Atmosferico, Acustico, Elettromagnetico**	
MySQL e PostgreSQL	

Amministratori di postazioni di lavoro individuali

Categoria	Amministratori – Cognome e nome
Sistemi Windows	

Amministratori di sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
R/3 Agenzie e Regione e Agenzie Amministrazione landscape	
R/3 Agenzie e Regione e Agenzie Amministrazione strato applicativo	
BW 3.5 (Sap Netweaver 2004)	
CRM 4.0 Amministrazione landscape	
CRM 4.0 Amministrazione strato applicativo	
Mobile 7 (Sap Netweaver 2004s)	
Solution Manager (Sap Netweaver 2004s)	

SAS

Categoria	Amministratori – Cognome e nome
Server	
SAS v.9.1.3	

Servizi di rete

Categoria	Amministratori - Cognome e nome
DNS esterni (titolarità Lepida)	

Posta elettronica

Categoria	Amministratori - Cognome e nome
Sistemi di Posta	

Protocollo informatico

Categoria	Amministratori - Cognome e nome
Egrammata	

Servizio FTP sicuro

Categoria	Amministratori - Cognome e nome
FTPS	

Sistemi CMS

Categoria	Amministratori - Cognome e nome
Web@Work	
Plone	

VmWARE

Categoria	Amministratori - Cognome e nome
VmWare ESX 3.5	

CITRIX

Categoria	Amministratori - Cognome e nome
Citrix Metaframe 4.5	

SAN - Storage Centralizzato

Categoria	Amministratori - Cognome e nome
SAN HEWLETT PACKARD ITALIANA S.R.L	

SAN IBM	Balestrini Roberto Pierno Paolo

Sistema di Monitoraggio – ZABBIX

Categoria	Amministratori – Cognome e nome
Sistema di monitoring integrato	

Sistema di Middleware

Categoria	Amministratori – Cognome e nome
Application Server (WebSphere)	
Application Server (Tomcat/JBoss)	
Framework Microsoft .NET	
Web Server (Apache e IIS)	

Atti amministrativi

Categoria	Amministratori – Cognome e nome
Atti	

Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori

Sistemi Server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows in Dominio	

RDBMS

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	

Sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione landscape	

SAP HR ECC 6.0 **(Sap Netweaver 2004s)** Amministrazione strato applicativo	

Applicazioni

Categoria	Amministratori – Cognome e nome
Applicazioni su mainframe	
Applicazioni SqlServer – interfaccia Access	
Applicazione Web – DB Oracle	

6 Allegato 3a - Lettera di incarico ad amministratore di sistema insourcing di un soggetto dipendente da fornitore esterno dell'Assemblea Legislativa

All'amministratore di sistema

_____

e p.c.
All'Azienda _____

OGGETTO: Lettera di incarico ad amministratore di sistema insourcing di un soggetto dipendente da Fornitore esterno

Come previsto dal paragrafo 6.2 del Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa, Vi si designa amministratori di sistema, in ragione delle caratteristiche di esperienza, competenza e affidabilità attestate dall'Azienda_____ con lettera Prot. _____del _____, con particolare riferimento alle funzioni analiticamente individuate nell'Allegato 1) alla presente nota.

Le regole tecniche ed organizzative in relazione alla sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche cui dovrà attenersi nell'espletamento dell'incarico attribuitole, sono descritte nel Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa reperibile in formato elettronico su Internos, Sezione "Privacy\Normativa sulla privacy".

Le si richiede di presentarsi entro il _____ presso la segreteria del Servizio scrivente per ricevere la presente e prendere visione del Disciplinare Tecnico sopra indicato.

Cordiali saluti.

Il Responsabile del
Servizio Sistemi informativi-informatici e innovazione

Allegato 1)

Amministratori di dominio

Categoria	Amministratori - Cognome e nome
Domain Controller	
Delega Amministrativa RERSDM	
Delega Amministrativa Extrarer	

Amministratori di server

Categoria	Amministratori - Cognome e nome
Sistemi Linux	
Sistemi Windows fuori Dominio	
Sistemi Windows in Dominio	
Sistemi Windows Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
Sistemi Windows Servizio Informativo-Informatico Agricolo Regionale	
Sistemi Windows Servizio geologico, sismico e dei suoli	
Apparati layer 2 di infrastruttura server (blade)	
Ms SQL Server	
Oracle	
Oracle Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
MySQL e PostgreSQL	

Amministratori di apparati di rete

Categoria	Amministratori - Cognome e nome
Apparati layer 2 di infrastruttura server (blade)	

Amministratori di base di dati

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	
Oracle **Servizio Risanamento Atmosferico, Acustico, Elettromagnetico**	
MySQL e PostgreSQL	

Amministratori di postazioni di lavoro individuali

Categoria	Amministratori – Cognome e nome
Sistemi Windows	

Amministratori di sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
R/3 Agenzie e Regione e Agenzie Amministrazione landscape	
R/3 Agenzie e Regione e Agenzie Amministrazione strato applicativo	
BW 3.5 (Sap Netweaver 2004)	
CRM 4.0 Amministrazione landscape	
CRM 4.0 Amministrazione strato applicativo	
Mobile 7 (Sap Netweaver 2004s)	
Solution Manager (Sap Netweaver 2004s)	

SAS

Categoria	Amministratori – Cognome e nome
Server	
SAS v.9.1.3	

Servizi di rete

Categoria	Amministratori - Cognome e nome
DNS esterni (titolarità Lepida)	

Posta elettronica

Categoria	Amministratori - Cognome e nome
Sistemi di Posta	

Protocollo informatico

Categoria	Amministratori - Cognome e nome
Egrammata	

Servizio FTP sicuro

Categoria	Amministratori - Cognome e nome
FTPS	

Sistemi CMS

Categoria	Amministratori - Cognome e nome
Web@Work	
Plone	

VmWARE

Categoria	Amministratori - Cognome e nome
VmWare ESX 3.5	

CITRIX

Categoria	Amministratori - Cognome e nome
Citrix Metaframe 4.5	

SAN - Storage Centralizzato

Categoria	Amministratori - Cognome e nome
SAN HEWLETT PACKARD ITALIANA S.R.L	

SAN IBM	Balestrini Roberto Pierno Paolo

Sistema di Monitoraggio – ZABBIX

Categoria	Amministratori – Cognome e nome
Sistema di monitoring integrato	

Sistema di Middleware

Categoria	Amministratori – Cognome e nome
Application Server (WebSphere)	
Application Server (Tomcat/JBoss)	
Framework Microsoft .NET	
Web Server (Apache e IIS)	

Atti amministrativi

Categoria	Amministratori – Cognome e nome
Atti	

Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori

Sistemi Server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows in Dominio	

RDBMS

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	

Sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione landscape	

SAP HR ECC 6.0 **(Sap Netweaver 2004s)** Amministrazione strato applicativo	

Applicazioni

Categoria	Amministratori – Cognome e nome
Applicazioni su mainframe	
Applicazioni SqlServer – interfaccia Access	
Applicazione Web – DB Oracle	

7 Allegato 4 - Lettera di integrazione-modifica delle funzioni di amministratore di sistema insourcing già designato dipendente di fornitore esterno della Giunta

All'amministratore di sistema

_____

p.c. All'Azienda _____

Al Responsabile Servizio sistema informativo-informatico regionale

OGGETTO: Lettera di integrazione/modifica delle funzioni di un amministratore di sistema insourcing già designato dipendente da Fornitore esterno

Come previsto dal paragrafo 6.2 del Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa, la sua designazione ad amministratore di sistema è aggiornata, in ragione delle valutate caratteristiche di esperienza, competenza e affidabilità attestate dall'Azienda _____con lettera Prot._____del_____, con le funzioni analiticamente individuate nell'Allegato 1) alla presente nota.

Le regole tecniche ed organizzative in relazione alla sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche cui dovrà attenersi nell'espletamento dell'incarico attribuitole, sono descritte nel Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa reperibile in formato elettronico su Internos, Sezione "Privacy\Normativa sulla privacy".

Le si richiede di presentarsi entro il _____ presso la segreteria del/della Servizio/Direzione scrivente per sottoscrivere l'avvenuta ricezione della presente.

Cordiali saluti.

Il Direttore Generale/Il Responsabile di Servizio

Allegato 1)

Amministratori di dominio

Categoria	Amministratori - Cognome e nome
Domain Controller	
Delega Amministrativa RERSDM	
Delega Amministrativa Extrarer	

Amministratori di server

Categoria	Amministratori - Cognome e nome
Sistemi Linux	
Sistemi Windows fuori Dominio	
Sistemi Windows in Dominio	
Sistemi Windows Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
Sistemi Windows Servizio Informativo-Informatico Agricolo Regionale	
Sistemi Windows Servizio geologico, sismico e dei suoli	
Apparati layer 2 di infrastruttura server (blade)	
Ms SQL Server	
Oracle	
Oracle Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
MySQL e PostgreSQL	

Amministratori di apparati di rete

Categoria	Amministratori - Cognome e nome
Apparati layer 2 di infrastruttura server (blade)	

Amministratori di base di dati

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	
Oracle **Servizio Risanamento Atmosferico, Acustico, Elettromagnetico**	
MySQL e PostgreSQL	

Amministratori di postazioni di lavoro individuali

Categoria	Amministratori – Cognome e nome
Sistemi Windows	

Amministratori di sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
R/3 Agenzie e Regione e Agenzie Amministrazione landscape	
R/3 Agenzie e Regione e Agenzie Amministrazione strato applicativo	
BW 3.5 (Sap Netweaver 2004)	
CRM 4.0 Amministrazione landscape	
CRM 4.0 Amministrazione strato applicativo	
Mobile 7 (Sap Netweaver 2004s)	
Solution Manager (Sap Netweaver 2004s)	

SAS

Categoria	Amministratori – Cognome e nome
Server	
SAS v.9.1.3	

Servizi di rete

Categoria	Amministratori - Cognome e nome
DNS esterni (titolarità Lepida)	

Posta elettronica

Categoria	Amministratori - Cognome e nome
Sistemi di Posta	

Protocollo informatico

Categoria	Amministratori - Cognome e nome
Egrammata	

Servizio FTP sicuro

Categoria	Amministratori - Cognome e nome
FTPS	

Sistemi CMS

Categoria	Amministratori - Cognome e nome
Web@Work	
Plone	

VmWARE

Categoria	Amministratori - Cognome e nome
VmWare ESX 3.5	

CITRIX

Categoria	Amministratori - Cognome e nome
Citrix Metaframe 4.5	

SAN - Storage Centralizzato

Categoria	Amministratori - Cognome e nome
SAN HEWLETT PACKARD ITALIANA S.R.L	

SAN IBM	Balestrini Roberto Pierno Paolo

Sistema di Monitoraggio – ZABBIX

Categoria	Amministratori – Cognome e nome
Sistema di monitoring integrato	

Sistema di Middleware

Categoria	Amministratori – Cognome e nome
Application Server (WebSphere)	
Application Server (Tomcat/JBoss)	
Framework Microsoft .NET	
Web Server (Apache e IIS)	

Atti amministrativi

Categoria	Amministratori – Cognome e nome
Atti	

Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori

Sistemi Server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows in Dominio	

RDBMS

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	

Sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione landscape	

SAP HR ECC 6.0 **(Sap Netweaver 2004s)** Amministrazione strato applicativo	

Applicazioni

Categoria	Amministratori – Cognome e nome
Applicazioni su mainframe	
Applicazioni SqlServer – interfaccia Access	
Applicazione Web – DB Oracle	

8 Allegato 4a - Lettera di integrazione-modifica delle funzioni di amministratore di sistema insourcing già designato dipendente di fornitore esterno dell'Assemblea Legislativa

All'amministratore di sistema

_____

p.c.
All'Azienda _____

OGGETTO: Lettera di integrazione/modifica delle funzioni di un amministratore di sistema insourcing già designato dipendente da Fornitore esterno

Come previsto dal paragrafo 6.2 del Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa, la sua designazione ad amministratore di sistema è aggiornata, in ragione delle valutate caratteristiche di esperienza, competenza e affidabilità attestate dall'Azienda _____con lettera Prot._____del_____, con le funzioni analiticamente individuate nell'Allegato 1) alla presente nota.

Le regole tecniche ed organizzative in relazione alla sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche cui dovrà attenersi nell'espletamento dell'incarico attribuitole, sono descritte nel Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa reperibile in formato elettronico su Internos, Sezione "Privacy\Normativa sulla privacy".

Le si richiede di presentarsi entro il _____ presso la segreteria del Servizio scrivente per ricevere la presente e prendere visione del Disciplinare Tecnico sopra indicato.

Cordiali saluti.

Il Responsabile del
Servizio Sistemi informativi-informatici e innovazione

Allegato 1)

Amministratori di dominio

Categoria	Amministratori - Cognome e nome
Domain Controller	
Delega Amministrativa RERSDM	
Delega Amministrativa Extrarer	

Amministratori di server

Categoria	Amministratori - Cognome e nome
Sistemi Linux	
Sistemi Windows fuori Dominio	
Sistemi Windows in Dominio	
Sistemi Windows Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
Sistemi Windows Servizio Informativo-Informatico Agricolo Regionale	
Sistemi Windows Servizio geologico, sismico e dei suoli	
Apparati layer 2 di infrastruttura server (blade)	
Ms SQL Server	
Oracle	
Oracle Servizio Risanamento Atmosferico, Acustico, Elettromagnetico	
MySQL e PostgreSQL	

Amministratori di apparati di rete

Categoria	Amministratori - Cognome e nome
Apparati layer 2 di infrastruttura server (blade)	

Amministratori di base di dati

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	
Oracle **Servizio Risanamento Atmosferico, Acustico, Elettromagnetico**	
MySQL e PostgreSQL	

Amministratori di postazioni di lavoro individuali

Categoria	Amministratori – Cognome e nome
Sistemi Windows	

Amministratori di sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
R/3 Agenzie e Regione e Agenzie Amministrazione landscape	
R/3 Agenzie e Regione e Agenzie Amministrazione strato applicativo	
BW 3.5 (Sap Netweaver 2004)	
CRM 4.0 Amministrazione landscape	
CRM 4.0 Amministrazione strato applicativo	
Mobile 7 (Sap Netweaver 2004s)	
Solution Manager (Sap Netweaver 2004s)	

SAS

Categoria	Amministratori – Cognome e nome
Server	
SAS v.9.1.3	

Servizi di rete

Categoria	Amministratori - Cognome e nome
DNS esterni (titolarità Lepida)	

Posta elettronica

Categoria	Amministratori - Cognome e nome
Sistemi di Posta	

Protocollo informatico

Categoria	Amministratori - Cognome e nome
Egrammata	

Servizio FTP sicuro

Categoria	Amministratori - Cognome e nome
FTPS	

Sistemi CMS

Categoria	Amministratori - Cognome e nome
Web@Work	
Plone	

VmWARE

Categoria	Amministratori - Cognome e nome
VmWare ESX 3.5	

CITRIX

Categoria	Amministratori - Cognome e nome
Citrix Metaframe 4.5	

SAN – Storage Centralizzato

Categoria	Amministratori - Cognome e nome
SAN HEWLETT PACKARD ITALIANA S.R.L	
SAN IBM	Balestrini Roberto Pierno Paolo

Sistema di Monitoraggio – ZABBIX

Categoria	Amministratori – Cognome e nome
Sistema di monitoring integrato	

Sistema di Middleware

Categoria	Amministratori – Cognome e nome
Application Server (WebSphere)	
Application Server (Tomcat/JBoss)	
Framework Microsoft .NET	
Web Server (Apache e IIS)	

Atti amministrativi

Categoria	Amministratori – Cognome e nome
Atti	

Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori

Sistemi Server

Categoria	Amministratori – Cognome e nome
Sistemi Linux	
Sistemi Windows in Dominio	

RDBMS

Categoria	Amministratori – Cognome e nome
Ms SQL Server	
Oracle	

Sistemi software complessi

SAP

Categoria	Amministratori – Cognome e nome
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione landscape	
SAP HR ECC 6.0 (Sap Netweaver 2004s) Amministrazione strato applicativo	

Applicazioni

Categoria	Amministratori – Cognome e nome
Applicazioni su mainframe	
Applicazioni SqlServer – interfaccia Access	
Applicazione Web – DB Oracle	

REGIONE EMILIA-ROMAGNA
Atti amministrativi

GIUNTA REGIONALE

Grazia Cesari, Responsabile del SERVIZIO SISTEMA INFORMATIVO - INFORMATICO REGIONALE, in qualità di Responsabile della Sicurezza della Giunta, esprime, ai sensi della deliberazione della Giunta Regionale n. 2416/2008, parere di regolarità amministrativa in merito all'atto con numero di proposta DPG/2012/462

data 16/01/2012

IN FEDE

Grazia Cesari