

REGIONE EMILIA-ROMAGNA

Atti amministrativi

GIUNTA REGIONALE

Atto del Dirigente: DETERMINAZIONE n° 6928 del 21/07/2009

Proposta: DPG/2009/7513 del 20/07/2009

Struttura proponente: DIREZIONE GENERALE CENTRALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA

Oggetto: Disciplinare Tecnico su modalità e procedure per verifiche di sicurezza sui Sistemi Informativi, per controlli sull'utilizzo dei beni messi a disposizione dall'ente per attività lavorativa con riferimento alle strumentazioni informatiche e telefoniche ed esemplificazioni di comportamenti per il corretto utilizzo dei beni, da applicare nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna

Autorità emanante: IL DIRETTORE - DIREZIONE GENERALE CENTRALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA

Firmatario: GAUDENZIO GARAVINI in qualità di Direttore generale

Luogo di adozione: BOLOGNA data: 21/07/2009

DIREZIONE GENERALE CENTRALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA

IL DIRETTORE

IL DIRETTORE GENERALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA

Visto il D.Lgs. n. 196 del 30 giugno 2003 “Codice in materia di protezione dei dati personali”, di seguito denominato Codice;

Viste:

- l'Appendice 5 della deliberazione di Giunta regionale n. 2416/2008 ed in particolare il paragrafo 3.2, lettera b), che attribuisce al Direttore generale competente in materia di organizzazione l'adozione di un Disciplinare Tecnico relativo alle modalità e alle procedure per l'effettuazione dei controlli sull'utilizzo delle strumentazioni informatiche;
- la deliberazione dell'Ufficio di Presidenza n. 173 del 24 luglio 2007 ed in particolare il paragrafo 3 che affida al Direttore generale dell'Assemblea Legislativa i compiti per l'applicazione uniforme degli adempimenti previsti dalla normativa;

Viste inoltre:

- la deliberazione di Giunta regionale n. 1264 dell'1 agosto 2005 “Linee guida della Giunta della Regione Emilia-Romagna in materia di protezione dei dati personali”;
- la deliberazione dell'Ufficio di Presidenza dell'Assemblea legislativa 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”,

di seguito denominate Linee guida;

Visti gli articoli delle suddette Linee guida denominati rispettivamente:

- con la lettera -G per la Giunta regionale;
- con le lettere -AL per l'Assemblea legislativa

ed in particolare:

- l'articolo 2 (G e AL) “Processo di gestione della sicurezza”, il quale prevede, al comma 2 lettera c), che siano effettuati controlli per verificare l'efficienza e la corretta applicazione delle misure di sicurezza adottate;
- l'articolo 11 (G) e l'articolo 10 (AL) “Uso delle strumentazioni informatiche”, che dispone, al comma 3, che le regole tecniche in materia di utilizzo delle strumentazioni informatiche siano definite ai sensi dell'art. 16 (G) e dell'15 (AL) delle stesse Linee guida, vale a dire con apposito Disciplinare Tecnico;

- l'articolo 13 (G) e l'articolo 12 (AL) "Controlli di sicurezza", che dispone che la Giunta e l'Assemblea legislativa possano effettuare i controlli ritenuti opportuni per la verifica della corretta applicazione e dell'efficienza delle misure di sicurezza adottate per la protezione dei dati personali e che le modalità di tali controlli devono essere preventivamente comunicate e adottate con i Disciplinari Tecnici previsti all'articolo 16 (G) e all'art. 15 (AL) delle stesse Linee Guida;

Vista altresì la propria determinazione n. 2653/2007 e la determinazione del Direttore Generale dell'Assemblea legislativa n. 479/2007, rispettivamente "Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna" e "Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nell'Assemblea legislativa della Regione Emilia-Romagna" ed in particolare:

- il paragrafo 4.5 "Verifiche di sicurezza", che prevede che siano effettuate verifiche per garantire l'efficienza, la disponibilità ed il rispetto di leggi e regolamenti ed in particolare dei requisiti minimi di sicurezza dei sistemi informativi regionali, demandando ad altro specifico Disciplinare Tecnico ulteriori verifiche finalizzate ad accertare la correttezza e la legalità dell'utilizzo delle strumentazioni fornite dall'amministrazione regionale e strumentali all'attività lavorativa;
- il paragrafo 7 "Protezione delle reti e delle comunicazioni", che dispone alcune regole comportamentali cui si devono conformare gli utenti dei sistemi informativi (ed in particolare i soggetti di cui al paragrafo 2 del medesimo disciplinare), con particolare riferimento alla navigazione in Internet e all'utilizzo della posta elettronica;

Visti altresì i seguenti Disciplinari tecnici:

- Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa di cui alla determinazione n. 1416 del 2 marzo 2009;
- Disciplinare Tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna di cui alla determinazione n. 1703 del 9 marzo 2009;

Viste inoltre le deliberazioni di Giunta regionale n. 2199/2005 e dell'Ufficio di Presidenza dell'Assemblea legislativa n. 183/2005, che hanno approvato il Codice di comportamento per la Regione Emilia-Romagna ed in particolare l'articolo 8 "Utilizzo dei beni della Regione" che dispone, tra l'altro, al comma 3 che la Regione si impegna ad effettuare controlli sull'utilizzo dei beni adottando criteri oggettivi preventivamente comunicati;

Vista la Legge n. 300 del 20 maggio 1970 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" ed in particolare l'art. 4 comma 2, che prevede che gli impianti e le apparecchiature di controllo a distanza possono essere installati previo accordo con le rappresentanze sindacali aziendali e l'art. 8, che dispone il divieto, per il datore di lavoro, di effettuare indagini sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;

Considerato che le verifiche e i controlli di seguito specificati devono essere normati ed attuati nell'assoluto rispetto dei principi e dei diritti sanciti dalla legge n. 300/1970, con particolare riferimento agli articoli sopra richiamati e comunque nel rispetto della dignità e libertà personale dei lavoratori;

Valutato quindi di dover disciplinare e conseguentemente applicare tipologie e modalità di controllo tali da garantire il massimo rispetto dei suddetti diritti, prevedendo, in accordo con le organizzazioni sindacali, tutte le precauzioni possibili a tal fine;

Valutato inoltre che le suddette tipologie e modalità di controllo devono essere specificate con criteri e regole oggettive e dettagliatamente predeterminate al fine di assicurarne l'imparzialità e la necessaria preventiva conoscenza nei confronti di tutti i soggetti potenzialmente coinvolti nei controlli stessi;

Considerato che la normativa richiamata in premessa fa riferimento a due tipologie di controlli, aventi diversa finalità, di seguito ulteriormente specificate:

- A. verifiche di sicurezza, previste in particolare dall'articolo 2, comma 2 lettera c) e dall'articolo 13 (G) e dall'art. 12 (AL) delle Linee guida, con la finalità di verificare l'efficienza e la corretta applicazione delle misure di sicurezza adottate per la protezione dei dati personali;
- B. controlli sull'utilizzo dei beni che l'amministrazione regionale mette a disposizione per lo svolgimento dell'attività lavorativa (con particolare riferimento agli strumenti informatici e di telefonia), previsti in particolare dall'articolo 8, comma 3 del Codice di comportamento della Regione Emilia-Romagna, con la finalità di effettuare, verificando il corretto utilizzo di tali beni, un controllo sulla spesa pubblica per raggiungere un contenimento e una razionalizzazione della stessa e garantire maggiore efficienza ed economicità dell'azione amministrativa;

Considerato, inoltre, che le due diverse tipologie di controlli sono entrambe necessarie, in quanto:

- A. le verifiche di sicurezza consentono di monitorare la concreta attuazione delle misure di sicurezza adottate dall'amministrazione e di effettuare un loro costante aggiornamento e adeguamento; ciò risponde all'obbligo, posto in capo a ciascun titolare di trattamenti di dati personali, di mettere in atto sia le misure minime previste dagli articoli 33-36 e dall'Allegato B del Codice, sia le misure idonee di cui agli articoli 15 e 31 del Codice, in modo da ridurre al minimo i rischi di distruzione e di perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta e pertanto costituiscono esse stesse una misura di sicurezza, che è, in quanto tale, obbligatoria per l'amministrazione regionale, titolare di dati personali;
- B. i controlli sull'utilizzo dei beni che l'amministrazione regionale mette a disposizione per lo svolgimento dell'attività lavorativa (con particolare riferimento agli strumenti informatici e alla telefonia, sia fissa sia mobile):
 - consentono di monitorare e mirano a ridurre la spesa pubblica, sia rilevando eventuali danni patrimoniali già posti in essere, sia agendo quale strumento di dissuasione rispetto a comportamenti impropri e potenzialmente dannosi, per cui la loro omissione potrebbe comportare responsabilità patrimoniali dirette a carico dell'amministrazione regionale;
 - possono evitare o comunque ridurre i rischi di coinvolgimento civile e penale, per concorso di reato, dell'amministrazione, nel caso di illeciti nei confronti di terzi, commessi mediante un utilizzo improprio dei beni messi a disposizione dall'amministrazione stessa;
 - possono concorrere a tutelare l'immagine dell'amministrazione e di coloro che vi prestano la propria attività;
 - concorrono ad approfondire elementi che emergono in seguito a segnalazioni di incidenti di sicurezza, in modo da evidenziare eventuali rischi al fine di una successiva attività di prevenzione.

Considerato quindi che i controlli sull'utilizzo degli strumenti informatici sono in alcuni casi strettamente connessi e conseguenti alle verifiche di sicurezza di cui alla lettera A;

Preso atto che le verifiche di sicurezza di cui alla lettera A sono in parte disciplinate al già richiamato punto 4.5 dei citati Disciplinari Tecnici per utenti sull'utilizzo dei sistemi informativi;

Valutato che sia opportuno che tali verifiche di sicurezza siano maggiormente e dettagliatamente disciplinate, con particolare riferimento alle modalità e alle procedure delle stesse, anche per garantire la necessaria e preventiva informazione a tutti i soggetti potenzialmente coinvolti in tali verifiche;

Visto il comma 595 dell'art. 2 della Legge n. 244/2007, che prevede che le pubbliche amministrazioni, nell'adottare i piani triennali per la razionalizzazione dell'utilizzo anche delle dotazioni strumentali previsti al comma 594, devono indicare le misure dirette a circoscrivere l'assegnazione delle apparecchiature di telefonia mobile e individuare, nel rispetto della normativa sulla protezione dei dati personali, forme di verifica anche a campione circa il corretto utilizzo delle relative utenze;

Viste inoltre le Direttive del Dipartimento della Funzione Pubblica dell'11 aprile 1997, del 25 settembre 1998 e del 30 ottobre 2001, che rappresentano, per le Regioni, uno schema di riferimento da tenere in considerazione nel disciplinare i propri sistemi di telefonia e che prevedono l'obbligo di effettuare controlli a campione sull'utilizzo delle utenze telefoniche ai fini di contenimento della spesa pubblica;

Dato atto che gli Allegati A e B di cui alla propria precedente determinazione 283/2008 sono stati applicati in via sperimentale a partire dal 17 aprile 2008 e che, a seguito della sperimentazione, sono state apportate le necessarie modifiche e integrazioni ai suddetti Allegati;

Valutato quindi di disciplinare i sopra esposti controlli e verifiche negli Allegati A e B al presente atto, quali parti integranti e sostanziali dello stesso, con la seguente ripartizione:

- A. Allegato A: modalità e procedure relative alle verifiche di sicurezza, previste dall'articolo 2, comma 2 lettera c) e dall'articolo 13 (G) e dall'art. 12 (AL) delle Linee guida;
- B. Allegato B: modalità e procedure relative ai controlli sull'utilizzazione dei beni messi a disposizione dall'amministrazione per lo svolgimento dell'attività lavorativa, con particolare riferimento all'utilizzazione delle strumentazioni informatiche e della telefonia sia fissa sia mobile;

Visto il provvedimento del Garante per la protezione dei dati personali "Lavoro: le linee guida del Garante per posta elettronica e internet", adottato con deliberazione n. 13 dell'1 marzo 2007;

Considerato di aver disciplinato gli allegati al presente atto nel rispetto dei principi contenuti nel provvedimento del Garante sopra richiamato;

Valutato inoltre che sia opportuno, anche al fine di evitare usi impropri derivanti da conoscenza non adeguata o incompleta, definire in via esemplificativa nell'Allegato C al presente atto, parte integrante e sostanziale dello stesso, i comportamenti da tenere nell'utilizzo delle strumentazioni informatiche e di telefonia messe a disposizione per lo svolgimento dell'attività lavorativa, come previsto dall'articolo 11 (G) e dall'art. 10 (AL), comma 3 delle Linee guida, con la precisazione che comunque tale Allegato C non è integrativo del Codice di comportamento già citato, contenendo un richiamo e una mera esemplificazione, in particolare, di quanto già previsto nel Codice di comportamento e nei Disciplinari Tecnici per utenti sull'utilizzo dei sistemi informativi;

Considerato di dover dare la massima diffusione del contenuto degli Allegati A, B e C a tutti i soggetti potenzialmente interessati e coinvolti dalle disposizioni contenute negli stessi Allegati;

Dato atto dell'accordo raggiunto con le rappresentanze sindacali in data 18 giugno 2009;

Acquisito il parere favorevole espresso dal Direttore generale dell'Assemblea legislativa, dott. Luigi Benedetti, con nota prot. n. 20744 del 16.07.2009;

Dato atto dei pareri allegati;

DETERMINA

1. di approvare l'Allegato A "Modalità e procedure relative alle verifiche di sicurezza, previste dall'articolo 2, comma 2 lettera c) e dall'articolo 13 (G) e dall'art. 12 (AL) delle Linee guida in materia di protezione dei dati personali della Giunta e dell'Assemblea legislativa della Regione Emilia-Romagna" e i relativi modelli di cui agli allegati A.1 e A.2;
2. di approvare l'Allegato B, "Modalità e procedure relative ai controlli sull'utilizzazione dei beni messi a disposizione dall'amministrazione per lo svolgimento dell'attività lavorativa, con particolare riferimento all'utilizzazione delle strumentazioni informatiche e della telefonia sia mobile sia fissa" e il relativo modello di cui all'allegato B.1;
3. di approvare l'informativa prevista dall'art. 13 del Codice per la protezione dei dati personali, allegata al presente atto e relativa ai trattamenti di dati personali conseguenti alle attività previste negli Allegati A e B;
4. di approvare l'Allegato C, "Comportamenti per un corretto utilizzo degli strumenti informatici e di telefonia messi a disposizione dall'Ente per lo svolgimento dell'attività lavorativa";
5. di disporre che i suddetti Allegati siano portati a conoscenza di tutti gli utenti del sistema regionale, con modalità tali da garantire la ricezione da parte degli stessi e quindi di procedere alla diffusione del contenuto degli Allegati A, B e C a partire dalla data di adozione del presente atto, fornendo contestualmente l'informativa prevista all'art. 13 del Codice per la protezione dei dati personali relativamente ai trattamenti di dati personali conseguenti alle disposizioni di tali Allegati; tale diffusione sarà effettuata tramite pubblicazione del presente atto, comprensivo degli Allegati, sul Bollettino Ufficiale della Regione Emilia-Romagna, contestualmente alla sua messa a disposizione nei siti Web regionali; successivamente, entro il periodo previsto al punto 7, sarà effettuata una distribuzione capillare a tutti i soggetti potenzialmente interessati all'applicazione degli Allegati A, B e C, con particolare riferimento ai dipendenti regionali;
6. di pubblicare, quindi, il presente atto integralmente nel Bollettino Ufficiale della Regione Emilia-Romagna, compresi gli Allegati A, B e C, parti integranti del medesimo atto;
7. di applicare gli Allegati A e B trascorsi due mesi dall'adozione del presente atto, durante i quali deve essere attuato quanto disposto al punto 5.

Il Direttore Generale

“Modalità e procedure relative alle verifiche di sicurezza, previste dall’articolo 2, comma 2 lettera c) e dall’articolo 13 (G) e dall’art. 12 (AL) delle Linee guida in materia di protezione dei dati personali della Giunta e dell’Assemblea legislativa della Regione Emilia-Romagna”

Indice

1. **Premessa**
2. **Ambito di applicazione**
3. **Finalità**
4. **Modalità delle verifiche di sicurezza**
5. **Personale addetto alle verifiche di sicurezza**
6. **Procedure di attuazione delle verifiche di sicurezza**
 - 6.1 **Verifiche puntuali preventive**
 - 6.2 **Verifiche puntuali a posteriori**
 - 6.3 **Verifiche periodiche**
 - 6.4 **Verifiche a campione**

Legenda:

Le citazioni relative agli articoli delle Linee guida della Giunta regionale e dell’Assemblea Legislativa sono denominati rispettivamente:

- con la lettera -G per la Giunta regionale;
- con le lettere -AL per l’Assemblea legislativa.

La denominazione “Responsabile della sicurezza” ricomprende sia il Responsabile della sicurezza della Giunta sia il Responsabile della sicurezza dell’Assemblea Legislativa, ciascuno per la propria area di competenza.

Allegato A.1: Modello di “Piano di test”

Allegato A.2: Modello di “Rapporto di incidente di sicurezza”

1. Premessa

Le verifiche di sicurezza sono effettuate sul sistema informativo della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna (di seguito denominate Ente quando ci si riferisce ad entrambe).

Per "sistema informativo" si intende 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.

Le verifiche di sicurezza sul sistema informatico condiviso e interconnesso tra Giunta e Assemblea Legislativa sono effettuate dal Responsabile della sicurezza della Giunta, dandone preventiva informazione al Responsabile della sicurezza dell'Assemblea Legislativa.

Le altre verifiche di sicurezza previste dal presente disciplinare sono effettuate rispettivamente dal Responsabile della sicurezza della Giunta e dal Responsabile della sicurezza dell'Assemblea Legislativa, ciascuno per la propria area di competenza.

A causa dell'interconnettività e dell'interdipendenza fra le componenti di un sistema informativo, i problemi di sicurezza su una sola di esse propagano i loro effetti incidendo gravemente sulla sicurezza del sistema nel suo complesso (per esempio: una postazione di lavoro non adeguatamente protetta può rendere vulnerabile la intranet dell'Ente anche in presenza di firewall o altri sistemi di sicurezza perimetrale). Le verifiche di sicurezza oggetto del presente disciplinare sono effettuate, pertanto, anche sulle strumentazioni assegnate ad altri titolari di trattamenti di dati personali quando vi è condivisione o interconnessione con le infrastrutture tecnologiche dell'Ente (ad esempio: dominio di autenticazione e servizi di rete). A tale fine gli altri titolari di trattamenti di dati personali che utilizzano strumentazioni in condivisione o interconnessione con le infrastrutture tecnologiche dell'Ente, ad esclusione dell'Assemblea Legislativa già ricompresa nel presente disciplinare, sottoscrivono con lo stesso Ente apposite convenzioni oppure effettuano la designazione a responsabile esterno della Giunta, come previsto al paragrafo 4 della deliberazione di Giunta regionale n. 2416/2008, precisando che le verifiche di sicurezza sulle strumentazioni sopra specificate sono effettuate dall'Ente con le modalità e le procedure stabilite dal presente disciplinare.

La verifiche sono effettuate:

- per preservare la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni;
- per garantire il rispetto di leggi e regolamenti in materia di protezione dei dati personali, in particolare dei requisiti minimi di sicurezza previsti dalla normativa vigente.

Le verifiche consistono in un'attività di monitoraggio sulla conformità dei sistemi informativi e dei comportamenti dei soggetti specificati al paragrafo 2, alle prescrizioni e regole comportamentali disposte dagli atti amministrativi di seguito richiamati:

- a) Linee guida della Giunta e dell'Assemblea legislativa della Regione Emilia-Romagna in materia di protezione dei dati personali (deliberazioni di Giunta regionale n. 1264 dell'1 agosto 2005 e dell'Ufficio di Presidenza n. 197 del 18 ottobre 2006);
- b) Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta/Assemblea legislativa della Regione Emilia-Romagna (determinazione D.G. Organizzazione, Personale, Sistemi informativi e Telematica n. 2653/2007; determinazione D.G. Assemblea legislativa n. 479/2007)

- c) Disciplinare tecnico relativo al controllo degli accessi ai locali della Giunta della Regione Emilia-Romagna (determinazione D.G. Organizzazione, Personale, Sistemi informativi e Telematica n. 2649/2007 e determinazione D.G. Assemblea legislativa n. 33/2008);
- d) Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta/Assemblea legislativa della Regione Emilia-Romagna (determinazione D.G. Organizzazione, Personale, Sistemi informativi e Telematica n.2651/2007; determinazione D.G. Assemblea legislativa n. 480/2007);
- e) Disciplinare tecnico in materia di videosorveglianza nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna (determinazione D.G. Organizzazione, Personale, Sistemi informativi e Telematica n.4856/2008).
- f) Disciplinare Tecnico per Amministratori di sistema della Giunta e dell'Assemblea Legislativa (determinazione n. 1416 del 2 marzo 2009);
- g) Disciplinare Tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna (determinazione n. 1703 del 9 marzo 2009).

b. Ambito di applicazione

L'ambito di applicazione del presente allegato si estende a tutti i soggetti che, a qualunque titolo, sono tenuti a rispettare le regole e i comportamenti contenuti nella normativa richiamata al paragrafo 1.

c. Finalità

Le verifiche di sicurezza sono eseguite al fine di:

- a) verificare la coerenza del funzionamento dei sistemi informativi con le politiche di sicurezza adottate dall'Ente;
- b) verificare la coerenza delle misure di sicurezza adottate con gli standard nazionali e/o internazionali e le normative vigenti in materia;
- c) verificare periodicamente la coerenza delle misure adottate con le politiche di sicurezza definite nei Documenti Programmatici sulla Sicurezza dell'Ente;
- d) individuare gli attacchi ai sistemi informativi (comportamenti che infrangono le politiche di sicurezza);
- e) proporre eventuali modifiche o nuove implementazioni ai sistemi di sicurezza sulla base delle verifiche effettuate.

d. Modalità delle verifiche di sicurezza

Le verifiche di sicurezza possono essere di quattro tipi:

- a) puntuali preventive;
- b) puntuali a posteriori;
- c) periodiche;

d) a campione.

Verifiche puntuali preventive: attività di verifica effettuate precedentemente all'implementazione o modifica sostanziale di un sistema o processo per verificarne la rispondenza alle politiche di sicurezza.

Verifiche puntuali a posteriori: attività di verifica effettuate a seguito del verificarsi di incidenti di sicurezza, come definiti al paragrafo 6.2.

Verifiche periodiche: attività di verifica, manuali o automatizzate, per contrastare minacce incombenti o potenziali, effettuate con cadenza periodica programmata.

Verifiche a campione: attività di verifica effettuate su campioni scelti secondo criteri prestabiliti e ad intervalli di tempo non fissi.

e. Personale addetto alle verifiche di sicurezza

Le verifiche di sicurezza possono essere effettuate esclusivamente da personale preventivamente autorizzato.

L'autorizzazione è data in forma scritta dal Responsabile della sicurezza della Giunta o dal Responsabile della sicurezza dell'Assemblea Legislativa, ciascuno per la propria area di competenza. Qualora l'effettuazione delle verifiche comprenda il trattamento di dati personali, gli addetti devono essere preventivamente individuati quali incaricati del trattamento dal soggetto competente ai sensi dell' Appendice 5 della D.G.R. n. 2416/2008 e della deliberazione dell'Ufficio di Presidenza dell'Assemblea legislativa n. 197 del 18 ottobre 2006.

f. Procedure di attuazione delle verifiche di sicurezza

6.1 Verifiche puntuali preventive

Prima della messa in produzione di un sistema (hardware o software) o di modifiche sostanziali di sistemi già in produzione, devono essere effettuate le verifiche necessarie per assicurare il rispetto delle politiche di sicurezza dell'Ente.

Le verifiche sono effettuate dal personale di cui al paragrafo 5, coadiuvato dal responsabile o referente del sistema.

Le verifiche sono condotte seguendo il "Piano di test" (di cui al modello *Allegato A.1*) preventivamente concordato fra i soggetti interessati.

Al termine delle verifiche, è redatto il "Verbale di test" secondo lo schema del "Piano di test". Il verbale è conservato agli atti a cura del Responsabile della sicurezza della Giunta o dell'Assemblea Legislativa, ciascuno per la propria area di competenza.

Il sistema può essere messo in produzione solo se le verifiche danno esito positivo. In caso contrario nel "Verbale di test" sono indicati gli adeguamenti necessari.

6.2 Verifiche puntuali a posteriori

Il Responsabile della sicurezza deve avviare un processo di verifica a posteriori nel caso in cui sia segnalato o riscontrato un incidente di sicurezza.

Per “incidente di sicurezza” si intende una violazione, o minaccia di imminente violazione, delle policy di sicurezza approvate dall’Ente.

Qualora si verifichi un incidente di sicurezza informatica si applica quanto previsto dallo specifico Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell’Assemblea Legislativa della Regione Emilia-Romagna (determinazione n. 1703/2009).

A seguito di un incidente di sicurezza il Responsabile della sicurezza deve quindi, in particolare:

- a) adoperarsi per contenere gli effetti dannosi provocati dall’incidente isolando il sistema o i sistemi colpiti;
- b) dare disposizioni affinché siano conservati i dati necessari da mettere eventualmente a disposizione delle autorità giudiziarie;
- c) adoperarsi per ripristinare il sistema o i sistemi coinvolti;
- d) effettuare un’analisi delle cause dell’incidente;
- e) effettuare, nell’ipotesi in cui riscontri elementi che inducano ad ipotizzare un utilizzo improprio degli strumenti dell’amministrazione, le ulteriori verifiche necessarie ad acquisire i dati, anche personali, strettamente necessari da comunicare ai soggetti di cui alla lettera g);
- f) redigere il “Rapporto di incidente di sicurezza” (*allegato A.2*). Tale rapporto è integrato, nel caso di cui alla lettera e), dai dati, anche personali, strettamente necessari affinché i Responsabili di cui alla lettera g) possano effettuare le ulteriori valutazioni e adottare le azioni conseguenti. Il Rapporto di incidente deve essere conservato agli atti a cura del Responsabile della sicurezza della Giunta o dell’Assemblea Legislativa, ciascuno per la propria area di competenza, per cinque anni (cfr. Manuale su internosi);
- g) inviare in forma riservata il Rapporto di incidente di sicurezza ai Responsabili coinvolti (Responsabili del trattamento di dati personali, Responsabili della sicurezza o Responsabili dei Sistemi Informativi di altri enti, Responsabili da cui il soggetto che ha provocato l’incidente dipende funzionalmente) o ad altri titolari del trattamento di dati personali.

Qualora l’incidente si sia verificato nel sistema informatico condiviso e interconnesso tra Giunta e Assemblea Legislativa, il Responsabile della sicurezza della Giunta deve inviare in forma riservata il Rapporto di incidente di sicurezza al Responsabile della sicurezza dell’Assemblea Legislativa.

6.3.1 Verifiche periodiche

I sistemi informativi dell’Ente sono soggetti costantemente a verifica per adempiere alle finalità di cui al paragrafo 3.

Le verifiche periodiche devono essere opportunamente documentate da parte del personale che le effettua e la documentazione è conservata agli atti a cura del Responsabile della sicurezza della Giunta o dell’Assemblea Legislativa, ciascuno per la propria area di competenza.

Le verifiche possono essere effettuate con cadenza periodica programmata (inferiore o meno a 15 giorni) o per contrastare minacce di sicurezza incombenti.

6.3.a Verifiche periodiche effettuate con cadenza inferiore ai 15 giorni

Tali verifiche riguardano le attività indicate nell'Informativa sui trattamenti di dati personali effettuati per attività di verifica di sicurezza periodica. Tutti gli utenti dei sistemi informativi dell'Ente devono essere portati a conoscenza di tale informativa. Esempi di tali attività sono:

- a) verifiche giornaliere sui log del sistema firewall;
- b) verifiche dei software installati sui sistemi server e client;
- c) verifiche sul traffico di rete;
- d) verifiche sull'efficienza dei sistemi proxy;
- e) verifiche sui sistemi antivirus;
- f) verifiche sull'efficacia dei filtri antispam.

Nel caso in cui a seguito delle verifiche si riscontri un incidente di sicurezza, il Responsabile della sicurezza della Giunta procede come specificato al paragrafo 6.2.

6.3.b Verifiche periodiche effettuate con cadenza superiore ai 15 giorni

Per verificare la corretta applicazione e l'efficiente funzionamento delle misure di sicurezza nell'Ente, il Responsabile della sicurezza della Giunta o il Responsabile della sicurezza dell'Assemblea Legislativa, ciascuno per la propria area di competenza, possono eseguire verifiche di sicurezza anche con cadenza periodica superiore ai 15 giorni, programmando le verifiche secondo un "Piano di test" (di cui al modello Allegato A.1).

In questo caso il Responsabile della sicurezza deve fornire preventiva e puntuale informazione sulle verifiche da effettuare ai soggetti interessati, compresi i responsabili esterni del trattamento di cui al paragrafo 4 dell'Appendice n. 5 della deliberazione di Giunta regionale n. 2416/2008 e deliberazione dell'Ufficio di Presidenza dell'Assemblea legislativa n. 197 del 18 ottobre 2006. Tale informazione deve essere fornita con un preavviso non inferiore ai 15 giorni inoltrando ai soggetti interessati il suddetto "Piano di test".

Al termine della verifica viene predisposto il "Verbale di test" secondo lo schema contenuto nello stesso Piano di test. Il verbale è conservato agli atti a cura del Responsabile della sicurezza competente e i risultati delle verifiche sono comunicati ai soggetti interessati.

A titolo esemplificativo, le verifiche effettuate con cadenza periodica superiore ai 15 giorni possono essere:

- a) verifiche sull'avvenuta adozione e sul contenuto degli atti di designazione dei responsabili esterni o degli incaricati dei trattamenti di dati personali;
- b) verifiche sui trattamenti censiti nelle schede del Registro Informatico dei trattamenti istituito ai sensi dell'art. 15 (G) e art. 14 (AL) delle Linee guida della Regione Emilia-Romagna in materia di protezione dei dati personali;
- c) verifiche sulla corretta applicazione delle procedure di controllo degli accessi presso le portinerie dell'Ente;
- d) verifiche sulle configurazioni dei sistemi server e client;
- e) verifiche su sviluppo, configurazione e deployment delle applicazioni informatiche;

- f) verifiche sugli accessi remoti ai sistemi informativi regionali (VPN, dial-up, ecc.);
- g) verifiche sugli apparati di rete e sui sistemi (vulnerability scan, penetration test, ecc.);
- h) Verifiche sulle corretta applicazione delle policy da parte degli amministratori di sistema;
- i) verifiche sulla corretta applicazione delle misure di sicurezza, tra le quali, in particolare, verifiche sul rispetto dei comportamenti esemplificati nell'Allegato C.

Al termine delle verifiche, in caso sia riscontrato un incidente di sicurezza, il Responsabile della sicurezza della Giunta procede come specificato al paragrafo 6.2.

6.4 Verifiche a campione

Il Responsabile della sicurezza può eseguire le medesime verifiche esemplificate al paragrafo 6.3.b anche a campione, con estrazione casuale.

L'estrazione è pubblica. Con avviso su Internos si comunicano luogo e modalità dell'estrazione almeno 15 giorni prima dell'estrazione stessa.

Dopo l'estrazione, si applicano le stesse modalità delle verifiche programmate di cui al paragrafo 6.3.b.

Al termine delle verifiche, in caso sia riscontrato un incidente di sicurezza, il Responsabile della sicurezza procede come specificato al paragrafo 6.2.

Piano di esecuzione dei test di sicurezza

1. Premessa:

.....

 (breve descrizione del sistema da sottoporre a test di sicurezza e del contesto di riferimento)

2. Responsabilità:

.....
(elenco del personale coinvolto nel test di sicurezza);
(referente del sistema da testare);
(responsabile del test di sicurezza).

3. Dettaglio dei test:

Id test	Descrizione	Data test	Risultato	Note

4. Note:

.....
 (eventuali considerazioni sul test di sicurezza, suggerimenti, adeguamenti da effettuare, ecc.)

5. Riferimenti:

.....
 (eventuali riferimenti ad allegati o altri documenti utili)

Bologna, li _____

Responsabile della Sicurezza
 (nome e cognome)

Rapporto incidente di sicurezza

1. Premessa:

.....
.....
(breve descrizione dell'incidente, dei sistemi coinvolti, degli utenti su cui l'incidente ha impatto, della durata dell'incidente, delle modalità attraverso le quali si è venuti a conoscenza dell'incidente)

2. Descrizione dettagliata dell'incidente:

.....(causa che ha determinato l'incidente);
.....(sistemi coinvolti);
.....(eventuali disservizi causati);
.....(utenti coinvolti);
.....(eventuali enti esterni coinvolti);
.....(dettagli tecnici rilevanti: es. log dei sistemi, traffico di rete, schermate, e-mail, ecc.).

3. Rilevazione dell'incidente:

.....
.....
(modalità attraverso le quali si è venuti a conoscenza dell'incidente:
- notifica automatica tramite sistemi di rilevazione
- individuazione a seguito di verifiche di sicurezza
- segnalazione da parte di un utente
- altro).

4. Contromisure adottate

.....
.....
(descrizione delle azioni intraprese per contenere i danni causati dall'incidente e per ripristinare i sistemi)

5. Conclusioni

.....(impatto dell'incidente sui sistemi o sui servizi);
.....(elementi che avrebbero consentito di prevenire il verificarsi dell'incidente);
.....(ulteriori azioni di approfondimento necessarie).

6. Note:

.....
(eventuali considerazioni sull'incidente, suggerimenti, adeguamenti da effettuare, ecc.)

7. Riferimenti:

.....
(eventuali riferimenti ad allegati o altri documenti)

Responsabile della Sicurezza
(nome e cognome)

Bologna, li _____

Allegato B

“Modalità e procedure relative ai controlli sull'utilizzazione dei beni messi a disposizione dall'amministrazione per lo svolgimento dell'attività lavorativa, con particolare riferimento all'utilizzazione delle strumentazioni informatiche e della telefonia sia mobile sia fissa”

Indice

1	Premessa
2	Ambito di applicazione
3	Principi
4	Finalità
5	Modalità dei controlli sull'utilizzo delle strumentazioni informatiche
6	Procedura dei controlli sull'utilizzo delle strumentazioni informatiche
7	Controlli sull'utilizzo della telefonia (sia fissa sia mobile)

Allegato B.1 : Modello di “Verbale di controllo”

1. Premessa

Tutti i beni che la Giunta e l'Assemblea legislativa della Regione Emilia-Romagna (di seguito denominate Ente quando ci si riferisce ad entrambe) mette a disposizione per lo svolgimento dell'attività lavorativa devono essere utilizzati, da parte di coloro che vi operano, a qualunque livello e con qualsiasi rapporto, come disposto dall'art. 8, comma 1 del Codice di comportamento per i dipendenti della Regione Emilia-Romagna:

- a) in modo strettamente pertinente alla propria attività lavorativa e impegnandosi a un utilizzo appropriato, efficiente, corretto e razionale;
- b) tenendo sempre presente l'interesse collettivo al risparmio delle risorse pubbliche, delle fonti di energia e delle risorse naturali, anche in un'ottica di tutela delle generazioni future.

Il comma 2 dello stesso art. 8, inoltre, specifica che gli stessi soggetti "con riferimento alle linee telefoniche, alla posta elettronica, a Internet e agli altri beni telematici si impegnano a:

- a) utilizzare tali beni per motivi non attinenti all'attività lavorativa soltanto in casi di urgenza e comunque non in modo ripetuto o per periodi di tempo prolungati;
- b) utilizzare la posta elettronica e Internet nel rispetto del principio di riservatezza, per le specifiche finalità della propria attività e rispettando le esigenze di funzionalità della rete e quelle di semplificazione dei processi lavorativi;
- c) evitare di inviare messaggi con contenuto censurabile, o che possano compromettere l'immagine della Regione;
- d) non appesantire il traffico della rete con operazioni particolarmente lunghe e complesse quando ciò non sia necessario;
- e) evitare di collegarsi a siti di per sé censurabili".

I comportamenti corretti nell'utilizzo dei beni di cui all'art. 8, comma 2 sono ulteriormente specificati ed esemplificati nell'Allegato C, anche al fine di evitare comportamenti potenzialmente pericolosi per la sicurezza del sistema informativo derivanti da conoscenza non adeguata o incompleta. Tale Allegato C non è integrativo del Codice di comportamento dell'amministrazione regionale.

Con riferimento all'utilizzo delle strumentazioni informatiche, i controlli di cui al presente allegato B sono relativi ai comportamenti di cui alle lettere a) e b) dello stesso Allegato C.

Il comma 3 dello stesso articolo, infine, dispone che la "Regione si impegna ad effettuare i controlli sull'utilizzo dei beni adottando criteri oggettivi preventivamente comunicati".

Il presente atto quindi in particolare disciplina regole, procedure e modalità relativamente ai controlli che riguardano l'utilizzazione delle strumentazioni informatiche e della telefonia sia fissa sia mobile, in quanto per loro stessa natura comportano la possibilità di effettuare controlli con apparecchiature a distanza.

Si specifica, infine, che nella definizione di "attività lavorativa" devono essere ricomprese anche le attività che siano strumentali e connesse alla stessa, quali ad esempio i rapporti con le organizzazioni sindacali.

2. Ambito di applicazione

L'Ente effettua i controlli su tutte le strumentazioni informatiche e sugli strumenti di telefonia, sia fissa sia mobile, messi a disposizione dall'Ente stesso al fine di verificarne il corretto utilizzo, con l'unica esclusione, al fine di preservare il libero esercizio delle funzioni politiche e sindacali, delle strumentazioni individuali messe a disposizione degli organi politici, delle strutture di diretta collaborazione degli stessi e delle organizzazioni sindacali nonché dei rappresentanti della RSU.

Qualora si rilevi, a seguito delle procedure disciplinate dai paragrafi successivi, che la strumentazione sia assegnata a un Direttore Generale o a un Direttore, per "dirigente di riferimento del soggetto coinvolto nel controllo" si intende:

- a) il Direttore Generale della Giunta competente in materia di strumentazioni informatiche e telefoniche;
- b) il Capo di Gabinetto qualora la strumentazione sia assegnata al soggetto di cui alla lettera a).

L'Ente non può in nessun caso controllare il contenuto dei messaggi di posta elettronica. Nel caso di specifica e circostanziata segnalazione relativa ad un utilizzo improprio di una casella di posta istituzionale, la segnalazione è conservata agli atti e trasmessa al Responsabile della sicurezza della Giunta e/o al Responsabile della sicurezza dell'Assemblea Legislativa e al Responsabile da cui dipende funzionalmente il soggetto titolare della casella di posta stessa perché i suddetti responsabili possano effettuare le ulteriori valutazioni e adottare le eventuali azioni conseguenti.

L'Ente può controllare anche il contenuto delle navigazioni su Internet, ma solo quando ciò sia indispensabile per accertare l'utilizzo improprio della strumentazione informatica.

3. Principi

L'Ente ritiene che l'attività di prevenzione debba essere prevalente rispetto all'attività di controllo. Si impegna pertanto a potenziare in misura crescente tale attività di prevenzione, in particolare tramite l'adozione di appositi disciplinari tecnici (ad es. per utenti sull'utilizzo dei sistemi informativi: determinazione del Direttore Generale all'Organizzazione, Personale, Sistemi Informativi e Telematica n. 2653/2007 e del D.G. dell'Assemblea Legislativa n. 479/2007), azioni di sensibilizzazione e di diffusione dei principi e delle regole nell'utilizzo delle strumentazioni telematiche e telefoniche (ad esempio tramite comunicazioni interne e la predisposizione e diffusione di opuscoli informativi), attività formative mirate, specifiche soluzioni tecnologiche ed ogni altra misura ritenuta idonea a tal fine.

I controlli effettuati dall'Ente devono in ogni caso rispettare i seguenti principi:

- a) necessità: i dati trattati durante l'attività di controllo devono essere sempre e soltanto quelli strettamente necessari a perseguire le finalità di cui al paragrafo 4;
- b) proporzionalità: i controlli devono sempre essere effettuati con modalità tali da garantire, nei singoli casi concreti, la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite e specificate al paragrafo 4;
- c) imparzialità: i controlli devono essere effettuati su tutte le strumentazioni informatiche e telefoniche messe a disposizione dall'amministrazione regionale e conseguentemente possono coinvolgere tutti gli utilizzatori delle stesse, a qualunque titolo abbiano assegnata la strumentazione. L'imparzialità inoltre deve essere garantita mediante sistemi automatici di estrazione casuale per l'effettuazione dei controlli a campione ed in nessun caso possono essere effettuati controlli mirati e ripetuti nei confronti di soggetti specifici con finalità discriminatorie o persecutorie o volutamente sanzionatorie. I controlli puntuali possono essere effettuati soltanto sulla base di specifiche, oggettive e circostanziate segnalazioni, come esplicitato al paragrafo 6 ovvero nel caso in cui si siano rilevate evidenti anomalie rispetto al volume assegnato di cui al paragrafo 7.1.
- d) trasparenza: in base a tale principio l'amministrazione deve mettere in atto tutte le azioni necessarie per garantire la preventiva conoscenza da parte di tutti i soggetti potenzialmente sottoposti ai controlli del presente disciplinare. Devono pertanto essere informati dei possibili controlli tutti i soggetti che operano, a qualunque titolo e con qualunque rapporto, per l'Ente, tra cui, in particolare, tutti i soggetti che hanno con lo stesso sia un rapporto di lavoro subordinato (di qualsiasi tipologia) sia un rapporto di lavoro autonomo. A tal fine l'Ente deve in particolare consegnare l'informativa ex art. 13 del Codice per la protezione dei dati personali all'atto della sottoscrizione del contratto e tale informativa deve contenere espresso riferimento al presente disciplinare.
- e) protezione dei dati personali: i controlli devono in ogni caso essere effettuati rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo nonché garantendo la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati devono essere conosciuti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento, tra i quali, in particolare, il Responsabile della sicurezza della Giunta o il Responsabile della sicurezza dell'Assemblea Legislativa, ciascuno per la propria area di competenza ed i soggetti specificati al paragrafo 6. Oltre a quanto specificato alla lettera c),

inoltre, i controlli devono essere effettuati rispettando la normativa vigente in materia di protezione dei dati personali ed in particolare le prescrizioni di cui all'art. 11 del Codice.

4. Finalità

I controlli di cui al presente Allegato B sono effettuati per le seguenti finalità:

- a) consentono di monitorare e mirano a ridurre la spesa pubblica, sia rilevando eventuali danni patrimoniali già posti in essere, sia agendo quale strumento di dissuasione rispetto a comportamenti impropri e potenzialmente dannosi, per cui la loro omissione potrebbe comportare responsabilità patrimoniali dirette a carico dell'amministrazione regionale;
- b) possono evitare o comunque ridurre i rischi di coinvolgimento civile e penale, per concorso di reato, dell'Ente, nel caso di illeciti nei confronti di terzi, commessi mediante un utilizzo improprio dei beni messi a disposizione dall'amministrazione stessa;
- c) possono concorrere a tutelare l'immagine dell'Ente e di coloro che vi prestano la propria attività;
- d) concorrono ad approfondire elementi che emergono in seguito a segnalazioni di incidenti di sicurezza, in modo da evidenziare eventuali rischi al fine di una successiva attività di prevenzione.

L'Ente intende, tramite una costante attività di comunicazione interna, sviluppare in particolar modo la finalità di dissuasione rispetto a comportamenti impropri.

La finalità dissuasiva deve infatti essere prevalente, insieme all'attività di prevenzione di cui al paragrafo 3, rispetto alle attività volte ad accertare l'effettuazione di utilizzi impropri delle strumentazioni.

5. Modalità dei controlli sull'utilizzo delle strumentazioni informatiche

Il controllo sull'utilizzo delle strumentazioni informatiche è di due tipologie:

- a) puntuale.
- b) a campione.

a) Controllo puntuale

Il controllo puntuale è effettuato su strumentazioni informatiche determinate, a seguito di specifica segnalazione effettuata da un soggetto terzo oppure in seguito ad una verifica di sicurezza.

Nel caso in cui la segnalazione del soggetto terzo si riferisca a una persona nominativamente individuata, il Responsabile della sicurezza della Giunta deve dare informazione del controllo in corso al soggetto cui si riferisce la segnalazione, specificando che può essere presentata richiesta di accesso ai relativi documenti amministrativi a norma della Legge n. 241/1990 e ss. mod. e int.

Il Responsabile della sicurezza della Giunta deve contestualmente informare il Responsabile della sicurezza dell'Assemblea Legislativa qualora il controllo rientri nell'ambito di competenza di quest'ultimo.

b) Controllo a campione

Estrazione della giornata

Il controllo a campione è effettuato, su strumentazioni informatiche non predeterminate, con cadenza trimestrale con estrazione a sorte, mediante un generatore di numeri casuali, di una giornata nell'arco dei tre mesi precedenti all'estrazione.

Il controllo è effettuato sui log di navigazione in Internet relativi alla giornata estratta e ai 6 giorni successivi e consecutivi alla giornata estratta.

Estrazione del campione

Il campione è costituito, in via alternativa:

b.1) da una percentuale pari allo 0,5% del totale delle postazioni client;

b.2) da tutte le postazioni client di una determinata struttura organizzativa.

L'identificativo univoco delle postazioni client è il numero di inventario della postazione stessa. Il numero di inventario è quindi associato all'indirizzo IP assegnato in automatico alla postazione al momento del login alla rete regionale nella giornata estratta. Le verifiche sui log di navigazione sono quindi effettuate sui record relativi a tale indirizzo IP.

Prima di procedere all'estrazione a sorte i file contenenti gli elenchi con i numeri di inventario delle postazioni client (b.1) ovvero con le strutture regionali (b.2), sono firmati digitalmente dalla Responsabile della sicurezza della Giunta che subito dopo vi appone la marca temporale.

Nel caso b.1) sono estratte a sorte, con un generatore di numeri casuali, le singole postazioni client fino al raggiungimento della percentuale sopra determinata.

Nel caso b.2) è estratta a sorte, con un generatore di numeri casuali, una struttura organizzativa tra tutte quelle dell'Ente (Servizio/ Direzione Generale/Agenzia) e sono sottoposte a controllo tutte le postazioni client assegnate alla struttura estratta.

Dopo l'estrazione tutti i documenti informatici (verbale dell'estrazione, file firmati digitalmente) sono protocollati nel sistema di protocollazione informatica.

Le estrazioni di cui sopra sono pubbliche. Con avviso su Internos si comunicano luogo e modalità dell'estrazione almeno 15 giorni prima dell'estrazione stessa.

6. Procedura dei controlli sull'utilizzo delle strumentazioni informatiche

6.1 Controllo puntuale

Il controllo puntuale è avviato:

- a) su segnalazione di un soggetto terzo;
- b) a seguito di una verifica di sicurezza.

Le segnalazioni di cui alla lettera a):

- non sono tenute in considerazione qualora siano anonime;
- devono essere rivolte per iscritto al Responsabile della sicurezza della Giunta. Nel caso in cui la segnalazione sia riferita nominativamente ad uno o più utilizzatori e riguardi anche

l'ambito di competenza del responsabile della sicurezza dell'Assemblea Legislativa, il Responsabile della sicurezza della Giunta deve informare immediatamente quest'ultimo.

Nel caso sub b) il controllo è effettuato qualora il Responsabile della sicurezza della Giunta riscontri, a seguito dell'analisi delle cause di un incidente di sicurezza, elementi che configurino un possibile utilizzo improprio delle strumentazioni informatiche. In questo caso, come specificato al paragrafo 6.2 dell'Allegato A, il Responsabile della sicurezza della Giunta effettua le ulteriori verifiche per acquisire i dati, anche personali, strettamente necessari da comunicare ai Responsabili di cui alla lettera g del paragrafo 6.2 già citato, perché gli stessi possano effettuare le ulteriori valutazioni e adottare le azioni conseguenti.

Le ulteriori verifiche possono ricomprendere controlli sui log di navigazione in Internet. E' possibile verificare il contenuto dei siti di navigazione soltanto nel caso in cui le relative informazioni siano indispensabili al fine di verificare se ci sia stato un utilizzo proprio o improprio dello strumento messo a disposizione dall'amministrazione.

Le ulteriori verifiche, inoltre, qualora sia necessario, possono essere effettuate sui dati relativi a più giornate consecutive, con un limite massimo di 28 giornate.

Qualora, anche a seguito delle ulteriori verifiche effettuate, il Responsabile della sicurezza della Giunta riscontri elementi che confermino un possibile uso improprio delle strumentazioni messe a disposizione dell'Ente, associa il nominativo dell'utilizzatore alla postazione client, per poter procedere come di seguito disciplinato.

Conseguentemente alle verifiche effettuate nei casi a) e b) e all'individuazione del nominativo dello/degli utilizzatore/i, il Responsabile della sicurezza della Giunta:

- trasmette al dirigente di riferimento del soggetto coinvolto nel controllo (di norma il responsabile di Servizio o, nel caso di soggetti alle loro dirette dipendenze, il Direttore Generale o il Direttore) un "Verbale di controllo" (allegato B.1) perché il Responsabile stesso possa effettuare le valutazioni conseguenti, con particolare riferimento ad una verifica relativa alla pertinenza (o stretta attinenza) o meno dei dati di navigazione, trasmessi nel Verbale di controllo, con l'attività lavorativa, come definita al paragrafo 1 del presente Allegato B;
- trasmette contestualmente il suddetto "Verbale di controllo" al Responsabile della sicurezza dell'Assemblea Legislativa qualora il soggetto coinvolto sia assegnato alla stessa;
- ne dà contestuale comunicazione al soggetto coinvolto.

La verifica di pertinenza (o stretta attinenza) con l'attività lavorativa, che deve essere effettuata dal dirigente di riferimento, deve comprendere anche una tempestiva audizione dello stesso soggetto, perché possa fornire chiarimenti, motivazioni ed osservazioni a proposito di quanto rilevato. Alla audizione può essere presente, su richiesta del dirigente di riferimento o del soggetto coinvolto nel controllo, il Responsabile della sicurezza (o altro tecnico addetto alla sicurezza individuato dal Responsabile della sicurezza).

A seguito delle verifiche sopra specificate, il dirigente di riferimento dell'utilizzatore della postazione client:

- comunica immediatamente per iscritto all'utilizzatore stesso l'esito del controllo;
- avvia, nel caso in cui si ritenga che vi sia stato un utilizzo improprio dello strumento informatico, i procedimenti conseguenti.

6.2 Controllo a campione

Sulle postazioni client oggetto di controllo a seguito delle estrazioni effettuate con le modalità di cui al paragrafo 5, il Responsabile della sicurezza della Giunta effettua i controlli necessari per verificare la conformità dell'utilizzo ai comportamenti esemplificati alle lettere a) e b) dell'allegato C.

Nel caso in cui il Responsabile della sicurezza della Giunta riscontri, a seguito dell'analisi dei dati di navigazione registrati nelle 7 giornate complessive di cui al paragrafo 5 lettera b), elementi che configurino un possibile utilizzo improprio delle strumentazioni informatiche, può verificare i dati relativi ad altre giornate consecutive a quella estratta con le modalità di cui al paragrafo 5, con un limite massimo di ulteriori 21 giornate (con un limite massimo complessivo quindi di 28 giornate).

Qualora, anche a seguito delle verifiche effettuate sulle ulteriori giornate, sia confermata la presenza di elementi che configurino un possibile utilizzo improprio delle strumentazioni informatiche, il Responsabile della sicurezza della Giunta effettua un avviso generalizzato:

- a tutti gli utenti del sistema informativo regionale nel caso di campione percentuale estratto su tutte le postazioni client (lettera b.1 del paragrafo 5);
- a tutti gli utilizzatori di postazioni client riferite alla struttura soggetta a controllo (lettera b.2 del paragrafo 5) con modalità tali da garantirne la ricezione da parte degli stessi.

Nell'avviso sono sinteticamente esplicitate le anomalie riscontrate e sono specificati i termini temporali per l'effettuazione di un ulteriore controllo:

- sulle postazioni client su cui si sono rilevate le anomalie nel caso di cui alla lettera b.1 del paragrafo 5;
- su tutte le postazioni client riferite alla stessa struttura organizzativa nel caso di cui alla lettera b.2 del paragrafo 5.

Nel caso in cui si riscontrassero ulteriori anomalie in seguito al controllo effettuato successivamente all'avviso, si procederà ad associare il nominativo dell'utilizzatore alla postazione client, per poter procedere come di seguito disciplinato. L'avviso deve contenere un richiamo anche a tale eventuale conseguenza.

A seguito dell'individuazione del nominativo dell'utilizzatore (effettuata nel caso di ulteriori anomalie riscontrate dopo l'avviso generalizzato), il Responsabile della sicurezza della Giunta:

- a) invia al dirigente di riferimento del soggetto coinvolto nel controllo (di norma il responsabile di Servizio o, nel caso di soggetti alle loro dirette dipendenze, il Direttore Generale o il Direttore) un "Verbale di controllo" per ciascun nominativo (allegato B.1) perché lo stesso possa effettuare le valutazioni conseguenti, con particolare riferimento ad una verifica relativa alla pertinenza o meno dei dati di navigazione, trasmessi nel Verbale di controllo, con l'attività lavorativa;
- b) trasmette contestualmente il suddetto "Verbale di controllo" al Responsabile della sicurezza dell'Assemblea Legislativa qualora il soggetto coinvolto sia assegnato alla stessa;
- c) dà, contestualmente all'invio di cui alla lettera a), comunicazione al soggetto coinvolto dell'invio stesso.

La suddetta verifica di pertinenza deve comprendere anche una tempestiva audizione dello stesso soggetto da parte del dirigente di riferimento, perché possa fornire chiarimenti, motivazioni ed osservazioni a proposito di quanto rilevato. Alla audizione può essere presente, su richiesta del

dirigente di riferimento o del soggetto coinvolto nel controllo, il Responsabile della sicurezza (o altro tecnico addetto alla sicurezza individuato dal Responsabile della sicurezza).

A seguito delle verifiche sopra specificate, il dirigente di riferimento dell'utilizzatore della postazione client:

- comunica immediatamente per iscritto all'utilizzatore stesso l'esito del controllo;
- avvia, nel caso in cui si ritenga che vi sia stato un utilizzo improprio dello strumento informatico, i procedimenti conseguenti.

6.3 Disposizioni comuni ai controlli di cui al paragrafo 6.1 e al paragrafo 6.2

Il controllo sui dati di navigazione è effettuato con i criteri e la metodologia di seguito esplicitati:

- a) è da considerare navigazione quella che comprende almeno 5 visualizzazioni di pagine html o xml (click del mouse) sulle pagine di uno stesso sito web nello spazio di 300 secondi (5 minuti), per non considerare eventuali accessi non voluti, ad esempio perché dovuti a meri errori di digitazione;
- b) l'utilizzo improprio della strumentazione (valutato su un periodo massimo complessivo di 28 giornate) è da considerare tale qualora sia ripetuto e non meramente episodico (su una sola giornata) salvo il caso in cui il singolo episodio sia, in base ai dati di navigazione, particolarmente rilevante in termini di tempo ovvero il sito visitato sia di contenuto evidentemente improprio e quindi non sia possibile in nessun modo presupporre la buona fede o il motivo di urgenza nella connessione (ad esempio qualora l'accesso sia a siti di giochi d'azzardo oppure a contenuto pornografico).

7. Controlli sull'utilizzo della telefonia (sia fissa sia mobile)

7. Controlli sull'utilizzo della telefonia (sia fissa sia mobile)

I controlli sugli strumenti di telefonia sono effettuati sia sulle strumentazioni di telefonia fissa sia sulle strumentazioni di telefonia mobile.

7.1 Controlli sull'utilizzo della telefonia fissa

I controlli sono effettuati su tabulati prodotti dall'Ente mediante un sistema di documentazione addebiti, gestito dalla Direzione Generale Centrale Organizzazione, Personale, Sistemi Informativi e Telematica. Le informazioni relative all'Assemblea Legislativa sono trasmesse al Servizio Gestione e Sviluppo della stessa.

I tabulati, che contengono il volume complessivo del traffico telefonico delle chiamate in uscita delle singole utenze con riferimento sia ai tempi sia all'importo addebitato all'Ente, sono periodicamente messi a disposizione dei Responsabili delle strutture a cui risultano assegnate le strumentazioni.

Nel caso in cui i Responsabili delle strutture a cui risultano assegnate le strumentazioni riscontrino evidenti anomalie nel volume complessivo di uno strumento di telefonia fissa, gli stessi possono richiedere, entro 30 giorni dall'invio delle informazioni, al Servizio competente in materia di telefonia della Direzione Generale Centrale Organizzazione, Personale, Sistemi Informativi e telematica e della Direzione Generale Assemblea Legislativa, le documentazioni analitiche delle chiamate in uscita effettuate dall'apparecchio di telefonia fissa con l'oscuramento delle ultime tre cifre per i dati telefonici, dando contestuale comunicazione della richiesta all'utilizzatore dell'apparecchio di telefonia.

Le evidenti anomalie in base alle quali il Responsabile può richiedere una documentazione analitica delle chiamate in uscita, effettuate con strumentazioni di telefonia fissa, devono consistere in rilevanti scostamenti rispetto ad un volume complessivo relativo alla singola utenza, preventivamente comunicato all'utilizzatore. Lo scostamento rispetto al volume complessivo preventivamente stabilito per la singola utenza, per potersi considerare rilevante, deve essere di almeno 30 punti percentuali.

Il Responsabile di riferimento deve valutare, ai fini di effettuare o meno la richiesta di documentazione analitica, le particolari ed eventuali specificità, anche temporalmente limitate, dell'attività lavorativa dell'utilizzatore della strumentazione telefonica.

L'assegnazione del volume di traffico a ciascuna utenza telefonica non intende infatti costituire un limite all'attività lavorativa del collaboratore che, anzi, può e deve poter effettuare tutte le chiamate telefoniche necessarie allo svolgimento della stessa: esso rappresenta soltanto un limite per il dirigente di riferimento il quale non può effettuare i controlli al di sotto di tale soglia. La richiesta del dettaglio analitico delle chiamate in uscita, quindi, è solo una possibilità del dirigente, che deve essere preceduta, come sopra esplicitato, da una valutazione che tenga conto dell'attività lavorativa del dipendente (continuativa o contingente).

Le documentazioni analitiche saranno poi esaminate congiuntamente e tempestivamente dal dirigente di riferimento e dall'utilizzatore, per verificarne in particolare la pertinenza con l'attività lavorativa. All'esame congiunto può essere presente, su richiesta del dirigente di riferimento o del soggetto coinvolto nel controllo, il Responsabile della sicurezza (o altro tecnico addetto alla telefonia individuato dal Responsabile della sicurezza).

7.2 Controlli sull'utilizzo della telefonia mobile

I controlli sulle strumentazioni di telefonia mobile sono effettuate, secondo quanto disposto anche dal comma 595 dell'art. 2 della Legge n. 244/2007, a campione.

Il controllo è effettuato sulle informazioni trasmesse dagli operatori telefonici al Servizio competente in materia di telefonia della Direzione Generale Centrale Organizzazione, Personale, Sistemi Informativi e Telematica e della Direzione Generale Assemblea Legislativa.

Estrazione del mese

Il controllo a campione è effettuato con cadenza trimestrale con estrazione a sorte, mediante un generatore di numeri casuali, di un mese tra i primi tre mesi dell'ultimo semestre rispetto alla data dell'estrazione (ad esempio se l'estrazione è effettuata nel mese di marzo, si estrae un mese tra ottobre, novembre e dicembre).

Estrazione del campione

Il campione è costituito da una percentuale pari al 5% del totale delle strumentazioni.

A seguito dell'estrazione, il Servizio competente in materia di telefonia della Direzione Generale Centrale Organizzazione, Personale, Sistemi Informativi e Telematica e della Direzione Generale Assemblea Legislativa inviano ai dirigenti di riferimento degli utilizzatori delle strumentazioni estratte un tabulato riepilogativo contenente i dati aggregati di traffico voce, sms, servizi e collegamenti Internet relativi al mese estratto.

Sono escluse dal controllo le chiamate private effettuate previa digitazione di un apposito codice che comporta l'addebito della chiamata direttamente all'utilizzatore.

Il tabulato riepilogativo è contestualmente inviato all'utilizzatore della strumentazione estratta, qualora la stessa gli sia assegnata in via esclusiva.

Il Responsabile di riferimento può, previa audizione dell'utilizzatore ed entro 30 giorni dall'invio del tabulato riepilogativo, richiedere il relativo dettaglio analitico, con oscuramento delle ultime tre cifre dei numeri chiamati, nei casi di seguito specificati:

a) qualora sia presente traffico in roaming internazionale non giustificato da trasferte lavorative oppure siano rilevati costi addebitati per servizi interattivi (a titolo esemplificativo per suonerie, loghi, giochi, ecc.);

b) qualora siano presenti chiamate verso direttrici internazionali.

La richiesta del dettaglio analitico è solo una possibilità del dirigente, il quale deve valutare, ai fini di effettuarla o meno, le particolari ed eventuali specificità, anche temporalmente limitate, dell'attività lavorativa dell'utilizzatore della strumentazione telefonica.

Le documentazioni analitiche saranno poi esaminate congiuntamente e tempestivamente dal dirigente di riferimento e dall'utilizzatore, per verificarne in particolare la pertinenza con l'attività lavorativa. All'esame congiunto può essere presente, su richiesta del dirigente di riferimento o del soggetto coinvolto nel controllo, il Responsabile della sicurezza (o altro tecnico addetto alla telefonia individuato dal Responsabile della sicurezza).

7.3 Disposizioni comuni

A seguito delle verifiche sopra specificate, il dirigente di riferimento dell'utilizzatore dello strumento di telefonia:

- comunica immediatamente per iscritto all'utilizzatore stesso l'esito del controllo;
- avvia, nel caso in cui si ritenga che vi sia stato un utilizzo improprio dello strumento di telefonia, i procedimenti conseguenti, compresi quelli finalizzati al recupero delle somme spese per chiamate rilevate quali personali e addebitate all'Ente.

**Verbale di controllo relativo alla postazione client assegnata
a..... (nome e cognome)**

1. Tipologia di controllo:

- Puntuale
- A campione

2. Descrizione del controllo:

.....
.....
(descrizione del controllo effettuato, tra cui: soggetto che ha effettuato la segnalazione nel caso di controllo puntuale; data di avviso estrazione e data di avvenuta estrazione nel caso di controllo a campione; giornata estratta e ulteriori giornate consecutive controllate fino ad un max di 28 giornate totali; ulteriore controllo effettuato dopo l'ulteriore avviso)

3. Risultati del controllo:

.....
.....
(descrizione dei risultati evidenziati a seguito del controllo effettuato, con descrizione dettagliata della postazione client per cui si sono evidenziate anomalie)

4. Note:

.....
.....

5. Riferimenti:

.....
.....
(eventuali riferimenti ad allegati o altri documenti utili)

Responsabile della Sicurezza
(nome e cognome)

Bologna, li _____

Informativa sui trattamenti di dati personali effettuati per le attività relative alle verifiche di sicurezza e ai controlli sull'utilizzazione dei beni messi a disposizione dall'amministrazione per lo svolgimento dell'attività lavorativa

1. Premessa

Ai sensi dell'art. 13 del D.Lgs. n. 196/2003 - "Codice in materia di protezione dei dati personali" (di seguito denominato "Codice"), la Regione Emilia-Romagna ed in particolare sia la Giunta regionale sia l'Assemblea Legislativa, in qualità di "Titolari" del trattamento, sono tenute a fornirle informazioni in merito all'utilizzo dei suoi dati personali.

Il trattamento dei suoi dati per lo svolgimento di funzioni istituzionali da parte della Regione Emilia-Romagna, in quanto soggetto pubblico non economico, non necessita del suo consenso.

2. Fonte dei dati personali

La raccolta dei suoi dati personali viene effettuata con la registrazione dei dati da lei stesso forniti al momento dell'utilizzo delle strumentazioni fornite dall'amministrazione per lo svolgimento dell'attività lavorativa ovvero già contenuti in altre banche dati presenti nel sistema informativo regionale.

3. Finalità del trattamento

I dati personali sono trattati per effettuare le verifiche di sicurezza e i controlli sull'utilizzazione dei beni dell'amministrazione regionale, con le modalità previste dagli Allegati A e B della determinazione del Direttore Generale Organizzazione, Personale, Sistemi Informativi e Telematica n..... del

4. Modalità di trattamento dei dati

In relazione alle finalità descritte, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità sopra evidenziate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi.

5. Facoltatività del conferimento dei dati

Il conferimento dei dati è automaticamente correlato all'utilizzazione degli strumenti messi a disposizione per lo svolgimento dell'attività lavorativa.

6. Categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati

I suoi dati personali potranno essere conosciuti esclusivamente dagli operatori del Servizio Sistema Informativo-informatico regionale della Giunta e dagli operatori del Servizio Gestione e sviluppo dell'Assemblea Legislativa, individuati quali Incaricati del trattamento.

Esclusivamente per le finalità previste al paragrafo 3 (Finalità del trattamento), tali dati possono essere trasmessi ai dirigenti di riferimento, per le eventuali ulteriori verifiche connesse al ruolo dirigenziale relativamente alla gestione del personale. Possono inoltre venirne a conoscenza società terze fornitrici di servizi per la Regione Emilia-Romagna, previa designazione in qualità di Responsabili del trattamento e garantendo il medesimo livello di protezione.

7. Diritti dell'Interessato

La informiamo, infine, che la normativa in materia di protezione dei dati personali conferisce agli Interessati la possibilità di esercitare specifici diritti, in base a quanto indicato all'art. 7 del "Codice" che qui si riporta:

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:

- a) dell'origine dei dati personali;

- b) delle finalità e modalità del trattamento;
- c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2;
- e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

- a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
- b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

- a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

8. Titolari e Responsabili del trattamento

I Titolari del trattamento dei dati personali di cui alla presente Informativa sono la Giunta regionale e l'Assemblea legislativa, con sede in Bologna, rispettivamente in Viale Aldo Moro n. 52 e n. 50, cap 40127. La Regione Emilia-Romagna ha designato quali Responsabili del trattamento il Direttore Generale Organizzazione, Personale, Sistemi Informativi e Telematica e il Direttore Generale dell'Assemblea Legislativa. Gli stessi sono responsabili del riscontro, in caso di esercizio dei diritti sopra descritti, ciascuno per il proprio ambito di competenza.

Al fine di avere chiarimenti sulla compilazione dei moduli, ovvero al fine di semplificare le modalità di inoltro e ridurre i tempi per il riscontro si invita a presentare le richieste, di cui al precedente paragrafo, alla Regione Emilia-Romagna, Ufficio per le relazioni con il pubblico (Urp), per iscritto o recandosi direttamente presso lo sportello Urp.

L'Urp è aperto dal lunedì al venerdì dalle 9 alle 13 in Viale Aldo Moro 52, 40127 Bologna (Italia): telefono 800-662200, fax 051-6395360, e-mail urp@regione.emilia-romagna.it.

Le richieste di cui all'art.7 del Codice comma 1 e comma 2 possono essere formulate anche oralmente.

Comportamenti per un corretto utilizzo degli strumenti informatici e di telefonia messi a disposizione dall'Ente¹ per lo svolgimento dell'attività lavorativa

Tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione dall'Ente per lo svolgimento dell'attività lavorativa, si devono impegnare, in particolare, a:

- a) Utilizzare la postazione di lavoro, fornita dall'Ente per lo svolgimento dell'attività lavorativa, in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi.
- b) Utilizzare l'accesso ad Internet, fornito dall'Ente per lo svolgimento dell'attività lavorativa, in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi. In particolare Internet può essere utilizzato per motivi personali in caso di urgenza e/o per il tempo strettamente necessario per assolvere incombenze amministrative e burocratiche quali adempimenti on line nei confronti di pubbliche amministrazioni ovvero per tenere rapporti con istituti bancari e assicurativi. L'utilizzazione per motivi personali non deve essere comunque effettuata in modo ripetuto o per periodi di tempo prolungati. Ciò significa, ad esempio che:
 - a. sono consultabili tutti i siti che siano visitati per motivi attinenti alla propria attività lavorativa. Ad esempio, se sto organizzando un convegno sull'agriturismo, posso consultare tutti i siti agrituristici che mi servono; non posso, al contrario, visitare ripetutamente gli stessi siti per organizzarmi una vacanza;
 - b. se mi sto collegando per motivi personali, è sicuramente ammessa un'utilizzazione dovuta a motivi di urgenza (quale può essere, ad es. una consultazione degli orari degli autobus o dei treni);
 - c. la consultazione della stampa per via telematica è di norma ammessa, anche perché l'articolo 9 del Codice di comportamento della Regione prevede, al comma 2, che "chiunque opera in nome e per conto della Regione si impegna a informarsi sulle politiche, sulle realizzazioni e sulle intenzioni dell'Ente relativamente al proprio settore". Il limite di "tolleranza" non sembra, da questo punto di vista, presentare differenze con la consultazione di giornali in formato cartaceo. E' evidente che, ad esempio, la connessione ripetuta quotidianamente a più giornali, compresi quelli sportivi o di moda, è di norma eccedente (come del resto un eccesso nella consultazione di quelli cartacei);
 - d. come specificato al paragrafo 1 dell'Allegato B del Disciplinare, "nella definizione di "attività lavorativa" devono essere ricomprese anche le attività che siano connesse e strumentali alla stessa, quali ad esempio i rapporti con le organizzazioni sindacali". Ciò significa, ad esempio, che si considera ricompresa nell'attività lavorativa la navigazione nel sito dell'ARAN o in siti che riportano normative o notizie inerenti il rapporto di pubblico impiego, compresi, come già specificato, i siti sindacali;
 - e. a corollario di quanto detto al punto precedente, è sempre ammessa la consultazione del sito Internos (rete aziendale interna);

¹ La definizione "Ente" ricomprende, come già specificato al Paragrafo 1 dell'Allegato B, sia la Giunta sia l'Assemblea Legislativa.

- f. per quanto riguarda la consultazione di Ermes Regione Emilia-Romagna (cioè il sito ufficiale della Regione), di norma è ammessa per “informarsi sulle politiche e sulle intenzioni dell’Ente relativamente al proprio settore”. Il collegamento alla Radio Emilia-Romagna, peraltro, deve essere limitato per le motivazioni riportate al punto seguente. Ovviamente anche tale “limitazione” è superata qualora il collegamento sia effettuato per specifiche ragioni lavorative;
- g. con specifico riferimento al collegamento a siti musicali, si chiarisce che, oltre all’evidente divieto di scaricare musica per interesse personale, non bisogna effettuare collegamenti finalizzati anche al solo ascolto di musica (pur continuando la propria attività lavorativa con il sottofondo musicale). Tali collegamenti infatti sono molto “pesanti” per la rete, in quanto i siti musicali sono siti cd. dinamici e occupano un’ampia banda della rete e, qualora fossero effettuati da più persone contemporaneamente, potrebbero creare problemi alla rete stessa. La musica è possibile ascoltarla ad esempio da un proprio lettore MP3 oppure utilizzando un proprio CD musicale (quest’ultima modalità è ammessa in ragione, in particolare, del fatto che non comporta né costi aggiuntivi né problemi di sicurezza relativamente alle strumentazioni dell’amministrazione);
- h. per quanto riguarda la possibilità di collegarsi a siti in lingua straniera, in particolare per mantenere aggiornata la conoscenza della lingua medesima, si specifica che mantenere aggiornate conoscenze/competenze relative a materie oggetto di specifica formazione effettuata dall’Ente è attività di norma considerata strettamente connessa alla propria attività lavorativa. Peraltro, per quanto riguarda in particolare la conoscenza di altre lingue (comunque necessaria o quanto meno utile in un contesto lavorativo sempre più allargato ad altri paesi, con particolare riferimento a quelli europei), il mantenimento/aggiornamento di questa conoscenza è sicuramente legittimo se effettuato per attività lavorativa (ad esempio consultazione di siti quali quello dell’Unione Europea, per aggiornamenti su tematiche riconducibili al proprio lavoro). Si considera ricompreso in un aggiornamento utile all’attività lavorativa ad esempio anche il collegamento al sito della BBC, qualora lo stesso sia effettuato in modo saltuario e non quotidianamente e/o continuativamente. Tutto ciò, evidentemente, sempre che tale collegamento non sia effettuato per altri motivi, strettamente collegati all’attività lavorativa, nel qual caso non c’è alcun limite (ad esempio nel caso in cui si cerchi nel sito una notizia inerente al proprio settore di attività);
- i. per quanto riguarda la consultazione di altri siti, questa è ammessa solo se episodica, saltuaria e non rilevante in termini di tempi di connessione (in questo caso infatti potrebbe tra l’altro essere giustificata da motivi d’urgenza oppure essere un mero errore di digitazione). Tutto ciò, ovviamente, sempre partendo dal presupposto che l’utilizzo non sia dovuto a motivi di lavoro per il quale non c’è limite;
- j. non si può, invece, neppure in via episodica e saltuaria, scaricare, per motivi personali, software, filmati, files musicali o simili; bisogna evitare di scaricare programmi anche gratuiti, se ciò non è indispensabile allo svolgimento dell’attività lavorativa e anche in quest’ultimo caso occorre segnalarlo sempre preventivamente al proprio referente informatico o all’assistenza utenti del Servizio competente in materia di sistemi informatici;
- k. è infine evidente che, come specificato anche all’articolo 8 del Codice di comportamento della Regione, è vietato il collegamento a “siti di per sé censurabili” (sempre che il collegamento non sia effettuato per specifici motivi lavorativi). Ci si riferisce, oltre evidentemente ai siti pornografici, a siti, ad esempio, a contenuto discriminatorio-razzista, di tecniche criminali, di gioco d’azzardo o simili. Il collegamento ad alcuni di tali siti, qualora gli stessi non siano già bloccati dai filtri di

sistema, può concretare ipotesi di reato ulteriori e diverse rispetto al cd. “peculato d’uso”. Anche in questo caso collegamenti del tutto isolati possono essere dovuti a meri errori di digitazione.

- c) Proteggere i computer e le altre strumentazioni informatiche, in caso di assenza, anche temporanea, dalla postazione di lavoro, tramite la sospensione o il blocco della sessione di lavoro (es. CTRL-ALT-CANC).
- d) Adottare le necessarie cautele per mantenere segrete le proprie password. Le password sono infatti strettamente personali, non devono in nessun caso essere comunicate ad altri (per es. non scrivere la password su post it affissi al monitor o sotto la tastiera, non dare la password a colleghi prima di assenze o periodi di ferie, ecc.): ogni utente è responsabile della sicurezza della propria password.
- e) Adottare, nello svolgimento della propria attività lavorativa, le necessarie cautele per assicurare la confidenzialità di dati personali e di dati che possono fornire indicazioni utili ad un eventuale attaccante dei sistemi informativi dell'Ente (per es. dati relativi ad incidenti di sicurezza pregressi, alla topologia di rete, alla configurazione dei software, all'ubicazione dell'hardware, al personale preposto alla gestione ed alla sicurezza dei sistemi).
- f) Utilizzare, in caso di trattamento di dati personali, le cartelle di rete o altri supporti di memorizzazione messi a disposizione dall'Ente al fine di garantire la disponibilità dei dati anche a seguito di errori o eventi accidentali. Le policy di backup centralizzato dell'Ente prevedono infatti l'esecuzione periodica di copie di sicurezza dei dati salvati su tali unità di rete sui sistemi di backup centrale. Le cartelle di rete, per cui si dispone delle necessarie autorizzazioni, sono accessibili tramite l'icona "Risorse del Computer" posta sul desktop.
- g) Utilizzare per le copie di sicurezza dei dati di uso quotidiano trattati in locale (per es. disco C:) la cartella di rete personale identificata come unità di rete U: (visibile nelle "Risorse del computer" come cartella denominata cognome_n\$). Anche per tale cartella valgono infatti le regole di backup centralizzato dell'Ente.
- h) Prevedere opportune misure che consentano, in caso di assenza dal luogo di lavoro, ad altri utenti autorizzati l'accesso a dati potenzialmente necessari (per es. salvare i dati presenti sul proprio disco rigido in cartelle condivise su file server, utilizzare cartelle di Outlook condivise, utilizzare la funzione di delega di Outlook, ecc.).
- i) Non connettere ad Internet, tramite modem o altri apparati di accesso remoto non espressamente autorizzati, macchine collegate alla rete interna dell'Ente.
- j) Non connettere alla rete interna dell'Ente strumenti elettronici personali o comunque non espressamente autorizzati.
- k) Non utilizzare strumenti peer-to-peer, di sniffing ,di cracking o di scanning (per es. Skype, Emule, LimeWare, Kazaa, Ares, BitTorrent, BitTornado, eDonkey, Winmx, Napster, Morpheus, Filetopia, SoulSeek, Shareaza, Azureus, ecc.).
- l) Non introdurre o diffondere programmi illeciti (per es. virus, worm, spyware,...) nella rete o nei sistemi.
- m) Non modificare le configurazioni standard del browser web o di altri software forniti dall'Ente.
- n) Utilizzare la posta elettronica, messa a disposizione dell'ente per lo svolgimento dell'attività lavorativa, esclusivamente per le specifiche finalità della stessa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi.
- o) Non utilizzare web mail esterne, in quanto le stesse comportano rischi per la sicurezza dei sistemi.

- p) Aver cura di non aprire allegati di posta in e-mail dal mittente e/o dall'oggetto sospetti per prevenire i rischi causati da software nocivi (per es. virus, worm, spyware, ecc.). Cancellare immediatamente tali messaggi e, in caso di dubbio, contattare l'indirizzo di posta dedicato alle problematiche di sicurezza (i riferimenti sono disponibili sul sito di supporto Computer Amico).
- q) Limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail istituzionale su siti web pubblici (per es. forum, mailing list, ecc.).
- r) Verificare, in caso di messaggi di dubbia provenienza (per es. phishing), che il mittente sia effettivamente quello dichiarato (per es. tramite meccanismi di firma digitale, tramite telefonata di verifica, ecc.). In caso di dubbio, contattare l'indirizzo di posta dedicato alle problematiche di sicurezza (i riferimenti sono disponibili sul sito di supporto Computer Amico).
- s) Non rimuovere il programma antivirus installato sulla postazione di lavoro.
- t) Verificare la presenza di eventuali virus prima di utilizzare supporti rimovibili.
- u) Nel caso in cui il software antivirus rilevi la presenza di un virus sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'evento alla struttura di Help Desk. Non inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti.
- v) Utilizzare sulle postazioni di lavoro esclusivamente il software autorizzato e fornito dall'Ente. Richiedere eventuale software aggiuntivo, rispetto all'installazione standard, al proprio referente informatico, al proprio responsabile funzionale o alla struttura di Help Desk.
- w) Non lasciare incustoditi i dispositivi mobili. Per esempio: custodire adeguatamente i dispositivi durante le ore notturne o in periodi di assenza (per es. non lasciare i dispositivi sulla scrivania ma custodirli in armadi o cassette chiuse a chiave); trasportarli come bagaglio a mano durante i viaggi in aereo; non lasciarli incustoditi, neanche temporaneamente, durante i viaggi effettuati in treno; non lasciarli in auto, se non in casi eccezionali, e comunque chiuderli nel bagagliaio non a vista in modo da non evidenziarne la presenza dall'esterno; non lasciarli in vista nelle stanze degli hotel, ma chiuderli in un armadio o in una valigia o depositarli in cassaforte se si prevede un'assenza prolungata.
- x) In caso di telelavoro utilizzare la postazione fornita esclusivamente per motivi inerenti l'attività lavorativa e senza manomettere in alcun modo gli apparati e la configurazione della postazione stessa. Se si utilizzano dispositivi mobili per il telelavoro, collegare gli stessi alla LAN dell'Ente almeno una volta ogni 30 giorni per l'aggiornamento automatico delle patch di sicurezza.
- y) In caso di incidente di sicurezza attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi. Tali indicazioni sono fornite agli utenti attraverso gli strumenti di comunicazione interna dell'Ente quali il sito Internos, il sito del supporto tecnico e la posta elettronica interna;
- z) Utilizzare gli strumenti di telefonia (sia fissa sia mobile) per lo svolgimento dell'attività lavorativa ed in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi. In particolare anche nell'utilizzo di tali strumenti deve essere rispettata la regola di cui alla lettera b).

Appendice all'Allegato C: Glossario

Backup: operazione di duplicazione su differenti supporti di memoria delle informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita.

Browser web: programma che consente all'utente di guardare, interagire e, in generale, scorrere o sfogliare file in Internet (per es. Internet Explorer, Mozilla Firefox, Opera, ecc.).

Cracking (strumenti di): software che consentono l'aggiramento illecito delle misure di sicurezza di un sistema informatico.

File Server: macchina progettata per mettere a disposizione degli utenti di una rete di computer dello spazio su disco nel quale sia possibile salvare, leggere, modificare, creare file e cartelle condivise da tutti, secondo regole o autorizzazioni che generalmente il gestore di rete organizza e gestisce.

LAN: acronimo per il termine inglese Local Area Network, in italiano rete locale. Identifica una rete costituita da computer collegati tra loro (comprese le interconnessioni e le periferiche condivise) all'interno di un ambito fisico delimitato (ad esempio in una stanza o in un edificio, o anche in più edifici vicini tra di loro) che non superi la distanza di qualche chilometro.

Modem: dispositivo elettronico che rende possibile la comunicazione di più sistemi informatici (ad esempio dei computer) utilizzando un canale di comunicazione composto tipicamente da un doppino telefonico.

Patch: aggiornamento di un software per la correzione di un problema di sicurezza o di funzionalità.

Peer-to-peer (strumenti): software che permettono l'utilizzo di una postazione di lavoro in modalità server per consentire lo scambio di file con altri utenti, anche esterni alla rete dell'Ente.

Phishing: tecnica finalizzata all'acquisizione, per scopi illegali, di dati riservati (codici di accesso, password, numeri carte di credito e altre informazioni personali) tramite l'invio di e-mail dal contenuto e dal mittente opportunamente falsificati (per es. simulando la provenienza del messaggio da parte di una banca o di uno studio legale).

Scanning: attività di raccolta di informazioni su un sistema propedeutica alla fase di attacco informatico vero e proprio.

Sniffing (strumenti di): software che consentono di intercettare ed analizzare il traffico in transito su una rete informatica.

Spyware: software che raccoglie informazioni riguardanti un utente senza il suo consenso, trasmettendole tramite Internet ad

un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata.

Webmail: applicazione che permette di gestire un account di posta elettronica attraverso un browser web. Generalmente viene fornita come servizio ad abbonati di un provider di connessione internet (es. Tin, Libero, Fiscali) oppure come servizio gratuito di posta elettronica (es. Yahoo, Google, Virgilio).

Worm: programma in grado di autodiffondersi sulla rete e verso altri sistemi.

Virus: programma in grado di autoreplicarsi in un sistema, per esempio copiando una parte di se stesso all'interno del codice di un altro programma.

REGIONE EMILIA-ROMAGNA

Atti amministrativi

GIUNTA REGIONALE

Grazia Cesari, Responsabile del SERVIZIO SISTEMA INFORMATIVO - INFORMATICO REGIONALE esprime, ai sensi della deliberazione della Giunta Regionale n. 2416/2008, parere di regolarità amministrativa in merito all'atto con numero di proposta DPG/2009/7513

data 20/07/2009

IN FEDE

Grazia Cesari