IIS Curie-Sraffa

Via Fratelli Zoia 130 - 20153 Milano (MI)
Tel.: +39 02 4525866
Mail: MIIS09300E@istruzione.it
PEC: MIIS09300E@pec.istruzione.it

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

IIS Curie-Sraffa

Regolamento per la gestione dei Sistemi Informativi dell'IIS Curie-Sraffa

Titolo documento:	**Regolamento per la gestione dei Sistemi Informativi dell'IIS Curie-Sraffa**
Codice documento:	IIS_Curie-Sraffa – Regolamento Gestione SI – Ver 1-0
Nome file:	IIS_Curie-Sraffa – Regolamento Gestione SI – Ver 1-0
Stato documento:	bozza per revisione e condivisione
Versione:	1.0
Data ultimo aggiornamento	10 aprile 2021

IIS Curie-Sraffa

Via Fratelli Zoia 130 - 20153 Milano (MI)
Tel.: +39 02 4525866
Mail: MIIS09300E@istruzione.it
PEC: MIIS09300E@pec.istruzione.it

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Indice

Art. 1 - Definizioni 3
Art. 2 – Applicabilità del presente Regolamento 6
Art. 3 – Ruolo del Responsabile dei Sistemi Informativi dell'IIS Curie-Sraffa 6
Art. 4 – Pianificazione delle operazioni di amministrazione e gestione di sistema 7
Art. 5 – Autorizzazione preventiva delle operazioni di amministrazione e gestione di sistema 8
Art. 6 – Installazione di componenti software o hardware 8
Art. 7 – Redazione e aggiornamento mappa dei sistemi 11
Art. 8 – Annotazione delle operazioni di amministrazione e gestione di sistema 12
Art. 9 – Documentazione scritta degli interventi effettuati 12
Art. 10 – Documentazione scritta delle configurazioni di sistemi ed apparati 13
Art. 11 – Verifica dell'operato degli Amministratori di Sistema e degli Operatori di Sistema 13
Art. 12 – Modifica delle password di administrator 13
Art. 13 – Salvataggio (backup) dei dati 14
Art. 14 – Minimo accesso ai dati e alle informazioni 14
Art. 15 – Divieto esplicito di accesso alla posta elettronica 15
Art. 16 – Divieto esplicito di accesso ai computer client 15
Art. 17 – Divieto di monitorare gli accessi ad internet 16
Art. 18 – Divieto di intercettare le comunicazioni informatiche o telematiche 16
Art. 19 – Dichiarazione di conformità ai sensi dell'art. 25 del Disciplinare Tecnico 16
Art. 20 – Comunicazione nominativi amministratori ed operatori di sistema esterni 17
Art. 21 – Conformità ai requisiti del Provvedimento del Garante per la protezione dei dati personali del 27-11-2008 relativo agli amministratori di sistema 17
Art. 22 – Conformità ai requisiti del Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003) ..... **Errore. Il segnalibro non è definito.**
Art. 23 – Divieto di alterazione o cancellazione dei file di log 17
Art. 24 – Estrazione periodica dei file di log 18
Art. 25 – Analisi dei files di log 18
Art. 26 – Disposizioni finali 18
Art. 27 – Soggetti responsabili della vigilanza sulla corretta applicazione del presente regolamento 19

Art. 1 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del Reg. UE 2016/679 – GDPR (per brevità nel seguito detto anche semplicemente "*Regolamento"* o "*GDPR*").

Ai sensi dell'art. 4 del Regolamento si intende per:

1) «dati personali»: qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti

riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «autorità competente»:

a)qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o

b)qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;

8) «titolare del trattamento»: l'autorità competente che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o dello Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione o dello Stato membro;

9) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

10) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o dello Stato membro non sono considerate destinatari; il trattamento di tali dati da parte di tali autorità pubbliche è conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento;

11) «violazione dei dati personali»: la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

12) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

13) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

14) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

15) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 41;

16) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Art. 2 – Applicabilità del presente Regolamento

Il presente regolamento si applica a tutti i sistemi informatici, telematici e di sicurezza dell'IIS Curie-Sraffa, in qualsiasi sede siano essi collocati.

In particolare, rientrano nell'ambito di applicazione del presente Regolamento i seguenti sistemi:

- sistemi software installati in locale
- sistemi software in cloud
- server e NAS
- stampanti in rete dotate di indirizzo ip
- PC, PC portatili, tablet
- apparati per la connettività ad internet tramite rete fissa, come ad esempio router, switch, switch level 3 etc.
- apparati per la connettività ad internet tramite rete senza fili, come ad esempio access point wi-fi
- apparati per la rilevazione delle presenze
- apparati di sicurezza come ad esempio firewall, siano essi di tipo "appliance" oppure mediante l'installazione di software open source su PC o server.

Art. 3 – Ruolo del Comitato per la gestione dei Sistemi Informativi dell'IIS Curie-Sraffa

La responsabilità della gestione, del presidio e della governance dei sistemi Informativi dell'IIS Curie-Sraffa è affidata al **Comitato per la gestione dei Sistemi**

Informativi dell'IIS Curie-Sraffa (per brevità nel seguito chiamato anche "Comitato").

Al Comitato è affidata la responsabilità di vigilare sul rispetto dei contratti di affidamento a soggetti esterni all'IIS Curie-Sraffa.

Relativamente agli aspetti afferenti la sicurezza e la privacy dei dati, al Comitato è affidata inoltre la responsabilità di vigilare sulla puntuale osservanza degli atti di nomina a Responsabile esterno del trattamento dei dati, relativamente ai trattamenti di dati personali e sensibili affidati a soggetti esterni all'IIS Curie-Sraffa (es. Argo Software).

Al Dirigente Scolastico dell'IIS Curie-Sraffa è data facoltà di designare uno o più Amministratori di Sistema e uno o più Operatori di Sistema.

Art. 4 – Pianificazione delle operazioni di amministrazione e gestione di sistema

Tutte le operazioni di amministrazione e gestione di sistema devono essere, nei limiti del possibile, pianificate in anticipo, dopo averne valutato l'effettiva necessità, correttezza, sicurezza, convenienza, efficacia ed economicità, nonché fattibilità tecnica e/o normativa.

A tale scopo il Comitato predispone, il PDS – Piano dei Sistemi, contenente la pianificazione di tutte le attività e di tutti gli interventi da effettuare sui sistemi informativi, informatici, telematici e di sicurezza.

La pianificazione contenuta nel PDS – Piano Dei Sistemi – deve essere di norma rivista con frequenza semestrale.

Art. 5 – Autorizzazione preventiva delle operazioni di amministrazione e gestione di sistema

Tutte le operazioni di amministrazione di sistema diverse dalle operazioni routinarie di salvataggio dei dati, siano esse pianificate o meno, devono essere autorizzate dal DS o dal Comitato.

Art. 6 – Installazione di componenti software o hardware

L'installazione di componenti hardware o software è un'operazione critica che può compromettere la stabilità, le performance e la sicurezza dei sistemi informatici o telematici, pertanto deve essere attentamente valutata e pianificata.

E' fatto tassativo divieto di installare componenti hardware o software senza l'autorizzazione scritta, richiesta e concessa anche tramite mail, del DS o del Comitato.

Tutte le installazioni di componenti software o hardware dovranno essere autorizzate per iscritto dal DS o dal Comitato.

Art. 7 – Scansione delle rete della segreteria

Deve essere effettuata con frequenza almeno bimestrale (ogni due mesi) una scansione completa delle rete della segreteria, con strumenti gratuiti come ad esempio "advanced ip scanner" o equivalenti, al fine di rilevare e censire tutti gli apparati presenti in rete, rilevando come minimo l'indirizzo ip ed il mac-address dei vari apparati rilevati.

L'obiettivo della scansione è quello di effettuare un censimento degli apparati presenti, ma soprattutto di individuare nuovi apparati che siano stati collegati senza autorizzazione o dei quali non sia ben chiaro l'obiettivo o la finalità.

Alla fine della scansione, il report relativo alla scansione stessa deve essere salvato in formato .csv e conservato in sicurezza per un periodo di almeno 24 mesi.

Art. 8 – Scansione delle reti della didattica

Deve essere effettuata con frequenza almeno quadrimestrale (ogni quattro mesi) una scansione completa delle varie reti utilizzate per finalità didattiche, con strumenti gratuiti come ad esempio "advanced ip scanner" o equivalenti, al fine di rilevare e censire tutti gli apparati presenti in rete, rilevando come minimo l'indirizzo ip ed il mac-address dei vari apparati rilevati.

L'obiettivo della scansione è quello di effettuare un censimento degli apparati presenti, ma soprattutto di individuare nuovi apparati che siano stati collegati senza autorizzazione o dei quali non sia ben chiaro l'obiettivo o la finalità.

Alla fine della scansione, il report relativo alla scansione stessa deve essere salvato in formato .csv e conservato in sicurezza per un periodo di almeno 24 mesi.

Art. 9 – Scansioni di vulnerabilità interne

Deve essere effettuata con frequenza almeno bimestrale (ogni due mesi) una scansione di vulnerabilità interna finalizzata ad individuare vulnerabilità e

configurazioni poco sicure ed eventuali mancanze di aggiornamenti, sui vari PC e sui server. Tali scansioni di vulnerabilità possono venire effettuate con strumenti gratuiti ufficiali forniti da Microsoft, come ad esempio MBSA – Microsoft Baseline Security Analyzer. Alla fine della scansione il report deve essere salvato e conservato in sicurezza per un periodo di almeno 24 mesi.

Art. 10 – Scansioni di vulnerabilità esterne

Deve essere effettuata con frequenza almeno bimestrale (ogni due mesi) una scansione di vulnerabilità esterna si tutti gli oggetti dotati di indirizzo ip pubblico finalizzata ad individuare vulnerabilità e configurazioni poco sicure ed eventuali mancanze di aggiornamenti. Tali scansioni di vulnerabilità devono essere eseguite da soggetti esperti, con strumenti professionali ceo offrano adeguate garanzie di accuratezza ed efficacia.

Alla fine della scansione il report deve essere salvato e conservato in sicurezza per un periodo di almeno 24 mesi.

Art. 11 – Inventario degli indirizzi ip pubblici

Deve essere mantenuto e regolarmente aggiornato un inventario degli indirizzi ip pubblici di proprietà o titolarità o comunque utilizzati dall'Istituto, come ad esempio il sito web, il registro elettronico, l'interfaccia pubblica del router di accesso ad internet, l'interfaccia pubblica dei vari firewall (se presente), eventuali attestazioni per VPN etc.

Tale inventario verrà utilizzato anche come baseline per l'effettuazione delle scansioni di vulnerabilità di cui all'articolo precedente.

Art. 12 – Redazione e aggiornamento mappa dei sistemi

Deve essere predisposta e regolarmente aggiornata con cadenza almeno semestrale una mappa dei sistemi informatici, di sicurezza e telematici di dell'Istituto, che rifletta fedelmente la situazione attuale. Tale mappa, che deve comprendere un inventario esaustivo delle risorse hardware e software, deve essere articolata sulle varie sedi dell'Istituto.

Art. 13 – Elenco dei software approvati dal Dirigente Scolastico

Si dovrà predisporre ed aggiornare con frequenza almeno annuale l'elenco dei software approvati dal Dirigente Scolastico, declinato per ciascuna tipologia di utenti. Il suddetto elenco dovrà comprendere sia I software installati in locale sia le eventuali piattaforme in cloud che possono essere utilizzate.

Art. 14 – Ricognizione dei software installati

Con frequenza almeno semestrale si dovrà effettuare una rilevazione/censimento dei software installati sui vari PC e sui vari server, possibilmente con strumenti automatici. Una volta effettuata la ricognizione, questa dovrà essere confrontata con l'elenco dei software approvati di cui all'articolo precedente, e si dovrà procedere alla disinstallazione/rimozione dei software no autorizzati.

Art. 15 – Annotazione delle operazioni di amministrazione e gestione di sistema

Tutte le operazioni di amministrazione di sistema, comprese le operazioni di salvataggio dei dati, devono essere sinteticamente annotate su apposito registro elettronico e/o cartaceo.

Nel caso venga adottato un registro elettronico, con frequenza almeno mensile deve essere creata e storicizzata una differente versione del suddetto registro elettronico, che dovrà essere prodotta in un formato non modificabile (es. pdf o tiff). Il suddetto registro dovrà essere in ogni caso sottoposto all'attenzione e formato per presa visione da parte del DS o del Comitato.

Art. 16 – Documentazione scritta degli interventi effettuati

Tutte le operazioni di amministrazione di sistema di una certa rilevanza (es. installazione di nuovo hardware, installazione di nuovo software, installazione di una major release software, attivazione di collegamenti telematici come ad esempio VPN-Rete Privata Virtuale, diverse dalle quotidiane operazioni di salvataggio dei dati, dovranno essere accuratamente documentate per iscritto.

Con frequenza almeno mensile dovrà essere documentata per iscritto l'effettiva leggibilità e completa ripristinabilità dei dati salvati mediante operazioni di backup, come spiegato più avanti.

Art. 17 – Documentazione scritta delle configurazioni di sistemi ed apparati

La configurazione di sistemi ed apparati (ad eccezione dei PC degli utenti finali) deve essere documentata per iscritto e mantenuta regolarmente aggiornata in caso di modifiche o integrazioni. La documentazione deve essere aggiornata e riflettere in qualsiasi momento la stato effettivo dei sistemi e degli apparti.

Laddove tecnicamente possibile, la configurazione dei sistemi e degli apparati deve essere salvata in formato elettronico in modo tale che in caso di necessità possa essere automaticamente ripristinata.

Art. 18 – Verifica dell'operato degli Amministratori di Sistema e degli Operatori di Sistema

L'operato degli amministratori e degli operatori di sistema potrà essere oggetto di controlli e verifiche sistematiche, effettuate ai sensi dell'art. 4.4 del Provvedimento del Garante per la protezione dei dati personali del 27-11-2008.

Art. 19 – Modifica delle password di administrator

Gli unici soggetti autorizzati e titolati a modificare le password di sistema sono i vari Amministratori di Sistema, a tale scopo designati dal DS.

E' fatto tassativo divieto agli operatori di sistema di modificare le password di sistema, se non in concomitanza della scadenza delle password o in caso di emergenza o necessità

In caso di necessità (ad esempio nel caso una password abbia perso la segretezza) gli operatori di sistema dovranno darne comunicazione al DS.

Art. 20 – Salvataggio (backup) dei dati

I dati devono essere salvati con frequenza giornaliera. Come minimo devono essere salvati i dati relativi ai seguenti sistemi:

- **Server locali**
- **Sistemi utilizzati mediante piattaforme in cloud.**

Con frequenza almeno trimestrale dovrà essere verificata ed annotata su apposito registro la ripristinabilità e l'effettiva leggibilità dei dati salvatati, e eventuali errori/anomalie/eccezioni dovranno essere documentati come "incident" seguendo l'apposita procedura di "incident reporting".

I backup giornalieri potranno essere eseguiti con tecnica incrementale, mentre con frequenza settimanale dovrà essere effettuato un full backup.

Tutti i backup locali dovranno essere replicati su backup server secondario, collocato in un luogo diverso dalla sala server ove è collocato il backup server primario.

Art. 21 – Minimo accesso ai dati e alle informazioni

Le attività di amministrazione e gestione di sistema dovranno essere svolte senza che vi sia accesso e conoscenza, ai dati e alle informazioni contenute nei documenti e nelle banche dati in formato elettronico e cartaceo; solo nel caso

risultasse **indispensabile** accedere ai dati e/o alle informazioni, l'accesso dovrà avvenire esclusivamente per accertate e documentate esigenze di operatività e gestione di sistema, e solo nei casi in cui le medesime finalità non possano venire perseguite senza che via sia accesso o conoscenza dei dati e/o informazioni, e comunque in ottemperanza al principio di liceità, non eccedenza e proporzionalità, fatte salve le responsabilità civili e penali qualora l'illecito sia compiuto con abuso o sfruttando il ruolo di amministratore di sistema.

Art. 22 – Divieto esplicito di accesso alla posta elettronica

E' fatto tassativo divieto a chiunque – compresi gli Amministratori di sistema e gli operatori di sistema - di accedere al contenuto dei messaggi di posta elettronica; l'accesso al contenuto potrà avvenire solo qualora si riveli essere indispensabile, e a fronte di autorizzazione scritta da parte del DS o del Comitato. Più in generale l'utilizzo di Internet, della posta elettronica dovrà avvenire conformemente a quanto stabilito con apposito Regolamento approvato dal DS e dal Comitato.

Art. 23 – Divieto esplicito di accesso ai computer client

E' fatto tassativo divieto di accedere, in locale o da remoto, alle postazioni client degli utenti, senza che gli utenti stessi siano stati previamente avvertiti e abbiamo dato il loro permesso esplicito. Gli accessi che si rendano indispensabili per operazioni di amministrazione e gestione di sistema dovranno avvenire se possibile alla presenza dell'interessato.

In caso di estrema necessità ed urgenza, nel caso il dipendente interessato, si potrà accedere alla postazione client solo alla presenza del "fiduciario" designato dal dipendente. Il dipendente dovrà essere avvertito alla prima occasione possibile dell'accesso effettuato e delle operazioni svolte, delle quali dovrà essere redatto verbale scritto da consegnare al DS e al diretto interessato.

Art. 24 – Divieto di monitorare gli accessi ad internet

Salvo quanto specificato di seguito, è fatto tassativo divieto di installare o utilizzare sistemi ed apparati che consentano di tenere traccia dei siti internet visitati dai dipendenti. Qualsiasi monitoraggio dei siti internet visitati dai dipendenti dovrà essere:

- normato da apposito regolamento
- avere finalità lecite ed esplicite
- comunicato in anticipo ai dipendenti
- avvenire in conformità ai principi di non eccedenza e proporzionalità.

Art. 25 – Divieto di intercettare le comunicazioni informatiche o telematiche

E' fatto tassativo divieto di intercettare, monitorare, interrompere o alterare qualsiasi tipo di comunicazione informatica o telematica, compresa la posta elettronica, le comunicazioni telefoniche, le comunicazioni tramite fax e il contenuto della memoria degli apparati di tipo fotocopiatore.

Art. 26 – Dichiarazione di conformità al GDPR

Tutte le operazioni di amministrazione e gestione di sistema effettuate da soggetti esterni dovranno essere accompagnate da dichiarazione scritta di conformità al GDPR.

Con frequenza annuale oppure in corrispondenza dell'installazione di major releases, dovrà essere verificata e dichiarata la conformità di apparati e programmi

applicativi e sistemi operativi ai requisiti previsti dal GDPR e al Provvedimento del Garante per la protezione dei dati personali del 27/11/2008.

Art. 27 – Comunicazione nominativi amministratori ed operatori di sistema esterni

Tutti i soggetti esterni designati in qualità di responsabili del trattamento ai sensi dell'art. 28 del GDPR, devono comunicare per iscritto all'Istituto l'elenco delle persone fisiche che svolgono operazioni di amministrazione e gestione di sistema.

Art. 28 – Conformità ai requisiti del Provvedimento del Garante per la protezione dei dati personali del 27-11-2008 relativo agli amministratori di sistema

Tutti i sistemi utilizzati devono essere conformi al Provvedimento del Garante per la protezione dei dati personali del 27-11-2008, e la conformità deve essere dichiarata e verificata per iscritto con frequenza almeno annuale.

Art. 29 – Divieto di alterazione o cancellazione dei file di log

E' fatto tassativo divieto di alterare in qualsiasi modo o di cancellare qualsiasi file di log, sia esso di sistema o applicativo. Il periodo di sovrascrittura dei files di log dovrà essere compatibile (superiore o uguale) alla periodicità con la quale i files di log sono estratti e storicizzati.

Art. 30 – Estrazione periodica dei file di log

Deve essere effettuata con frequenza almeno semestrale una copia dei file di log dei vari server e dei programmi applicativi su cd-rom non modificabile, previa apposizione di firma digitale. Entro sei mesi dall'entrata in vigore del presente regolamento saranno comunque valutate tecniche e strumenti (anche di tipo open-source, quindi gratuiti) per l'automatizzazione dell'estrazione dei files di log e la loro storicizzazione in sicurezza, con eventuale implementazione di un log-server centralizzato in locale oppure in cloud.

Art. 31 – Analisi dei files di log

I files di log di cui ai punti precedenti potranno essere oggetto di verifica nel rispetto della normativa vigente (Provvedimento del Garante per la protezione dei dati personali del 27-11-2008 e successive mm. ii.). La verifica dovrà essere effettuata ai sensi del Provvedimento del Garante per le protezione dei dati personali del 27-11-2008, definitivamente entrato in vigore il 15-12-2009. La verifica dovrà essere documentata mediante verbale e relazione scritta, da consegnare al DS e al Comitato.

Art. 32 – Disposizioni finali

Al fine di dare concreta attuazione alle disposizioni contenute nel presente regolamento, copia dello stesso dovrà essere consegnata ai vari amministratori di sistema ed ai docenti ed assistenti tecnici che sono in qualche modo coinvolti nelle attività di amminist5razione e gestione di sistema.

Art. 33 – Soggetti responsabili della vigilanza sulla corretta applicazione del presente regolamento

Il compito di vigilare sull'ottemperanza e sulla corretta ed efficace applicazione del presente regolamento è affidata al Responsabile della protezione dei dati designato ai sensi dell'art. 37 del GDPR ed ai membri del Comitato, I quali potranno effettuare verifiche e controlli periodici o a campione.