I.S.I.S "VITTORIO VENETO"- NAPOLI
Servizi Commerciali e per l'Enogastronomia e l'Ospitalità Alberghiera - Tecnico per il Turismo
Distretto Scolastico 44 - Codice meccanografico NAIS098007 – Codice Fiscale 95170390637

NAIS098007@ISTRUZIONE.IT

Procedura Nr P 12

La gestione del Sistema Informatico di Segreteria

Distribuzione: Tutto il personale, DSGA, AA;

Pubblicazione: l'ultima revisione del presente documento protocollato e in formato pdf è disponibile per i **destinatari** nei seguenti archivi:

1. Archivio del protocollo ufficiale;
2. Sito web sezione privacy.

Tabella degli Indici delle revisioni

Prot. n°	Modifiche rispetto alla revisione precedente	Data
xxxxxx	Prima emissione	Gg/mm/aaaa

Nota: in caso di revisione della procedura le modifiche attuate saranno evidenziate in giallo nel corpo del documento.

INDICE:

1. SCOPO

Stabilire le linee guida per una corretta gestione e protezione del **Sistema Informatico di Segreteria** utilizzato per il trattamento dei dati con strumenti elettronici della **Istituzione Scolastica**.

2. VALIDITÀ

Il presente documento ha validità all'interno della presente **Istituzione Scolastica**.

3. RIFERIMENTI NORMATIVI

CODICE	OGGETTO
REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Consiglio, del 27 aprile 2016	Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
D. Lgs. n. 101/2018	Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.
D. Lgs 196/2003	Codice in materia di protezione dei dati personali" (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174) (così come modificato dal **D. Lgs. n. 101/2018**)
Ministero dello Sviluppo Economico Decreto 22 gennaio 2008, n. 37	Regolamento concernente l'attuazione dell'articolo 11-quaterdecies, comma 13, lettera a) della legge n. 248 del 2 dicembre 2005, recante riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici. (GU Serie Generale n. 61 del 12-03-2008)
Provvedimento del Garante del 1/03/2007	Lavoro: le linee guida del Garante per posta elettronica e internet *Gazzetta Ufficiale n. 58 del 10 marzo 2007*
Provvedimento del Garante del 13/10/2008	Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008 *G.U. n. 287 del 9 dicembre 2008*
Provvedimento del Garante del 27/11/2008	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 *(G.U. n. 300 del 24 dicembre 2008)* *(così modificato in base al provvedimento del **25 giugno 2009**)*
Circolare AGID n° 2/2017 del 18 aprile 2017	Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». *(Gazzetta Ufficiale serie generale n° 103 del 5/05/2017)*
Computer Security Incident Response Team (CSIRT) Ministero dell'Istruzione – Comunicazione del 13/05/2021	Raccomandazioni e indicazioni per la sicurezza
Vademecum del Garante della Protezione dei Dati Personali Ottobre 2021	Suggerimenti per creare e gestire password a prova di privacy

4. DEFINIZIONI

Per tutte le definizioni dei termini inerenti la privacy usati in tale documento si fa riferimento all'**art. 4** del **Regolamento UE 2016/679 "Regolamento Generale per la protezione dei dati"** (**GDPR**). Laddove ritenuto necessario, nel corpo del documento saranno date le informazioni relative a termini e/o acronimi usati nel testo.

Per le altre principali definizioni dell'argomento in oggetto si rimanda alla sottostante tabella.

Termine/Acronimo	Definizione
Sistema di Gestione per la Privacy (SGP)	L'insieme delle modalità, delle strutture tecniche e organizzative, del personale e di quant'altro necessario per stabilire le politiche e gli obiettivi e per guidare e tenere sotto controllo un'organizzazione con riferimento alla Privacy nel rispetto di quanto stabilito dal REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Consiglio, del 27 aprile 2016.
Pericolo	Causa o origine di un danno o di una perdita potenziali. (UNI 11230 – Gestione del rischio).
Danno	Qualunque conseguenza negativa derivante dal verificarsi dell'evento (UNI 11230 – Gestione del rischio).
Rischio	Insieme della possibilità di un evento e delle sue conseguenze sugli obiettivi (UNI 11230 – Gestione del rischio).
Sistema Informatico di Segreteria (SIS)	L'insieme delle strutture hardware e software utilizzate dall'**Istituzione Scolastica** per il trattamento dei dati con strumenti elettronici.
Server	Dispositivo hardware e/o software di notevole capacità preposto a fornire servizi ad altri dispositivi detti **client** collegati ad esso in rete.
Client	In una **rete informatica**, ogni computer collegato al **server** e in grado di scambiare dati con esso.
Sistema client-server	In **informatica** indica un'**architettura di rete** nella quale genericamente un **computer client** o **terminale** si connette ad un **server** per la fruizione di un certo servizio, quale, ad es., la condivisione di una certa risorsa **hardware/software** con altri **client**.
Local Area Network (LAN)	**Rete informatica** di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.
Linea Ethernet	Insieme delle tecnologie standardizzate basate fisicamente su connessioni tramite cavi (coassiali, doppini intrecciati in rame, fibra ottica) utilizzate per le **LAN**.
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.
Credenziali di autenticazione	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
Parola chiave (password)	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
Sistema di autorizzazione	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
Rack	**Rastrelliera**. In **informatica** e **telecomunicazioni** è un **sistema standard** d'**installazione fisica** di componenti **hardware** costituito da una **struttura modulare** larga **19 pollici** (482,6 mm), alta **1,75 pollici** (44,45 mm) per ogni unità ospitata e lunghezza variabile, solitamente maggiore di **600 mm**.

5. RESPONSABILITÀ

Titolare del trattamento dei dati	• Effettuare la valutazione dei rischi correlati al trattamento dei dati personale; • Definire piani di miglioramento e attuare le disposizioni previste per attenuare i rischi se essi risultano non accettabili.
RPD (Responsabile Protezione Dati)	• Verificare la corretta applicazione della presente procedura; • Valutare l'efficacia delle azioni implementate.
Incaricati	• Applicare le misure individuate nella presente procedura.

6. VALUTAZIONE DEL RISCHIO

6.1 ANALISI DEL RISCHIO

Per determinare i rischi occorre:

1. Individuare le possibili minacce che possono essere condotte contro un sistema;
2. Individuare i punti critici dello stesso.

Dall'incrocio di queste due dimensioni si possono prevedere i rischi e, quindi, determinare le strategie e gli accorgimenti per ridurli al massimo.

Gli attacchi possono determinare o una perdita di dati o un accesso ad essi non autorizzato.

6.2 NOZIONI GENERALI

I requisiti generici di sicurezza delle reti presentano le seguenti caratteristiche interdipendenti:

a. **Disponibilità:** i dati sono accessibili e i servizi sono ripristinabili anche in caso di interruzioni dovute alla cessazione dell'alimentazione elettrica, a catastrofi naturali, eventi imprevisti o ad attacchi di pirateria informatica;
b. **Autenticazione:** conferme dell'identità dichiarata da un utente;
c. **Integrità:** conferma che i dati trasmessi, ricevuti o conservati sono completi e inalterati;
d. **Riservatezza:** protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la lettura da parte di persone non autorizzate. La riservatezza è particolarmente necessaria per la trasmissione di dati sensibili ed è uno dei requisiti che garantiscono il rispetto della vita privata.

Gli attacchi possono essere portati da diverse tipologie di persone, con vari intendimenti, comunque malevoli, tutti profondamente esperti di informatica e genericamente indicati con il termine di **hacker**.

6.3 PRINCIPALI MINACCE

Le principali fonti di rischio, o minacce, sono:

1. **Intrusioni:** persone non autorizzate accedono nei locali in cui sono presenti banche dati o penetrano nei sistemi informatici e consultano o alterano o copiano dati o documenti.
   Contromisure: per i sistemi informatici sono i **firewall, i Proxy server, il sistema di account e password;** per i luoghi fisici sono **porte con serrature, registri d'ingresso e cartellini di riconoscimento.**
2. **Intercettazione delle comunicazioni:** le comunicazioni elettroniche possono essere intercettate e i dati in esse contenuti copiati o modificati. I punti più vulnerabili e sensibili ad una intercettazione del traffico sono i punti di gestione e di concentrazione della rete come i *router*, le *gateway* e i *server di rete.*
   Contromisure: per i sistemi informatici sono i **firewall, i Proxy server, il sistema di account e password;** per i luoghi fisici è il **trasporto dei dati sensibili in contenitori con serratura.**

3. **Virus:** sono piccoli programmi che si replicano automaticamente e che possono causare danni di vario tipo. Esempi: *virus del Kernel* (distruggono il cuore del sistema operativo), *virus eseguibile* (possono essere software maligni, detti malware ossia malicious software, che modificano o distruggono i dati), *virus delle macro* (in Word o Excel di Microsoft), *virus del Boot Sector* (si attivano quando si accende il computer e si duplicano sui supporti di memoria), *Bombe logiche* (rimangono inerti fino al momento in cui vengono innescati da un determinato evento), *worms* (non infettano gli altri programmi ma si auto duplicano in copie che, riproducendosi a loro volta, finiscono per saturare il sistema), *Trojans* (spiano il contenuto del computer e lo trasmettono all'esterno in maniera invisibile; spesso permettono un controllo remoto), *key sniffing* (registra ogni singolo tasto battuto, comprese le password e le trasmette via Internet).
   Contromisure: programmi antivirus, copie di back-up.
4. **Spy ware:** è un software che minaccia la privacy tracciando un profilo sulla base delle navigazioni in Internet.
   Contromisure: programmi di ricerca degli spy ware, programmi antivirus, firewall, Proxy server.
5. **Attacchi alle impostazioni delle password:** *Brute force* (un apposito programma prova tutte le possibili combinazioni di chiavi per decrittare il file protetto), *Attacco a dizionario* (prova lunghissimi elenchi di parole, nomi e sigle di uso comune in una data lingua), *Attacco all'algoritmo* (prevede la possibilità di intervenire su particolari debolezze matematiche o computazioni dell'algoritmo utilizzato), *Password sniffing* (ruba la password con qualche trucco, facendosela dire con una scusa, o fingendosi responsabili di un servizio assistenza clienti, o della sicurezza).
   Contromisure: per i sistemi informatici sono gli accessi con password elaborate come previsto nel presente documento; per i locali fisici sono le porte con serrature e chiavi custodite e gestite secondo la procedura prevista.
6. **Defacing:** la sostituzione della homepage del sito della scuola con immagini o scritte.
   Contromisure: sistema di accesso al server web con password e controllo quotidiano per pronta sostituzione.
7. **Violazione del diritto d'autore:** copie e/o installazioni di programmi informatici di cui la scuola non possiede regolare licenza; download, illegale e non autorizzato, dal web di file audio e/o video.
   Contromisure: sistema di autorizzazione con limitazioni per l'installazione di programmi software, informazioni agli utenti, controlli periodici.
8. **Crimini informatici:** i sistemi informatici della scuola potrebbero essere utilizzati per compiere crimini informatici con implicazioni di tipo civile e penale: spamming, tentativi d'intrusione, pubblicazione sul web di testi o immagini proibite, ecc.
   Contromisure: sistema di accesso con account e Proxy server, in modo tale da impedire alcuni comportamenti illegali ed, in ogni caso, risalire all'autore dell'azione non consentita.
9. **Danni all'hardware:** l'elemento più delicato è il disco fisso; se si dovesse danneggiare, a meno di ricorrere a pratiche costosissime sviluppate da centri specializzati, tutti i dati andrebbero persi. Per i luoghi fisici s'intende la rottura delle serrature o delle chiavi.
   Contromisure: per i sistemi informatici si ripristina con copie di back-up; per i luoghi fisici c'è la sostituzione immediata o chiusura con lucchetto della porta o dell'armadio, ovvero il trasporto in un'altra stanza blindata dei dati sensibili o in altro armadio blindato.
10. **Usurpazione di identità:** al momento di stabilire un collegamento alla rete o di ricevere dati, l'utente deduce l'identità del suo interlocutore in funzione del contesto in cui avviene la comunicazione, potrebbe scaricare software maligno da un sito web che si fa passare per fonte affidabile e si potrebbero anche rivelare informazioni riservate alla persona sbagliata.
    Contromisure: controllo sistematico dell'autenticità delle fonti.
11. **IP spoofing:** l'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo Spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.
    Contromisure: riservatezza di user-id e password costruite come di seguito indicate.
12. **Spamming:** saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella di posta elettronica e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.
    Contromisure: software specifico.

13. **Incidenti ambientali ed eventi imprevisti:** catastrofi naturali (tempeste, inondazioni, incidenti, terremoti); terzi estranei a qualsiasi rapporto contrattuale con l'operatore o l'utente (ad es. guasti all'hardware o del software dei componenti o dei programmi consegnati); errore umano dell'operatore (compreso il fornitore di servizio) o dell'utente (ad es. problemi di gestione della rete, installazione errata del software).
Contromisure: per i sistemi informatici copie di back-up per il ripristino; per i luoghi fisici ricorso ad altre stanze o armadi.
14. **Phishing:** truffa informatica effettuata inviando un'e-mail con il logo contraffatto di una azienda, istituto di credito, di una società di commercio elettronico o anche di una PA, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico. Ci sono diverse varianti di phishing (spear phishing, whale phishing, ecc.) ma tutte si basano su cosiddette tecniche di ingegneria sociale che tendono a sfruttare l'inesperienza del destinatario.
Contromisure: formazione; segretezza, complessità e diversificazione delle password; utilizzo delle tecniche di sicurezza generali (ad es., screen saver, back up, ecc.).

6.4 VALUTAZIONE DEI RISCHI

Si è effettuata una valutazione del rischio di tipo macro utilizzando i seguenti livelli qualitativi:

- **Lieve:** rischio molto basso corrispondente ad una minaccia remota e comunque rapidamente reversibile od ovviabile.
- **Media:** rischio superiore al precedente corrispondente ad una minaccia remota i cui effetti non sono facilmente o totalmente reversibili od ovviabili.
- **Grave:** rischio che occorre assolutamente prevenire con un insieme di contromisure (di natura fisica, logica, etc.) per abbatterlo o contenerlo a livelli accettabili.

Di seguito vengono riportate delle tabelle che riassumono l'**analisi dei rischi** effettuata per tutte le **risorse** presenti nell'**Istituzione Scolastica**.

TABELLA DI ANALISI DEI RISCHI RISORSE HARDWARE

Risorsa	Elemento di Rischio	Livello
Tutti i computer	Uso non autorizzato dell'hardware	grave
Tutti i computer	Manomissione	medio
Tutti i computer	Probabilità/frequenza di guasto	medio
Tutti i computer	Possibilità di sabotaggio	lieve
Tutti i computer	Furto	medio
Tutti i computer	Intercettazioni delle trasmissioni dati	medio
Tutti i computer	Eventi naturali (allagamenti, terremoti, etc.)	lieve
Tutti i computer	Incendi	medio
Tutti i computer	Guasti ad apparecchiature connesse	medio
Tutti i computer	Black out	medio

TABELLA DI ANALISI DEI RISCHI DEI LUOGHI FISICI

Risorsa	Elemento di Rischio	Livello
Archivi	Possibilità di intrusione, accesso di persone non autorizzate	medio
Archivi	Furto	lieve
Armadi blindati casseforti	Possibilità intrusione / furto	lieve
Armadi, classificatori	Possibilità intrusione / furto	grave
Locali segreteria, presidenza, altri locali	Possibilità di intrusione, accesso di persone non autorizzate	grave
Locali segreteria, presidenza, altri locali	Eventi naturali (allagamenti, terremoti etc.)	grave

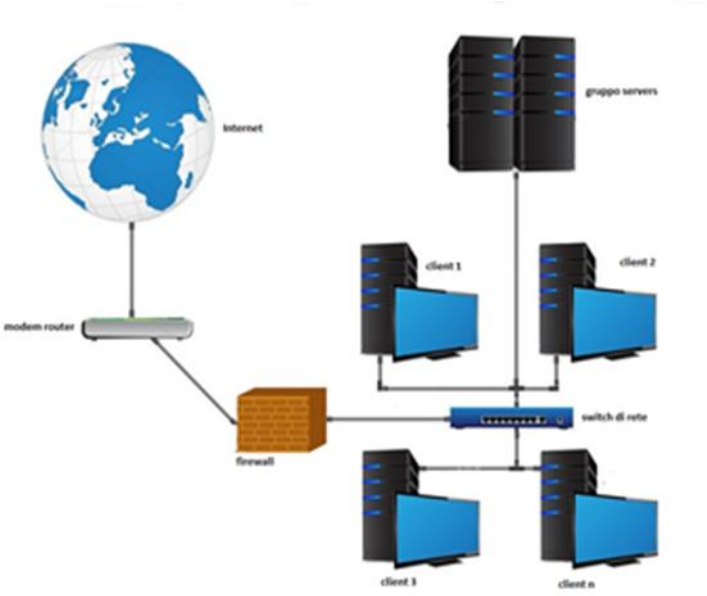
Locali segreteria, presidenza, altri locali	Incendi	grave

TABELLA DI ANALISI DEI RISCHI RISORSE DATI

Risorsa	Elemento di Rischio	Livello
Tutte le banche dati	Cancellazione non autorizzata di dati	Grave
Tutte le banche dati	Manomissione di dati	Grave
Tutte le banche dati	Perdita di dati	Grave
Tutte le banche dati	Accesso non autorizzato	Grave
Tutte le banche dati	Incapacità di ripristinare copie di back-up	Lieve

TABELLA DI ANALISI DEI RISCHI RISORSE SOFTWARE

Risorsa	Elemento di Rischio	Livello
Procedure	Possibilità di accesso non autorizzato a base dati	Grave
Procedure	Errori software che minacciano l'integrità dei dati, presenza di codice non conforme alle specifiche dei programmi	Lieve
Sistemi Operativi	Possibilità di accesso non autorizzato a base dati	Grave
Internet e posta elettronica	Possibilità di accesso non autorizzato a base dati	Grave
Programmi di masterizzazione CD / back - up	Mancata registrazione dei dati	Grave
Programmi antivirus e di protezione	Mancato aggiornamento dei file di riconoscimento virus	Grave
Programmi Office	Malfunzionamento a livello software	Lieve



7. IL SISTEMA INFORMATICO DI SEGRETERIA

7.1 GENERALITÀ

Lo schema adottato del **SIS** per il **trattamento dei dati** è il caratteristico sistema d'ufficio, come quello schematizzato in figura, ossia una rete **LAN** con struttura tipo **client – server** con linea fisica **Ethernet** e collegamento alla rete esterna (**Internet**).

Lo scopo della **sicurezza informatica** è la **difesa nel tempo** del **sistema**, per cui occorre gestire il **sistema di sicurezza**.

Le **misure di sicurezza** previste possono essere classificate nel seguente modo:

1. Misure di sicurezza **fisiche**;
2. Misure di sicurezza **tecnologiche hardware e software**;
3. Misure di sicurezza **logico – organizzative**.

Alcune misure possono essere classificate in più modi. Alle misure **fisiche** e **tecnologiche** si affiancano sempre delle misure **logico – organizzative** atte a tenere sotto controllo l'efficacia e l'efficienza delle misure adottate (gestione delle disposizioni).

7.2 L'AMMINISTRATORE DI SISTEMA

Come indicato nel **Provvedimento del Garante del 27/11/2008** (così come modificato in base al provvedimento del **25 giugno 2009**), referenziato, per <*"amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.*>. Dal punto di vista della **protezione dei dati**, il **Garante** precisa, inoltre, che <*vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi*>. Per i tipi di dati trattati e per la complessità delle strutture informatiche utilizzate, sia hardware che software, l'**Amministratore di Sistema** assume un **ruolo fondamentale** per la gestione del **SIS**. Infatti, **tutte le attività** riportate in **questo documento** sono di competenza dell'**Amministratore di Sistema** (**AS**), se non diversamente specificato.

L'**AS** deve essere opportunamente nominato. Egli può essere figura **interna** e/o **esterna** e la sua **nomina** è effettuata secondo quanto previsto dalla procedura **P02 "Incarichi"**. In particolare, se la scelta è rivolta a una **ditta fornitrice esterna** questa va nominata **Responsabile del Trattamento** e deve fornire i nominativi delle **persone fisiche** incaricate come **AS**.

L'attribuzione delle funzioni di **AS** deve avvenire previa valutazione dell'esperienza, della capacità, delle conoscenze tecniche e dell'affidabilità del soggetto designato, il quale deve fornire anche idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Le disposizioni che seguono sono estratte dalla circolare **AGID 2/2017**, referenziata:

1. Tutte le utenze, in particolare quelle **amministrative**, debbono essere **nominative** e riconducibili ad **una sola persona**.
2. Limitare i **privilegi di amministrazione** ai soli **utenti** che abbiano le **competenze adeguate** e la **necessità operativa** di modificare la **configurazione dei sistemi**.
3. Utilizzare le **utenze amministrative** solo per effettuare operazioni che ne richiedano i privilegi, **registrando** ogni **accesso** effettuato (**access log**).
4. Prima di collegare alla rete un nuovo dispositivo sostituire le **credenziali dell'amministratore predefinito** con valori coerenti con quelli delle **utenze amministrative in uso**.
5. Le **utenze amministrative anonime**, quali "**root**" di **UNIX** o "**Administrator**" di **Windows**, debbono essere utilizzate solo per le **situazioni di emergenza** e le **relative credenziali** debbono essere gestite in modo da assicurare l'**imputabilità** di chi ne fa uso.
6. Assicurare la completa distinzione tra **utenze privilegiate** e **non privilegiate** degli **amministratori**, alle quali debbono corrispondere **credenziali diverse**.

Il **DSGA** manterrà l'**inventario** di tutte le **utenze amministrative**, garantendo che ciascuna di esse sia **debitamente** e **formalmente autorizzata**, **disponibili** e **riservate**.

L'**AS** documenterà tutti gli interventi effettuati secondo quanto previsto da questa procedura con un apposito **Rapporto Tecnico d'Intervento, Installazione e/o Collaudo** che il **DSGA** o il **RGDS** conserverà in modo adeguato rendendoli disponibili alle autorità di controllo in caso di necessità.

7.3 LE MISURE DI SICUREZZA FISICHE

Le misure di sicurezza di tipo **fisico** sono accorgimenti che mirano a difendere, con sistemi "**fisici**" diversi dai dispositivi tecnologici hardware, le strutture (locali, attrezzature, dispositivi, supporti) da intrusioni e danneggiamenti dolosi e/o accidentali. Le **protezioni** di tipo **fisico** presenti sono descritte nel **Registro Trattamento Dati** dell'**Istituzione Scolastica**. La **gestione delle disposizioni** per tenere sotto controllo l'efficienza e l'efficacia delle misure esistenti è regolamentata dalla procedura **P05 "Accessi fisici"**.

7.4 LE MISURE DI SICUREZZA TECNOLOGICHE

Le misure di sicurezza **tecnologiche** sono accorgimenti che mirano a difendere le **attrezzature** e la **rete** da intrusioni e comportamenti illeciti dolosi e/o accidentali con dispositivi **hardware specifici** e programmi **software dedicati**.

La **Circolare AGID n° 2/2017 del 18 aprile 2017**, referenziata, recita all'art. 1:

*Art. 1. – S c o p o – Obiettivo della presente circolare è indicare alle **pubbliche amministrazioni** le misure minime per la **sicurezza ICT** che **debbono** essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi.*

Le misure minime di cui al comma precedente sono contenute nell'allegato 1, che costituisce parte integrante della presente circolare.

In tale allegato l'**AGID** (**Agenzia per l'Italia Digitale**) individua **3 livelli di sicurezza** denominati "**Minimo**" (il livello più basso), "**Standard**" e "**Alto**" ad ognuno dei quali corrispondono le varie azioni da attuare di complessità sempre più elevata man mano che il livello di sicurezza richiesto si eleva. Il **MIUR**, con la comunicazione n° **3015 del 20/12/2017**, stabiliva tra l'altro che il **livello di sicurezza di riferimento** per le **Istituzioni Scolastiche** è quello "**Minimo**".

Le misure previste per il livello "**Minimo**" si possono riassumere nei seguenti punti:

1. Dominio server;
2. Antivirus;
3. Firewall;
4. Backup;
5. Cifratura dei dati (crittografia).

7.4.1 Dominio server

In **Informatica** un **dominio** è "**un insieme di computer che condividono un database di risorse di rete e che vengono amministrati come un'unità con regole e procedure comuni**" (secondo la definizione di **Microsoft**).

In termini molto semplici, un **dominio** è una **rete di computer**, tipicamente una **LAN** di un'organizzazione (ad esempio un'**azienda** o un **ente pubblico**), ove la logica **client-server** è supportata, oltre che da connessioni fisiche e relativi protocolli (ad esempio il comune **indirizzo IP**), anche da regole (**policy**) di connessione logica di tipo autorizzativo (**regole di sicurezza**). In questo contesto, un **client** deve sottostare a procedure di **autenticazione** specifiche, definite da servizi che risiedono su un **server**. Queste procedure, che solitamente sottendono una gerarchia di profili (in termini di permessi e accessi alle risorse o ai sistemi), determinano l'appartenenza o meno al **dominio**, la struttura di distribuzione e la condivisione centralizzata.

Grazie al **dominio** molte operazioni sistemistiche possono essere automatizzate e gestite centralmente quali:

1. Distribuzione di aggiornamenti di sistemi operativi o di pacchetti di applicazioni (**patch management**);
2. Invio di comandi e script mirati;
3. Utilizzo di strumenti e programmi centralizzati e condivisi;
4. Imposizione di set di configurazione e impostazione (hardware e software) alle risorse (server, desktop, notebook, workstation, dispositivi mobili, periferiche e apparati, ecc.) "**forzati**" e resi immodificabili dagli utenti;
5. Impiego delle periferiche monitorato;
6. Determinazione degli accessi ai dati o alle risorse (permessi);
7. Organizzazione delle credenziali in gruppi di utenti;
8. Gestione dei profili di sicurezza (esempio dell'**antimalware**);
9. Impostazione delle modalità degli accessi remoti;
10. Monitoraggio di qualsiasi operazione o prestazione o funzione dei sistemi informatici;
11. Assegnazione o negazione di diritti;
12. Controllo granulare di ciascun componente anche HD (sino alla singola periferica di un determinato dispositivo mappato);
13. Implementazione di strutture articolate, ad esempio, le "**foreste**";
14. Salvataggio, replica e migrazione "**con un click**" del dominio;

e tante altre. Tali funzionalità, con una semplice struttura e accesso di rete, sarebbero impossibili o estremamente complicate o comunque senza le più banali regole di sicurezza. Un **utente/risorsa** che ha avuto la possibilità di eseguire un accesso al **dominio** (o, meglio, alla rete, in questo caso) ma senza essere membro di dominio si chiama "**utente non autenticato**" o "**risorsa non mappata**".

Inoltre mediante un'opportuna configurazione denominata "**folder redirection**", è possibile direzionare tutti i desktop e i documenti degli utenti in dominio in modo che essi risiedano sul **server**.

In questo modo:

- ✓ Tutti i lavori effettuati dall'**incaricato** (**file** di qualsiasi tipo che prima venivano salvati sul **disco rigido** del **pc client**) sono salvati sul **disco rigido** del **server** nell'area a sua disposizione (e alla quale, comunque, ha solo lui l'accesso grazie al meccanismo delle **credenziali di autenticazione**);
- ✓ Di conseguenza, è possibile effettuare il **backup** solo del **server**;
- ✓ È possibile ottimizzare meglio le risorse di rete (stampanti, scanner, ecc.);
- ✓ È possibile ottenere reti più economiche in quanto l'unico elemento "**nobile**" è il **server**; questo vale anche in caso di **rottamazione** degli **elementi della rete** in quanto le procedure di cancellazione dei dati vanno applicate solo al **server** perché sui **client** non è memorizzato alcunché.

Per consentire tale configurazione l'**AS** deve verificare periodicamente (secondo necessità e almeno una volta all'anno e ne da conto al **Titolare**) che:

1. L'**hardware server** sia di capacità tale da sostenere la struttura descritta;
2. Il **Sistema Operativo Server** sia di livello, tipologia e aggiornamento adeguato per consentire la configurazione descritta;
3. L'**hardware** e il **Sistema Operativo** dei **client** siano di livello, tipologia ed aggiornamento adeguato per consentire la configurazione descritta;
4. Il **server** sia protetto contro gli sbalzi della tensione delle rete elettrica e mancanze di alimentazione dell'energia di rete tramite opportuno **UPS** (**Uninterruptible Power Supply** ossia il **Gruppo di Continuità**);
5. Il **server** e tutti gli altri dispositivi a corredo (UPS, firewall, switching, router, modem ADSL, NAS, ecc.) siano custoditi in un **rack** con **accesso controllato** (chiave) gestito secondo quanto previsto dalla procedura **P05 "Gestione accessi fisici"**;
6. Il **cablaggio della rete** sia **adeguato**, secondo quanto previsto dalle norme tecniche di buona pratica e dalla legge (ex **D. Lgs 46/90** le cui prescrizioni in materia di **dichiarazione di conformità** sono state sostituite dalle disposizioni contenute nel **Decreto Interministeriale del 22 gennaio 2008, n. 37**, referenziato) ed eseguito da un cablatore autorizzato e certificato.

Il **Titolare del Trattamento** valuta le informazioni ricevute dall'**AS** e stabilisce le risorse (economiche e tecniche), le responsabilità e le tempistiche per eventuali adeguamenti.

Inoltre, come disposto dalla circolare **AGID 2/2017**, referenziata, occorre:

1. Utilizzare **configurazioni** sicure **standard** per la **protezione** dei **sistemi operativi**;
2. Definire ed impiegare una **configurazione standard** per **client**, **server** e altri tipi di **sistemi** usati dall'**Istituzione Scolastica**;
3. Eventuali **sistemi in esercizio** che vengano **compromessi** devono essere **ripristinati** utilizzando la **configurazione standard**;
4. Le **immagini d'installazione** devono essere **memorizzate offline**;
5. Eseguire tutte le operazioni di **amministrazione remota** di **server**, **client**, **dispositivi di rete** e analoghe **apparecchiature** per mezzo di **connessioni protette** (protocolli intrinsecamente sicuri, ovvero su canali sicuri).

7.4.2 Antivirus

La protezione verso qualsiasi tipo di **software malevolo** deve essere attuata tramite **programmi**, detti **antivirus**, che impediscano l'accesso illecito o il danneggiamento del sistema da parte di tali software. L'**AS** deve verificare che il programma da utilizzare o utilizzato copra tutti i tipi di **software malevoli** e protegga tutte le **piattaforme presenti**, quali PC, Server, file, portatili e dispositivi mobili offrendo la possibilità di monitorare qualsiasi dispositivo connesso.

Ad ulteriore protezione da tali **software malevoli** occorre:

1. Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili;
2. Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione;
3. Scansionare periodicamente per la ricerca di virus le postazioni di lavoro e i dispositivi utilizzati per lavoro (se necessario);
4. Disattivare l'esecuzione automatica dei contenuti dinamici (ad esempio, le macro) presenti nei file.

7.4.3 Firewall

Il **firewall** è un dispositivo **hardware e/o software** che si posiziona tra la rete **Lan** (switch di rete) e la **linea Internet** (dispositivo di connettività per la linea Internet ovvero **modem router**) e ha lo scopo specifico di impedire attacchi dall'esterno. I **firewall** devono essere forniti della funzione **IPS** (**Intrusion Prevention System** ossia **Sistema di Prevenzione delle Intrusioni**) e devono possedere funzioni di **URL Filtering** (hardware o software) per controllare e limitare il **traffico dall'interno** verso determinati **siti Internet** per migliorare il lavoro degli **incaricati**, per ridurre gli effetti dannosi indotti (inserimento nelle liste di spamming, download di software pericoloso) e ridurre la probabilità che vengano commessi **crimini informatici** da dipendenti interni, oltre che ottimizzare l'utilizzo di banda di connessione ad Internet. Le tecniche comunemente adottate da questi strumenti sono principalmente due:

- **Black list.** L'indirizzo richiesto dall'utente viene confrontato con una lista di indirizzi non consentiti ed inseriti in precedenza. Se il confronto è positivo viene negato l'accesso alla risorsa;
- **URL database**. Rappresenta la tecnica più sofisticata e consiste in un database di indirizzi Web che, aggiornato periodicamente, classifica i contenuti Internet in appositi gruppi. L'utente viene assegnato ad uno o più gruppi o configurato per essere escluso da alcuni di essi. In questo modo è possibile applicare restrizioni su categorie di siti, piuttosto che censire manualmente ciascun indirizzo.

L'accesso a **Internet** e l'uso della **posta elettronica** è gestito tramite le **linee guida** riportate nella procedura **P03 "Accesso a internet e email"**.

7.4.4 Back up

In informatica per **backup** s'intende il **processo** atto a ottenere **ridondanza** delle informazioni ovvero **una o più copie** di **riserva dei dati**, da utilizzare in caso di eventi malevoli accidentali o intenzionali. Si tratta dunque di un tipico procedimento di **sicurezza delle informazioni**, in particolare di **disaster recovery**, ossia di recupero a seguito di un evento disatroso. Può essere considerato senz'altro come l'attività più importante di protezione. Si possono adottare diverse tecniche di **backup** che sono, in **ordine di priorità**:

1. **NAS:** il **Network Attached Storage** (**Immagazzinamento Collegato alla Rete**) è un dispositivo **hardware e software** costituito in genere da 2 o più dischi rigidi che, collegato al **server**, consente di effettuare le copie di **backup** in **automatico** a periodi stabiliti;
2. **Cloud:** le copie di sicurezza vengono effettuate periodicamente in automatico tramite trasmissione dei dati su linea protetta a **server specifici esterni** che formano delle **web farm** blindate.

È assolutamente da evitare il **backup in manuale** su supporti **fisici esterni o interni** al **server**.

Qualunque sia il tipo di **backup** scelto occorre garantire le seguenti linee guida (tratte dalla **Circolare Agid 2/2017**, referenziata):

1. Il **backup completo** deve essere effettuato almeno **una volta a settimana**; è altamente auspicabile la possibilità di effettuare **backup incrementali giornalieri**;
2. Assicurare la **riservatezza delle informazioni** contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante **cifratura**;
3. In caso di **cloud** effettuare la **cifratura** prima della **trasmissione**;
4. **Assicurarsi** che i **supporti** contenenti almeno **una delle copie** non siano **permanentemente accessibili** dal **sistema** onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza;
5. **Effettuare** una prova di **data recovery** (ripristino dei dati in caso di crash o di attacco informatico del sistema) almeno una volta l'anno.

7.4.5 Cifratura dei dati

La **cifratura** è una modalità di **conversione del testo originale** in una sequenza apparentemente casuale di lettere, numeri e segni speciali che solo la persona in possesso della corretta **chiave di decifratura** potrà riconvertire nel file di testo originale. La **conversione** viene ottenuta mediante un **apposito software** che impedisce ad eventuali **hacker** di poter comunque accedere alle informazioni, soprattutto di tipo sensibile, contenute nei documenti.

7.5 LE MISURE DI SICUREZZA LOGICO – ORGANIZZATIVE E ALTRE DISPOSIZIONI

7.5.1 La gestione delle credenziali di autenticazione e dei profili di autorizzazione

Nella presente **Istituzione Scolastica** le **credenziali di autenticazione** sono costituite da **due codici** specifici tra loro associati:

1. **Codice utente** (**user – id** o anche **user name**): è il **nome identificativo** assegnato a **ciascun incaricato** (opportunamente nominato così come previsto dalla procedura **P02 "Incarichi"**) che gli consente di accedere ai sistemi di trattamento delle banche dati. La **user-id** viene consegnata al singolo **incaricato** (ad esempio, utilizzando il modulo **01P/P12 "Consegna user – id"**, in allegato) e l'**AS** avrà un **registro**, cartaceo e/o informatico, conservato in luogo sicuro e a disposizione anche del **DSGA**, dove sono riportate le **user-id** emesse associate al singolo incaricato. Inoltre si attuano le seguenti disposizioni:
   a. Non sono ammessi **nomi identificativi di gruppo**;
   b. Un **codice identificativo** assegnato ad un **incaricato** deve essere **annullato** se l'**incaricato decade** dal suo compito: il **DSGA** comunicherà immediatamente l'evento all'**AS** che provvederà a disattivare la possibilità di accesso al sistema per il soggetto in questione;
   c. Similmente il **codice utente** deve essere annullato se **non è usato** da almeno **6 mesi**;
   d. Non è possibile assegnare un **codice utente** ad **altro incaricato** anche se a **distanza di tempo**;
   e. Ad ogni **codice utente** deve essere associato un appropriato **profilo di autorizzazione** per consentire l'**accesso** dell'**incaricato** alle sole **risorse** e ai **trattamenti di dati** per i quali è stato nominato; l'**AS**, coadiuvato dal **DSGA**, almeno una volta all'anno verificherà la congruenza di tali profili.
2. **Parola chiave** (**password**): è un **codice assolutamente segreto** noto solo all'**incaricato** che, inserito insieme al **codice utente**, consente l'**accesso** al sistema. L'**AS** consegnerà all'**incaricato**, insieme al **codice utente**, una **password provvisoria** che l'**incaricato** dovrà **obbligatoriamente cambiare** al **primo accesso** al sistema. Il sistema deve prevedere il **cambiamento** della **password** almeno ogni **3 mesi**. Per **gestire** nel modo migliore e per avere delle **password** quanto più "**robuste**" possibili attenersi alle seguenti disposizioni (tali disposizioni si applicano **qualsiasi sia la piattaforma o il sistema** a cui un qualsiasi **dipendente scolastico**, docenti e ata, deve accedere per motivi di lavoro):
   a. Usare **password diverse** per **servizi diversi**;
   b. **Non scrivere mai le password su biglietti** che poi magari si conservano nel portafoglio o indosso, o che si possono distrattamente lasciare in giro, oppure in file non protetti sui propri dispositivi personali (computer, smartphone o tablet).
   c. **Evitare sempre di condividere le password via e-mail, sms, social network, instant messaging, ecc..** Anche se le si comunicano a **persone conosciute, le credenziali** potrebbero essere diffuse involontariamente a terzi o «rubate» da malintenzionati.
   d. Se si usano **pc, smartphone e altri dispositivi non di proprietà, evitare sempre che possano conservare in memoria le password utilizzate.**
   e. È consigliabile usare dei **gestori di password**; si tratta di **programmi specializzati** che generano **password sicure** e consentono di appuntare in formato digitale tutte le password salvandole in un database cifrato sicuro. Ce ne sono di vario tipo, gratuiti o a pagamento;
   f. La password deve essere formata da almeno **8 caratteri**, preferibilmente di più (ad esempio, almeno **14/15 caratteri**), costituiti da **cifre**, **caratteri speciali** e **lettere**, **maiuscole e minuscole**. Sono da evitare:
      - la ripetizione di due parole brevi anche rovesciate (ad es. "melapera" o "melaalem");
      - le cifre all'inizio o in fondo alla password (ad es. "nicola57");

- riferimenti espliciti (nomi, date di nascita, eventuali soprannomi) alla propria persona, ai membri della famiglia (compreso eventuali riferimenti ai propri animali domestici) o alla scuola;
- l'utilizzo della **user-id** o sequenze scontate e nomi o **parole** comuni;

g. Il sistema dovrebbe essere dotato di **password history** per evitare l'utilizzo della stessa password o di password troppo simili tra di loro a breve distanza di tempo;
h. In caso di **necessità** o di **particolare pericolo** il **DS** può stabilire, laddove possibile, di utilizzare, per alcuni tipi di **sistemi/piattaforme**, meccanismi di **autenticazione multi fattore** (es. codici **OTP one-time-password**), che rafforzano la protezione offerta dalla password; tale decisione sarà resa nota tramite opportuna circolare interna.

Solo se il **DSGA** lo reputerà **necessario**, si potrà adottare la seguente **procedura** per lo svolgimento di un **servizio specifico** in caso di **assenza prolungata** dell'**incaricato** ad esso addetto:

1. Tutti gli **incaricati** consegneranno al **DSGA**, ad ogni **cambio di password**, copia **scritta** in **busta chiusa** di tale **password** (ad esempio, utilizzando il modulo **02P/P12 "Comunicazione password"**, in allegato); il **DSGA** custodirà tali **buste chiuse** in **luogo sicuro** e provvederà a **distruggere** le **buste vecchie** ad ogni nuova consegna da parte degli **incaricati**;
2. Se un **incaricato** dovesse essere assente e accertata la necessità del servizio e l'impossibilità di dare ad altro **incaricato** il servizio stesso, il **DSGA** consegnerà la **busta chiusa** contenente la **password** necessaria ad altro **incaricato**, registrando tale evento in modo opportuno, consentendo a tale **incaricato** lo svolgimento del servizio richiesto; l'**incaricato** designato sarà, quindi, l'**unico** ad avere accesso alla **password** necessaria per lo svolgimento del servizio;
3. Al rientro dell'**incaricato** temporaneamente assente, il **DSGA** lo avvisa dell'evento e l'**incaricato** provvederà a **modificare** immediatamente la **password**, consegnandola ovviamente in **busta chiusa** al **DSGA**.

7.5.2 L'aggiornamento delle risorse hardware e software utilizzate e analisi delle vulnerabilità

L'**AS** dovrà (secondo quanto previsto dalla **Circolare Agid 2/2017**, referenziata):

1. **Implementare** un **inventario** delle **risorse attive**;
2. **Aggiornare** l'**inventario** quando **nuovi dispositivi** approvati vengono **collegati in rete**;
3. **Gestire** l'**inventario** delle risorse di tutti i **sistemi collegati alla rete** e dei **dispositivi di rete stessi**, registrando almeno l'indirizzo **IP**;
4. **Stilare** un **elenco di software autorizzati** e relative versioni necessari per ciascun tipo di **sistema**, compresi **server**, **client** e laptop di vari tipi e per diversi usi. Non consentire l'**istallazione** di **software** non compreso nell'elenco;
5. **Eseguire** regolari **scansioni** (almeno una volta all'anno) sui **sistemi** al fine di rilevare la presenza di **software non autorizzato.**

L'**AS** ha il compito di **verificare** almeno una volta all'anno la situazione delle **apparecchiature hardware** installate con cui vengono trattati i dati e delle **apparecchiature periferiche**, in particolare, dei **dispositivi di collegamento** con le **reti pubbliche**. Tale **verifica** ha lo scopo di controllare l'**affidabilità** del **sistema** (**analisi delle vulnerabilità**) per quanto riguarda:

1. La sicurezza dei dati trattati;
2. Il rischio di distruzione o perdita;
3. Il rischio di accesso non autorizzato o non consentito tenendo conto dell'evoluzione tecnica.

L'esito della verifica va messo per iscritto e consegnata al **DSGA** che la conserva in modo adeguato.

In caso di evidente rischio il **DSGA**, coadiuvato dall'**AS**, avvisa il **Titolare** affinché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme vigenti.

La stessa prassi va seguita anche per quanto riguarda i **Sistemi Operativi** (**server** e **client**) e per tutti i **software** operativi utilizzati per il **trattamento dati**, assicurando un loro corretto **aggiornamento** per una ottimale sicurezza contro i rischi d'intrusione o di danneggiamento dei dati. È essenziale, quindi, verificare:

1. L'avvenuto **rinnovo** delle **licenze**, laddove è previsto e necessario;

2. Il corretto svolgimento del **patch management** (la procedura automatica dell'aggiornamento dei dispositivi previsti).

7.5.3 La gestione dei client

Il **pc** affidato a ciascun dipendente, compreso eventuali persone esterne non dipendente dell'**Istituzione Scolastica**, è da intendersi esclusivamente "**strumento di lavoro**" per cui è vietato ogni suo utilizzo che non sia strettamente necessario ed inerente l'attività lavorativa. Il soggetto che utilizza tali pc è responsabile della sua custodia e del suo corretto utilizzo, per cui, salvo specifiche **autorizzazioni** del **DS** con l'intervento dell'**AS** o nei casi previsti, si applicano le seguenti disposizioni:

1. È assolutamente **proibito** collegare **dispositivi esterni** e **memorie di massa** (**pen drive**, **dvd/cd**, altro) ai **client**; è altamente consigliabile, comunque, per prevenire qualsiasi tipo di problema, verificare la possibilità di **inibire** da sistema l'utilizzo delle **porte USB/lettore CD** dei **client**;
2. È assolutamente proibito, altresì, effettuare sul **pc** in dotazione il **backup** ovvero la **sincronizzazione** di apparecchi **smartphone** e **tablet**;
3. È altamente consigliato **non effettuare** la **memorizzazione di file** contenenti **informazioni e dati di persone fisiche** sull'**hard disk** del **client**; tutti i **file** devono essere conservati sul **server** (si veda quanto riportato al par. **7.4.1** a proposito del "**folder redirection**");
4. Su tutti i **client** deve essere attivata la funzione di "**screen saver**" con ripristino dell'**operatività** mediante la reintroduzione delle **credenziali di autenticazione**; orientativamente tale funzione, che è un sistema di protezione quando ci si allontana dalla postazione lasciando il pc acceso o in caso di presenza di **persone estranee** all'interno dell'ufficio (politica dello "**schermo pulito**"), dovrebbe entrare in funzione al **massimo** dopo **2/3 minuti** di inattività;
5. È assolutamente **proibito** lasciare incustodito e accessibile il proprio **pc** senza aver precedentemente provveduto a bloccarlo attraverso l'apposito comando (**CTRL+ALT+CANC** e successivamente cliccare su "**Blocca il computer**"), al fine di evitarne un utilizzo improprio in caso di assenza anche temporanea;
6. È assolutamente **proibito** modificare qualsiasi caratteristica **HW** e **SW pre-impostata** sul proprio **pc**;
7. È assolutamente **proibito** installare e/o eseguire qualsiasi tipologia di programmi informatici diversi da quelli pre-installati, previsti e autorizzati, anche nel caso si tratti di **SW** opportunamente licenziato, di **SW** in prova ("**shareware**"), ovvero di **SW gratuito** e liberamente scaricabile da Internet ("**freeware**");
8. È assolutamente **proibito** scaricare da internet, copiare e/o archiviare, anche temporaneamente, sul **pc** in dotazione qualsiasi file audio, video, eseguibile, ecc., (tale elencazione è esemplificativa e non esaustiva) non necessario allo svolgimento dell'attività lavorativa;
9. È assolutamente **proibito** effettuare visualizzazioni di file di qualunque tipo in streaming, salvo ciò non sia necessario per fini lavorativi e previa informazione all'**AS**;
10. È assolutamente **proibito** cedere a **soggetti non autorizzati** il proprio pc, soprattutto successivamente al superamento della **fase di autenticazione**;
11. Ogni utilizzatore ha l'obbligo di provvedere allo **spegnimento** della propria postazione di lavoro, al termine della giornata lavorativa, salvo espliciti e contrari avvisi da parte dell'**AS**;
12. È assolutamente **proibito eliminare o comunque rendere inaccessibile** qualsiasi tipologia di **informazione lavorativa** dal proprio **pc** in caso di cessazione del rapporto di lavoro.

Ogni utente è avvisato e ha contezza del fatto che le informazioni presenti all'interno del pc assegnato, trattandosi di "**strumento di lavoro**", siano considerate e trattate come lavorative e non personali. Pertanto, in conformità con i principi di necessità, pertinenza e non eccedenza della normativa sul trattamento dei dati personali, il **Titolare** si riserva il diritto di poter eventualmente accedere in qualunque momento, previo avviso all'incaricato, alle informazioni e ai dati eventualmente presenti al suo interno per esclusive finalità lavorative, di continuità operativa dell'**Istituto** e/o di salvaguardia dei propri diritti in sede giudiziaria. Inoltre il **Titolare** si riserva di provvedere, in qualsiasi momento e anche senza preavviso, alla rimozione di ogni file o SW o applicazione che si ritenessero dannosi o pericolosi per la sicurezza ovvero che violino le regole previste in questa procedura o che, in ogni caso, possano costituire una alterazione della configurazione prevista per lo strumento di lavoro.

7.5.4 Disposizioni per lo smaltimento o destinazione ad altro uso dei dispositivi elettronici

Occorre utilizzare tecniche sicure di **cancellazione** dei dati o metodi di **distruzione fisica** dei **supporti rimovibili** che contenevano **dati personali** (in particolare **dati sensibili o giudiziari** secondo quanto indicato dagli **artt. 9** e **10** del **GDPR**) e **non sono più utilizzabili** o sono destinati **ad altro uso**.

Il **Provvedimento del Garante** del **13/10/2008**, referenziato, fornisce precise indicazioni su cosa fare in caso di **destinazione ad altro uso** o di **smaltimento come rifiuto** di **strumenti elettronici** che contengono **dati personali o sensibili e giudiziari**. Esso prevede:

- In caso di smaltimento come rifiuto, da attuarsi in conformità a quanto previsto dal **D. Lgs 151/2005** circa lo smaltimento di rifiuti di apparecchiature elettriche ed elettroniche in ottemperanza a quanto prescritto, in particolare, dalla **direttiva europea 2002/96/CE** sui rifiuti di apparecchiature elettriche ed elettroniche (**RAEE**), la distruzione dei supporti con tecniche varie a seconda del tipo:
  - ✓ Sistemi di punzonatura o deformazione meccanica;
  - ✓ Distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
  - ✓ Demagnetizzazione ad alta intensità.
- In caso di reimpiego o riciclo, ma anche in caso di rottamazione:
  - ✓ Uso preventivo di tecniche di memorizzazione sicura mediante protezione dei singoli file o gruppi di file o dischi interi (funzionalità detta file system crittografico disponibile su vari sistemi operativi) con password nota solo all'utente proprietario dei dati;
  - ✓ Poco prima della dismissione o della nuova destinazione, uso di tecniche di cancellazione sicura dei dati tramite uso di opportuni programmi informatici (wiping program o file shredder) o formattazione a basso livello dei dischi rigidi; tali tecniche si possono utilizzare, ovviamente, solo se l'apparecchiatura funziona. In caso contrario occorre applicare le tecniche di distruzione fisica.

L'attuazione delle operazioni sopra descritte vanno opportunamente verbalizzate dall'**AS**. Esse possono essere eseguite anche da una struttura esterna tecnicamente qualificata con rilascio del rapporto tecnico dettagliato dell'operazione eseguita.

7.5.5 Disposizioni nel caso di utilizzo di PC personali (telelavoro/smart working/DDI)

Nel caso sia necessario utilizzare un proprio dispositivo (**PC** personale) per il lavoro, occorre che anche questo strumento rispetti dei minimi criteri di sicurezza. Occorre, quindi, che siano assicurate le seguenti disposizioni:

1. Il **Sistema Operativo** del dispositivo sia **aggiornato**;
2. Sia presente un **antivirus** e che questo sia **aggiornato**;
3. **Scansionare** periodicamente il dispositivo con l'**antivirus**;
4. Utilizzare **password robuste** (vedere quanto indicato al **par. 7.5.1 punto 2**);
5. Non usare l'**account di lavoro** per registrarsi in **internet** per fini non ricondicibili a fini lavorativi;
6. Non salvare le **password** nei **browser di navigazione internet**;
7. Non lasciare il **PC** incustodito;
8. Usare **pen drive**, **CD** e **hard disk esterni** con **molta cautela**; è opportuno che quando si collega uno di questi dispositivi al **PC** venga effettuata una **scansione** completa con l'**antivirus**;
9. Fare attenzione all'uso dell'**e-mail** per evitare il pericolo di messaggi di **phishing**; a tale scopo attenersi a quanto previsto su questo argomento nella procedura **P03 "Internet e e-mail"** al **par. 6.3**;
10. Fare un **back up** periodico dei dati elaborati nell'ambito della sfera lavorativa;
11. In caso di furto o smarrimento si ha l'obbligo d'informare immediatamente e senza ritardo il **Titolare**, nonché di denunciare tempestivamente l'accaduto alle **Forze dell'Ordine**, fornendo al **Titolare**, entro al massimo **48 ore** dall'evento, copia dell'atto di denuncia che dovrà indicare marca e modello dello strumento. A tal proposito si ricorda che, anche in questo caso, se lo strumento conteneva dati personali inerenti l'ambito lavorativo (e ciò accade qualunque sia lo strumento smarrito o rubato, quali ad esempio **hard disk esterni** o altri dispositivi utilizzati per il backup dei dati lavorativi), si configura un **data breach** con tutte le conseguenze del caso che sono da gestire con la relativa **procedura**.

7.6 SANZIONI

L'**inosservanza** delle **disposizioni comportamentali e logiche – organizzative** riportate in questa **procedura** possono costituire un **inadempimento contrattuale** sia se a commetterla sono **dipendenti interni** dell'**Istituzione Scolastica** sia **fornitori terzi** di servizi e altro. Per i **dipendenti**, si potrà provvedere a **sanzioni disciplinari** secondo quanto previsto dalla **legislazione vigente** e dal **CCNL**, per i **terzi** si potrà arrivare alla **risoluzione del contratto** con eventuali richieste **risarcitorie** in ordine al **danno causato**. Ovviamente, rimane salva l'eventuale **responsabilità penale** per gli **autori dell'illecito** che sarà stabilita dalle **autorità preposte.**

8. MODULI E ALLEGATI

Codice	Titolo
01P/P12	Consegna user – id
02P/P12	Gestione password