Gianfausto Vincenzi rpd@vincenzi.com 3404057298
Via Fante d'Italia, 9 25080 Puegnago del Garda (BS)

Linee guida per la valutazione e l'applicazione delle misure di sicurezza per il corretto trattamento dei dati personali

Revisione 18_11_01 del 20/11/2018

Il responsabile protezione dati, d'ora in avanti RPD,

designato da questo istituto scolastico, ai sensi dell'articolo 37 del Regolamento UE 2016/679, d'ora in poi GDPR,

visto l'articolo 4 del GDPR (definizioni);

visto l'articolo 39 comma 1 del GDPR;

visto l'articolo 39 comma 2 del GDPR;

vista la circolare AgID 18 aprile 2017;

adotta le seguenti linee guida per l'applicazione delle misure di sicurezza ai dispositivi e alle procedure impiegati nei trattamenti di dati personali trattati nelle attività svolte dalle unità e sotto unità organizzative:

segreteria

- alunni
- personale
- bilancio e servizi amministrativi
- protocollo e servizi web

direzione

didattica.

È compito del Dirigente scolastico affidare la verifica dell'adeguatezza delle misure adottate alle funzioni tecniche a ciò preposte sia interne (ATA tecnici, funzioni strumentali) che esterne (amministratori di sistema, responsabili dei trattamenti esterni);

è compito del RPD, acquisite le informazioni dalle funzioni tecniche preposte dal Dirigente scolastico, valutare l'attuale livello di sicurezza e prescrivere l'adozione di azioni correttive o di adeguamento da applicare alla struttura ed agli strumenti impiegati.

Lo scopo delle presenti linee guida è di individuare i settori di applicazione del GDPR, quindi definirne i criteri di analisi e le necessità operative al fine di indicare le misure di sicurezza per mezzo delle quali ridurre i rischi di agire in violazione del GDPR stesso.

Dall'applicazione delle misure così individuate dovrà derivare, quale complemento per la loro corretta adozione, un documento di natura regolamentare da sottoporre ai collaboratori e sul quale basare una adeguata formazione.

Gianfausto Vincenzi rpd@vincenzi.com 3404057298
Via Fante d'Italia, 9 25080 Puegnago del Garda (BS)

Premessa

I trattamenti informatizzati dei dati personali, elencati e dettagliati nel c.d. registro dei trattamenti, suddivisi nei seguenti capitoli:

- T1 Dati personali di alunni e famigliari utilizzabili per finalità didattiche da docenti e, con mansioni accessorie, da collaboratori scolastici
- T2 Dati personali di alunni e famigliari utilizzabili per finalità amministrative, gestionali e di raccordo fra le diverse strutture operative e, con mansioni accessorie, da collaboratori scolastici
- T3 Dati personali del personale dipendente
- T4 Dati personali di collaboratori del Dirigente
- T5 Dati personali contenuti nelle pratiche di acquisto e rapporti con i fornitori
- T6 Dati personali contenuti nelle pratiche amministrative e contabili, gestione finanziaria e bilancio
- T7 Dati personali contenuti nei documenti protocollati o necessari per lo svolgimento delle attività istituzionali
- T8 Dati personali relativi a genitori, docenti, collaboratori scolastici necessari alla gestione dell'attività degli organi collegiali e della loro formazione
- T9 Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario

vengono posti in essere utilizzando due distinte strutture informatiche, didattica e segreteria, ognuna dotata di proprie caratteristiche, distinte per strumenti di trattamento, dati trattati, finalità.

Didattica

Struttura di accesso

Parte del trattamento T1 avviene da parte dei docenti utilizzando la struttura informatica a disposizione per la didattica. Questa struttura deve essere separata, fisicamente (scelta preferibile) o logicamente (ammissibile in alcuni casi) dalla struttura informatica della segreteria.

La valutazione delle misure di sicurezza della struttura didattica terrà inoltre conto della limitata possibilità di accesso ai dati dalle postazioni o dagli apparati che la compongono. L'adozione di strumenti quali firewall, proxy server, antivirus, domain controller, potrà incontrare esigenze di natura didattica o di opportunità, raramente di sicurezza.

L'utilizzo di tale struttura è principalmente di natura didattica e di supporto alle lezioni dei docenti. Il solo punto di incontro fra i trattamenti di dati personali e la struttura didattica è rappresentato dall'utilizzo delle postazioni installate nelle aule, nei laboratori o nell'aula docenti, del **registro elettronico** (si veda apposita sezione) mediante portale web da parte dei docenti.

Tale utilizzo può avvenire utilizzando diverse tipologie di dispositivi:

a) postazioni di tipo PC fissi collegate alla rete didattica mediante infrastruttura cablata;
b) postazioni di tipo PC mobili collegate alla rete didattica mediante infrastruttura cablata;
c) postazioni di tipo PC mobili collegate alla rete didattica mediante infrastruttura WiFi;
d) in rarissimi casi postazioni di tipo PC fissi collegate alla rete didattica mediante infrastruttura WiFi;
e) dispositivi Android o iOS collegati alla rete didattica mediante infrastruttura WiFi;
f) dispositivi Android o iOS collegati direttamente al web mediante rete cellulare (da 2 a 4g).

Nella maggior parte dei casi i dispositivi sono in dotazione all'Istituto, quindi impostati dall'amministratore di sistema. in alcuni casi, nei tipi b), c), e), f), i docenti possono utilizzare dispositivi personali, previa autorizzazione del Dirigente, sentito, di norma, il parere dell'amministratore di sistema.

Dove ciò sia possibile è preferibile collegare i punti di accesso mediante rete cablata, sia per ragioni di prestazioni che di sicurezza.

Nella maggior parte dei casi, tuttavia, è stato necessario installare una struttura WiFi composta, spesso, da più di un apparato di tipo "access point" (AP).

L'opportunità di consentire, o meno, l'utilizzo dell'infrastruttura AP anche a dispositivi non in dotazione all'Istituto, è da valutare tenendo conto di diversi elementi:

- quantità di banda di navigazione web a disposizione;
- capacità dei punti di accesso di gestire più richieste contemporaneamente;
- possibilità di creare sottoreti di accesso (docenti, alunni, ospiti);
- possibilità di creare elenchi di dispositivi autorizzati.

Riteniamo che, se si dimostrasse una imprescindibile esigenza didattica, la possibilità di garantire l'utilizzo da parte degli alunni della rete d'Istituto debba essere legata alla possibilità di creare e gestire una rete parallela, quindi separata, da quella dei docenti.

Qualora questa non fosse una necessità, la rete WiFi dovrà soddisfare solo la necessità di collegamento di postazioni o dispositivi da utilizzare in locali non raggiunti da cablaggio.

In questo caso le misure di sicurezza da adottare saranno da scegliere fra le seguenti:

- utilizzo di AP che consentano la configurazione WDS o Wireless Bridge;
- utilizzo preferibile di sistemi di gestione Central WiFi Manager con preimpostazione degli utenti e accesso mediante captive portal;
- utilizzo di AP o di sistemi di gestione centrale che consentano la registrazione del mac address dei dispositivi autorizzati;
- utilizzo di crittografia ameno WPA + AES (meglio WPA2 + AES).

Si chiede all'amministratore di sistema un inventario degli apparati utilizzati per gestire una o più reti WiFi e uno schema che ne illustri la configurazione e la struttura.

In caso per la didattica sia stata approntata una rete basata su un domain controller, con la conseguente codifica degli utenti (docenti e / o alunni) e la adozione di un sistema di cartelle condivise sulla intranet (si veda la sezione seguente), si chiede all'amministratore di sistema di descrivere la struttura utilizzata (gruppi, utenti policy).

Didattica Struttura dati

Raramente abbiamo riscontrato l'utilizzo di una struttura di condivisione dati in una rete didattica. Ove ciò fosse necessario bisognerà analizzare le esigenze per le quali si è adottata questa impostazione:

- adozione di una credenziale nominale per ogni docente da usare su qualsiasi risorsa alla quale possa accedere;
- condivisione di risorse fra docenti;
- creazione di aule virtuali;
- creazione di una credenziale nominale per ogni studente con assegnazione controllata delle risorse utilizzabili;
- adozione di una struttura centralizzata delle attività di laboratorio.

In alcuni casi è necessario inserire nella rete un server con funzioni di Domain Controller, al fine di definire sia gli utenti (docenti e alunni) sia i permessi di accesso e gestione delle risorse condivise.

Le misure di sicurezza da adottare in questi casi non si discostano da quelle che indicheremo per il Domain Controller e le condivisioni della segreteria.

Si richiede all'amministratore di sistema di indicare se è presente una condivisione dati sulla rete didattica o se viene utilizzato un Domain Controller ed, eventualmente, con quale configurazione (gruppi, utenti, permessi) e quali sistemi di back up.

Non serve, in questa fase, indicare condivisioni che utilizzino strumenti diversi dalla rete interna d'Istituto, quali piattaforme di condivisione o applicativi legati al registro elettronico.

Analizzeremo più avanti eventuali piattaforme web o appendici del registro elettronico gestite da funzioni strumentali. Se presenti, sarà necessario definirne la struttura amministrativa (chi concede o revoca le autorizzazioni) e i rapporti fra gli altri profili (tipi diversi di utilizzatori).

Allegati:

tabella inventario AP e altri dispositivi (tab_a5_1)

tabelle Active Directory e server (tab_a5_1, tab_a5_2, tab_a5_3)

Segreteria

Trattamenti cartacei

La totalità dei documenti cartacei arriva, o nasce, o viene comunque conferita, nell'unità organizzativa "segreteria". A questa unità fanno anche capo gli archivi dei documenti relativi agli anni passati, sia quelli ormai "storici", di pressoché nulla necessità di consultazione o utilizzo, che quelli relativi ad un passato più prossimo, dei quali potrebbe essere ancora necessaria la disponibilità per consultazione o utilizzo.

Anche se l'obiettivo da perseguire è quello della dematerializzazione dei documenti, siamo consapevoli che ancora per molto tempo la massa dei documenti cartacei costituirà un fattore e, ai fini della corretta applicazione del Regolamento UE, un problema.

Il concetto di "trattamento" si applica anche ai dati presenti su documenti in formato cartaceo, di conseguenza anche le misure di sicurezza da adottare (riduzione del rischio di distruzione o perdita, accesso non autorizzato, utilizzo non conforme alle finalità della raccolta), oltre che alla eventuale applicazione dei principi di minimizzazione e pseudonimizzazione.

Iniziamo dagli:

Archivi

Consideriamo gli archivi a prescindere dal contenuto. Può trattarsi, per macro categorie, di documenti contabili, contratti, atti e determine, verbali, registri, elaborati, fascicoli personali. All'interno di queste categorie si possono trovare diverse "informazioni riconducibili ad una persona fisica", quindi tutelate dal GDPR.

Fisicamente l'archivio in questione può essere composta da scatole, faldoni, fascicoli più o meno consultabili senza particolari sforzi o senza violare sigilli o chiusure. Questo comporta la necessità di **conservare questi archivi in locali adeguati**.

Si noti che abbiamo dato al termine "archivio" un accezione figurata (composto da scatole ecc…). Potevamo anche parlarne in termini più concreti, partendo direttamente dai locali (o in alcuni casi dai dispositivi) adibiti a tale scopo. L'archivio, in questo caso, si configurerebbe come "**il locale (o dispositivo) nel quale vengono conservati documenti** raccolti in scatole, faldoni, fascicoli".

In entrambi i casi i documenti che si riferiscono ad anni scolastici o di esercizio oltre quello in corso vanno conservati, se le norme ce lo impongono, in locali adeguati, cioè ad accesso controllato (chiusura a chiave). L'ideale sarebbe che fossero locali il cui utilizzo sia esclusivo, cioè non in condivisione con altre necessità: deposito materiali, laboratori, locali di passaggio. In caso ciò non fosse possibile aumenterebbero notevolmente tutti i fattori di rischio che il GDPR ci impone di ridurre.

Documenti con dati particolari ex articoli 9 e 10 GDPR

Per alcuni "archivi" (quelli con documenti relativi al personale, ad esempio) contenuti negli archivi, c'è inoltre la necessità di provvedere ad una conservazione in scatole chiuse. Questa modalità costringe ad adottare procedure di accesso tracciabile in caso di necessità.

Per rilevare gli archivi (locali o armadi) attualmente utilizzati useremo due tabelle tipo.

Tabella A1 (locali archivio)

Identificazione locale			
Ubicazione (plesso, piano)			
Come è segnato in planimetria?			
È dotato di serratura		Modalità di conservazione e utilizzo chiave	
Utilizzo esclusivo come archivio?	|__| SI |__| NO, altro utilizzo: _____		
Documenti conservati			
Tipologia	❑ 1) Amministrazione e bilancio ❑ 2) Personale ❑ 3) Alunni (esclusi alunni H, relazioni funzionali) ❑ 4) Atti e determine, contratti ❑ 5) Verbali e registri		
Anni (approssimativi)			
Documenti conservati separatamente	❑ 1) Amministrazione e bilancio ❑ 2) Personale ❑ 3) Alunni (esclusi alunni H, relazioni funzionali) ❑ 4) Atti e determine, contratti ❑ 5) Verbali e registri	❑ _____ ❑ _____ ❑ _____ ❑ _____ ❑ _____	

Tab_a1

Tabella A2 (armadi archivio)

Identificazione armadio			
Ubicazione (plesso, piano, locale)			
È dotato di serratura		Modalità di conservazione e utilizzo chiave	
Utilizzo esclusivo come archivio?	|__| SI |__| NO, altro utilizzo: _____		
Documenti conservati			
Tipologia	❑ 1) Amministrazione e bilancio ❑ 2) Personale ❑ 3) Alunni (esclusi alunni H, relazioni funzionali) ❑ 4) Atti e determine, contratti ❑ 5) Verbali e registri		
Anni (approssimativi)			

Tab_a2

Archivi correnti o anni più recenti

Locali di segreteria

La possibilità di conservare, oltre all'anno corrente, anche anni passati nei locali delle segreterie (a adiacenti, o nelle disponibilità) dipende da fattori strutturali o logistici, o da scelte organizzative (ad esempio i dati del personale in servizio si conservano sempre in segreteria e vengono spostati in archivio solo quelli relativi al personale dimesso o trasferito da almeno due anni), o da una combinazione di questi fattori.

Di base dovremmo adottare la misura di sicurezza di consentire l'accesso ai locali di segreteria la solo personale autorizzato e incaricato al trattamento. L'accesso da parte di estranei (personale di altre unità organizzative, alunni, famigliari, fornitori, visitatori) dovrà essere consentito solo in presenza di almeno un incaricato, applicando le misure di sicurezza logistiche adottate. Ad esempio ricevere qualcuno per un colloquio alla propria scrivania può non essere la scelta più sicura in quanto non si può escludere la visibilità di documenti, dati o informazioni.

I locali nei quali possono eventualmente accedere visitatori per colloqui o riunioni (ufficio del Dirigente, ufficio del D.s.g.a.) dovranno essere valutati in merito alla accessibilità alle informazioni durante la presenza di estranei. Possibilmente dovrà essere approntato un tavolo dedicato alle riunioni che non renda necessario ricevere alla scrivania i visitatori.

Inoltre eventuali necessità di consentire l'accesso agli uffici "personale" o "alunni" all'utenza o al personale per richieste, ritiro o consegna di documenti, dovranno comportare la valutazione delle migliori soluzioni al fine di non consentire ai visitatori l'accesso, anche solo visivo, o il contatto con documenti, tabelle, elaborati, fascicoli, contenenti informazioni o dati personali.

Ove ciò sia possibile dovrà essere utilizzata una delle seguenti modalità:

a) uno sportello attraverso il quale comunicare con l'utenza senza che sia necessario ammetterla all'ufficio;

b) dove non sia possibile la soluzione precedente, all'interno dell'ufficio un bancone che delimiti e divida l'area di lavoro da quella fino alla quale il visitatore può arrivare.

Inoltre sarà necessario organizzare un area di attesa non a ridosso dello sportello o del bancone e indicare a chi sta aspettando di non sostare nelle vicinanze di queste aree durante il colloquio di un altro visitatore.

Chiusura

Di norma i locali nei quali avvengono i trattamenti dovrebbero consentire la chiusura degli stessi in assenza di almeno un incaricato. Non intendiamo anche durante l'orario di lavoro, anche se alcune tipologie di trattamento, o la presenza di alcuni dispositivi, potrebbero renderlo necessario, ma almeno al termine dell'orario o a seguito di una assenza prolungata.

Non è infrequente che nei locali di segreteria siano posizionati, oltre ai Personal Computer utilizzati dagli impiegati, anche dispositivi quali Server, dischi di copia, apparati di rete, firewall, router, centralino telefonico, non contenuti in armadi idonei a preservarli dall'accesso da parte di estranei.

Questi apparati sono importanti per l'utilizzo del sistema informatico nel suo complesso e, quindi, per la disponibilità dei dati, e vanno tutelati in modo adeguato (si veda il capitolo relativo al server). L'ideale sarebbe che avessero un locale "tecnico" a loro disposizione ma non sempre questo è possibile.

Senz'altro vanno sottoposti a chiusura anche in caso di assenza breve e anche durante l'orario di lavoro, l'ufficio del Dirigente e l'ufficio del D.s.g.a.

I locali nei quali si effettuano i trattamenti dei dati di alunni e famiglie e quali nei quali si effettuano i trattamenti dei dati del personale possono, e nella maggior parte dei casi lo sono, essere separati. Tuttavia non è fondamentale adottare questa separazione mediante misure quali la non accessibilità fra diverse unità organizzative. Raramente le "sotto attività" di segreteria vengono svolte in modalità esclusiva da un gruppo di incaricati. È possibile, e a volte necessario, consentire l'accesso e lo scambio di informazioni al personale dei due settori, tanto è vero che viene data, e spesso usata, la possibilità di identificare una unica unità organizzativa alla quale attribuire la possibilità di operare indifferentemente su tutti i trattamenti.

Ai fini della chiusura, a meno che non si tratti di due locali completamente distinti e separati, li consideriamo un unico locale. Questo locale va reso inaccessibile al termine dell'orario di lavoro o in caso di assenza prolungata di tutti gli incaricati. Il personale ausiliario avrà sempre la possibilità di consentire l'accesso con la copia delle chiavi che ha in dotazione o alle quali ha comunque accesso per la propria funzione.

Conservazione e utilizzo di documenti

Utilizzo

Nei locali di segreteria e Direzione, nei locali a disposizione per la conservazione dei documenti correnti o delle annualità più recenti non ancora spostate in archivio, i documenti vengono conservati in dispositivi che possono o meno essere provvisti della possibilità di venire chiusi. Fra questi: armadi, classificatori a cartelle sospese, mobiletti ad ante, cassettiere.

Inoltre alcuni contenitori possono essere posizionati su scaffalature o mensole aperte.

Anche sulle scrivanie possono trovarsi documenti che non vengono riposti al termine dell'orario di lavoro, contenuti in faldoni, fascicoli o cartelle.

Il disciplinare tecnico allegato b) al D.L.196/03, il vecchio Codice in vigore fino al 19 settembre 2018, imponeva che i documenti contenenti dati sensibili (salute, inscrizione a sindacati per semplificare) venissero riposti al termine del loro utilizzo. Anche se è stata abolita questa specifica indicazione, il buonsenso ci fa dire la stessa cosa. Anzi, ce la dovrebbe fare estendere a tutti i documenti.

L'indicazione che dovrebbe essere data al personale è che non possono essere lasciati sulle scrivanie al termine dell'orario di lavoro documenti, anche contenuti in fascicoli, cartelle o faldoni. Tali documenti vanno riposti nei dispositivi che possono essere poi chiusi.

Questa potrebbe sembrare una misura eccessiva, soprattutto in quei casi nei quali sia stato possibile adottare la misura di chiudere a chiave gli uffici in caso di assenza o al termine dell'orario.

Concordiamo, ma ci permettiamo di sollevare due questioni:

a) alcuni documenti, e i dati che contengono, DEVONO essere tutelati in modo particolare;

b) non sappiamo se dopo che lasciamo l'ufficio qualcuno non debba, autorizzato, comunque accedervi.

Riporre tutti i documenti ci consentirà di non dovere andare a valutare caso per caso, con il rischio di non farlo correttamente.

Conservazione

I dispositivi, sia quelli dotati di chiusura di sicurezza sia quelli che ne sono privi, presenti nei locali di trattamento andranno inventariati, utilizzando la tabella A3.

Tabella A3 (dispositivi di conservazione)

Identificazione e tipologia dispositivo	❑ armadio _____ ante |_| scorrevoli |_| battente ❑ classificatore cartelle sospese _____ cassetti ❑ cassettiera _____ cassetti ❑ mobile _____ ante |_| scorrevoli |_| battente ❑ scaffalatura aperta ❑ mensola ❑ armadietto sospeso ❑ armadio tecnologico _____		
Ubicazione (plesso, piano, locale)			
È dotato di serratura		Modalità di conservazione e utilizzo chiave	
Utilizzo esclusivo come archivio?	|__| SI |__| NO, altro utilizzo: _____		
Documenti conservati			
Tipologia	❑ 1) Amministrazione e bilancio ❑ 2) Personale ❑ 3) Alunni (esclusi alunni H, relazioni funzionali) ❑ 4) Atti e determine, contratti ❑ 5) Verbali e registri ❑ 6) apparati tecnologici		
Anni (approssimativi)			

Tab_a3

Sulla base degli elementi contenuti nell'inventario (tipologia di documenti contenuti, posizione, possibilità di chiusura) andrà fatta la valutazione della necessità di modificare o sostituire alcuni dispositivi o modificarne la destinazione d'uso.

Distruzione

Dobbiamo distinguere fra:

1. distruzione controllata di intere raccolte di documenti;
2. eliminazione di documenti, o parti di essi in quanto non attuali, incompleti, non necessari.

Mentre il primo caso è un evento poco frequente e andrà affrontato lasciando traccia burocratica del materiale eliminato (di norma conferito in discarica per mezzo di smaltitori autorizzati), il secondo riguarda la quotidianità.

Di norma si può dire che i documenti cestinati devono prima essere resi illeggibili. Questo può avvenire in diverse modalità, a volte anche per mezzo di dispositivi meccanici, i c.d. distruggi documenti.

L'adozione di tali dispositivi non è obbligatoria, ma da valutare in caso di quantità importanti di documenti da eliminare frequentemente. Per la eliminazione, anche se frequente, di minori quantità è sufficiente impartire agli incaricati istruzioni in tal senso.

È anche sconsigliato il riutilizzo del retro di documenti dei quali non si sia valutato il contenuto.

Uso di stampanti e fotocopiatrici

Un elemento di rischio è costituito dalla possibilità di stampare documenti su una stampante che non sia nelle vicinanze del soggetto che stampa. In questo caso questo dispositivo dovrà essere inserito nell'inventario degli apparati informatici e il responsabile della protezione dati dovrà, unitamente all'amministratore di sistema, individuare le misure di sicurezza idonee a ridurre il rischio di accesso ai documenti da parte di altri soggetti.

Termini di conservazione dei documenti

Il GDPR impone di valutare costantemente la legittimità della conservazione dei documenti. Per questa materia il riferimento è costituito dal D.lgs. 42/2004 ai sensi del quale il Ministero per i Beni e le attività Culturali ha emanato:

1. Linee guida per gli archivi delle istituzioni scolastiche;
2. Piano di conservazione e scarto degli archivi delle istituzioni scolastiche;

che alleghiamo alle presenti linee guida.

Segreteria

Struttura informatica

I trattamenti da T1 a T8, come codificati in "Premessa", avvengono anche mediante l'utilizzo di procedure informatizzate.

La struttura informatica principale utilizzata per tali trattamenti è quella della segreteria.

Abbiamo già sviluppato alcune osservazioni nel capitolo relativo alla didattica, evidenziando come le due reti, appunto segreteria e didattica, debbano essere gestite come due entità distinte.

Il rispetto di questa suddivisione sarà il primo elemento oggetto di valutazione da parte dell'RPD.

Consideriamo, quindi, in questo capitolo, la sola struttura di segreteria al fine di valutarne gli elementi che ne caratterizzano la sicurezza. Alcuni applicativi, nello specifico il r**egistro elettronico**, consentono di essere utilizzati anche utilizzando altre infrastrutture (rete didattica) e, addirittura, accedendo da dispositivi non posizionati all'interno dell'Istituto.

Di questi aspetti tratteremo nel capitolo relativo all'autenticazione sulle piattaforme cosiddette "cloud".

L'amministratore di sistema

Con provvedimento emanato dal Garante per la protezione dei dati personali il 27 novembre 2008 (G.U. 300 del 24 dicembre 2008) è stato introdotto l'obbligo per i titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice, e successivamente del GDPR, di attribuire le funzioni di amministratore di sistema designando soggetti che per esperienza, capacità e affidabilità forniscano idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo relativo alla sicurezza.

Traducendo dal burocratese possiamo affermare che il sistema informatico utilizzato per gestire l'attività di un titolare deve essere conforme alle vigenti disposizioni in materia di sicurezza e che questa conformità deve essere garantita da operatori che forniscano idonee garanzie, cioè da operatori professionali.

In alcuni livelli di Istituti, secondari di secondo grado, queste professionalità si possono trovare in organico, a volte coprendo l'intera gamma di competenze richieste, altre volte parziale.

I vari elementi che compongono un sistema informatico possono avere necessità di competenze diverse:

- sicurezza dei dispositivi di collegamento da e verso il web;
- sicurezza interna attiva (antivirus, antimalware);
- copie o ridondanza;
- configurazione della struttura di accesso ai dati;
- accesso ad applicativi interni o esterni.

Il Garante stesso prevede che ci possa essere più di un amministratore di sistema, in alcuni casi il ruolo può essere assegnato anche per la sola gestione di un programma applicativo o di un dispositivo.

Quello che distingue un amministratore di sistema è la possibilità di intervenire sul dispositivo o sul programma di sua competenza con credenziali che gli consentano di operare senza limitazioni o con permessi maggiori rispetto ad un utente ordinario (attribuzioni di permessi, configurazione di nuovi utenti, disattivazione di utenti dimessi).

A volte l'amministratore di sistema opera da remoto sui sistemi dell'Istituto, più spesso direttamente sul sistema informatico dell'Istituto.

Sempre più spesso si verifica che i dati e i programmi non siano posizionati sui sistemi dell'Istituto. In questo caso il fornitore del servizio si configura in qualità di responsabile dei trattamenti ai sensi dell'articolo 28 del GDPR. È un ruolo diverso da quello dell'amministratore di sistema e non sarà oggetto di trattamento in questa sede. Tuttavia sarà necessario affidare ad un collaboratore interno il ruolo di amministrare alcuni aspetti di questi programmi, agendo con credenziali amministrative. Di volta in volta sarà necessario valutare l'opportunità di assegnare il ruolo a queste funzioni o, in alternativa, di limitarsi a incaricare il collaboratore di quella funzione.

Sarà cura del RPD tenere aggiornata una tabella nella quale siano riportati gli estremi e le competenze degli amministratori di sistema.

Amministratore	nominato il	competenza

Tab_a4

Amministratore di sistema principale

In questa fase ci occupiamo del ruolo di amministratore del sistema **PRINCIPALE** nella sua accezione più classica: **gestore dell'insieme dei dispositivi ai quali gli operatori accedono per svolgere il proprio lavoro**.

In alcuni casi si può trattare di un team ma il provvedimento del Garante citato parla espressamente di nomina individuale, quindi, all'interno del team, ci si riferirà all'incaricato con compiti di coordinamento. In un caso come questo, nelle nomine sarà necessario indicare eventuali gerarchie o ruoli subordinati.

La struttura del sistema informatico

Quello che noi vediamo quando entriamo in una segreteria è un insieme di personal computer, PC (non mi risulta ci siano segreterie di soli Apple), dai quali è possibile, con modalità diverse:

- accedere a documenti (testi e tabelle);
- leggere ed inviare posta elettronica;
- accedere a portali o applicativi web;
- accedere ad applicativi e dati installati all'interno della struttura dell'Istituto.

Ognuno di questi PC è collegato al medesimo sistema, tranne casi molto specifici di PC che svolgono funzioni limitate, e questo rende possibile condividere documenti o dati fra diversi operatori, secondo uno schema di livelli di permessi impostato dal Dirigente o dal D.s.g.a. a seconda delle mansioni e delle necessità operative.

Queste modalità operative sono rese possibili dalla progettazione e dalla configurazione di un sistema cosiddetto "di rete", nel quale i PC sono fisicamente collegati tramite cavo, raramente tramite wi-fi, e gestiti da un sistema operativo di tipo "server" opportunamente configurato.

Ogni volta che si inserisce o si modifica un elemento di questa rete, sia un PC che un operatore o un programma, si deve tenere conto della sua compatibilità con la struttura nel suo complesso.

L'amministratore di sistema al quale è affidato questo compito dovrà rendere disponibili i seguenti elementi:

a) inventario dei dispositivi che compongono la rete:

server fisico	IP	nome	sistema operativo	caratteristiche fisiche
server virtuali	IP	nome	sistema operativo	ruoli
router	IP	caratteristiche		
firewall	IP	caratteristiche	ruoli	
Domain controller	nome completo	amministratore		
PC collegati a dominio	(elenco)	Software speciali installati		
PC non collegati a dominio	(elenco e ruoli)			
Dispositivi di rete	(elenco con IP) (NAS, stampanti,	Credenziali di aaccesso		

Anche access point	switch, ecc)	amministrativo		
Software in dotazione a server				
Software in dotazione ai PC				
Antivirus o altre sicurezze	Centralizzati (gestiti da server) S/N			

Tab_a5_1

b) descrizione del sistema di copia. Per ogni processo:

dati copiati	Software	frequenza	rotazione	tipo supporto e posizione

Tab_a5_2

Le copie di sicurezza assolvono principalmente a due scopi:

consentire di recuperare uno o più documenti (necessità di avere più versioni dello stesso documento, anche in tempi diversi);

ripristinare lo stato di un dispositivo alla situazione più recente possibile (caso di guasto)

il bilanciamento fra queste necessità dovrà portare alla scelta di uno o più sistemi che possano agire in tempi e con modalità diverse.

I sistemi di ridondanza dei dischi in un sistema server riducono l'incidenza del fattore "guasto" e consentono, il più delle volte, la continuità del servizio, ma da soli non bastano.

Una copia su un supporto esterno riduce anche il rischio di guasti ad elementi particolari del server, quali controller raid, memoria, processore. La conservazione in un locale diverso da quello in cui è conservato il server riduce notevolmente l'incidenza del rischio di danno ambientale o furto. Ancora meglio, ma da valutare in base alle risorse non solo economiche, la conservazione presso una struttura esterna, tipo server farm o centro servizi.

Ricordiamo che in un sistema virtualizzato il sistema di copia può sfruttare alcuni vantaggi dovuti al tipo di struttura logica sul quale è impostata la virtualizzazione.

c) check list delle misure di sicurezza

c.1) server e DC

tutte le credenziali di accesso amministrativo ad ogni elemento del sistema informatico DEVONO essere nelle disponibilità del titolare che ne curerà la conservazione e l'aggiornamento con la collaborazione degli amministratori di sistema. Le credenziali dell'utenza di Active Directory DEVONO essere nominali o, se identificano un ruolo, devono essere usate da un solo operatore e non rassegnate ad altri successivamente.

in caso di virtualizzazione è stata consegnata al titolare la credenziale di accesso al sistema Hyper-v o VMWare	S/N
viene gestito, e consegnato al titolare, un elenco degli utenti di Active Directory (AD) con permessi amministrativi	S/N

in caso di utenti sia operatori che con funzioni amministrative è stato assegnata una credenziale diversa	S/N
le policy di sicurezza per gli utenti di AD devono essere almeno le seguenti	
credenziale nominale	non ripetibile, disattivata in caso di cambio operatore
Prima password	Cambio immediato imposto
Lunghezza minima password	8
controllo complessità	almeno 3 elementi
non ripetibile	Valore massimo consentito
Durata	90 giorni
blocco utente	Dopo 5 tentativi e sblocco a cura dell'amministratore o dopo 10 minuti

Tab_a5_3

c.2) Condivisione dati su server

ogni operatore deve avere a disposizione sul server una struttura di cartelle nella quale posizionare e trovare i documenti da lui o da altri prodotti, secondo la propria mansione e le proprie competenze.

Può essere utile alla condivisione dei documenti la creazione di gruppi omogenei per settore (didattica, personale, bilancio).

In uno schema tipo l'operatore dovrà avere a disposizione:

- una cartella propria (da usare in luogo del desktop)
- una cartella condivisa con il gruppo di appartenenza
- una cartella condivisa con tutti (gruppo scuola, oppure segreteria, ma non "everyone")

inoltre si possono creare condivisioni per ruoli o funzioni, tipo Dirigente + D.s.g.a. o altro

Gli utenti sono suddivisi in gruppi S/N			
Gruppo	Utenti	utenti	utenti
Gruppo	Utenti	utenti	utenti

È stato configurato un gruppo "generale" (così da non usare "everyone" nei permessi			S/N
È prevista una cartella con accessi riservati al solo utente			S/N
È prevista una cartella con accessi riservati al gruppo			S/N
È prevista una cartella con accessi riservati al gruppo generale			S/N

Tab_a5_4

c.3) PC a dominio

sono quelle postazioni dalle quali ogni operatore può accedere alle risorse condivise e ai programmi installati sul server. La postazione non è, di norma, vincolata ad un singolo operatore il quale, all'accensione, vede proposto il nominativo dell'ultimo incaricato che ha utilizzato quella risorsa.

Ogni operatore che utilizza una determinata risorsa disporrà di un profilo (desktop, menù programmi, preferiti) proprio e non potrà accedere ai dati utilizzati da un diverso operatore sullo stesso PC.

Se sul PC viene installato un particolare software in uso ad un operatore, questi, se utilizzerà un PC diverso, non troverà a disposizione tale programma, a meno che non sia stato installato sul server (da valutare da parte dell'amministratore di sistema la possibilità).

Per ogni PC andrà compilata la seguente tabella

Codice o nome PC	
È stato mantenuto un utente locale per accesso di emergenza fuori da dominio	S/N
Con password conforme alle policy di sicurezza (vedi)	S/N
È stato disattivata la possibilità di installare programmi o cambiare impostazioni (utente di dominio non amministratore del PC)	S/N
Sono stati disattivati i drive di input (USB, CD/DVD)	S/N
Installato software locale ? Quale	S/N
Sono presenti archivi o documenti locali?	S/N
Se SI, sono copiati su server o su altri supporti, con quali modalità	S/N

Tab_a5_5

c.4) PC fuori dominio (elenco)

può essere necessario utilizzare uno o più dispositivi per funzioni particolari senza che da queste postazioni sia necessario collegarsi ai documenti sul server (raccolta timbrature, ad esempio) anche se è possibile che siano collegati alla rete per sfruttare la connessione web..

L'accesso degli utenti a questi dispositivi non sarà sottoposto al controllo del server (funzione AD) ma alle definizioni di utenti locali, secondo le necessità. Queste caratteristiche devono essere riportate

Codice o nome PC	
Rete S/N se si IP	Funzione
Utente di accesso	password consegnata al titolare S/N
Contiene archivi o documenti S/N	Se Sì è attivo un backup dei dati S/N
Collegato a internet S/N	antivirus S/N

Tab_a5_6

c.5) elenco dei software di propria competenza

All'amministratore di sistema può competere la gestione di alcuni software, quali l'antivirus ad esempio, il cui accesso è sottoposto alla conoscenza delle credenziali amministrative. Ad alcuni di questi software è possibile che sia necessario concedere l'accesso ad altri utenti o che l'installazione richieda configurazioni particolari.

Nome	accesso amministrativo user+pwd	accessi per utente S/N
su server S/N	accesso client S/N	su dispositivo locale S/N quale

Tab_a5_7

L'amministratore di sistema, che abbiamo definito "principale", collaborerà inoltre con il RDP per:

- verificare la conformità delle misure adottate con quanto contenuto nelle indicazioni emanate dall'AgID il 18/4/2017
- aggiornarne le tabelle applicabili a livello M: CSC1, CSC2, CSC3, CSC4, CSC5, CSC8, CSC10, CSC13.

Altri amministratori di sistema

Apparati tecnici o software specifici

Alcuni apparati possono essere dati in gestione a imprese esterne, oppure può essere necessario acquistare un servizio che preveda l'installazione di apparati presso l'Istituto, e che a questi apparati sia necessario consentire l'accesso al personale della ditta fornitrice.

Quando non si rende necessario che i dati siano posizionati sui loro sistemi (nel qual caso si avrebbe il ruolo di responsabile dei trattamenti esterni) si dovrà optare per l'inquadramento nel ruolo di amministratore di sistema.

In questo caso il RPD chiederà le informazioni necessarie a rilevare le caratteristiche del dispositivo o del software, redigendo una scheda identificativa all'aggiornamento della quale verrà chiesto, periodicamente, il contributo dell'amministratore stesso.

Amministratore di sistema	
Ambito di competenza	
Dispositivo o software-archivi	
luogo di posizionamento	
credenziali di accesso consegnate al titolare	S/N
Note	

Tab_a6

Funzioni strumentali

Alcune attività possono prevedere che venga utilizzata una piattaforma per gestire l'accesso al contenuto da parte degli operatori. Si può trattare di software (registro elettronico, protocollo), di piattaforme di condivisione, di aree ad accesso limitato all'interno di altre piattaforme (area riservata di sito web), di attivazione di utenti all'uso di determinati apparati (captive portal).

Il ruolo di amministrare queste aree o alcune funzioni di alcuni programmi (autorizzare o revocare docenti nel registro, ad esempio), di norma viene dato ad incaricati che ricoprono altri ruoli, anche in altre unità organizzative rispetto alla segreteria. Raramente viene incaricato un amministratore di sistema esterno.

Le credenziali saranno definite e gestite dal titolare dei trattamenti

È necessario redigere una tabella per l'identificazione degli assegnamenti di questi ruoli.

Funzione	
Addetto	
Data inizio	
Data termine	
Credenziale di accesso	
Note	

Tab_a7

Programmi

Interni

Le impostazioni di controllo degli accessi al sistema fino ad ora descritte hanno consentito di controllare gli incaricati autorizzati ad accedere ai documenti o ad alcuni dispositivi. Per accedere ai dati è necessario utilizzare appositi programmi. A volte questi programmi sono installati sui PC o sul server della segreteria e gli archivi di conseguenza.

Ai dati contenuti negli archivi si può accedere solo utilizzando l'apposito programma al quale si può a sua volta accedere utilizzando credenziali che identifichino l'incaricato, abbinandolo ad un profilo operativo che lo metta in condizione di operare con i permessi stabiliti dal titolare per il suo ruolo.

Per ogni programma installato sui sistemi interni è necessario rilevare le seguenti informazioni:

nome del programma	
finalità	
Posizionamento programma	Server o PC client _____
posizionamento archivi	server o PC client _____
utente amministrativo	
password	
operatore autorizzato credenziali amministrative	
Procedura di back up (*)	

Tab_a8

(*) In caso gli archivi siano posizionati sul client sul quale è installato il programma dovrà essere definita una procedura di back up degli stessi.

L'utente amministrativo può configurare altri utenti che possono accedere al programma con normali funzioni operative definite dal programma stesso mediante l'abbinamento con profili operativi ai quali viene permessa l'operatività compatibile con la mansione.

Cloud

Le attuali procedure possono prevedere l'utilizzo di programmi accessibili su portali web esterni mediante browser. Le modalità di gestione non sono diverse da quelle previste per i programmi installati sui sistemi interni. La differenza risiede nel posizionamento sia del programma che degli archivi.

Di norma non è necessario installare localmente sui PC della segreteria programmi di gestione. Qualche applicativo prevede il posizionamento da parte del fornitore di dispositivi di raccolta dati che gestiscono una fase transitoria di raccolta documenti in ingresso (email, fax virtuali) che poi vengono gestiti dal sistema di protocollazione e inseriti nel sistema cloud.

In questa categoria rientrano i programmi per la gestione del registro elettronico e il protocollo o segreteria digitale.

La particolarità di questi programmi consiste nella loro utilizzabilità sia dall'interno della rete d'Istituto che dall'esterno. Alcuni prevedono la possibilità di limitare l'accesso, oltre che alle credenziali autorizzate, solo da determinate reti o solo in determinate fasce orarie.

È necessario rilevare se i programmi consentono controlli di accesso basati su molteplici fattori al fine di determinare consapevolmente le modalità di limitazione dell'utilizzo che, tradotte in pratica, determinano l'effettiva riduzione del rischio di accesso non autorizzato imposta dal GDPR.

È anche necessario rilevare se il software è in grado di controllare il corretto utilizzo delle credenziali di autenticazione: obbligo di modifica al primo accesso, controllo degli elementi di complessità, procedura di recupero password automatica.

È quindi necessario compilare la seguente tabella:

nome del software	
casa produttrice	
Nominato responsabile esterno	In data
Conservatore digitale (nome altra società e data nomina)	
Ambito operativo (registro, segreteria, protocollo)	
consente la limitazione dell'accesso da determinati IP pubblici	
consente la determinazione di giorni e orari di utilizzabilità	
Consente di imporre il cambio della password al primo accesso	
Consente la gestione delle credenziali di autenticazione (lunghezza, durata, complessità, scadenza)	
Consente di recuperare la password senza l'intervento dell'amministratore	

Consente di stampare o estrarre un elenco degli utenti per profilo operativo	
Consente di produrre una pagina di istruzioni personalizzate al momento di assegnazione di una credenziale (ATA, docenti, genitori, alunni)	
Consente di assegnare solo a determinati operatori o profili la possibilità di pubblicare sul sito determinati atti o documenti	

credenziale amministrativa	
Password	
ruolo assegnato a (vedi tab_a7)	

credenziale amministrativa	
Password	
ruolo assegnato a (vedi tab_a7)	

Tab_a9

Per che svolge funzioni amministrative di autorizzazione degli operatori è necessario, da parte del Dirigente, determinare le modalità di attivazione e disattivazione delle utenze. La trasmissione delle modalità operative stabilite è a discrezione del Dirigente ai sensi dell'articolo 2-quaterdieces del D.Lgs.196/03

--

Linee guida per la valutazione e l'applicazione delle misure di sicurezza per il corretto trattamento dei dati personali

Revisione 18_11_01 del 20/11/2018

Le presenti linee guida sono soggette a revisione periodica da parte del responsabile della protezione dati, sentiti i pareri e le indicazioni da parte delle dirigenza d'Istituto, degli amministratori di sistema, delle funzioni strumentali preposte alla gestione di parti di trattamento.

Le tabelle citate in testo verranno fornite separatamente corredate dalle istruzioni per la compilazione.

Vengono allegati alle presenti linee guida:

circolare AGID 17 marzo 2017 nr.1/2017 e suoi allegati

linee guida per la conservazione e lo scarto della Direzione generale Archivi