# MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO

## *ALLEGATO 12*
## *PIANO SULLA SICUREZZA*

# Sommario

## Riferimenti normativi

Riportiamo le seguenti normative di riferimento per il servizio in oggetto:

- Misure minime di sicurezza ICT per le PA (Circolare n. 2/2017 del 18/04/2017)
- Regolamento europeo in materia di protezione dei dati personali (GDPR) 2016/679.
- AGID - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

## Definizioni

Il Decreto legislativo 10 agosto 2018, n. 101 adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679 (GDPR)

***trattamento di dati***:

si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4 GDPR);

***dati personali:***

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

***profilazione:***

qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

***pseudonimizzazione:***

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

***dati particolari (sensibili)*** :

dati personali idonei a rivelare l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;

***dati giudiziari***:

rivelano l'esistenza di provvedimenti penali suscettibili di iscrizione nel casellario giudiziale, oppure la qualità di indagato o imputato. Tali tipi di dati - una volta definiti dati sensibili - oggi rientrano nella categoria dei dati a trattamento speciale (ex art. 9 GDPR). Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

***responsabile del trattamento»:***

persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento e in base alle sue istruzioni (art. 4, par. 1, n. 8 GDPR).

***autorizzato al trattamento:***

Il Regolamento europeo non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4, n. 10 GDPR).

***Addetti alla custodia delle parole chiave:*** persone incaricate della custodia delle parole chiave di accesso ad informazioni o di accedere alle stesse.

***Amministratore di sistema (ADS):***

Il Regolamento europeo (GDPR) non prevede espressamente la figura dell'amministratore di sistema, la cui definizione si riscontra, invece, nei provvedimenti del Garante italiano. in ambito informatico, la figura professionale finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, facendo però rientrare in essa anche le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

***Incaricati della manutenzione***: persone addette alla manutenzione dell'hardware, del software applicativo e del software di base degli elaboratori sui quali sono memorizzati i dati personali.

***PDL:*** postazione di lavoro.

***HOST – Server :*** con HOST si identificano le macchine fisiche che ospitano i Server, ovvero le macchine virtuali che svolgono funzioni informatiche od ospitano gli applicativi software.

***POS :*** i POS sono le postazioni di pagamento del servizio di ristorazione, i TOTEM sono postazioni che permettono al cliente di utilizzare alcuni servizi on-line relativi al servizio di ristorazione.

***ESUNET :*** è la rete di trasmissione dati, privata, che l'ESU utilizza per interconnettere le proprie strutture e quelle che erogano servizi in convenzione.

***SIE :*** Sistema di gestione informatica dei servizi erogati dall'ESU.

***ESAM :*** sistema di gestione informatica delle attività amministrative/contabili dell'ESU.

***SPORTELLO STUDENTE:*** sistema di gestione informatica dei servizi online per il diritto allo studio

***SLA :*** Service_level_agreement - consiste in un contratto che assicura la fornitura dei servizi a livelli pre-negoziati e comporta il pagamento di penalità in caso di mancato raggiungimento di tali livelli.

## Oggetto

Il presente documento riporta le misure organizzative e tecnologiche riferite alla sicurezza messe in atto o da adottare a cura del Titolare e relative alla formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

## Sistema di autenticazione informatica

**Sistema di Identity e Access Management**

1. E' attivo un sistema di "*Identity and Access Management*" (IAM) basato su un servizio di Directory Service (LDAP) che raccoglie la globalità delle utenze .
   Il sistema di *Identity* consente di gestire in maniera integrata il processo di *provisioning* delle utenze (creazione, modifica, sospensione e rimozione), nonché la funzione di autenticazione ed Autorizzazione.
   Il servizio di *directory realizza* le funzioni di "autenticazione" e di "profilatura" necessarie all'accesso ai servizi di Dominio (stampa, archivi).
   Per gli utenti già autenticati a livello di dominio, esiste un secondo livello di autorizzazione gestito a livello applicativo basato sulla profilatura delle risorse e dei diritti di accesso ai dati
   I gestionali verticali della piattaforma ESAM utilizzano l'autenticazione integrata con LDAP. Il sistema di messaggistica, collaborazione e condivisione, basato sulla piattaforma Google Workspace, utilizza un meccanismo di profilazione ed autenticazione proprietario interno.

2. L'identificazione dell'incaricato si basa su un primo codice –userid- e l'autenticazione su un secondo codice – password - .
   Le procedure di cassa nelle strutture di ristorazione prevedono l'identificazione e l'autenticazione dell'incaricato tramite tessera MIFIRE+

3. Ad ogni incaricato sono assegnate più credenziali: una per l'utilizzo dei servizi di dominio di rete, una per l'accesso alla piattaforma di messaggistica e collaborazione ed eventuali altre per accedere a specifici applicativi con i quali è incaricato di trattare i dati.

4. L'incaricato deve attivare tutte le cautele per mantenere la segretezza della password e custodire i dispositivi (pc, portatili, smart-phone, ecc.) utilizzati.
   Deve fare la stessa attenzione quando usa le proprie credenziali su dispositivi che non sono la propria PDL in azienda o che sono connessi ai servizi dell'Azienda attraverso una rete di comunicazione diversa da ESUNET (es.: rete cellulare, rete di casa).
   Per motivi di manutenzione o per nuove installazione l'Uff. IT può cancellare la password dell'incaricato previo suo assenso ed entrare con proprie credenziali. Successivamente l'Uff. IT dovrà avvisare l'incaricato di cambiare la propria password.
   Nel caso in cui l'incaricato smarrisse la Password deve chiedere all'Uff. IT di annullarla ed inserire immediatamente una nuovo codice.

5. Viene configurato il Sistema di Identity e Access Management LDAP in modo che ogni incaricato sia obbligato a cambiare password al primo accesso e successivamente ogni 90 giorni ed usare codici di almeno 16 caratteri alfanumerici in cui devono essere presenti almeno una maiuscola un numero un carattere speciale; la parola chiave deve essere diversa dalle ultime 5 utilizzate e non deve contenere nome e/o cognome o parti di esso dell'utente;

6. L'associazione tra 'codice di identificazione' e 'persona fisica' una volta avvenuta non può più essere annullata (il 'codice di identificazione' non deve mai essere assegnato a persone diverse);

7. Le credenziali non utilizzate per 6 mesi vengono disattivate salvo quelle utilizzate per gestioni tecniche.

8. Le credenziali di identificazione assegnate a utenti per i quali vien meno l'incarico al trattamento del dato (es: dimissioni) vengono disattivate entro un mese dall'evento;

9. Ogni incaricato deve attivare il blocco della sessione di lavoro sulla propria postazione di Lavoro PDL (attivando lo screen-saver) quando si allontana da essa;

10. Se l'accesso a dispositivi e/o dati richiede l'utilizzo del codice di autenticazione ed è necessario che venga utilizzato da più incaricati, devono essere emanate per iscritto dal Titolare le disposizioni secondo cui il Titolare rende disponibile il dispositivo ed i dati per interventi indifferibili per esclusive necessità operative e di sicurezza; devono essere individuati per iscritto i soggetti incaricati della custodia del codice di autenticazione e devono essere documentati i trattamenti svolti.

11. Il trattamento di dati personali destinati alla diffusione non richiede l'applicazione delle prescrizioni sopra dette.

## Sistema di autorizzazione

12. Gli incaricati possono avere profili di autorizzazione diversi in ambiti diversi. Sono usati sistemi di autorizzazione per ambito (es.: sono gestiti profili dal SIE, dall'ESAM, dall'Active Directory (gestione dei servizi in rete, proprio pc compreso), dalla piattaforma di collaborazione).

13. Ad ogni incaricato vengono assegnati i profili di autorizzazione al trattamento contemporaneamente all'attribuzione delle credenziali.

14. Annualmente viene verificato se l'incaricato è nelle condizioni per mantenere i profili di autorizzazione assegnati.

## Altre misure di sicurezza

15. L'incaricato deve chiedere le autorizzazioni indispensabili per svolgere le attività a cui è preposto e che l'attività in rete della propria PDL sia ristretta al massimo alle funzioni che interessano.

## Antiintrusione e Sistema antivirus ed antispam

16. Controllo dei servizi accessibili da remoto**:** sui *server* sono attivi i servizi di rete strettamente necessari. Il personale addetto provvede alla regolare verifica dei servizi accessibili via rete (servizi in ascolto su porte prestabilite), procedendo alla disattivazione dei servizi non strettamente necessari.

    Il sistema di firewalling realizzato consente di collegare reti diverse caratterizzate da servizi di rilevanza e affidabilità diversa e di filtrare il traffico di rete consentendo o inibendo la comunicazione in base ai protocolli usati, alla provenienza e/o destinazione. Alcune reti (zone) collegate al firewall sono:

- internet
- DMZ – zona di frontiera (detta area demilitarizzata)
- rete servizi esterni (alla sede ESU)
- rete servizi convenzionati
- rete server
- …..

Il sistema è costituito da più dispositivi fisici: firewall, router e proxy.
In caso di incidente di sicurezza intervenendo opportunamente sulle regole che governano il traffico (Access Control List) caricate a bordo dei dispositivi sopra citati, si può contrastare il coinvolgimento dell'intera infrastruttura di rete isolando per il tempo necessario le aree che richiedono interventi di bonifica.

Parte del sistema di firewalling utilizza hardware in alta affidabilità (ridondato in configurazione fail-over).
I firewall sono monitorati e configurati solo dal personale addetto.

Le varie reti utilizzano connessioni ridondate al firewall nel caso di servizi critici (per es: zona server).

Segregazione delle Reti (Virtual Local Area Network VLAN)

Sfruttando le funzionalità degli apparati di rete (switch) sono state realizzate delle reti virtuali locali (VLAN) che consentono di raggruppare e confinare il traffico dei dispositivi che fisicamente condividono lo stesso mezzo trasmissivo, virtualmente come se fossero appartenenti a reti distinte e separate.
Tale tecnica è stata utilizzata in sede ESU per gestire le connessioni di switch senza interruzione della LAN e per realizzare più LAN usando un solo switch.
In questo modo sono associate alla stessa VLAN macchine connesse a switch diversi che a loro volta sono connessi in dorsale ottica. Con gli stessi switch sono gestite, inoltre, VLAN diverse a supporto di servizi diversi.

Proxy

L'accesso ai servizi pubblicati su Internet avviene attraverso un reverse proxy per gestire in modo agile il cambiamento dei server e aumentare la sicurezza dei server.

Per i servizi accessibili dalla rete Internet la soluzione architetturale adottata prevede l'aggregazione di server con funzioni analoghe (Web Server, Application Server e Data Base Server) sulla stessa rete.
L'accesso ai *server* e dispositivi critici è consentito attraverso l'utilizzo di protocolli sicuri quali SSL, SSH e HTTPS, ovvero tramite la realizzazione di tunnel VPN/IPSEC.

Le reti VPN (Virtual Private Network)

Vengono usate connessioni VPN tra client periferici e il firewall dell'Azienda, VPN "Client to Site" o tra il firewall dell'Azienda ed i firewall di terze parti, VPN "Site to Site.

L'impiego dei collegamenti VPN riguardano prevalentemente l'accesso alla rete aziendale da parte di:

A. fornitori di servizi di gestione e manutenzione;
B. personale in mobilità che accede da Internet a servizi del sistema informativo;
C. soggetti esterni che interagiscono con servizi erogati dall'Azienda.

I dispositivi di networking che consentono la realizzazione dei collegamenti VPN sono apparati ridondati in configurazione ad alta affidabilità, gestiti da personale incaricato.
Il collegamento alla rete ESUNET del personale in mobilità che deve accedere a risorse condivise quali cartelle di rete, stampanti ecc. avviene esclusivamente tramite assegnazione di PDL mobili di proprietà dell'Ente configurate opportunamente per consentire la navigazione in internet solamente dopo l'accesso tramite VPN alla rete aziendale (navigazione in modo controllato dal firewall).

Sulle PDL e sui server è attivo un sistema antivirus con aggiornamento automatico del motore di scansione/analisi e del DB delle minacce. L'antivirus lavora a livello di macchina sui dati che vengono letti o scritti su disco. Il monitoraggio dell'operatività dell'antivirus e delle *detections* avviene in modalità centralizzata dalla specifica console di amministrazione. Le *detections* vengono gestite automaticamente in base alla policy impostata dall'operatore in modo personalizzato per le diverse tipologie di device.
I responsabili IT verificano che l'antivirus sia presente ed aggiornato sul dispositivo prima della consegna all'utilizzatore. L'antivirus e le varie policies di protezione della PDL possono essere modificate/abilitate/disabilitate esclusivamente da utenti con privilegio di amministratore.
Al variare degli strumenti informatici e/o delle possibilità del loro uso dovrà essere definita la politica comportamentale d'uso di tali strumenti.

Attualmente la gestione dello spam nelle comunicazioni mail PEO e la scansione di sicurezza delle stesse in ingresso/uscita è integrata nella piattaforma di comunicazione/collaborazione utilizzata Google Workspace. Tale piattaforma garantisce anche la scansione di sicurezza sul contenuto dati letto/scritto nel file server in cloud Google Drive. Per quanto riguarda il filtro spam e la scansione di sicurezza delle comunicazioni mail PEC viene implementata e gestita dal fornitore del servizio stesso.

## Aggiornamento del software installato

17. Il personale incaricato provvede direttamente o attraverso ditta terza, all'aggiornamento periodico, del software di sistema degli host e dei server mediante l'installazione di: nuove release, service pack, patch, suggerite dal produttore, nonché le hotfix di sicurezza per eliminare le vulnerabilità individuate e/o note e correggere difetti. Gli hosts e lo storage sono periodicamente monitorati per attività proattive di manutenzione.
    L'incaricato deve evitare la condivisione in rete di documenti che stanno sulla propria PDL e utilizzare le aree di lavoro comune rese disponibile su file-server.

## Sistema di back-up

**18.** La politica di salvataggio adottata consiste nell'effettuare le seguenti tipologie di backup:

- backup integrale (full backup): salvataggio di tutti i dati, file di sistema e software presenti sul sistema;
- backup incrementale (incremental backup): salvataggio delle modifiche intervenute dopo l'ultimo full backup.

I backup usano uno storage presente nella sala-server on-prem.
Le operazioni di salvataggio sono effettuate in automatico e controllate da personale incaricato.
Gli incaricati devono copiare i documenti da conservare, presenti nella loro PDL, in aree personali o comuni presenti su un file-server della server-room.
Le postazioni POS gestiscono tramite lo specifico software di cassa il salvataggio dei dati per il funzionamento off-line della POS e l'allineamento del DB con quello centralizzato in Cloud del fornitore al ritorno on-line; non è previsto che memorizzino altri dati localmente.

## Ulteriori misure per il trattamento di dati particolari o giudiziari

**19.** I trattamenti dei dati particolari e giudiziari devono essere realizzati sui servers e sulle PDL degli Uffici che li trattano.
**20.** I dati particolari e giudiziari non devono stare su supporti removibili. Nel caso fosse indispensabili devono essere raccolti in file chiusi con password di lettura e modifica.
**21.** I supporti removibili devono essere distrutti fisicamente quando non più utilizzati.
**22.** In caso di danneggiamento del dato, viene recuperata la informazione come presente nel back-up (con la disponibilità stabilita nella 'politica' di back-up) ed in tempi inferiori ai sette giorni. Il Responsabile del trattamento lo deve richiedere per iscritto all'incaricato preposto;
Per i dispositivi hardware che costituiscono il CED on-prem sono previsti specifici contratti di assistenza e manutenzione con SLA definite che permettono il ripristino dell'operatività in tempi ridotti.

## Sistema di Disaster Recovery

23. Il back-up dei dati viene salvato anche in un secondo luogo diverso dalla sede dell'E.S.U.

## Misure di tutela e garanzia

**24.** Per l'esecuzione dei punti sopra descritti, il Titolare si avvale di ditte esterne alla propria struttura alle quali richiede una descrizione scritta dell'intervento.