ALLEGATO 2

REGOLE COMPORTAMENTALI PER L'UTILIZZO DI APPARECCHIATURE TELEMATICHE DA PARTE DEI DIPENDENTI

Sommario

1. Contesto di riferimento

La tecnologia impiegata dall'Azienda Socio Sanitaria Territoriale Lariana (d'ora in poi ASST Lariana) nelle proprie attività di servizio alla collettività è diventata complessa e richiede che il comportamento dei dipendenti sia reso coerente con un suo uso corretto ed efficiente.
Le statistiche internazionali, peraltro, dimostrano che la maggior parte degli incidenti informatici sono dovuti a comportamenti non corretti, per lo più involontari, da parte dei lavoratori.
È necessario, dunque, che i dipendenti raggiungano una consapevolezza che serva a limitare i rischi, di qualsiasi natura, per l'Ente e per i soggetti che con essa hanno rapporti.

2. Principi

I principi che ispirano il presente documento sono contenuti:

- nel Regolamento UE 2016/679 – Regolamento generale sulla protezione dei dati (GDPR);
- nell'art. 2104 del Codice Civile;
- nel DPR 62/2013 - Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165 (Codice di comportamento);
- Contratto Collettivo Nazionale di Lavoro relativo al personale del comparto Sanità - Triennio 2019-2021 (CCNL).

GDPR

L'art. 5 del GDPR riporta alcuni principi ai quali deve ispirarsi il trattamento dei dati personali, cioè ogni informazione riferita ad una persona fisica identificata o identificabile. Si richiamano, tra gli altri, ai fini del presente documento i seguenti principi:

- *esattezza ed aggiornamento* – ogni informazione che riguardi una persona fisica deve corrispondere alla realtà che rappresenta in quel momento;
- *minimizzazione della conservazione* – i dati personali non possono essere conservati oltre il tempo necessario al raggiungimento delle finalità per le quali sono trattati; una volta raggiunta la finalità, non si possono conservare dati personali solo per potenziali richieste di terzi o *comodità personali* (vedi considerando n. 64 del GDPR);
- *sicurezza* – i dati personali devono essere preservati da accessi di soggetti non autorizzati, da modifiche di persone non autorizzate e da perdite (accidentali o volontarie).

Codice Civile

L'art. 2104 del Codice Civile obbliga il lavoratore a "usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale".

Codice di comportamento

Il Codice di comportamento tra i principi generali dell'art. 3, riporta l'obbligo dei dipendenti di evitare "situazioni e comportamenti che possano ostacolare il corretto adempimento dei compiti o nuocere agli interessi o all'immagine della pubblica amministrazione".

Questo significa che il comportamento dei dipendenti dell'ASST Lariana deve essere ispirato a tutelare gli interessi dei cittadini e gli interessi dell'amministrazione di appartenenza, finalizzando a questo, e non ad altro, l'uso di strumenti di lavoro.

Contratto

L'art. 83 (comma 3 punto j) del CCNL fissa, tra gli obblighi del dipendente dell'ASST Lariana, quello di "avere cura dei locali, mobili, oggetti, macchinari, attrezzi, strumenti ed automezzi a lui affidati". Esiste, quindi, un principio di "corretto uso" della strumentazione in dotazione al dipendente che si differenzia dai principi più generali del GDPR e del Codice di comportamento perché è più orientato alla concreta correttezza dei gesti quotidiani dall'accensione della postazione di lavoro, la mattina, al suo spegnimento, a fine giornata.

3. Obiettivi

Il primo obiettivo di questo documento è indicare ai dipendenti ed ai collaboratori che, a vario titolo, operano all'interno dell'ASST Lariana:

- "cosa è possibile fare" (i comportamenti saranno indicati con l'icona );
- "cosa si deve fare" (i comportamenti saranno indicati con l'icona );
- "cosa non è possibile fare" (i comportamenti saranno indicati con l'icona ).

Inoltre, il documento esplicita:

- quali sono i controlli che l'amministrazione effettua a fronte delle indicazioni di comportamento;
- come questi controlli sono effettuati;
- chi è autorizzato ad effettuare i controlli.

4. Definizioni

Dispositivi di elaborazione	Sono i dispositivi che agiscono direttamente sui dati sottoponendoli a trasformazione come previsto dai programmi informatici (software) utilizzati dall'organizzazione
Dispositivi di memorizzazione	Sono i dispositivi che conservano i dati per la loro successiva elaborazione
Dispositivi di comunicazione	Sono i dispositivi che consentono di trasferire i dati da un dispositivo all'altro
Software	Insieme di istruzioni che consentono il funzionamento dei dispositivi di elaborazione, di memorizzazione e di comunicazione
Hardware	Sono le componenti materiali (che si possono toccare) di un sistema informatico. Si differenza dal software perché quest'ultimo è immateriale (non si può toccare)
Credenziali	Informazioni che servono ad accedere alle risorse hardware o software. Normalmente le credenziali sono composte da *nome_utente* e *password*
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)

5. Uso dei dispositivi di elaborazione

I dispositivi di elaborazione corrispondono, per gli utenti dell'ASST Lariana, alle postazioni di lavoro fisse, alle postazioni di lavoro portatili o a computer nell'ambito dei quali vengono eseguiti i software che sono utilizzati da più utenti collegati (server).
Esistono alcune regole di base comuni a tutte le precedenti tipologie di apparecchiature alle quali si aggiungono regole specifiche per le singole categorie.
I dispositivi di elaborazione, di solito, sono equipaggiati con dispositivi di memorizzazione e dispositivi di comunicazione. Pertanto, nel loro utilizzo, occorre rispettare sia le indicazioni fornite in questo capitolo, sia le indicazioni fornite nei successivi capitoli dedicati all'"Uso dei dispositivi di memorizzazione" ed all'"Uso dei dispositivi di comunicazione".
I dispositivi di elaborazione sono di proprietà dell'ASST Lariana e sono affidati al dipendente esclusivamente per finalità di servizio. Questo implica che il dipendente non può utilizzarli per scopi personali.

Le postazioni di lavoro fisse

Il più comune dispositivo di elaborazione, per la maggior parte degli utenti dell'ASST Lariana, corrisponde postazione di lavoro informatica fissa cioè il personal computer, sia esso ad uso esclusivo o condiviso.

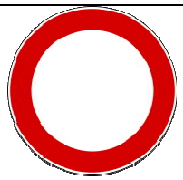
	È possibile accedere al personal computer solo con le proprie credenziali (personali e non cedibili)[1]
	È possibile connettere al personal computer dispositivi personali portatili (p.e. smartphone) **esclusivamente per la loro ricarica** ed avendo cura che siano **preventivamente spenti.**

	Ciascun utente deve verificare che il programma antivirus sia attivo ed aggiornato sulla postazione di lavoro
	Ciascun utente deve informare l'UOC Sistemi Informativi Aziendali (per comodità, d'ora in poi "SIA") in caso di comportamenti anomali della postazione di lavoro che possano sembrare conseguenza di virus informatici
	In caso di furto della postazione di lavoro, l'utente assegnatario, ovvero il coordinatore o il responsabile del servizio, deve, senza alcun ritardo, sporgere denuncia alle forze dell'Ordine, quindi trasmetterne tempestivamente copia al SIA e al Responsabile della protezione dei dati personali.
	Ciascun utente deve bloccare la postazione di lavoro (attraverso la combinazione di tasti CTRL+ALT+CANC + "Blocca il computer" oppure attraverso la combinazione di tasti Windows + L) in caso di allontanamento dalla stessa, anche per brevi periodi[2]
	Ciascun utente deve spegnere la postazione di lavoro al termine dell'attività lavorativa[3], salvo comunicazioni aziendali che richiedono di mantenere i computer accesi limitatamente allo svolgimento di attività manutentive notturne e programmate.
	La password di accesso alla postazione deve essere cambiata con periodicità non superiore a 90 giorni.
	La password di accesso alla postazione deve rispondere ai requisiti previsti dalle "Linee guida sulla formazione delle password", Appendice 1 al presente regolamento.
	In caso di password dimenticata o di altro tipo di impedimento all'accesso alla postazione tramite le proprie credenziali, si deve informare immediatamente l'help desk informatico che verificherà l'eventuale anomalia e provvederà al rilascio di una nuova password.
	Ciascun utente deve copiare o spostare i propri file elaborati in locale (cartella "Documenti" o "Desktop") nei percorsi di rete G: o H: (in funzione dell'uso e del livello di riservatezza), ciò affinché detti file possano essere protetti da backup notturno.

1 Solo per le postazioni del Dipartimento Gestionale di Emergenza Rianimazione ed Anestesia e altri servizi critici individuati di concerto con la Direzione Sanitaria Aziendale è consentito l'accesso a specifiche postazioni tramite utenze di reparto che non hanno alcun permesso sui dispositivi di memorizzazione

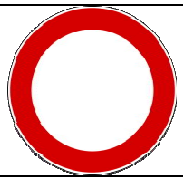
2 Qualora il computer sia utilizzato da più utenti e si prevede di allontanarsi per un periodo prolungato (oltre i 15 minuti) è necessario altresì eseguire la disconnessione, in modo da consentire ai colleghi di utilizzare la postazione

3 Questa indicazione deve risultare compatibile con la specifica attività svolta dall'Unità operativa ed eventuali deroghe devono essere preventivamente e formalmente concordate con il SIA. In ogni caso, ogni postazione deve essere riavviata almeno una volta alla settimana per consentire l'attivazione di eventuali aggiornamenti di sicurezza

	Non è consentito disattivare o disinstallare il software antivirus o altri programmi di sicurezza installati sulla postazione di lavoro.
	Non è consentito modificare l'equipaggiamento hardware della postazione di lavoro, aggiungendo o togliendo elementi (modem, masterizzatori, ecc.). Queste operazioni possono essere effettuate esclusivamente da personale del SIA o da eventuali partner esterni incaricati della manutenzione dell'infrastruttura tecnologica.
	Non è consentito modificare l'equipaggiamento software della postazione di lavoro, installando o disinstallando programmi. Queste operazioni possono essere effettuate esclusivamente da personale del SIA o da eventuali partner esterni incaricati della manutenzione dell'infrastruttura tecnologica.
	Non è consentito agli utenti l'accesso alla postazione con credenziali connesse a privilegi amministrativi[4].
	Non è consentito agli utenti l'accesso alla postazione con credenziali di un altro soggetto.
	Non è consentito agli utenti utilizzare la stessa password per l'accesso alla postazione di lavoro in ambiti diversi da quelli di servizio (p.e. l'accesso al proprio profilo su un social network).
	Non è consentito scattare delle fotografie con il proprio smartphone di videate dei personal computer aziendali, né catturare istantanee dello schermo con appositi software (es. screen capture). A maggior ragione è vietata la pubblicazione di tali immagini sui social media.
	Non è consentito memorizzare documenti o creare cartelle sul desktop della propria postazione di lavoro.

Le postazioni di lavoro portatili

Per le postazioni di lavoro portatili, valgono le stesse indicazioni relative alle postazioni di lavoro fisse alle quali si aggiungono le seguenti.

	Ciascun utente deve custodire il computer portatile che gli è stato assegnato in modo da ridurre al minimo il rischio di furto o smarrimento.
	In caso di furto della postazione portatile, l'utente assegnatario deve, senza alcun ritardo, sporgere denuncia alle forze dell'Ordine, quindi trasmetterne tempestivamente copia al SIA e al Responsabile della protezione dei dati personali.
	Ciascun utente deve assicurarsi che il software antivirus sia attivo, aggiornato e funzionante prima di collegare il computer portatile all'infrastruttura di comunicazione interna all'ASST Lariana
	Non è consentito lasciare il computer portatile in auto o in altri luoghi non custoditi in considerazione della possibilità tecnica di rilevare la loro presenza da parte di malintenzionati anche quando sono spenti[5].

[4] Solo i tecnici informatici formalmente autorizzati a i trattamenti di manutenzione dei software e dei dispositivi hardware possono accedere con credenziali amministrative limitatamente all'espletamento delle attività manutentive stesse.

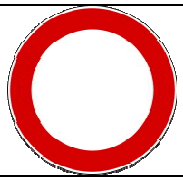
[5] Questo, quindi, può comportare anche il danneggiamento di risorse personali (rottura di vetri dell'auto o effrazione in luoghi privati).

I server

I server svolgono una funzione delicata nell'organizzazione dell'ASST Lariana visto che servono l'intera infrastruttura informatica aziendale. Pertanto, oltre alle normali indicazioni fornite per l'utilizzo delle postazioni di lavoro fisse, occorre particolare attenzione alle seguenti prescrizioni:

	È possibile accedere alla gestione del server solo con l'autorizzazione del SIA

	Gli accessi alla gestione del server sono tracciati e rimangono memorizzati per un periodo non superiore ai due anni, comunque non inferiore a tre mesi, ai fini di un'eventuale ricostruzione di eventi che hanno avuto conseguenze negative sul funzionamento del sistema informativo aziendale.
	Le operazioni di gestione effettuate sul server sono tracciate e rimangono memorizzate per un periodo non superiore ai due anni, comunque non inferiore a tre mesi, ai fini di un'eventuale ricostruzione di eventi che hanno avuto conseguenze negative sul funzionamento del sistema informativo aziendale.
	La password di accesso ai server deve rispondere ai requisiti previsti dalle "Linee guida sulla formazione delle password", Appendice 1 al presente regolamento, con le ulteriori precauzioni di una lunghezza minima di 15 caratteri e di avere almeno un numero, una lettera maiuscola ed un carattere speciale (p.e. $, @, #, ecc.).

	Non è consentito spegnere i server se non con l'autorizzazione del SIA **(diversamente da quanto previsto per le postazioni di lavoro fisse)**

6. Uso dei dispositivi di memorizzazione

I dispositivi di memorizzazione possono essere:

- i dischi interni a ciascuna postazione di lavoro;
- i dispositivi mobili come, per esempio, le pen-drive USB, i dischi esterni, i dischi ottici;
- le cartelle presenti sui dispositivi di memorizzazione centralizzati dell'ASST Lariana.

	È consentita la connessione di pen-drive USB alla postazione di lavoro solo se precedentemente sottoposte a scansione completa da parte del programma antivirus reso disponibile sulla postazione stessa.

	È consentita la connessione di pen-drive USB alla postazione solo per lo scambio di file la cui dimensione non permette una efficiente trasmissione per posta elettronica (tipicamente per file di dimensione superiore a 2 Mbyte)[6].
	È consentita la connessione di dischi magnetici esterni alla postazione di lavoro solo per trasferimento di file dalla postazione stessa al disco per il salvataggio (backup) dei dati presenti sulla postazione. In ogni caso, il disco esterno deve essere di proprietà dell'ASST Lariana e, al termine delle operazioni, deve essere custodito in un luogo che garantisca riservatezza, integrità e disponibilità[7].
	È consentita la memorizzazione su dischi ottici solo per trasferimento di file dalla postazione stessa al disco per il salvataggio (backup) dei dati presenti sulla postazione. In ogni caso, il disco ottico deve essere di proprietà dell'ASST Lariana e, al termine delle operazioni, deve essere custodito in un luogo che garantisca riservatezza, integrità e disponibilità[8].

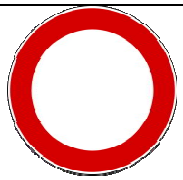
	Ciascun utente deve conservare, sui dispositivi di memorizzazione affidatigli (compreso quello interno alla postazione di lavoro di uso abituale), i dati personali che tratta per il periodo strettamente necessario a conseguire la finalità per la quale i dati devono essere trattati
	Ciascun utente, al momento del conseguimento della finalità per la quale i dati personali sono stati trattati, deve assicurarsi che i documenti amministrativi connessi al trattamento siano opportunamente conservati, tramite gli appositi software messi a disposizione dall'ASST Lariana, conformemente alle disposizioni del Codice dell'Amministrazione Digitale ed in considerazione dell'art. 10 del Codice dei beni culturali ed ambientali[9]
	Ciascun utente, al momento del conseguimento della finalità per la quale i dati personali sono stati trattati, deve assicurarsi che i dati personali non più strumentali alla redazione dei documenti sanitari/amministrativi connessi al trattamento siano rimossi da ogni dispositivo di memorizzazione

6 Si avverte che le pen-drive USB sono dispositivi esposti a frequenti guasti, pertanto non idonei ad essere impiegati per la produzione di copie di salvataggio.

7 Si avverte che i dischi magnetici esterni non costituiscono una modalità sicura atta a garantire la conservazione dei dati nel tempo, essendo gli stessi soggetti a guasti; per tale motivo può esserne fatto un uso limitato a particolari situazioni in cui vi è comunque una unità di memorizzazione primaria deputata alla conservazione dei dati, sono previste molteplici copie (almeno due) su dischi esterni, le dimensioni particolarmente elevate dei dati da preservare eccedono le quote di spazio dedicate a ciascun servizio/utente sui sistemi centralizzati preposti (disco G:, H:)

8 Si avverte che i dischi ottici non costituiscono una modalità sicura atta a garantire la conservazione dei dati nel tempo, essendo gli stessi soggetti a difetti; è onere dell'utente creare più copie di sicurezza (es. replicando il dato su due supporti)

9 Testo dell'art. 10, comma 2 del Codice dei beni culturali ed ambientali: *Sono inoltre beni culturali: a) [omissis] b) gli archivi e i singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico; c) [omissis]*

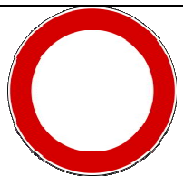
	Non è consentito copiare dati trattati dall'ASST Lariana su dispositivi di memorizzazione personali, né la loro pubblicazione sui social media.
	Non è consentito copiare dati trattati dall'ASST Lariana su dispositivi di memorizzazione in *cloud* se non preventivamente acquisiti formalmente dall'azienda ed esplicitamente autorizzati dal SIA.
	Non è consentito creare cartelle condivise sulla propria postazione di lavoro.
	Non è consentito memorizzare documenti personali sui dispositivi di memorizzazione di proprietà dell'ASST Lariana.

7. Uso dei dispositivi di comunicazione

I dispositivi di comunicazione sono quelli che permettono di *scambiare dati* tra la postazione di lavoro e altri dispositivi per utilizzarne le risorse.
In questo capitolo, sono riepilogate sia le indicazioni riferite ai dispositivi di comunicazione sia ai programmi che servono a comunicare (browser Internet, posta elettronica, ecc.).

	È consentito accedere alla posta elettronica personale (diversa da quella fornita dall'ASST Lariana per ragioni di servizio) tramite Internet (webmail) per il tempo strettamente necessario a gestire situazioni contingenti e, comunque, con la limitazione di 10 minuti al giorno
	È consentito accedere ad Internet solo per motivi di servizio
	E' consentito inviare messaggi di posta elettronica a **interlocutori esterni** all'ASST Lariana unicamente **se autorizzati** dal Direttore della Unità Organizzativa di competenza, avendo riguardo di rispettare le modalità indicate dallo stesso: **uso della casella di gruppo** assegnata all'unità organizzativa o al servizio (es. urp@asst-lariana.it), uso della casella personale (nome.cognome@asst-lariana.it).

	Ciascun utente accede alla posta elettronica esclusivamente con credenziali personali e non cedibili.
	I messaggi di posta elettronica inviati a più destinatari esterni (p.e. messaggi a cittadini o a colleghi di altre pubbliche amministrazioni), non devono consentire a ciascun destinatario di conoscere gli altri indirizzi ai quali il messaggio è diretto, salvo che questo non sia necessario rispetto al contenuto del messaggio stesso. La forma più opportuna per l'invio di messaggi a più destinatari è quella di inserire gli indirizzi in conoscenza nascosta.
	Prima di aprire i collegamenti presenti nei messaggi ricevuti dalla casella di posta elettronica fornita dall'ASST Lariana, ciascun utente verificherà, tramite **contatto telefonico con il mittente, che il link sia stato effettivamente inviato dallo stesso (escludendo un tentativo di "adescamento tramite link", cosiddetto *phishing*) e che sia affidabile.**
	Prima di aprire gli allegati ai messaggi ricevuti dalla casella di posta elettronica fornita dall'ASST Lariana, ciascun utente verificherà, tramite **contatto telefonico con il mittente, che il messaggio sia stato effettivamente inviato dallo stesso e che sia affidabile.**
	I messaggi di posta elettronica o qualsiasi altra modalità di trasferimento di dati personali riguardanti la salute devono essere preceduti da apposite procedure di cifratura indicate dal SIA.

	Non è consentito scaricare programmi da Internet né, quindi, installarli sulla postazione di lavoro.
	Non è consentito scaricare allegati dalla posta elettronica personale (diversa da quella fornita dall'ASST Lariana per ragioni di servizio) tramite Internet (webmail).

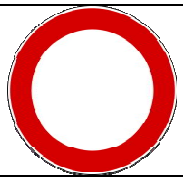
	Non è consentito aprire i collegamenti presenti nei messaggi ricevuti dalla posta elettronica personale (diversa da quella fornita dall'ASST Lariana per ragioni di servizio) tramite Internet (webmail).
	Non è consentito connettere ai dispositivi di proprietà dall'ASST Lariana dispositivi di comunicazione personali (compresi smartphone, tablet, access point WIFI, ecc.).
	Non è consentita l'installazione all'interno del perimetro dell'ASST Lariana di alcun dispositivo di comunicazione (es. router o hotspot WIFI, tethering WIFI con smartphone, qualunque tipologia di modem). Eventuali eccezioni devono essere formalmente autorizzate dal SIA e rispondere alle prescrizioni da questi comunicate.
	Non è consentito inviare all'esterno, per mezzo di posta elettronica, social media o altri canali di comunicazione, documenti che possono contenere dati personali appartenenti a particolari categorie o dati riguardanti condanne penali o reati, oltreché a informazioni relative ai lavoratori. In questi casi, ove sussistano comprovate esigenze di servizio, occorre concordare con il SIA apposite procedure di cifratura dei documenti, preferibilmente basate su chiave asimmetrica.
	Non è consentito inserire regole di inoltro automatico della propria corrispondenza presso altre caselle di posta elettronica personali; non è altresì consentito usare strumenti di posta elettronica personali (es. gmail.com, libero.it, client di posta quali thunderbird o MS outlook installati su computer personali, etc) per accedere alla casella email aziendale.
	Non è consentito utilizzare l'indirizzo di posta elettronica fornito dall'ASST Lariana per iscriversi a Social media, forum, newsletter ed iniziative estranee ad esigenze di servizio.
	Non è consentito partecipare alle cosiddette "Catene di Sant'Antonio".
	Non è consentito l'uso di app per smartphone o tablet per trasferire dati personali appartenenti alle particolari categorie o a quelli riguardanti condanne penali o reati.
	Non è consentito l'uso di applicazioni software non fornite da ASST Lariana (per smartphone, tablet o PC) che implichino l'archiviazione di dati personali riguardanti gli interessati (pazienti, dipendenti, fornitori, ecc.) o credenziali di accesso a sistemi resi disponibili dall'ASST Lariana.

8. Uso del software

I software in uso ai dipendenti dell'ASST Lariana rappresentano un importante strumento a supporto delle molteplici attività svolte dall'Azienda; al contempo, sono il mezzo che consente l'accesso ad informazioni, anche di natura personale, che è necessario proteggere attenendosi alle seguenti indicazioni.

	È consentito l'accesso ai software solo tramite credenziali, personali e non cedibili, fornite dal SIA o dal fornitore del software

	Le password di accesso ai programmi che ciascun utente impiega per la propria attività lavorativa devono essere cambiate con periodicità non superiore a 90 giorni
	Le password di accesso ai programmi deve rispondere ai requisiti previsti dalle "Linee guida sulla formazione delle password", Appendice 1 al presente regolamento
	In caso di password dimenticata o di altro tipo di impedimento per l'accesso al software tramite le proprie credenziali, si deve informare immediatamente l'help desk informatico (o il fornitore del software) che verificherà l'eventuale anomalia e provvederà al rilascio di una nuova password

	Non è consentito agli utenti utilizzare la stessa password per l'accesso ai programmi resi disponibili dall'ASST Lariana in ambiti diversi da quelli di servizio (p.e. l'accesso al proprio profilo su un social network)

9. Le attività di assistenza tecnica

Il personale incaricato del SIA ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso all'incaricato.

10. I controlli

I controlli effettuati dall'ASST Lariana sono diretti a raccogliere informazioni per escludere le seguenti problematiche:

- tentativi di violazione della sicurezza dei dispositivi informatici e dell'intero sistema informativo dell'Ente;
- comportamenti anomali, anche involontari, che possano compromettere il funzionamento delle risorse tecnologiche dell'ASST Lariana;
- presenza di fattispecie che possano incidere sui diritti e le libertà dei soggetti di cui l'ASST Lariana tratta dati personali.

È inevitabile, dunque, acquisire informazioni che riguardano le azioni sviluppate all'interno dei dispositivi informatici aziendali e, quindi, le azioni svolte dai dipendenti senza, tuttavia, che questo comporti un controllo a distanza dell'attività dei lavoratori.

Quali controlli vengono effettuati

Di seguito sono esposti i controlli che vengono effettuati per gli scopi predetti.

Tipo di azione memorizzato	**Controllo effettuato**
Accesso ai server	Vengono memorizzati data, ora ed utente che ha effettuato l'accesso al server.
Operazioni di gestione sui server (compresi i dispositivi di memorizzazione condivisi)	Vengono memorizzati data, ora ed utente che ha effettuato l'operazione di gestione.
Accesso alle postazioni	Vengono memorizzati data, ora ed utente che ha effettuato l'accesso alla postazione di lavoro.
Accesso alle risorse di memorizzazione condivise	Vengono memorizzati data, ora ed utente che ha effettuato l'accesso alle cartelle condivise o ad altri dispositivi di memorizzazione comuni.
Accesso ai siti internet	Vengono memorizzati data, ora, URL ed utente che ha tentato l'accesso a siti web.
Posta elettronica	Vengono memorizzati data, ora, mittente, primo destinatario, oggetto, delle mail in entrata ed in uscita dal dominio asst-lariana.it; vengono inoltre memorizzati i contenuti delle email stesse.
Software applicativi	Vengono memorizzati data, ora ed utente che ha effettuato l'accesso al software. In base alla finalità per cui viene usato il software, possono inoltre essere memorizzate le informazioni relative alle modifiche apportate ai documenti: modifica effettuata, data, ora ed utente che ha effettuato la modifica.

Come si effettuano i controlli

Di seguito sono esposte le modalità con le quali si effettuano i predetti controlli.

Tipo di azione memorizzato	**Durata della conservazione[10]**	**Modalità di controllo**
Accesso ai server	3 mesi	I dati vengono memorizzati ma non sono analizzati se non in presenza di eventi che hanno compromesso la sicurezza del patrimonio informativo aziendale.
Operazioni di gestione sui server (compresi i dispositivi di memorizzazione condivisi)	3 mesi	I dati vengono memorizzati ma non sono analizzati se non in presenza di eventi che hanno compromesso la sicurezza del patrimonio informativo aziendale.
Accesso alle postazioni	3 mesi	I dati vengono memorizzati ma non sono analizzati se non in presenza di eventi che hanno compromesso la sicurezza del patrimonio informativo aziendale. Inoltre, il SIA può procedere a disabilitare le credenziali di utenti che, dall'analisi dei dati memorizzati non risultano avere effettuato accessi da oltre 90 giorni.
Accesso alle risorse di memorizzazione condivise	3 mesi	I dati vengono memorizzati ma non sono analizzati se non in presenza di eventi che hanno compromesso la sicurezza del patrimonio informativo aziendale.
Accesso ai siti internet	3 mesi	I dati vengono analizzati, senza identificazione dell'utente, da un sistema automatico che intercetta i tentativi di collegamento a siti che rientrano nella black list del firewall. In presenza di 20 tentativi di collegamento a siti che rientrano nella black list del firewall, effettuati nelle 24 ore solari, viene identificato l'utente e vengono svolte ulteriori analisi per verificare la volontarietà dell'azione.

[10] Fatta salva la periodicità delle procedure di cancellazione che può, per ragioni di economicità, prevedere la concreta rimozione del dato entro 24 mesi

Accesso ai siti internet	12 mesi	I dati vengono memorizzati in ottemperanza alla normativa vigente; restano a disposizione dell'Autorità per finalità di accertamento e repressione dei reati.[11]
Posta elettronica	3 mesi	I dati vengono analizzati acquisendo un campione casuale di 10 messaggi al mese per verificare il rispetto delle indicazioni fornite ai dipendenti oltre che per verificare eventuali illeciti commessi in danno dell'azienda.
Posta elettronica	12 mesi	I dati vengono memorizzati in ottemperanza alla normativa vigente; restano a disposizione dell'Autorità per finalità di accertamento e repressione dei reati. [12]
Software applicativi	3 mesi	I dati vengono memorizzati ma non sono analizzati se non in presenza di eventi che hanno compromesso la sicurezza del patrimonio informativo aziendale.
Dati relativi al traffico telefonico	24 mesi	I dati vengono memorizzati in ottemperanza alla normativa vigente, ma non sono analizzati; restano a disposizione dell'Autorità per finalità di accertamento e repressione dei reati. [13]

Chi effettua i controlli

Tutti i controlli, compresi quelli a valle di eventuali analisi automatiche, sono effettuati a cura del SIA o da partner tecnologici che lo stesso SIA ha individuato e designato quale Responsabili del trattamento dei dati personali ai sensi dell'art. 28 del GDPR. Il SIA potrà avvalersi, in casi specifici e fortemente anomali, di consulenze esterne per eventuali ricostruzioni forensi.

In nessun caso i controlli riguarderanno l'attività lavorativa dei dipendenti ma saranno effettuati con un approccio *top-down* ovvero approfondendo, per quanto possibile, fenomeni anomali di carattere generale e senza alcun riferimento iniziale ai singoli dipendenti.

[11] In ottemperanza al D.lgs 30 giugno 2003 n.196, art. 132.
[12] In ottemperanza al D.lgs 30 giugno 2003 n.196, art. 132.
[13] In ottemperanza al D.lgs 30 giugno 2003 n.196, art. 132.

Appendice 1. Linee guida sulla formazione delle password

1. Le password devono essere di almeno **10** caratteri
2. Le password non possono essere riutilizzate.
3. Le password non devono contenere il nome account dell'utente o il nome o il cognome della persona. In particolare non possono contenere più di due caratteri consecutivi del nome completo dell'utente o del nome dell'account utente
4. Le password devono contenere caratteri presi da almeno TRE delle categorie seguenti:
    - Lettere maiuscole delle lingue europee (da "A" a "Z", con segni diacritici, caratteri greci e cirillici)
    - Lettere minuscole delle lingue europee (da "a" a "z", Sharp-s, con segni diacritici, caratteri greci e cirillici)
    - cifre (da 0 a 9)
    - Caratteri non alfanumerici (caratteri speciali): (~! @ # $% ^& * _-+ =' | \ \ (){}\ []:; "' <>,.? /) I simboli di valuta come l'euro o la sterlina britannica non vengono accettati come caratteri speciali.

Tali raccomandazioni valgono anche per tutti i programmi in uso presso la ASST Lariana che utilizzino credenziali di accesso, fatto salvo eventuali limitazioni imposte dal programma stesso. Ad esempio, gli stessi criteri devono essere applicati anche alle password di Priamo (sia per l'accesso che per la validazione), SISS (sia PIN di accesso che di firma), fatto salvo che in questi casi la password è limitata a massimo 8 caratteri.

Esempi di password non valide:

- 11111111 NON è una password valida per mancanza di lettere e caratteri non alfanumerici, oltre che avere caratteri ripetuti più di 2 volte
- 34563456 (esempio di matricola ripetuta 2 volte) NON è una password valida per mancanza di lettere e caratteri alfanumerici
- password NON è una password valida per mancanza di lettere maiuscole e caratteri alfanumerici o numerici
- Mario_1970 (relativa all'utente mario.rossi) NON è una password valida per troppi caratteri consecutivi presenti anche nel nome utente, anche se ha maiuscole, minuscole, punteggiatura ed è lunga 10 caratteri