1. **Il documento di analisi dei rischi**

Il presente documento di Analisi dei rischi costituisce uno strumento per far fronte all'obbligo, di cui all'art. 32 del Regolamento UE 2016/679, relativamente alla sicurezza dei dati personali, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento mediante l'adozione di idonee e preventive misure di sicurezza in modo da ridurre al minimo rischi di:

a) distruzione o perdita, anche accidentale, dei dati personali (causati ad es. da comandi applicativi/operativi errati; software pericolosi, malfunzionamento dell'Hardware, eventi disastrosi);
b) accesso non autorizzato (nel caso in cui i dati siano consultati ad opera di soggetti diversi da quelli preposti oppure siano oggetto di comunicazione/diffusione non consentita)
c) trattamento non consentito o non conforme alle finalità della raccolta

2. **Analisi dei rischi:**

Il criterio adottato per definire il processo di analisi è consistito nell'associare valori "discreti" (1-4), in base alla gravità-rilevanza della problematica.
Si è inteso effettuare l'analisi ricorrendo alla seguente loro classificazione in:
- Banche dati
- Piattaforme Informatiche Aziendali, (PIA)
- Piattaforme Informatiche Aziendali Centralizzate; (PIAC)
- Piattaforme Informatiche Aziendali Locali; (PIAL);
- Piattaforme Informatiche Aziendali Esterne) PIAE
- Server (Fisici e Virtualizzati)
- Minacce
- Vulnerabilità

Scopo dell'analisi dei rischi è di:
a) identificare le cause più probabili di rischio in una organizzazione,
b) valutare il grado di esposizione e
c) determinare quali misure di sicurezza, quante e in che modo debbano essere realizzate.
Il numero degli elementi di rischio, per il quale si rende necessaria l'attuazione di adeguate misure di sicurezza, dipende dal grado di esposizione al rischio che si è disposti a tollerare. Si può, infatti, identificare una soglia che suddivida i rischi in accettabili (a fronte di una gravità stimata ' bassa ') e non accettabili (a fronte di una gravità stimata:'media ' o ' alta ').
Criteri per la identificazione dei rischi: sono stati presi in esame i rischi più probabili per il caso concreto tra quelli possibili. I rischi analizzati possono esser raggruppati secondo i seguenti principali criteri:
- INTEGRITÀ, intesa come correttezza e consistenza del dato e, quindi, come la completa corrispondenza del dato originale a quello inserito nel sistema di trattamento;
- RISERVATEZZA, intesa come garanzia che l'informazione sia accessibile solo alle persone autorizzate;
- DISPONIBILITÀ, intesa come garanzia che l'informazione sia disponibile, quando necessario, alle persone autorizzate.

Matrice dei rischi, al fine di individuare i rischi, è stata approntata una matrice, relativamente ai rischi incombenti sui trattamenti informatici così come ai rischi derivanti dai trattamenti in modalità cartacea. Nello specifico, per ciascuna possibile minaccia sono state individuate:
la vulnerabilità
il danno
le contromisure

MATRICE DEI RISCHI PER I TRATTAMENTI INFORMATICI E CARTACEI

MINACCIA	VULNERABILITA'	DANNO	CONTROMISURE INDIVIDUATE	CONTROMISURE ADOTTATE □**Parzialmente applicate** ■ **Totalmente applicate** ☒ **Da implementare**
Furto di credenziali di autenticazione	Personale non formato. Strumenti non conformi;	Accesso o trattamento da parte di soggetti non autorizzati; Perdita totale o parziale dei dati; Alterazione delle informazioni.	• Formazione del personale. • Implementazione di una procedura per la nomina del custode delle password, • Adeguamento periodico parco macchine. • Aggiornamento dei sistemi operativi.	• Formazione del personale ■ • Implementazione di una procedura per la nomina del custode delle password ■ • Adeguamento periodico parco macchine ■ • Aggiornamento dei sistemi operativi ■
Carenza di consapevolezza, disattenzione o incuria	Personale non formato	Accesso o trattamento da parte di soggetti non autorizzati	Formazione del personale. Consegna del mansionario per ciascun incaricato;	Formazione del personale. Consegna del mansionario per ciascun Incaricato □ ;
Comportamenti sleali o fraudolenti	Accesso indesiderato alle postazioni o ai server, fisicamente o per mezzo della rete.	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati. Asportazione o blocco operativo, perdita dell'integrità, decadimento delle prestazioni del sistema.	• Formazione del personale. • Consegna del mansionario	• Formazione del personale ■. • Consegna del mansionario □
Errore Materiale	Personale non formato. Strumenti non conformi. Software non certificato. Assenza di backup	Perdita totale o parziale dei dati; alterazione delle informazioni. accesso o trattamento da parte di soggetti non autorizzati	• Formazione del personale. Consegna del mansionario	• Formazione del personale ■ Consegna del mansionario □
Azione di virus informatici	Antivirus non aggiornato. Comportamenti scorretti	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati.	• Formazione del personale. • Aggiornamento dei sistemi operativi;	• Formazione del personale ■. • Aggiornamento dei sistemi operativi ■;

Spamming o altre tecniche di sabotaggio	Antivirus non aggiornato. Comportamenti scorretti	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati.	• Formazione del personale. • Aggiornamento dei sistemi operativi.	• Formazione del personale ■ • Aggiornamento dei sistemi operativi ■
Malfunzionamento, indisponibilità o degrado degli strumenti	Risorse obsolete, strumenti non conformi, impianti elettrici non a norma.	Perdita totale o parziale dei dati;blocco operativo e perdita dell'integrità della banca dati.	• Adeguamento periodico parco macchine. • Aggiornamento dei sistemi operativi.	• Adeguamento periodico parco macchine ■ • Aggiornamento dei sistemi operativi ■
Accessi esterni non autorizzati	Accessi non controllati	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati. Asportazione o alterazione delle informazioni.	Firewall aziendale	Firewall aziendale ■
Intercettazione di informazioni in rete	Accessi non controllati	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati. Asportazione o alterazione delle informazioni.	Firewall aggiornato Anti virus con aggiornamento automatico	Firewall aggiornato Anti virus con aggiornamento automatico ■
Accessi non autorizzati a locali/reparti ad accesso ristretto	Accessi non controllati	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati. Asportazione o alterazione delle informazioni.	Sistema di video sorveglianza. Badge. Registro degli accessi.	Sistema di video sorveglianza ☒ Badge ☐ Registro degli accessi ■
Asportazione e furto di strumenti contenenti dati	Accessi non controllati	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati. Asportazione o alterazione delle informazioni.	Sistema di video sorveglianza. Badge. Registro degli accessi.	Sistema di video sorveglianza ☒ Badge ☐ Registro degli accessi ■
Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Personale non formato.	Perdita totale o parziale dei dati.	Formazione del personale. Piano di disaster recovery	Formazione del personale ■ Piano di disaster recovery ☒
Guasto ai sistemi complementari (impianto elettrico, idrico, climatizzazione, ecc.)	Personale non formato.	Perdita totale o parziale dei dati.	Formazione del personale. Piano di disaster recovery	Formazione del personale ■ Piano di disaster recovery ☒
Errori umani nella gestione	Personale non formato.	Perdita totale o parziale dei dati;	Formazione del personale.	Formazione del personale ■

della sicurezza fisica				

Tabella di analisi dei rischi, per cui si è proceduto alla individuazione di tre "fonti" del rischio:

a) comportamento degli operatori;
b) eventi relativi agli strumenti;
c) eventi relativi al contesto.

Successivamente si è scrutinata la possibilità che il rischio evidenziato potesse accerarsi (SI/NO) e, quindi, se ne è descritto l'impattp sulla sicurezza (stimato in alta/medio/bassa). Sono state quindi individuate le Misure per contrastare il rischio, con relativa indicazione di quelle già poste in essere.

Tipologia	**RISCHI**	**SI/NO**	**DESCRIZIONE DELL'IMPATTO SULLA SICUREZZA gravità stimata: alta/media/bassa**	**Misure di azione**
Comportamenti degli operatori	Furto di credenziali di autenticazione	SI	bassa	.
	Carenza di consapevolezza, disattenzione o incuria	SI	bassa	
	Comportamenti sleali o fraudolenti	SI	bassa	
	Errore Materiale	SI	bassa	
	Altro evento	SI	bassa	
Eventi relativi agli strumenti	Azione di virus informatici	si	bassa	
	Spamming o altre tecniche di sabotaggio	si	bassa	
	Malfunzionamento, indisponibilità o degrado degli strumenti	si	bassa	
	Accessi esterni non autorizzati	si	bassa	
	Intercettazione di informazioni in rete	si	bassa	
	Altro evento	si	bassa	
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	si	bassa	
	Asportazione e furto di	si	bassa	

	strumenti contenenti dati			
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	si	bassa	
	Guasto ai sistemi complementari (impianto elettrico, idrico, climatizzazione, ecc.)	si	bassa	
	Errori umani nella gestione della sicurezza fisica	si	bassa	
	Altro evento	si	bassa	

Quindi tenuto conto di quanto esposto come indagine effettuata sull'analisi del rischio, si è proceduto a calcolare l'indice di rischio per ogni minaccia valutata e ad identificare la rilevanza della minaccia stessa percentualizzandone l'importanza ed adottando, ove ritenuto opportuno, idonee e preventive misure di sicurezza.

Al fine di dare una classificazione fruibile dei livelli di rischio rilevati, essi sono schematizzabili nel seguente modo:

0- 25% Rischio basso
26 – 50% Rischio medio
51 – 75% Rischio Alto
76- 100% Rischio Altissimo

Da come si evince dall'analisi svolta, il livello di rischio non è mai oltre il valore "Bassa", pertanto non è stato necessario individuate ed adottate misure opportunamente studiate al fine di ridurre l'impatto delle minacce.

LEGENDA ORIGINE DEL RISCHIO
A: ACCIDENTAL
D: DELIBERATE
E: ENVIROMENTAL

Tipo	**Minaccia**	**Origine**
Danno Fisico	Fuoco	ADE
Danno Fisico	Danni causati dall'Acqua	ADE
Danno Fisico	Inquinamento	ADE
Danno Fisico	Incidente rilevante	ADE
Danno Fisico	Distruzione di apparato o supporti	ADE
Danno Fisico	Polvere, corrosione, congelamento	ADE
Eventi naturali	Fenomeni climatici	E
Eventi naturali	Fenomeni sismici	E
Eventi naturali	Fenomeni vulcanici	E
Eventi naturali	Fenomeni meteorologici	E
Eventi naturali	Inondazione	E
Perdita di servizi essenziali	Guasto di apparati di aria condizionata o del sistema idrico	AD
Perdita di servizi essenziali	Mancanza di energia elettrica	ADE
Perdita di servizi essenziali	Guasto di apparati di telecomunicazioni	AD
Disturbi dovuti alle radiazioni	Disturbi elettromagnetici	ADE
Disturbi dovuti alle radiazioni	Radiazioni termiche	ADE

Disturbi dovuti alle radiazioni	Impulsi elettromagnetici	ADE
Compromissione delle informazioni	Intercettazione di segnali (sovrapposizione)	D
Compromissione delle informazioni	Spionaggio remoto	D
Eventi naturali	Fenomeni meteorologici	E
Eventi naturali	Inondazione	E
Perdita di servizi essenziali	Guasto di apparati di aria condizionata o del sistema idrico	AD
Perdita di servizi essenziali	Mancanza di energia elettrica	ADE
Perdita di servizi essenziali	Guasto di apparati di telecomunicazioni	AD
Disturbi dovuti alle radiazioni	Disturbi elettromagnetici	ADE
Disturbi dovuti alle radiazioni	Radiazioni termiche	ADE
Disturbi dovuti alle radiazioni	Impulsi elettromagnetici	ADE
Compromissione delle informazioni	Intercettazione di segnali (sovrapposizione)	D
Compromissione delle informazioni	Spionaggio remoto	D
Compromissione delle informazioni	Intercettazioni	D
Compromissione delle informazioni	Furto di supporti magnetici o documenti	D
Compromissione delle informazioni	Furto di apparati	D
Compromissione delle informazioni	Recupero di supporti riciclati o scartati	D
Compromissione delle informazioni	Rivelazione di informazioni riservate	AD
Compromissione delle informazioni	Dati provenienti da fonti non affidabili	AD
Compromissione delle informazioni	Manomissione di hardware	D
Compromissione delle informazioni	Manomissione di software	AD
Compromissione delle informazioni	Rivelazione della collocazione di informazioni	D
Guasti tecnici	Guasto di apparati	A
Guasti tecnici	Malfunzionamento di apparati	A
Guasti tecnici	Saturazione del sistema informativo	AD
Guasti tecnici	Malfunzionamento software	A
Guasti tecnici	Problemi con la manutenzione del sistema informativo	AD
Azioni non autorizzate	Uso non autorizzato di apparati	D
Azioni non autorizzate	Copia non autorizzata di software	D
Azioni non autorizzate	Uso di software contraffatto o copiato	AD
Azioni non autorizzate	Corruzione di dati	D
Azioni non autorizzate	Trattamento illecito di dati	D
Compromissione di funzioni	Errore nell'utilizzo	A
Compromissione di funzioni	Abuso di diritti	AD
Compromissione di funzioni	Clonazione di diritti	D
Compromissione di funzioni	Negazione di permesso	D
Compromissione di funzioni	Mancanza di disponibilità del personale	ADE

Tipo	**Vulnerabilità**	**Minacce**

Hardware	Manutenzione non sufficiente/fallimento installazioni di supporti di memorizzazione	Problemi con la manutenzione del sistema informativo
	Mancanza di un periodico schema di sostituzione	Distruzione di apparato o supporti
	Suscettibilità all'umidità, polvere, sporco	Polvere, corrosione, congelamento
	Sensibilità a radiazioni elettromagnetiche	radiazioni elettromagnetiche
	Mancanza di un controllo efficiente per il cambiamento di configurazione	Errore nell'utilizzo
	Suscettibilità a variazioni di voltaggio	Mancanza di energia elettrica
	Suscettibilità a variazioni di temperatura	Fenomeni meteorologici
	Storage non protetto	Furto di supporti magnetici o documenti
	Mancanza di attenzione nel posizionamento	Furto di supporti magnetici o documenti
	Copia non controllata	Furto di supporti magnetici o documenti
Software	Assenza o insufficiente testing di software	Abuso di diritti
	Difetti ben conosciuti nel SW	Abuso di diritti
	Mancata effettuazione della disconnessione al momento dell'abbandono della postazione di lavoro	Abuso di diritti
	Riuso di supporti senza appropriato formattazione o ripristino	Abuso di diritti
	Errata assegnazione di diritti di accesso	Abuso di diritti _
	Software largamente distribuiti	Corruzione di dati
	Applicazione di programma a dati errati in termini di tempo i	Corruzione di dati
	Interfaccia utente di difficile uso	Errore nell'utilizzo
	Mancanza di documentazione	Errore nell'utilizzo
	Errato set up	Errore nell'utilizzo
	Date non corrette	Errore nell'utilizzo
Rete	Mancanza di meccanismi di identificazione ed autenticazione	Clonazione di diritti
	Tabelle di password non protette	Clonazione di diritti
	Gestione delle password non adeguata	Clonazione di diritti
	Abilitazione di servizi non necessari	Trattamento illecito di dati
	Software "immaturo" o nuovo	Malfunzionamento software
	Specifiche per lo sviluppo non chiare o incomplete	Malfunzionamento software
	Mancanza di un "change control" efficace	Malfunzionamento software
	Mancanza di controllo per il	Manomissione di software

	download e l'utilizzo di software	
	Mancanza di copie di backup	Manomissione di software
	Mancanza di protezione fisica degli edifici, delle porte e delle finestre	Furto di supporti magnetici o documenti
	Malfunzionamenti nella produzione di report di gestione	Uso non autorizzato di apparati
	Mancanza di conferme per l'invio e la ricezione di messaggi di posta	Negazione di permesso
	Mancanza di meccanismi di identificazione ed autenticazione	Clonazione di diritti
	Linee di comunicazione non protette	Intercettazioni
	Traffico "sensibile" non protetto	Intercettazioni
	Cablaggio non a norma	Malfunzionamento di apparati
	"Single point of failure" – collo di bottiglia critico	Malfunzionamento di apparati
	Architettura di rete non sicura	Spionaggio remoto
	Trasferimento password in chiaro	Spionaggio remoto
	Gestione della rete non adeguata (mancanza di "magliatura")	Saturazione del sistema informativo
	Connessioni di rete pubblica non protette	Uso non autorizzato di apparati
Personale	Assenza di personale	Mancanza di disponibilità del personale
	Procedure di reclutamento non adeguate	Distruzione di apparato o supporti
	Training sulla sicurezza non sufficiente	Errore nell'utilizzo
	Uso non corretto di software ed hardware	Errore nell'utilizzo
	Mancanza di avvertimenti sulla sicurezza	Errore nell'utilizzo
	Mancanza di sistemi di monitoraggio	Trattamento illecito di dati
	Mancata supervisione di lavoro effettuato da parte di personale esterno o delle pulizie	Furto di supporti magnetici o documenti
	Mancanza di politiche per il corretto uso di sistemi di telecomunicazioni e messaggistica	Uso non autorizzato di apparati
Strutture fisiche	Uso non appropriato o non attento di controllo degli accessi fisici alle strutture ed alle stanze	Distruzione di apparato o supporti
	Posizionamento in area suscettibile di allagamenti	Inondazione
	Rete elettrica non stabilizzata	Mancanza di energia elettrica
	Mancanza di protezione fisica degli edifici, porte e finestre	Furto di apparati
Organizzazione	Mancanza di procedure formali per la registrazione e la registrazione degli utenti	Abuso di diritti
	Mancanza di un processo formale di revisione dei diritti di accesso	Abuso di diritti

	Mancanza o indicazioni non sufficienti riguardanti la sicurezza nei contratti con terze parti	Abuso di diritti
	Mancanza di una procedura di monitoraggio delle strutture di elaborazione delle informazioni	Abuso di diritti
	Mancanza di audit regolari	Abuso di diritti
	Mancanza di procedure per l'identificazione e la gestione del rischio	Abuso di diritti
	Mancanza di report di guasti registrati nei log di amministratori ed operatori	Abuso di diritti
	Tempi di risposta della manutenzione non adeguati	Problemi con la manutenzione del sistema informativo
	Mancanza o insufficienti Service Level Agreement	Problemi con la manutenzione del sistema informativo
	Mancanza di una procedura di change management	Problemi con la manutenzione del sistema informativo
	Mancanza di una procedura formale per la gestione documentale di un sistema di gestione della sicurezza delle informazioni	Corruzione di dati
	Mancanza di una procedura formale per la registrazione del monitoraggio del sistema di gestione della sicurezza delle informazioni	Corruzione di dati
	Mancanza di un processo formale per l'autorizzazione di informazioni pubblicamente disponibili	Mancanza di un processo formale per l'autorizzazione di informazioni pubblicamente disponibili
	Mancanza di una appropriata assegnazione di Responsabilità inerenti la sicurezza delle informazioni	Negazione di permesso
	Mancanza di un piano di continuità	Guasto di apparati
	Mancanza di una politica di utilizzo della posta elettronica	Errore nell'utilizzo
	Mancanza di procedure per l'introduzione di software all'interno di sistemi già operativi	Errore nell'utilizzo
	Mancanza di registrazioni nei log di amministratore ed operatore	Errore nell'utilizzo
	Mancanza di procedure per la gestione di informazioni classificate	Errore nell'utilizzo
	Mancanza di assegnazione di Responsabilità nell'ambito della sicurezza delle informazioni nelle descrizioni delle mansioni	Errore nell'utilizzo

	Mancanza o insufficienti clausole riguardanti la sicurezza delle informazioni nei contratti con i dipendenti	Trattamento illecito di dati
	Mancanza di un processo disciplinare definito in caso di incidente sulla sicurezza delle informazioni	Furto di apparati
	Mancanza di una politica formale per la gestione dei computer portatili	Furto di apparati
	Mancanza di controllo di asset fuori sede	Furto di apparati
	Mancanza di strutture di autorizzazione per la gestione delle informazioni	Furto di supporti magnetici o documenti
	Mancanza di strumenti di controllo per l'identificazione di "buchi" di sicurezza	Furto di supporti magnetici o documenti
	Mancanza di procedure di reporting per debolezze relative alla sicurezza delle informazioni	Uso non autorizzato di apparati
	Mancanza di procedure di conformità per diritti intellettuali	Uso di software contraffatto o copiato

3. MISURE DI SICUREZZA

Le dimensioni dell'analisi, le misure di sicurezza che l'organizzazione ha adottato sono state scelte con riferimento a criteri e procedure logiche, fisiche e tecniche ed organizzative, in grado di assicurare: I. la protezione delle aree e dei locali in cui sono conservati i dati personali interessati dalle misure di sicurezza; II. il controllo sull'accesso nei predetti locali delle persone autorizzate; III. la integrità dei dati; IV. la trasmissione dei dati, ivi comprese le misure di sicurezza da adottarsi per le restrizioni di accesso per via telematica. L'obiettivo è esplicitare lo stato dell'arte dell'organizzazione in termini di copertura rispetto ai requisiti minimi ed idonei delle misure di sicurezza previste dalla Legge, come dettagliato nei paragrafi successivi.

MISURE DI SICUREZZA 'ORGANIZZATIVE' Sono comprese le misure che impattano sulle procedure organizzative interne, quali: l'assegnazione di incarichi, la predisposizione di istruzioni operative, ecc.

1. Rilascio e revoca dell'autorizzazione da parte del Titolare o Responsabile agli incaricati per trattare i dati sensibili
2. Previsione di diversi livelli di autorizzazione di accesso ai dati in relazione ai compiti e mansioni assegnate
3. Verifica di validità delle autorizzazioni per l'accesso ai dati sensibili
4. Istruzioni scritte per lo svolgimento dei compiti assegnati
5. Verifica della restituzione dei documenti originali al termine delle operazioni affidate
6. Custodia dei dati da parte degli incaricati durante le operazioni di trattamento, in modo tale che ad essi non possano accedere persone prive di autorizzazione.
7. Identificazione e registrazione accessi dopo l'orario di chiusura degli archivi

8. Designazione del custode della copia delle password
9. Esistenza di diversi profili di autorizzazione in funzione delle diverse necessità di accesso ai dati
10. Individuazione di Profili di Autorizzazione anteriore al trattamento
11. Verifica almeno annuale delle condizioni di sussistenza per la conservazioni dei diversi profili di autorizzazione.
12. Predisposizione di istruzioni organizzative e tecniche in forma scritta per il backup
13. Previsione di interventi formativi per rendere edotti gli incaricati delle principali novità normative intervenute
14. Verifiche periodiche dei dati o trattamenti non consentiti o non corretti
15. Designazione formale di un Responsabile del trattamento dei dati personali e sensibili

MISURE DI SICUREZZA 'FISICHE' Sono comprese tutte le misure minime ed idonee finalizzate alla conservazione dei dati (ad es: i dispositivi antincendio, i gruppi di continuità elettrica, ecc.); le misure atte a tutelare la sicurezza della logistica (ad es: la vigilanza della sede, la adozione di sistemi di allarme, ecc.) e le misure volte a garantire la custodia dei dati (ad es: la custodia in armadi blindati e/o ignifughi).

1. Archivio ad accesso selezionato e controllato
2. Back- up almeno settimanale dei dati.
3. Dispositivi di allarme in archivi cartacei
4. Dispositivi antintrusione in archivi cartacei
5. Sistemi antincendio in archivi cartacei
6. Vigilanza esterna archivi
7. Sistemi allarme in locali PC
8. Dispositivi antintrusione in locali PC
9. Dispositivi antincendio in locali PC
10. Vigilanza esterna nei locali PC
11. Gruppi di continuità elettronica

MISURE DI SICUREZZA 'LOGICHE' Sono comprese tutte le misure riguardanti gli aspetti relativi alla sicurezza informatica, quali: la identificazione e la autenticazione degli utenti, il rilascio di profili di autorizzazione, l'installazione di antivirus, ecc.

1. Codice identificativo personale associato ad una parola chiave per l'accesso al PC
2. Codice identificativo personale univoco per l'accesso al PC
3. Disattivazione del codice identificativo personale in caso di mancato utilizzo per oltre 6 mesi
4. Disattivazione del codice identificativo personale in caso di cambiamento/termine della mansione
5. Password di almeno 8 caratteri
6. Predisposizione di istruzioni relative alla diligente custodia dell'elaboratore e della parola chiave
7. Autonoma sostituzione della parola chiave al primo utilizzo e successivamente ogni 3 mesi

8. Utilizzo di programmi anti-virus
9. Aggiornamento programmi anti-virus con cadenza almeno semestrale
10. Dispositivi per la limitazione dell'accesso a particolari siti web potenzialmente pericolosi (black list)
11. Dispositivi per la sospensione temporanea o definitiva (previo intervento dell'Amministratore di Sistema) dell'accesso, dopo la digitazione errata per n. 3 volte della password all'accensione del computer (BIOS)
12. Divieto di utilizzo di software non approvato
13. Predisposizione di linee e/o numeri dedicati per la trasmissione di dati sensibili con la limitazione dell'accesso
14. Installazione di solo software licenziato
15. Controlli sul tipo di software installato al fine di rilevare quelli non appropriati