



Documento programmatico sulla sicurezza dei dati

Ai sensi del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

(GDPR -Regolamento Generale sulla Protezione dei Dati)

Sommario

0	Premessa	3
1	Organizzazione	3
1	Matrice del trattamento dati	5
2	Registro dei trattamenti	6
3	Esito del vulnerability assessment	34
3.1	Collegamento ad internet	34
3.2	Backup	34
3.3	Tipologia di accesso e di connessione	34

0 Premessa

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

La direttiva 95/46/CE del Parlamento europeo e del Consiglio (4) ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va temperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

Sulla base di tali principi la nostra organizzazione ha ritenuto necessario valutare i processi che sono sottesi alle attività svolte per comprendere come i dati sono ricevuti, trattati, conservati, resi disponibili, archiviati e cancellati.

Nel seguito saranno riportati:

- Organizzazione;
- Registro dei trattamenti con relativa valutazione del rischio e pianificazione per mitigazione/eliminazione del rischio residuo;
- Esito del vulnerability assessment con analisi del rischio e pianificazione temporale mitigazione/eliminazione rischio.

1 Organizzazione

L'organizzazione ai fini della sicurezza dei dati è la seguente:

Titolare del trattamento dei dati:	Castello della Quiete S.r.l.
Data Protection Officer:	Dott. Matteo Accornero
Responsabile del trattamento dati Struttura Residenziale Psichiatrica (SRP):	Dott. Marco Capozza

Responsabile del trattamento dati Residenza Sanitaria Assistenziale (RSA): Dott. Ciro Ruocco

Responsabile del trattamento dati Area Amministrativa: Sig.ra Antonella Gabellone

Incaricati al trattamento

Nominativo	Mansione
Emanuele Kirieleison	Coord.Infermieristico SRP
Francesco di Renzo	Coord.Infermieristico RSA
Dott. Sebastiano Pulina	Assistente Sociale
Serena Tanda	Amministrativa
Dott.Francesco del Tutto	Medico SRP
Dott.Pierluigi Zuchegna	Medico SRP
Dott.Emanuele Viaggio	Psicologo SRP

Nella tabella che segue, la matrice di trattamento dati in cui è possibile evincere per ciascuna categoria di dati chi sono i soggetti autorizzati al loro trattamento.

1 Matrice del trattamento dati

Nome e Cognome	Mansione	Area Amministrativa				Area Sanitaria				
		Fornitori	Clienti	Personale	Contabilità	Cartelle Sanitarie SRP	Cartelle Sanitarie RSA	SIPC	Archivio Cartelle Sanitarie pazienti dimessi	Lista di attesa SRP
Matteo Accornero	Legale Rappresentante	X	X	X	X	X	X	X	X	X
Marco Capozza	Medico Resp. SRP					X		X		X
Francesco Del Tutto	Medico SRP									
Pierluigi Zuchegna	Medico SRP					X		X		X
Emanuele Viaggio	Psicologo SRP					X		X		X
Emanuele Kirieleison	Coord. Inferm. SRP					X		X		
Ciro Ruocco	Medico Resp. RSA						X			
Francesco di Rienzo	Coord. Inferm. RSA						X			
Sebastiano Pulina	Assistente sociale					X	X	X		X
Antonella Gabellone	Contabile	X	X	X	X					
Serena Tanda	Amministrativa	X	X	X						
Sabatino Salerni	Servizi generali	X								

2 Registro dei trattamenti

Id Trattamento		01	
Trattamento		Fornitori - Anagrafe	
Nome ed indirizzo del Responsabile del trattamento		Matteo Accornero – Via di Tor Cervara 112 - 00155 Roma	
Data di implementazione		28.04.2018	
Principale finalità		Gestione Elenco Fornitori e Scheda Fornitore. Gestione forniture e relativi processi contabili.	
Dettaglio degli scopi del trattamento		Gestione Elenco Fornitori e Scheda Fornitore. Gestione forniture e relativi processi contabili.	
Servizio Responsabile dell’attuazione		Ufficio Acquisti	
Funzione della persona o del servizio che esercita il diritto accesso		Acquisti.	
Categorie di persone interessate dal trattamento		Fornitori	
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Fornitori	Anagrafici	Cartacea
		Fiscali	Server :Tango QRP (locale)
		Livelli di servizio	
		Non conformità	
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Contabilità	Anagrafici e fiscali	
	Consulente fiscale	Anagrafici e fiscali	
	Agenzia delle entrate	Anagrafici e fiscali	
	Qualità	Anagrafici, livelli di servizio, Non conformità	
Durata di conservazione		Per un anno dopo l’uscita dall’Elenco Fornitori. Successivamente segregata.	
Consenso		Richiesto con Modulo Consenso Fornitori	
Misure di sicurezza – Tecniche organizzative		Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata del Server Tango QRP (locale)solo ad incaricati.	
Aggiornamento (data ed oggetto)		28.04.2018	

Id Trattamento	02
-----------------------	-----------

Trattamento	Fornitori – Preventivi		
Nome ed indirizzo del Responsabile del trattamento	Matteo Accornero – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione acquisti.		
Dettaglio degli scopi del trattamento	Selezione fornitori.		
Servizio Responsabile dell’attuazione	Ufficio Acquisti		
Funzione della persona o del servizio che esercita il diritto accesso	Acquisti.		
Categorie di persone interessate dal trattamento	Fornitori		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Fornitori	Anagrafici	Cartacea
		Offerta	Posta elettronica Gmail / PEC
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Area relativa al richiedente acquisto	Anagrafici e offerta	
Durata di conservazione	Fino ad eventuale chiusura del processo di acquisto. Successivamente segregata.		
Consenso	n.a.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata della Posta elettronica Gmail / PEC, solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	03
-----------------------	-----------

Trattamento	Fornitori – Ordini di acquisto farmaceutici		
Nome ed indirizzo del Responsabile del trattamento	Emanuele Kirieliesson – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione acquisti.		
Dettaglio degli scopi del trattamento	Gestione acquisti.		
Servizio Responsabile dell’attuazione	Ufficio Acquisti		
Funzione della persona o del servizio che esercita il diritto accesso	Acquisti.		
Categorie di persone interessato dal trattamento	Fornitori		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Fornitori	Anagrafici	Cartacea
		Dati fiscali	Gmail / PEC
		Offerta	
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Contabilità	Anagrafici, dati fiscali e offerta	
Durata di conservazione	Fino a chiusura del processo di acquisto. Successivamente segregata per almeno 5 anni.		
Consenso	n.a.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nella Casella di posta Gmail / Pec.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	04
-----------------------	-----------

Trattamento	Fornitori – Ordini di acquisto (tranne farmaceutici)		
Nome ed indirizzo del Responsabile del trattamento	Matteo Accornero – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione acquisti.		
Dettaglio degli scopi del trattamento	Gestione acquisti.		
Servizio Responsabile dell’attuazione	Ufficio Acquisti		
Funzione della persona o del servizio che esercita il diritto accesso	Acquisti.		
Categorie di persone interessato dal trattamento	Fornitori		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Fornitori	Anagrafici	Cartacea
		Dati fiscali	Gmail / PEC
		Offerta	
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Contabilità	Anagrafici, dati fiscali e offerta	
Durata di conservazione	Fino a chiusura del processo di acquisto. Successivamente segregata per almeno 5 anni.		
Consenso	n.a.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nella Casella di posta Gmail / Pec.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	05
-----------------------	-----------

Trattamento	Fornitori – Contratti		
Nome ed indirizzo del Responsabile del trattamento	Matteo Accornero – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione acquisti.		
Dettaglio degli scopi del trattamento	Gestione acquisti.		
Servizio Responsabile dell’attuazione	Ufficio Acquisti		
Funzione della persona o del servizio che esercita il diritto accesso	Acquisti.		
Categorie di persone interessate dal trattamento	Fornitori		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Fornitori	Anagrafici	Cartacea
		Dati fiscali	Server: LogicalDoc (locale)
		Prodotti/servizi acquistati	
		Condizioni di acquisto	
		Livelli di servizio	
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Contabilità	Anagrafici, dati fiscali, prodotti/servizi, condizioni di acquisto	
	Acquisti	Anagrafici, dati fiscali, prodotti/servizi, condizioni di acquisto	
	Protocollo	Contratto	
Durata di conservazione	Per un anno dopo l’uscita dall’Elenco Fornitori. Successivamente segregato.		
Consenso	n.a.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata del Server LogicalDoc (locale) solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	06
-----------------------	-----------

Trattamento	Fornitori – Fatture		
Nome ed indirizzo del Responsabile del trattamento	Antonella Gabellone – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione acquisti.		
Dettaglio degli scopi del trattamento	Gestione acquisti.		
Servizio Responsabile dell’attuazione	Ufficio Acquisti		
Funzione della persona o del servizio che esercita il diritto accesso	Acquisti.		
Categorie di persone interessate dal trattamento	Fornitori		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Fornitori	Anagrafici	Cartacea
		Dati fiscali	Server : Easyfatt (locale) e PC Tanda / Gabellone
		Prodotti/servizi acquistati	
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Contabilità	Anagrafici, dati fiscali, prodotti/servizi	
	Acquisti	Anagrafici, dati fiscali, prodotti/servizi	
	Protocollo	Fattura	
Durata di conservazione	Per un anno dopo l’uscita dall’Elenco Fornitori. Successivamente segregato.		
Consenso	n.a.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo. La documentazione digitale è accessibile nell’area dedicata del Server Easyfatt (locale) e PC Tanda / Gabellone.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	07
-----------------------	-----------

Trattamento	Clienti – ASL		
Nome ed indirizzo del Responsabile del trattamento	Antonella Gabellone – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Erogazione del servizio.		
Dettaglio degli scopi del trattamento	Dati relativi alla gestione del servizio. Fatturazione attiva.		
Servizio Responsabile dell’attuazione	Amministrazione		
Funzione della persona o del servizio che esercita il diritto accesso	Amministrazione		
Categorie di persone interessate dal trattamento	Utenti del servizio.		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	ASL	Anagrafici	Cartacea
		Dati fiscali	Server : Portale Pagamenti Regione Lazio (remoto)
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Area Sanitaria	Anagrafici	
	Contabilità	Anagrafici e fiscali	
Durata di conservazione	Sempre		
Consenso	n.a.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata del Server Portale Pagamenti Regione Lazio (remoto) solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	08
-----------------------	-----------

Trattamento	Clienti – Comuni		
Nome ed indirizzo del Responsabile del trattamento	Antonella Gabellone – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Erogazione del servizio.		
Dettaglio degli scopi del trattamento	Dati relativi alla gestione del servizio. Fatturazione attiva.		
Servizio Responsabile dell’attuazione	Amministrazione		
Funzione della persona o del servizio che esercita il diritto accesso	Amministrazione		
Categorie di persone interessate dal trattamento	Utenti del servizio.		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Comuni	Anagrafici	Cartacea
		Dati fiscali	Server : EasyFatt (locale)
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Area Sanitaria	Anagrafici	
	Contabilità	Anagrafici e fiscali	
Durata di conservazione	Sempre		
Consenso	n.a.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata del Server EasyFatt (locale) solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	09
-----------------------	-----------

Trattamento	Clienti – Famiglie		
Nome ed indirizzo del Responsabile del trattamento	Antonella Gabellone – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Erogazione del servizio.		
Dettaglio degli scopi del trattamento	Dati relativi alla gestione del servizio. Fatturazione attiva.		
Servizio Responsabile dell’attuazione	Amministrazione		
Funzione della persona o del servizio che esercita il diritto accesso	Amministrazione		
Categorie di persone interessate dal trattamento	Utenti del servizio. Famiglie degli Utenti.		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Utenti	Anagrafici	Cartacea
		Dati fiscali	Server : Easyfatt (locale)
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Area Sanitaria	Anagrafici	
	Contabilità	Anagrafici e fiscali	
Durata di conservazione	Sempre		
Consenso	Modulo consenso Utenti.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata del Server EasyFatt (locale) solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	10
-----------------------	-----------

Trattamento	Personale – Dipendenti		
Nome ed indirizzo del Responsabile del trattamento	Serena Tanda – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione Dipendenti.		
Dettaglio degli scopi del trattamento	Gestione fascicolo personale ed adempimenti verso Enti preposti.		
Servizio Responsabile dell’attuazione	Amministrazione		
Funzione della persona o del servizio che esercita il diritto accesso	Personale		
Categorie di persone interessate dal trattamento	Personale.		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Personale	Anagrafici	Cartacea
		Dati fiscali	Server : PaCo (locale)
		Formazione / Curricula	
		Professionali	
		Presenze	
		Medicina del lavoro	
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Amministrazione	Anagrafici	
	Area sanitaria	Anagrafici, Formazione, Professionali	
	Contabilità	Anagrafici, fiscali, presenze	
Durata di conservazione	Fino a presenza in azienda. Dopo il dato viene segregato.		
Consenso	Modulo consenso Dipendenti.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata del Server PaCo (locale) solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	11
-----------------------	-----------

Trattamento	Personale – Liberi professionisti		
Nome ed indirizzo del Responsabile del trattamento	Serena Tanda – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione professionisti.		
Dettaglio degli scopi del trattamento	Gestione fascicolo professionisti ed adempimenti verso Enti preposti.		
Servizio Responsabile dell’attuazione	Amministrazione		
Funzione della persona o del servizio che esercita il diritto accesso	Personale		
Categorie di persone interessate dal trattamento	Personale.		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Personale	Anagrafici	Cartacea
		Dati fiscali	Server: PaCo (locale)
		Formazione / Curricula	
		Professionali	
		Presenze	
		Medicina del lavoro	
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Amministrazione	Anagrafici	
	Area sanitaria	Anagrafici, Formazione, Professionali	
	Contabilità	Anagrafici, fiscali, presenze	
Durata di conservazione	Fino a presenza in azienda. Dopo il dato viene segregato.		
Consenso	Modulo consenso Liberi Professionisti.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata del Server PaCo (locale) solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	12
-----------------------	-----------

Trattamento	Contabilità		
Nome ed indirizzo del Responsabile del trattamento	Antonella Gabellone – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione contabile/fiscale.		
Dettaglio degli scopi del trattamento	Gestione contabile fiscale (Bilancio, prima nota, scheda contabile, situazione trimestrale, controllo di gestione)		
Servizio Responsabile dell’attuazione	Amministrazione		
Funzione della persona o del servizio che esercita il diritto accesso	Contabilità. Controllo di gestione.		
Categorie di persone interessate dal trattamento	Dipendenti Collaboratori Liberi professionisti Fornitori Utenti		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Fornitori	Anagrafici, fiscali, fatture	Cartacea
	Dipendenti	Anagrafici, fiscali, presenze	Server : Numilia (Cloud)
	Collaboratori	Anagrafici, fiscali, presenze	
	Liberi professionisti	Anagrafici, fiscali, fatture	
	Utenti	Anagrafici, fiscali	
	Comuni	Anagrafici, fiscali, fatture	
	Famiglie	Anagrafici, fiscali, fatture	
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Organo amministrativo	Bilancio, Controllo di gestione	
	Consulente del lavoro	Presenze dipendenti e collaboratori	
	Consulente fiscale (Sa.CO S.r.l.s.)	Prima nota, scheda contabile, situazione trimestrale	
	Agenzia delle entrate	Destinatari, contenuti comunicazione	
	Famiglie	Compartecipazione	
	Comuni	Compartecipazione	
Durata di conservazione	Anno in corso. Dopo il dato viene segregato.		

Consenso	n.a.
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata del Server Numilia (Cloud) solo ad incaricati.
Aggiornamento (data ed oggetto)	12/02/2019 – Il Servizio è in migrazione su piattaforma AGYO con software “Senior” , la software House produttrice “Advenias” garantisce la totale compatibilità con il GDPR

Id Trattamento	13
-----------------------	-----------

Trattamento	Cartelle cliniche RSP		
Nome ed indirizzo del Responsabile del trattamento	Dott. Marco Capozza - Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Erogazione del servizio		
Dettaglio degli scopi del trattamento	Raccolta di tutti i dati anagrafici e sanitari dell’Utente sia in ingresso che in itinere.		
Servizio Responsabile dell’attuazione	Area Sanitaria		
Funzione della persona o del servizio che esercita il diritto accesso	Legale Rappresentante Medico Responsabile RSP Assistente sociale Coordinatore RSP Operatori coinvolti nei progetti riabilitativi Medici specialisti Medici di Medicina Generale		
Categorie di persone interessate dal trattamento	Utenti		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Sanitari	Anagrafici e sanitari	Cartacea
			Server : CartellaClinica.NET (Cloud Aruba)
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Medici specialisti	Anagrafica e sanitari utili per il controllo	
	Medici di Medicina Generale	Anagrafica e dati per la continuità terapeutica	
	Famiglia	Anagrafici e sanitari	
Durata di conservazione	Per sei mesi dopo le dimissioni. Dopo il dato viene segregato.		
Consenso	Consenso al trattamento dati Modulo Utente.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Archivio Cartelle Sanitarie al piano semiinterrato della Palazzina Amministrativa. La documentazione digitale è accessibile nell’area dedicata del Server CartellaClinica.NET (Cloud Aruba) solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	14		
Trattamento	Cartelle cliniche RSA		
Nome ed indirizzo del Responsabile del trattamento	Dott. Ciro Ruocco – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Erogazione del servizio		
Dettaglio degli scopi del trattamento	Raccolta di tutti i dati anagrafici e sanitari dell’Utente sia in ingresso che in itinere.		
Servizio Responsabile dell’attuazione	Area Sanitaria		
Funzione della persona o del servizio che esercita il diritto accesso	Legale Rappresentante Medico Responsabile RSA Assistente sociale Coordinatore RSA Operatori coinvolti nei progetti riabilitativi Medici specialisti Medici di Medicina Generale		
Categorie di persone interessate dal trattamento	Utenti		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Sanitari	Anagrafici e sanitari	Cartacea
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Medici specialisti	Anagrafica e sanitari utili per il controllo	
	Medici di Medicina Generale	Anagrafica e dati per la continuità terapeutica	
	Famiglia	Anagrafici e sanitari	
Durata di conservazione	Per sei mesi dopo le dimissioni. Dopo il dato viene segregato.		
Consenso	Consenso al trattamento dati Modulo Utente.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Archivio cartelle Sanitarie al piano terra della Palazzina “G”		

Aggiornamento (data ed oggetto)	03.01.2019 – il fascicolo Sanitario sta transitando su piattaforma informatica denominata E-Personam. La Software House produttrice “Advenias” garantisce la totale adesione al GDPR con pacchetto acquistato ad hoc.
--	---

Id Trattamento	15
-----------------------	-----------

Trattamento	SIPC		
Nome ed indirizzo del Responsabile del trattamento	Dott. Matteo Accornero – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Erogazione del servizio		
Dettaglio degli scopi del trattamento	Raccolta di tutti i dati anagrafici e sanitari dell’Utente sia in ingresso che in itinere. (https://www.regione.lazio.it/servizi/sipc/sipclogin.php)		
Servizio Responsabile dell’attuazione	Area Sanitaria		
Funzione della persona o del servizio che esercita il diritto accesso	Legale Rappresentante Medico Responsabile RSP Assistente sociale Coordinatore RSP Operatori coinvolti nei progetti riabilitativi Medici specialisti Medici di Medicina Generale		
Categorie di persone interessate dal trattamento	Utenti		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Sanitari	Anagrafici e sanitari	Cartacea
			Server: SIPC (Cloud)
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Medici specialisti	Anagrafica e sanitari utili per il controllo	
	Medici di Medicina Generale	Anagrafica e dati per la continuità terapeutica	
	Famiglia	Anagrafici e sanitari	

Durata di conservazione	Per sei mesi dopo le dimissioni. Dopo il dato viene segregato.
Consenso	Consenso al trattamento dati Modulo Utente.
Misure di sicurezza – Tecniche organizzative	La documentazione digitale è accessibile nell'area dedicata del Server SIPC (Cloud) solo ad incaricati.
Aggiornamento (data ed oggetto)	28.04.2018

Id Trattamento	16
-----------------------	-----------

Trattamento	Archivio Cartelle Cliniche Pazienti dimessi		
Nome ed indirizzo del Responsabile del trattamento	Dott. Matteo Accornero – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione Cartelle Cliniche Pazienti dimessi.		
Dettaglio degli scopi del trattamento	Gestione delle Cartelle Cliniche segregate da rendere eventualmente disponibili ai sanitari e/o ai familiari che ne hanno titolo.		
Servizio Responsabile dell’attuazione	Area Sanitaria		
Funzione della persona o del servizio che esercita il diritto accesso	Segreteria Sanitaria		
Categorie di persone interessate dal trattamento	Utenti Famiglie		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Sanitari	Anagrafici e sanitari	Cartacea
			Server : CartellaClinica:NET (Cloud Aruba)
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Utenti	Anagrafici e sanitari	
	Famiglie	Anagrafici e sanitari	
Durata di conservazione	Tempo indeterminato.		
Consenso	n.a.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Archivio Cartelle Sanitarie nel piano seminterrato Palazzina “C” La documentazione digitale è accessibile nell’area dedicata del Server Cartella Clinica: NET solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Id Trattamento	17
-----------------------	-----------

Trattamento	Lista di attesa SRP		
Nome ed indirizzo del Responsabile del trattamento	Emanuele Kirieleison – Via di Tor Cervara 112 - 00155 Roma		
Data di implementazione	28.04.2018		
Principale finalità	Gestione Lista di attesa RSP		
Dettaglio degli scopi del trattamento	Gestione della lista di attesa di ciascun servizio secondo i criteri previsti.		
Servizio Responsabile dell’attuazione	Area Sanitaria		
Funzione della persona o del servizio che esercita il diritto accesso	Caposala SRP		
Categorie di persone interessate dal trattamento	Utenti Famiglie		
Dati elaborati	Categorie di dati trattati	Dettaglio dei dati trattati	Modalità di conservazione
	Sanitari	Anagrafici e sanitari	Cartacea
			Server: SIPC (Cloud)
Categorie dei destinatari	Categorie dei destinatari	Dati interessati	
	Utenti	Anagrafici e sanitari	
	Famiglie	Anagrafici e sanitari	
Durata di conservazione	Fino ad ingresso in terapia dell’Utente o fino a rinuncia.		
Consenso	Consenso al trattamento Modulo Utente.		
Misure di sicurezza – Tecniche organizzative	Tutta la documentazione cartacea è conservata presso l’archivio identificato come: Ufficio Amministrativo La documentazione digitale è accessibile nell’area dedicata del Server Server: SIPC (Cloud) solo ad incaricati.		
Aggiornamento (data ed oggetto)	28.04.2018		

Materiali e metodi

La tecnica FMEA è un metodo qualitativo, attraverso il quale, dall'analisi delle singole attività di un processo, è possibile individuare i difetti o gli errori che possono accadere durante un processo e, quindi, implementare azioni di miglioramento per evitarne l'accadimento. A integrazione della FMEA viene solitamente utilizzata la tecnica FMECA, che, rispetto alla prima, introduce delle valutazioni quantitative di ogni failure mode.

Il presupposto sottostante l'applicazione delle tecniche FMEA e FMECA è il principio secondo il quale il rischio, definito come «una combinazione tra la probabilità di accadimento di un danno e la severità di quest'ultimo», sia correlato non soltanto alla probabilità che si verifichi un errore, ma anche alla gravità delle sue conseguenze e alla possibilità di intercettarlo prima che si verifichi (rilevabilità). Pertanto, ad ogni failure mode sono assegnati tre valori numerici relativi a: gravità, probabilità di accadimento e rilevabilità. Il prodotto dei tre valori è definito come Indice di Priorità di Rischio (IPR) e permette di attribuire una priorità alle azioni di miglioramento da realizzare.

L'applicazione della FMEA/FMECA si compone solitamente di 5 step:

1. scelta del processo critico da analizzare;
2. costituzione del team multidisciplinare;
3. raccolta e organizzazione delle informazioni inerenti il processo da sottoporre ad analisi;
4. conduzione dell'analisi dei rischi;
5. sviluppo e implementazione delle azioni di miglioramento e monitoraggio degli outcome.

La scelta del processo critico da analizzare è generalmente influenzata dalla sua complessità e dalla pericolosità sulla sicurezza.

È opportuno che il team, coordinato da un leader, sia multidisciplinare e composto da professionisti con compiti diversi, ma tutti esperti del processo da analizzare.

Successivamente, il team scompone il processo nelle diverse fasi e attività e in una flow chart viene rappresentato "ciò che accade realmente" nella pratica.

I failure mode, che rappresentano ciò che può andare "storto" in ogni fase del processo, possono dipendere da errori umani, difficoltà comunicative, criticità nelle attrezzature, od ogni altra criticità che possa interrompere il processo e influire sulla sicurezza del paziente. Obiettivo del team è quindi l'identificazione del maggior numero possibile di failure mode.

Successivamente, il team descrive gli effetti dei failure mode individuati: se non vi sono meccanismi di controllo sufficienti, i failure mode potrebbero avere esiti importanti.

In ogni caso, anche se ogni evento potrebbe produrre un danno, non tutti risultano ugualmente significativi in termini di esito. Durante quest'attività, al team è richiesta una stima della gravità di ogni failure mode, attraverso scale di valutazione, disponibili in letteratura.

In un secondo tempo, il team deve stimare, allo stesso modo, la probabilità di accadimento di ogni failure mode e la loro rilevabilità, per arrivare, attraverso il prodotto dei punteggi ottenuti con i tre criteri di valutazione, a definire l'Indice di Priorità di Rischio (IPR).

Il piano delle azioni di miglioramento viene quindi costruito a partire dalla classificazione, secondo i valori IPR, dei failure mode. Il team, quindi, periodicamente monitorerà e valuterà periodicamente la sicurezza del processo e delle azioni di miglioramento adottate.

Il progetto si è articolato nelle seguenti fasi:

1. revisione e analisi della letteratura;
2. costituzione di un gruppo aziendale di progetto;
3. realizzazione di un percorso formativo;
4. analisi quali-quantitativa dei processi individuati con applicazione della FMEA;
5. individuazione degli interventi di miglioramento;

successivamente sarà effettuata una valutazione di efficacia degli interventi realizzati e messa a regime degli interventi validati.

F.M.E.A.

Il Metodo F.M.E.A. Failure mode and effect analysis - Analisi dei modi di guasto/errore e dei loro effetti - , può essere applicato anche alla Stima/Valutazione del Rischio Sicurezza lavoro e può risolvere delle incoerenze e semplificazioni eccessive degli algoritmi $R = P \times D$.

Indice di Rischio (R) = P x D

P = Probabilità accadimento dell'evento

D = Danno

Score	Probabilità di accadimento	Danno a seguito dell'accadimento
1	Improbabile	Lieve
2	Poco probabile	Medio
3	Probabile	Grave
4	Altamente probabile	Gravissimo

F.M.E.C.A.

F.M.E.C.A Failure Mode, Effects, and Criticality Analysis - Analisi dei modi, degli effetti e della criticità dei guasti

Gravità

Livello di Gravità	Criteri di gravità	Score
Molto alta	L'errore può provocare gravissimi danni	10-9
Alta	L'errore può provocare gravi danni	8-7
Media	L'errore può provocare danni transitori	6-5
Bassa	L'errore non provoca danni al paziente ma genera alterazioni nel normale flusso di lavoro	4-3
Nulla	L'errore non provoca nessun tipo di danno	2-1

Probabilità

Livello di Probabilità	Criteri di probabilità	Score
Molto frequente	Frequenza settimanale/giornaliera	9-10
Frequente	Frequenza mensile/più volte al mese	7-8
Moderata	Frequenza annuale/più volte l'anno	5-6
Bassa	Ogni 1-5 anni	3-4
Molto bassa	Frequenza > 5 anni	1-2

Rilevabilità

Livello di rilevabilità	Rilevabilità	Score
Rilevabilità dell'errore quasi impossibile	I controlli disponibili non permettono di rilevare l'evento prima che esso si verifichi se non in modo del tutto casuale	9-10
Rilevabilità dell'errore bassa	I controlli disponibili permettono di rilevare l'evento prima che esso si verifichi in un basso numero di casi	7-8
Rilevabilità dell'errore alta	I controlli disponibili permettono di rilevare l'evento prima che esso si verifichi in un alto numero di casi	4-5-6
Rilevabilità dell'errore quasi certa	I controlli disponibili permettono di rilevare l'evento prima che esso si verifichi nella quasi totalità dei casi	1-2-3

Indice di Priorità del Rischio (I.P.R.) = G x P x R

G = Score Gravità evento lesivo

P = Score Probabilità evento lesivo

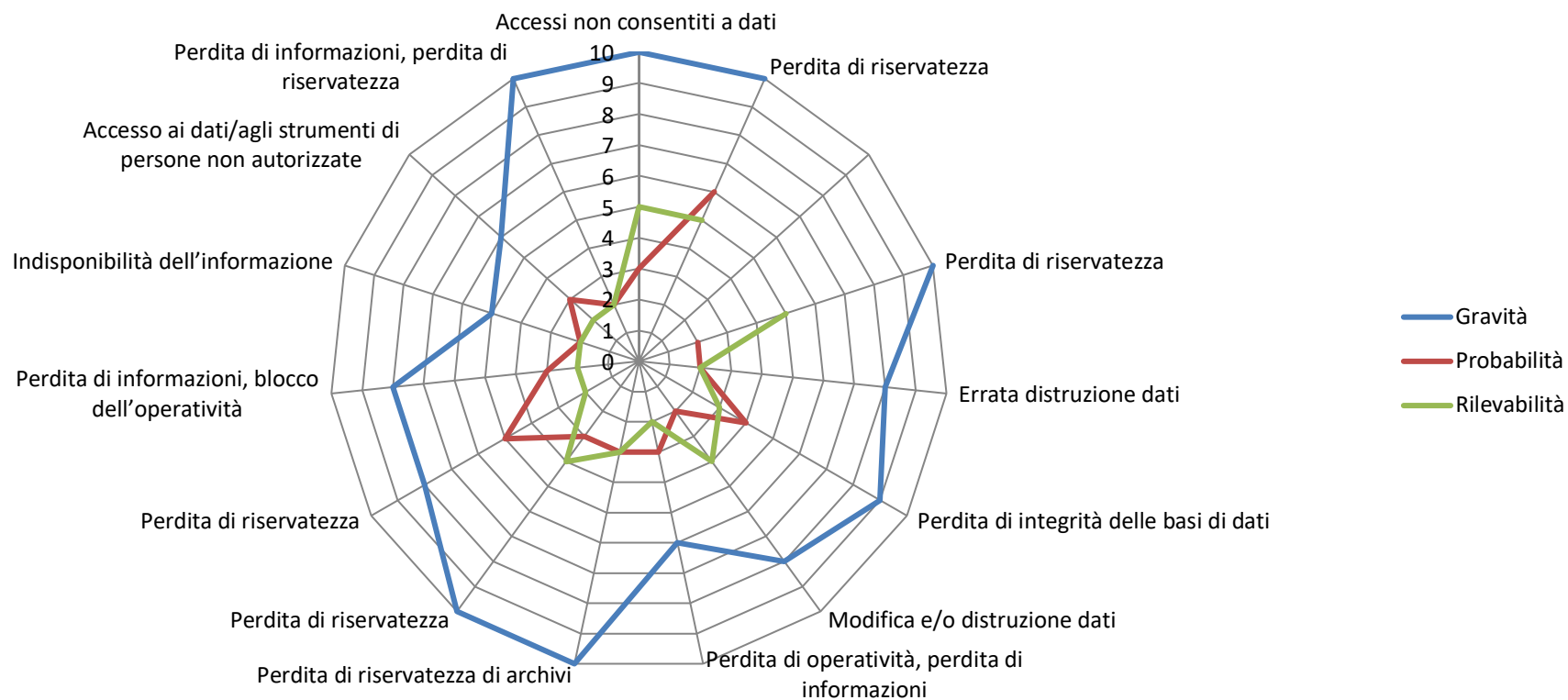
R = Score Rilevabilità evento lesivo

Livelli di intervento

Criticità	I.P.R. (Indice Priorità del Rischio)
Nessuna criticità	1 <= I.P.R. <= 20
Bassa criticità	21 <= I.P.R. <= 50
Media criticità	51 <= I.P.R. <= 70
Elevata criticità	71 <= I.P.R. <= 100
Altissima criticità	I.P.R. >= 101

Categoria	Evento	Rischio	G	P	R	I.P.R.	Azione
OPERATORI	Furto di credenziali di autenticazione	Accessi non consentiti a dati	10	3	5	150	A01
	Carenza di consapevolezza, disattenzione o incuria nella conservazione della documentazione	Perdita di riservatezza	10	6	5	300	A02 A07
	Comportamenti sleali o fraudolenti Sottrazione documentazione	Perdita di riservatezza	10	2	5	100	A03
	Errore materiale	Errata distruzione dati	8	2	2	32	
STRUMENTI	Azione di virus informatici o di codici malefici	Perdita di integrità delle basi di dati	9	4	3	108	A04
	Spamming o altre tecniche di sabotaggio	Modifica e/o distruzione dati	8	2	4	64	A02
	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita di operatività, perdita di informazioni	6	3	2	36	A05
	Accessi esterni non autorizzati	Perdita di riservatezza di archivi	10	3	3	90	A03
	Intercettazione di informazioni in rete	Perdita di riservatezza	10	3	4	120	A12
CONTESTO	Accessi non autorizzati a locali/reparti ad accesso ristretto	Perdita di riservatezza	8	5	2	80	A07
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di informazioni, blocco dell'operatività	8	3	2	48	A09
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	Indisponibilità dell'informazione	5	2	2	20	A11
	Errori umani nella gestione della sicurezza fisica: chiusura sede fuori orario	Accesso ai dati/agli strumenti di persone non autorizzate	6	3	2	36	A10
	Asportazione e furto di strumenti contenenti dati	Perdita di informazioni, perdita di riservatezza	10	2	2	40	A10

Grafico dei rischi secondo l'attuale valutazione F.M.E.C.A.



Azioni da porre in essere

Di seguito sono riportate, in forma sintetica, le misure in essere e da adottare a contrasto dei rischi individuati dall'analisi dei rischi. Per misura qui s'intende non solo lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia ma anche tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia. Senza procedure di controllo periodico, infatti, nessuna misura può essere considerata completa.

Informazioni contenute nelle tabelle

Misure: la descrizione sintetica della misura di sicurezza adottata.

Data base/trattamento interessato: riporta l'identificativo del (dei) data base o dell'archivio informatizzato e dei trattamenti interessati per ciascuna delle misure adottate.

E' da notare che determinate misure possono non essere riconducibili a specifici trattamenti o basi di dati.

Trattamento interessato: il trattamento dei dati interessati (o la categoria).

Data di effettività: per ogni misura si è indicata la data, a partire dalla quale, la misura è operativa o se già operativa una dicitura standard (ad es.: 'in essere').

Periodicità e responsabilità dei controlli: contiene l'indicazione della periodicità con cui sono verificate la funzionalità e l'efficienza della misura in questione e della struttura operativa che ne ha la responsabilità.

Data di aggiornamento: indica sempre la data a cui l'informazione si riferisce.

Informazioni descrittive analitiche delle misure di sicurezza

Oltre alle informazioni sintetiche sopra riportate può essere utile compilare, per ciascuna misura una scheda analitica contenente un maggior numero di informazioni, utili nella gestione operativa della sicurezza ed, in particolare, nelle attività di verifica e controllo.

Queste schede sono a formato libero e le informazioni utili devono essere decise in funzione della specifica misura.

A puro titolo di esempio, potranno essere inserite informazioni relative a:

- la minaccia che s'intende contrastare;
- la tipologia della misura di sicurezza (preventiva, di contrasto, di contenimento degli effetti,...);
- le informazioni relative alla responsabilità dell'attuazione e della gestione della specifica misura;
- i tempi di validità delle scelte adottate (contratti esterni, aggiornamento di prodotti, ...)
- gli ambiti a cui si applica (ambiti fisici: un reparto, un edificio, ... – o logici: una procedura, un'applicazione, ...)
- ...

E' comunque opportuno mantenere l'indicazione di chi ha compilato la scheda e della data in la compilazione è stata terminata.

Le misure di sicurezza adottate o da adottare					
Id	Misura	Data base interessato	Trattamento interessato	Data di effettività o 'in essere'	Periodicità e responsabilità dei controlli
A01	Sensibilizzazione del personale sulla riservatezza delle credenziali (formazione)	Amministrazione Sanitario	Tutti	In essere	Annuale
A02	Adozione di procedure per la gestione delle pratiche	Amministrazione Sanitario	Tutti	In essere	Aggiornamento quotidiano
A03	Definizione più stretta dei profili di autorizzazione e controllo delle dimissioni (togliere badge accesso uffici chiudere account)	Amministrazione Sanitario	Tutti	In essere	Aggiornamento semestrale
A04	Antivirus e controlli perimetrali già in funzione	Amministrazione Sanitario	Tutti	In essere	Aggiornamento quotidiano
A05	Disponibilità di risorse hardware di back up	Amministrazione Sanitario	Tutti	In essere	Aggiornamento quotidiano
A07	Chiusura dei locali in dedicati alla conservazione della documentazione	Amministrazione Sanitario	Tutti	In essere	Aggiornamento quotidiano
A09	Custodia delle copie di backup	Amministrazione Sanitario	Tutti	In essere	Aggiornamento quotidiano
A10	Videosorveglianza	Amministrazione Sanitario	Tutti	In essere	Aggiornamento quotidiano
A11	Manutenzione agli impianti (continuità elettrica, etc.)	Amministrazione Sanitario	Tutti	In essere	Aggiornamento annuale
A12	Vulnerability assessment / Penetration test. Installazione sistemi di sicurezza (Firewall fisici)	Amministrazione Sanitario	Tutti		Aggiornamento quindicinale

3 Esito del vulnerability assessment

3.1 Collegamento ad internet

Il collegamento Internet avviene attraverso Fibra Ottica (ISP Vodafone S.p.A.) oppure tramite RTG, inoltre la Società possiede

l'accreditamento per l'effettuazione del servizio "R.O.L." (Raccomandate On Line) erogato da Poste Italiane S.p.A.

Specificatamente ai PC:

- I PC, equipaggiati con S.O. Windows 10 sono protetti da Windows Defender; i computer di Apple dotati della versione 10.13.4 di macOS sono protetti dal software Bitdefender.
- Tutti i PC utilizzano i software del pacchetto "Office" della Microsoft

Specificatamente alla Connessione Internet:

- Tutta la intranet del Castello della Quiete è protetto da un firewall hardware prodotto da CISCO (idoneo a proteggere i PC contro il rischio di intrusione e dall'azione di programmi idonei a danneggiare i dati in essi contenuti).

3.2 Backup

Luogo di custodia dei supporti di memorizzazione

Tutti i backup, che vengono effettuati con cadenza giornaliera, sono custoditi su uno specifico NAS presso la sede operativa della Società all'interno di cassetto, munito di chiusura a chiave, sito nei locali archivio. Tale NAS è protetto all'accesso da un'autenticazione a due fattori.

Le chiavi di apertura del locale archivio sono detenute dai dipendenti dell'ufficio Amministrativo.

3.3 Tipologia di accesso e di connessione

La connessione a ciascun PC avviene tramite il codice di identificazione (Password di Postazione) che viene modificato dal personale utente dei PC medesimi con cadenza trimestrale (90 giorni).

Tutto il Personale non inquadrato con la tipologia di "Quadro" della Società, prima di accedere alla sede operativa effettua la timbratura del proprio "Turno di Presenza" utilizzando il proprio Cartellino di Identificazione munito di banda magnetica nell'apposito lettore.