PQ009: REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (RGPD)
(GDPR General Data Protection Regulation)

N. Rev.	Descrizione Modifiche
1	Prima emissione (In sostituzione della procedura PQ 4.2.3-02-01 ISO 9001:2008)
2	Integrazioni e modifiche in base al nuovo regolamento europeo 679/2016
3	Ulteriori precisazioni capitolo 7
4	Inserito schema attività creazione account e gestione documentazione
5	Ampliato prf 6.5.1 data breach
6	Inserito prf 6.1.7 Firma Grafometrica
7	Inserito nuovo controllo con software antivirus ESET prf 7.1

INDICE

1. SCOPO

Pianifica, disegna, implementa e gestisce le opportune contromisure di natura fisica, logica ed organizzativa al fine di realizzare un sistema di sicurezza efficace ed efficiente per il trattamento dei dati sensibili e non sensibili. L'approccio globale prevede l'esecuzione delle seguenti attività:

- Analisi del rischio
- Definizione delle Politiche della Sicurezza
- Gestione del rischio
- Piano Operativo
- Audit
- Formazione
- Organizzazione

2. CAMPO DI APPLICAZIONE

La procedura si applica a tutte le attività previste nell'ambito della gestione ed il trattamento dei dati sensibili e non sensibili (riservati), siano essi archiviati su supporto elettronico, cartaceo o su qualsiasi altro supporto, e dell'accesso agli stessi da parte delle varie funzioni aziendali.

3. RIFERIMENTI

Norme e Leggi:

UNI EN ISO 9001:2015 Sistemi di gestione per la qualità. Requisiti.

	7.5.2 Creazione e aggiornamento
	7.5.3 Controllo delle informazioni documentate
MGQ01	Manuale della Qualità
Regolamento Europeo 679/2016	Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali
Provvedimento del garante 9 novembre 2005	Provvedimento e considerazioni riguardanti art.83 del Codice Privacy

Procedure, Protocolli ed Istruzioni:

Le procedure e le istruzioni operative in vigore e utilizzate dal sistema sono presenti, elencate e disponibili per la stampa e la consultazione nella pagina intranet aziendale dedicata al servizio.

4. DEFINIZIONI / ABBREVIAZIONI

DA	Direttore Amministrativo
DS	DIRETTORE SANITARIO
IO	Istruzione Operativa
LC	Lista di controllo
LG	Linee Guida
M	Modulo
MQ	Manuale della Qualità
PERS	Direttore del Personale
PI	Protocollo infermieristico
PM	Protocollo medico
PQ	Procedure
RDQ	Responsabile della direzione per la qualità
RQ	Responsabile qualità
RTD	Responsabile trattamento dati

5. MODULISTICA CORRELATA

Figure:

Fig. 1	Organigramma del Servizio

Moduli e Liste di controllo:
I moduli e le liste di controllo in vigore utilizzate dal sistema sono presenti, elencate e disponibili per la stampa e la consultazione nella pagina intranet aziendale dedicata al servizio.

6. ANALISI DEL RISCHIO

La fase di partenza della progettazione del piano aziendale della sicurezza è costituita dalla definizione degli obiettivi per la sicurezza procedendo ad un'analisi dettagliata degli elementi che necessitano di una protezione e delle minacce cui possono essere sottoposti.

6.1 CATALOGAZIONE, IDENTIFICAZIONE E VALUTAZIONE DEI BENI DA PROTEGGERE

Si è proceduto ad una dettagliata catalogazione dei beni stabilendo alcuni criteri di valutazione numerici al fine di valutare il livello d'impatto sia ai fini della sicurezza ma anche della strategicità degli stessi all'interno del Sistema Informativo.
Allo scopo si utilizza la DPIA: DATA PROTECTION IMPACT ASSESSMENT emessa dal team di consulenti esterni coordinato dal DPO.

6.1.1 Risorse Hardware

Rientrano in questa categoria le CPU, i terminali, le workstation, i personal computer, le stampanti, i disk drive, le linee di comunicazione, i router, i server, e in generale tutti i dispositivi (inclusi i telefoni cellulari). Le minacce principali su questi dispositivi sono:

- mal funzionamenti dovuti a guasti o sabotaggi;
- mal funzionamenti dovuti ad eventi naturali quali allagamenti, temporali ed incendi;
- furti ed intercettazioni: questa minaccia interessa particolarmente le linee di comunicazione, i router ed i server. E' infatti possibile effettuare il monitoraggio indebito o l'alterazione della trasmissione di dati effettuata su questi apparati, sia che questa avvenga tra terminali, tra computer, tra stazioni di lavoro periferiche e sistemi centrali di elaborazione, intercettazione delle onde elettromagnetiche emesse dai video per ricostruire remotamente l'immagine.

L'elenco dettagliato delle risorse hardware è gestito da apposito programma.

6.1.2 Risorse Software

Rientrano in questa categoria i Sistemi Operativi e Software di base (Utility e diagnostici), Software Applicativi, Gestori di basi di dati, Software di rete, i programmi in formato sorgente ed oggetto. Le minacce principali legate all'uso di questi prodotti sono:

- la presenza di errori involontari commessi in fase di progettazione e/o implementazione che consentono ad utenti non autorizzati l'esecuzione di operazioni e programmi riservati a particolari categorie di utenti;
- la presenza di codice malizioso inserito volontariamente dai programmatori dell'applicazione stessa, al fine di poter svolgere operazioni non autorizzate sul sistema o per danneggiare lo stesso. Rientrano in questa categoria i Virus, i cavalli di troia, le bombe logiche, le backdoor;
- attacchi del tipo denial of service che vengono portati a servizi di rete ma sono facilmente estendibili ad un qualunque servizio. Si tratta di attacchi non distruttivi il cui obbiettivo è saturare la capacità di risposta del servizio con l'obiettivo di renderlo inutilizzabile agli altri utenti del sistema.

Particolare importanza rivestono anche i formati sorgente delle applicazioni che possono essere oggetto di furto per eventuale rivendita ad altre organizzazioni o di modifica per l'inserimento di codice malizioso.

L'elenco dettagliato delle risorse Software è contenuto in programma apposito.

6.1.3 Banche dati

Rientrano in questa categoria il contenuto degli archivi, delle basi di dati, dati di transito, copie storiche, file di log. Le minacce a cui sono sottoposti sono legate alle debolezze dei sistemi operativi e delle applicazioni che operano sulle macchine su cui risiedono e sono riconducibili a due categorie:

- accesso non autorizzato cioè la possibilità per utenti esterni od interni di visualizzare informazioni riservate a particolari categorie di utenti;
- modifiche deliberate o accidentali provocate nel primo caso da utenti non autorizzati che procedono alla cancellazione o alla modifica di dati a loro non appartenenti, e nel secondo caso provocate da utenti autorizzati che inavvertitamente procedono alla modifica o cancellazione di informazioni significative.

6.1.4 Le risorse professionali

Rientrano in questa categoria gli amministratori di sistemi, i sistemisti, i programmatori, gli operatori, gli utenti finali, i manutentori hardware e software, i consulenti.
Questa categoria può essere oggetto di minacce che compromettono la sicurezza del sistema ma a loro volta può costituire una minaccia per la sicurezza dello stesso.
Nel primo caso il personale può essere soggetto ad attacchi così detti di social engineering in cui estranei cercano attraverso varie strategie di ottenere informazioni utili ad attaccare il sistema quali le password utenti, il contenuto dei file di configurazione, gli indirizzi IP delle macchine ecc.
Il personale diventa una minaccia quando matura motivi di rivalsa nei confronti dell'azienda o quando ha una scarsa consapevolezza del problema sicurezza.

6.1.5 Documentazioni cartacee

Rientrano in questa categoria tutti i documenti cartacei relativa a documentazione contenente dati personali sensibili, ai programmi, all'hardware, ai sistemi, alle procedure di gestione. Le principali minacce sono:

- la distruzione accidentale e/o alterazione ad opera di eventi naturali, di azioni accidentali e di comportamenti intenzionali.

6.1.6 Supporti di memorizzazione

Rientrano in questa categoria i supporti su cui vengono tenute le copie dei software installati, le copie dei file di log e dei backup. Le principali minacce oltre a quelle elencate per i dispositivi cartacei sono:

- deterioramento nel tempo;
- inaffidabilità del mezzo fisico che in alcuni casi può presentare difetti di costruzione che ne compromettono il buon funzionamento nel tempo;
- l'evoluzione tecnologica del mercato.

6.1.7 Firma Grafometrica: archiviazione e consenso

CARATTERISTICHE DEL SISTEMA IN ESSERE PRESSO LA CASA DI CURA ERETENIA SPA PER L'USO DELLA FIRMA ELETTRONICA (ai sensi dell'art. art. 57, lett. e) delle Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, pubblicate in Gazzetta Ufficiale n. 117 del 21.05.2013, attuative del Codice dell'Amministrazione Digitale (decreto legislativo 07.03.2005, n. 82, e successive modificazioni).

La Casa di Cura Eretenia utilizza un sistema di Firma Elettronica per la sottoscrizione di documenti informatici.

Il processo associato al sistema di Firma Elettronica garantisce l'identificazione del firmatario, la connessione univoca della firma al firmatario, il controllo esclusivo del firmatario del sistema di generazione della firma, la possibilità di verificare che il documento non abbia subito modifiche dopo l'apposizione della firma, la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto e l'individuazione dell'intermediario Casa di Cura Eretenia Spa che realizza la soluzione di Firma Elettronica.
La Casa di Cura Eretenia Spa identifica preliminarmente il firmatario dei documenti richiedendo il relativo documento d'identità in corso di validità.

Il software registra le caratteristiche dinamiche della firma autografa, che il firmatario appone di suo pugno con penna elettronica su un apposito dispositivo, il tablet. la rappresentazione informatica della firma racchiude informazioni superiori alla raccolta della firma autografa su carta. L'univocità della connessione viene garantita dalla sottoscrizione effettuata davanti all'operatore, previa identificazione del firmatario, e alla possibilità di effettuare opportuna perizia grafica, in modo del tutto equivalente ad una firma autografa su carta.

Le tecnologie di firma elettronica utilizzate (sia per la firma grafometrica che per le "firme tecniche", includono le impronte informatiche (hash) del contenuto soggetto a sottoscrizione. Il controllo della corrispondenza tra un'impronta ricalcolata e quella "sigillata" all'interno delle firme permette di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma.

Il certificato di firma della "Firma Elettronica" individua il soggetto erogatore del servizio ed è emesso da un'autorità di certificazione tecnica, riconducibile alla Casa di Cura Eretenia Spa per tramite del fornitore della soluzione tecnologica Multimedia S.r.l.

I documenti prodotti dal sistema utilizzano esclusivamente formati atti a garantire l'assenza, nell'oggetto della sottoscrizione, di qualunque elemento idoneo a modificare gli atti, i fatti e i dati in essi rappresentati. Ad esempio, attualmente, i documenti sono esclusivamente in formato standard ISO PDF/A.

I dati della firma, nel caso in cui conceda il consenso, vengono inseriti nel documento in una struttura, detta "vettore grafometrico", che li unisce indissolubilmente all'impronta informatica del documento sottoscritto. Questa struttura è protetta con opportuna tecnica crittografica, al fine di preservare la firma da ogni possibilità di estrazione o duplicazione. L'unica chiave crittografica in grado di estrarre le informazioni è in esclusivo possesso della Casa di Cura Eretenia Spa e potrà essere usata in sede di perizia per attestare l'autenticità del documento e della sottoscrizione.

Il programma si appoggia su delle librerie di terze parti, ovvero la soluzione Firma Certa SDK sviluppata dalla società Namirial e studiata per gestire in digitale quei documenti che prevedono un passaggio cartaceo per l'apposizione di firme autografe.

Le principali caratteristiche della soluzione FirmaCerta di Namirial sono:

1. La misurazione dei parametri biometrici che consente di identificare **univocamente la firma di una persona**; un'altra persona che cerchi di imitare la firma originale fa rilevare parametri diversi e può essere riconosciuta.
2. I falsi positivi (falsificazione di firma) sono quasi impossibili
3. Ogni singola **firma** ha una sua **validità legale**.
4. La firma che viene apposta è trattata in **vettoriale**, mantiene quindi le caratteristiche di integrità e di qualità, con un'incidenza minima sull'aumento delle dimensioni del file.
5. Utilizzabile da postazioni fisse in rete o in terminal server (Windows, Citrix) senza rallentamenti.

L'ambiente di sviluppo utilizzato è PowerBuilder 9.02, l'integrazione utilizza un componente ActiveX (fcx.dll) che opportunamente installato e registrato mette a disposizione un interfaccia che espone una serie di metodi necessari per gestire il processo di firma.

L'intero processo può essere così riassunto:

1) Generazione del documento da firmare
2) Apposizione della firma
3) Archiviazione del documento firmato

I documenti sono generati in formato PDF sul quale viene apposta la firma. Al termine del processo di firma il documento viene archiviato nel Repository di Medica ed è disponibile per l'eventuale consultazione. L'informazione raccolta durante la fase di produzione del documento della Privacy quale il consenso alla pubblicazione del referto, il consenso alla produzione del fascicolo sanitario ed altro viene opportunamente tratta in Medica così da predisporre le eventuali azioni di tutela privacy secondo le volontà espresse dal paziente.

I clienti possono richiedere gratuitamente presso lo sportello dell'accettazione (CUP) o tramite email all'indirizzo urp@eretenia.com , allegando la copia della carta d'identità, copia cartacea del modulo di adesione al servizio di Firma Elettronica nonché degli atti e dei documenti così sottoscritti.
La firma elettronica può essere utilizzata per la firma della Dichiarazione di consenso al trattamento dei dati e al dossier sanitario elettronico al fine di ottimizzare la gestione dei documenti comprovanti il consenso al trattamento dei dati dei pazienti.

6.2 CONTROMISURE DA ADOTTARE PER INNALZARE IL LIVELLO DI SICUREZZA

Le contromisure da attuare sono contenute nel **M0006 PrivacyImpactAssessment** che fanno una istantanea del sistema di sicurezza attraverso un complesso audit specifico e vengono poi esplicitate nello stesso documento che analizzare le misure necessarie per minimizzare, mitigare o innalzare il livello di sicurezza aziendale e in particolare:

- vulnerabilità;
- danno potenziale;
- probabilità che si verifichi un evento negativo;
- costo di ripristino;
- priorità nell'implementazione dei meccanismi di sicurezza;
- contromisure urgenti, ordinarie, future.

Per la valutazione del rischio ci affidiamo ad una analisi numerica attraverso una matrice di rischio inclusa nel **M0006 PrivacyImpactAssessment**.
Ad un rischio maggiore corrisponderanno maggiori controlli e viceversa ad un rischio minore minori controlli secondo quanto specificato in Tabella 1. Le situazioni ad alto rischio vanno comunque sanate con interventi radicali.

6.3 INDIVIDUAZIONE DEGLI OBIETTIVI DI SICUREZZA (Politiche di Sicurezza), STRATEGIE DI GESTIONE DEL RISCHIO

La Casa di Cura Eretenia Spa si impegna a garantire il massimo della riservatezza nel trattamento dei dati personali in applicazione delle misure minime elencate nel regolamento definito nel Regolamento Europeo n. 2016/679.
A questo scopo nomina un responsabile della protezione dei dati (RDP) che avvalendosi della collaborazione dei responsabili interni ed esterni, si incaricherà di verificare nel tempo e indicare opportune misure di adeguamento del sistema di sicurezza della Casa di Cura Eretenia Spa e la gestione del dato sensibile.
In particolare RDP dovrà:

- Eseguire opportuni audit sul sistema informativo e in generale sulla gestione della documentazione anche in forma cartacea in osservanza del Regolamento Europeo n. 2016/679 avvalendosi della collaborazione dei responsabili interni ed esterni.
- Collaborare e applicare le prescrizioni impartite dal Garante.
- Coordinare assieme ai responsabili interni ed esterni, attività operative degli incaricati del trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento nell'ambito del sistema informatico.
- Predisporre ed aggiornare il sistema di sicurezza idoneo a rispettare le prescrizioni, nonché fornire istruzioni per adeguare il sistema alle future norme regolamentari in materia di sicurezza in osservanza alle disposizioni del Regolamento Europeo n. 2016/679.
- Comunicare al titolare e ai responsabili qualsiasi elemento oggettivo o soggettivo che possa compromettere il corretto trattamento dei dati personali

Rientrano nel campo di applicazione tutti i documenti che contengano dati personali idonei a rivelare lo stato di salute e la vita sessuale dei pazienti, dati che rientrano nel novero delle informazioni definite sensibili come descritto nel decreto.
Le risorse informative sono un patrimonio che deve essere protetto dal momento in cui viene creato, installato, utilizzato fino al momento in cui viene distrutto. Con questi obiettivi mettiamo in evidenza gli aspetti più significativi.

6.3.1 Classificazione delle informazioni

Obiettivo: Classificare le informazioni e le banche dati sia su supporto informatico che cartaceo.

Nota 1: Definiamo come informazioni riservate tutte quelle che possano rivelare lo stato di salute del paziente, altre informazioni ad uso interno sono anch'esse da ritenersi riservate ma con contenuti non collegabili all'ambito del trattamento dei dati sensibili.

Attività 1	Registro dei trattamenti
Soggetto	Resp. trattamento dati
Elementi in ingresso	Nuova banca dati
Informazioni esistenti:	Precedente aggiornamento del modulo M-16-20 Registro dei trattamenti.
Controlli	Controlli semestrali creazione nuove banche dati
Elementi in uscita	M-16-20 Registro dei trattamenti.

6.3.2 Protezione fisica delle risorse

Obiettivo: Predisporre un ambiente di lavoro sicuro che impedisca perdite di informazione.

Le risorse informatiche e documentali debbono essere adeguatamente protette predisponendo un ambiente di lavoro sicuro che impedisca perdite di informazioni e di patrimonio intellettuale, promuovendo la protezione delle risorse e la riduzione dei rischi di interruzione del servizio. Per questo è necessario tenere aggiornate nel tempo le seguenti informazioni :

- la classificazione delle aree aziendali protette
- l'accesso controllato alle aree considerate critiche

- la sicurezza fisica e la sorveglianza di queste aree
- la tempestiva rilevazione di eventuali incidenti di sicurezza

Attività 1	Classificazione delle aree aziendali
Soggetto	Responsabile. trattamento dati
Elementi in ingresso	Nuova ubicazione-area basi dati-documentazione contenente dati sensibili
Informazioni esistenti:	Elenco aree protette (M-16-03) Tipo di sorveglianza / sistemi di sicurezza passivi in essere nell'area
Controlli	Controlli (audit) verifica elenco protette
Elementi in uscita	Elenco aree protette (M-16-03) aggiornato con le seguenti informazioni: a. Descrizione documentazione archiviata b. Ubicazione c. Area d. Protezioni passive e sorveglianza in essere Elenco personale interno autorizzato accesso aree protette (M-16-04) aggiornato Elenco personale esterno autorizzato accesso aree protette (M-16-02) aggiornato

Attività 2	Autorizzazione accesso alle aree protette (**personale interno**)
Soggetto	Responsabile. trattamento dati
Elementi in ingresso	Nuovo personale in servizio
Informazioni esistenti:	Elenco personale interno autorizzato accesso aree protette (M-16-04)
Controlli	Verifica condizioni iniziali acceso aree: Consegna linea guida: Guida all'utente per l'utilizzo delle risorse informatiche e documentali (LG-RDI-001) Esecuzione test di verifica: Test di verifica misure di sicurezza (M-16-06)
Elementi in uscita	Elenco personale interno autorizzato accesso aree protette (M-16-04) aggiornato. Archivio test aggiornato

Attività 3	Autorizzazione accesso alle aree protette (**personale esterno**)
Soggetto	Responsabile. trattamento dati
Elementi in ingresso	Nuovo ditta-personale in servizio
Informazioni esistenti:	Elenco personale esterno autorizzato accesso aree protette (M-16-02)
Controlli	Verifica condizioni iniziali acceso aree: Consegna misure: Misure di sicurezza minime di protezione dati sensibili e limitazioni di accesso per il personale esterno (M-16-12)
Elementi in uscita	Elenco personale esterno autorizzato accesso aree protette (M-16-02) aggiornato.

Attività 4	Segnalazione incidenti di sicurezza
Soggetto	Responsabili reparti servizi
Elementi in ingresso	Avvenuto o probabile incidente di sicurezza
Informazioni esistenti:	Elenco personale esterno autorizzato accesso aree protette (M-16-02)
	Elenco personale interno autorizzato accesso aree protette (M-16-04)
	Guida all'utente per l'utilizzo delle risorse informatiche e documentali (LG-RDI-001)
Elementi in uscita	Compilazione Modulo Non conformità ripetitive (M-13-04) e/o Rapporto di Non conformità (M-13-01)

Attività 5	Classificazione delle aree aziendali: sicurezza passiva e sorveglianza
Soggetto	Responsabile. trattamento dati
Elementi in ingresso	Nuovo ditta-personale in servizio
Informazioni esistenti:	Elenco personale esterno autorizzato accesso aree protette (M-16-02)
Controlli	Verifica condizioni iniziali acceso aree:
	Consegna misure: Misure di sicurezza minime di protezione dati sensibili e limitazioni di accesso per il personale esterno (M-16-12)
Elementi in uscita	Elenco personale esterno autorizzato accesso aree protette (M-16-02) aggiornato da consegnare agli incaricati del trattamento dati delle varie aree.

Le aree sono in ogni caso protette da porte e serrature e sempre presidiate.
In particolare:

- i punti di accettazione sono protetti da porte e serrature e sempre presidiati;
- gli archivi cartacei e gli archivi delle lastre sono situati in locali sempre chiusi a chiave;
- i documenti in uso presso le varie aree, non ancora archiviati nei locali definitivi, non vengono mai lasciati in vista ma riposti negli appositi armadi o carrelli dotati di serratura;

6.4 PROTEZIONE LOGICA DELLE INFORMAZIONI

Le misure di sicurezza logiche sono commisurate al livello di classificazione delle informazioni e considerano i seguenti aspetti:

- il controllo degli accessi alle informazioni
- il mantenimento della loro integrità e riservatezza
- la sicurezza delle trasmissioni e delle comunicazioni interne e con l'esterno
- la sicurezza delle stazioni di lavoro e dei computer
- la sicurezza nel processo di sviluppo delle applicazioni informatiche
- la sicurezza operativa delle installazioni informatiche

Sistemi di protezione in caso intrusioni per software non autorizzato di origine esterna
Le intrusioni, i possibili malfunzionamenti, la diffusione all'esterno di informazioni non autorizzate, vengono protette da software specializzati. Questi software garantiscono una buona protezione curando o eliminando i programmi/documenti infetti provenienti da: internet, posta elettronica, cd, dv, penne USB o qualsiasi altro supporto

rimovibile. E' stato inoltre introdotto un filtro, presso il nostro provider di posta, che blocca presso il server del fornitore la posta contenente virus o altri software indesiderati. .

Obiettivo: Mantenimento nel tempo del software di protezione antivirus, antispamming e spyware. Protezione da attacchi esterni.

Attività 1	Aggiornamento giornaliero antivirus
Soggetto	Responsabile. trattamento dati
Elementi in ingresso	Aggiornamento immunizzazioni ai nuovi virus
Informazioni esistenti:	Questa procedura
Controlli	Verifica aggiornamento effettuato
Elementi in uscita	Elementi di aggiornamento scaricati dal sito internet.
	Postazioni di lavoro aggiornate

Attività 2	Filtro sulla posta elettronica in ingresso
Soggetto	Responsabile. trattamento dati
	Provider internet
Elementi in ingresso	Rischi di infezioni
Informazioni esistenti:	Questa procedura
	Informazioni su riviste specializzate o su siti specializzati
Controlli	Verifica efficacia filtro
Elementi in uscita	Eliminazione e-mail contenenti virus prima del loro arrivo a destinazione presso la nostra sede.

Attività 3	Antispamming e spyware
Soggetto	Responsabile. trattamento dati
Elementi in ingresso	Rischi di infezioni e malfunzionamento posta
	Aggiornamento immunizzazione nuovi spyware e regole di anti spam
Informazioni esistenti:	Questa procedura
	Informazioni su riviste specializzate o su siti specializzati
Controlli	Verifica efficacia filtro attivato dal fornitore esterno servizio mail
Elementi in uscita	Eliminazione e-mail di spam
	Protezione spyware – malware attiva

6.4.1 Sistemi di protezione per accesso indesiderato alla rete interna

Vengono attualmente utilizzati due livelli di protezione da accessi ai database contenenti dati personali sensibili in dotazione con i sistemi operativi oggi installati presso l'azienda:

4) identificazione di accesso alla rete aziendale con nome utente e password per rendere disponibili all'utente specifiche cartelle di rete (non contenenti dati personali sensibili) e per consentire l'accesso al computer locale. E' stata impostata le seguente regola generale: l'utente può accedere solo al computer a cui è stato autorizzato.
5) identificazione di accesso al software contenente i dati sensibili con limitazioni d'uso in base alle autorizzazioni concesse.

6.4.2 Gestione account utente, lettera di incarico, autorizzazioni e profili

Obbiettivo: definire le modalità di consegna degli account accesso, lettere di incarico trattamento dati personali e consegna misure minime di sicurezza.

Tutti i dipendenti concorrono alla realizzazione della Sicurezza pertanto dovranno proteggere le informazioni a loro assegnate nel rispetto di quanto stabilito dalle politiche in termini di:

- utilizzo delle risorse informatiche
- accesso ai sistemi e ai dati
- uso della password e dell'account

Ad ogni utenza viene consegnata un account e pwd di accesso personale. L'accesso è profilato in base alle mansioni previste. Per semplicità di gestione sono state categorizzate le seguenti figure:

- Account di accesso a programmi e procedure per i reparti di degenza, sala operatoria, radiologia
- Account di accesso a programmi e procedure per gli operatori agli sportelli e/o segreteria referti
- Account di accesso a programmi e procedure per il personale amministrativo
- Account di accesso a programmi e procedure per il personale medico
- Account di accesso a programmi e procedure per il personale di laboratorio

Attività 1	Autorizzazione accesso ai dati aziendali (**personale interno**)
Soggetto	Responsabile. trattamento dati
Elementi in ingresso	Nuovo personale in servizio e/o personale con variazioni di incarico
Informazioni esistenti:	Elenco personale interno
	Profilo aziendale legato all'account/mansioni
Controlli	Verifica condizioni iniziali accesso:
	Consegna linea guida: Guida all'utente per l'utilizzo delle risorse informatiche e documentali (LG-RDI-001)
	Esecuzione test di verifica: Test di verifica misure di sicurezza (M-16-06)
	Consegna lettera di in incarico al trattamento
Elementi in uscita	Elenco account e profili aggiornato (gestione specifica nel software aziendale).
	Archivio test aggiornato
	Check list consegna incarichi firmata dal dipendente, collaboratore, professionista

N..b.: Viene consegnata l'autorizzazione iniziale per un periodo di tempo definito e confermata solo quando viene effettuato il corso interno specifico sulla sicurezza informatica.

Lo schema del processo di autorizzazione è dettagliato nel modulo **M-16-22 Check list/schema creazione e consegna account di accesso**.

6.5 PIANO DI CONTINUITÀ OPERATIVA

Obiettivo: garantire la continuità del servizio informativo e la disponibilità delle informazioni evitando o limitando i danni al patrimonio informativo a fronte di una emergenza attraverso un Piano di Ripristino dettagliato che elenca le informazioni, le modalità e le risorse di backup necessarie per la ripresa delle attività a seguito di un'emergenza.

Il sistema attuale è dotato di alcuni dispositivi che limitano la possibilità di guasto e/o interruzione del servizio:

SERVER
Dispositivi passivi:

- Doppio alimentatore (in caso di guasto di uno degli alimentatori è in funzione un secondo di emergenza)
- Tre dischi in modalità raid 5 (in caso di guasto del disco primario entrano in funzione in automatico gli altri due)
- Gruppo di continuità (in assenza di alimentazione dalla rete elettrica è possibile garantire il funzionamento dei server)
- Gruppo elettrogeno (entra in funzione in caso di prolungata assenza di alimentazione dalla rete elettrica)

Dispositivi software attivi:
Backup giornaliero dei database e dei documenti su unità disco esterna (SNAP server) ubicata in altri locali per minimizzare, in caso di incendio nelle stanze dove sono installati i server, la possibilità di perdita dei dati.
Backup quindicinale su disco portatile da depositare in una cassetta di sicurezza.

Obiettivo: Predisporre un piano di ripristino efficace e rapido dei dati in caso di guasti.
N.b. 1: In caso di guasto di altri elementi del Server (scheda madre, processore, alimentatori, controller) è necessario accertare l'integrità dei dati, dopo la riparazione. Non è detto che sia assolutamente necessario il ripristino delle informazioni dal backup se queste non sono state toccate dal guasto.
N.b. 2: Il tempo di ripristino stimato per la ripresa del lavoro in caso del guasto più grave è paria a un giorno lavorativo.

Attività 1	Ripristino dati dopo guasto irreversibile sul server
Soggetto	Amministratore del sistema
Elementi in ingresso	Guasto irreversibile server in caso di guasto di tutti i dischi o danno sul sistema operativo
	Copie backup
	Contratto di manutenzione software e hardware
	Cd di installazione software originali
Informazioni esistenti:	Questa procedura
Elementi in uscita	Ripristino della funzionalità hardware (sostituzione dischi o di altri elementi)
	Ripristino delle funzionalità software:
	Server WIN 2012 server
	Installazione sistema operativo con relativi service pack
	Installazione SQL server con relativi service pack
	Ripristino dei backup dei database SQL (Master, MEDICA310, Preno_tab) da SNAP server o dall'altro server

Attività 2	Ripristino dati dopo guasto irreversibile su posto di lavoro
Soggetto	Amministratore del sistema
Elementi in ingresso	Guasto irreversibile in caso di guasto sul disco o danno sul sistema operativo
	Computer alternativo presso amministratore di sistema pronto per sostituzione immediata
	Copie backup (solo per le postazioni che hanno informazioni archiviate su computer locale)
	Contratto di manutenzione software e hardware
	Cd di installazione software originali
Informazioni esistenti:	Questa procedura
Elementi in uscita	Ripristino della funzionalità hardware (sostituzione dischi)
	Ripristino delle funzionalità software:
	Installazione sistema operativo con relativi service pack
	Installazione del software di base (office, antivirus, gestionale)

6.5.1 Gestione degli incidenti (Data Breach), monitoraggio eventi avversi – violazioni, comunicazioni

Obiettivo: Monitoraggio e controllo rischi informatici, definizione delle responsabilità e le modalità di gestione di eventuali incidenti di sicurezza.
La violazione dei dati personali consiste in una violazione della sicurezza che, in modo accidentale o illecito, provoca la distruzione, la perdita, la modifica, la divulgazione ovvero l'accesso, la copia o la consultazione non autorizzate dei dati personali oggetto del trattamento.

Le cause più ricorrenti di violazione dei dati personali sono gli attacchi informatici, gli accessi abusivi ai sistemi informativi, gli incidenti (es. incendi, allagamenti, etc.), lo smarrimento di supporti informatici (smartphone, notebook, chiavetta USB, etc.) o la sottrazione dei supporti o dei documenti contenenti dati personali (furto, etc.).

La violazione dei dati personali può avere effetti differenti sui dati, a seconda che abbia per oggetto:

– la riservatezza del dato: la violazione consiste nella divulgazione o nell'accesso non autorizzato o accidentale ai dati personali;

– la disponibilità del dato: la violazione in questo caso consiste nell'alterazione non autorizzata o accidentale di dati personali;

– l'integrità del dato: la violazione consiste nella modifica non autorizzata o accidentale di dati personali.

L'articolo 33 del GDPR, rubricato *"Notifica di una violazione dei dati personali all'autorità di controllo"* prevede che:
"1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".

In caso di violazione dei dati personali, occorre un'immediata attività di valutazione interna, finalizzata a stabilire, nel termine più breve possibile:
a) se la violazione abbia *"un impatto significativo sui dati personali contenuti nelle proprie banche dati"* oppure se *"presenti un rischio per i diritti e le libertà delle persone fisiche"*;
b) la natura della violazione e le probabili conseguenze;
c) se il rischio di cui al punto a) sia di grado elevato.
I termini per l'eventuale notifica al Garante non sono puramente indicativi ma perentori, con la conseguenza che il mancato rispetto, se non adeguatamente motivato, può integrare di per sé un fatto sanzionabile.
Quanto invece alla comunicazione della violazione agli interessati, il titolare del trattamento dovrà provvedervi, senza ingiustificato ritardo, a meno che non ricorrano le condizioni previste dall'art. 34, il quale prevede che la comunicazione non è richiesta se:
d) il titolare aveva messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
e) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
Qualsiasi evento anche di basso impatto e/o potenzialmente sintomo di successive violazioni va riportato nel registro **Registro eventi avversi / violazioni sistema informativo e archivi cartacei (M-16-19)** al fine di tener traccia di ogni evento utile anche nel tempo per ricostruire eventuali successive violazioni.
Violazioni gravi vanno segnalate entro le 48 ore utilizzando il modulo specifico del Garante disponibile nell'intranet aziendale: "Modulo di comunicazione Data Breach al garante AD-DIREZ-011". Il modulo va compilato in maniera puntuale in tutte le sue parti e inviato al garante via pec: **protocollo@pec.gpdp.it .**

Qualsiasi violazione va segnalata come da schema qui di seguito proposto illustrando i flussi organizzativi conseguenti al verificarsi di una violazione dei dati, indicando:
- chi è soggetto alle prescrizioni contenute nella presente procedura (CHI),
- chi sono i destinatari delle azioni (A CHI),
- i termini entro i quali le azioni vanno poste in essere (QUANDO),
- le modalità di esecuzione delle azioni prescritte (COME)

ATTIVITÀ	CHI	A CHI	QUANDO	COME
Rilevazione e segnalazione di violazione dei dati	Organi dell'Ente, personale dipendente, collaboratori, fornitori	Al referente privacy Eventualmente al fornitore di servizi IT	Appena se ne viene a conoscenza	Utilizzando le vie più brevi (telefono, di persona, e-mail)
Messa in atto delle azioni correttive immediate possibili	referente privacy, insieme ai soggetti coinvolti nella violazione ed eventualmente al fornitore di servizi IT		Appena ricevuta la comunicazione	Raccogliendo tutte le informazioni disponibili sulle cause e sugli effetti della violazione
Raccolta informazioni sulla violazione	referente privacy, insieme ai soggetti coinvolti nella violazione ed eventualmente al fornitore di servizi IT		Appena ricevuta la comunicazione	Raccogliendo tutte le informazioni disponibili sulle cause e sugli effetti della violazione
Comunicazione della violazione dati	referente privacy	Al Responsabile della protezione dei dati (RPD) Al titolare (Presidente dell'Ordine)	Appena ottenute le informazioni sufficienti per analizzare i rischi della violazione	Utilizzando le vie più brevi (telefono, di persona, e-mail)
No impatto significativo sui dati personali e no rischio per i diritti e le libertà delle persone fisiche	referente privacy RPD Titolare		Appena possibile	Annotazione sul registro delle violazioni e conservazione della registrazione, pur in assenza di notificazione o comunicazione
Si impatto significativo sui dati personali e/o si rischio per i diritti e le libertà delle persone fisiche	referente privacy RPD Titolare	Garante	Entro 48 ore per l'impatto ed entro 72 ore per il rischio	Notifica mediante la modulistica per la notifica del data breach predisposta dal Garante e annotazione nel registro
Il rischio per i diritti e le libertà delle persone fisiche è elevato e non sono state poste in essere le misure di cui all'art. 34	referente privacy RPD Titolare	Agli interessati (le persone fisiche i cui dati sono stati violati)	Senza ingiustificato ritardo	Comunicazione diretta alle singole persone o mediante pubblicazione in sito a loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate

Attività 1	Monitoraggio rischi informatici – eventi avversi - violazioni
Soggetto	Responsabile IT, Responsabile privacy, Personale dipendente, Fornitori
Elementi in ingresso	Possibile rischio o evento sulla sicurezza
Informazioni esistenti:	Elenco aree protette (M-16-03)
	Tipo di sorveglianza / sistemi di sicurezza passivi in essere nell'area
Controlli	Controlli file di log sistema operativo, sistema di intercettazione, segnalazioni via mail, telefoniche, cartacee.
Elementi in uscita	Controlli accessi non autorizzati verificata attraverso i file di log di sistema
	Comunicazione al personale che ha violato le regole di sicurezza
	Registrazione evento nel registro eventi avversi.
	Comunicazione al Garante in caso di gravi violazioni e accessi a dati sensibili con modulo reperibile nel sito del garante.

6.5.2 Sviluppo e manutenzione dei sistemi hardware e software

Obiettivo: Manutenzione ed aggiornamento dell'hardware ed del software utilizzato per realizzare il piano di Sicurezza; definizione modalità e tempi di effettuazione degli aggiornamenti e delle modifiche e/o sostituzione dispositivi e software.

Attività 1	Aggiornamento – modifiche dispositivi software
Soggetto	Amministratore di sistema
Elementi in ingresso	Possibile rischio o evento negativo sulla sicurezza
	Obsolescenza dei prodotti software
Informazioni esistenti:	Sito internet microsoft contenente segnalazioni di possibili rischi sulla sicurezza (causati da difetti del sistema operativo) con relativo rilascio di software di aggiornamento e/o specifiche di configurazione del sistema
	Scadenza aggiornamenti per obsolescenza del software
Controlli	Controlli periodici sul sito microsoft e su riviste specializzate
Elementi in uscita	Aggiornamento del sistema operativo e dei relativi servizi installati
	Sostituzione del software con acquisto licenze versione aggiornata

Attività 2	Aggiornamento – modifiche dispositivi hardware
Soggetto	Amministratore di sistema
Elementi in ingresso	Possibile rischio o evento negativo sulla sicurezza
	Obsolescenza dei prodotti hardware
Informazioni esistenti:	Sito internet microsoft contenente segnalazioni di possibili rischi sulla sicurezza (causati da difetti del sistema operativo legati all'hardware)
	Scadenza per obsolescenza temporale dell'hardware (impossibilità di reperire i ricambi sul mercato, inadeguatezza dell'hardware a svolgere le

	funzioni richieste)
Controlli	Controlli periodici sul sito microsoft e su siti specializzati
Elementi in uscita	Aggiornamento dell'hardware (ampliamento memoria, installazione sistema operativo aggiornato, ampliamento dischi) Sostituzione totale dell'hardware (vita massima di un posto di lavoro 5-6 anni, vita massima per un server 4-5 anni)

6.5.3 Definizione delle Regole per la Sicurezza

Le regole generali per l'applicazione delle Politiche della Sicurezza sono allegate alla presente procedura nel documento: POLITICHE PER LA SICUREZZA.

6.5.4 Strategia di gestione del rischio

Definito nei paragrafi precedenti il sistema di calcolo del valore di rischio definiamo anche i criteri di valutazione che poi scaturiscono in opportuni piani di miglioramento.

(vedi Tabella 1)

7. PIANO OPERATIVO

Definite nei documenti di cui ai punti precedenti le risorse da proteggere, le strategie del rischio ed il livello di rischio ritenuto accettabile ora passiamo alla stesura di un piano operativo per l'attuazione, la verifica, il monitoraggio, lo stato di avanzamento delle attività e delle contromisure da adottare per raggiungere gli obiettivi della Politica della sicurezza.
Le aree critiche verranno monitorate ogni sei mesi e tramite apposite analisi verranno aperte opportune azioni correttive per eliminare le criticità.
I risultati delle verifiche e le evidenze delle azioni sono archiviate presso l'ufficio del responsabile trattamento dati sensibili.

7.1 AUDIT

Gli audit specifici sul sistema di sicurezza verranno svolti con cadenza annuale. La check list attualmente utilizzata si basa sulle linee guida AGID e il regolamento Europeo.
Eventuali violazioni di sicurezza avvenute nel corso delle attività ordinarie sono oggetto di audit continuo attraverso appositi sistemi automatici di rilevazione delle violazioni tra i quali:

- Controllo event log del server
- Controllo event log dei client
- Controllo log sql
- Monitoraggio di rete e inventario apparecchiature con apposito programma
- Scansioni regolari degli indirizzi ip per verificare congruenza con inventario
- Registro eventi avversi significativi
- Monitoraggio accessi amministrativi
- Monitoraggio infezioni e segnalazioni e controllo con pulizia dei pc (tramite software antivirus in cloud ESET)

A seguito dell'audit verrà prodotta apposita relazione tecnica dove verranno esposte le eventuali misure di sicurezza da implementare e di monitoraggio da effettuare con cadenze temporali commisurate alla gravità.

In caso di gravi violazioni verrà inviata apposita comunicazione (Data breach) al garante privacy come da regolamento europeo.

7.2 SICUREZZA FISICA

7.2.1 Sicurezza di area

Il personale è stato addestrato a:

- segnalare eventuali violazioni delle norme sulla sicurezza;
- esprimere suggerimenti per innalzare il livello di sicurezza;
- non violare le norme di sicurezza

7.2.2 Sicurezza delle apparecchiature Hardware

Sono stati aperti opportuni contratti di manutenzione con ditte esterne per il controllo delle apparecchiature hardware e il mantenimento nel tempo dei prodotti software.

7.3 SICUREZZA LOGICA

E' stato attivato un sistema organico di identificazione ed autenticazione.

7.4 SICUREZZA LOGICA REFERTI ON LINE

Per l'accesso hai documenti on line attraverso il sito internet è necessario possedere una password di accesso che verrà consegnata al paziente al momento dell'effettuazione dell'esame.
Il foglio password viene consegnato come documento a parte rispetto al foglio di ritiro in modo da non associare password a codice fiscale.
Per accedere al servizio bisogna inserire codice fiscale e password personale.
Al primo accesso il paziente è obbligato a creare una propria password personale per accedere al servizio che sarà poi quella che gli permetterà di accedere al portale ma non ai referti, per accedere ai referti e quindi visualizzarli e/o scaricarli sul proprio computer bisognerà comunque avere una password referto valida che è associata solo ad un referto e solo a quello. La password referto ha una durata di 30 giorni, dopo questo periodo viene automaticamente invalidata.
La password referto insieme alla password personale creata al primo accesso sono a garanzia del paziente al fine di rendere sicuro tutto il sistema di refertazione on line. I referti sono in formato PDF e firmati digitalmente con firma del responsabile che li emette.

7.5 SICUREZZA ORGANIZZATIVA

Sono stati organizzati appositi corsi di formazione rivolti a tutto il personale con test finale di verifica.

POLITICA PER LA SICUREZZA

La Casa di Cura Eretenia Spa si impegna a garantire il massimo della riservatezza nel trattamento dei dati personali in applicazione delle misure minime elencate nel regolamento definito nel Regolamento Europeo n. 2016/679.
A questo scopo definisce le seguenti misure per la sicurezza:

1. Attivazione di un sistema di identificazione e autenticazione per gli utenti che hanno accesso alle banche dati informatiche interne tramite password ed account utilizzabile solo in una stazione di lavoro e non utilizzabile da più utenti nemmeno in tempi diversi
2. Gli accessi alle aree classificate come riservate debbono essere autorizzati. Vi potrà accedere solo il personale elencato in apposita circolare interna. Qualsiasi altro accesso dovrà essere autorizzato dalla Direzione e/o dal Responsabile Trattamento dati. Gli accessi interessano anche il personale esterno che effettua operazioni di manutenzione e/o pulizia.
3. L'accesso alle aree protette può essere concesso in via straordinaria senza autorizzazione del responsabile trattamento dati se il personale senza autorizzazione viene accompagnato e rimane sotto la vigilanza dal personale interno incaricato al trattamento dati, personale addestrato sulla politica della sicurezza della presente azienda.
4. Assegnazione di un UserID tramite lettera ufficiale dopo esecuzione test di verifica apprendimento delle norme sulla sicurezza.
5. Password consegnate agli incaricati al trattamento come al punto precedente e in scadenza ogni tre mesi per i posti di lavoro collegati in rete, ogni anno per i posti di lavoro non collegati in rete. Le password debbono essere composte da minimo 8 caratteri, una lettera maiuscola e almeno 1 numero.
6. Le risorse hardware e le aree riservate dovranno essere protette da sistemi di sicurezza attivi e passivi quali password, chiavi di accesso, porte e altri dispositivi tecnici.
7. Il codice sorgente del software sviluppato internamente non potrà essere messo a disposizione di terzi senza l'autorizzazione della Direzione. Ogni personalizzazione effettuata da software house esterne dovrà essere effettuata in presenza dell'Amministratore del Sistema e/o da persona da egli delegata, sotto la loro diretta supervisione.
8. Ogni utente sarà autorizzato all'accesso delle risorse, dati e/o informazioni in base al profilo utente definito dall'amministratore del sistema. Non sono concessi altri accessi al di fuori dell'elenco consegnato.
9. Tutti i file di log potranno essere consultati solo dall'Amministratore di Sistema e dal responsabile trattamento dati che, con periodicità settimanale, provvederanno all'archiviazione di questi file e all'analisi degli eventi procedendo ad eventuale relazione alla Direzione in caso di grave violazione delle regole di sicurezza da parte dell'utenza.
10. Tutti i tentativi di intrusione dovranno essere monitorati ed immediatamente segnalati all'Amministratore di Sistema.
11. Nomina di un RDP che si incaricherà di monitorare e con la collaborazione di esperti interni ed esterni di mantenere efficiente il sistema di sicurezza adottato.
12. Adeguata istruzione agli utenti sugli obblighi e sulle regole di sicurezze attivate nella Casa di Cura Eretenia Spa.
13. Attivazione e aggiornamento dei programmi antivirus, spyware e antispamming installati.
14. Aggiornamento periodico dei sistemi operativi alle versioni più recenti al fine di mantenere alto il livello tecnologico e di conseguenza la sicurezza intrinseca del software di sistema.
15. Controllo sull'operato delle software house esterne e dello sviluppo software interno avvalendosi anche della consulenza di terzi.
16. Rilevazione tempestiva di eventuali incidenti di sicurezza.
17. Monitoraggio delle attività di rete e della singola stazione di lavoro.

18. Attivazione di un Audit annuale delle attività dell'utenza per la verifica nel tempo dell'efficacia del sistema di sicurezza adottato.
19. Verifica periodica della sussistenza delle condizioni che hanno portato alla concessione delle autorizzazioni d'accesso agli archivi contenenti dati personali sensibili.
20. Adeguamento dei locali dal punto di vista tecnico ed organizzativo per la protezione delle aree interessate dalle misure di sicurezza
21. Monitoraggio giornaliero delle attività di backup.
22. Attivazione di un sistema di manutenzione ordinaria e straordinaria del sistema informativo per ridurre al minimo i tempi di disservizio.
23. Manutenzione e aggiornamento di un elenco dettagliato delle risorse hardware e software per la definizione del livello di criticità del singolo elemento.
24. Elenco dettagliato delle basi dati gestite e definizione del loro livello di criticità.
25. Definizione di un Piano di Continuità Operativa per garantire nel tempo la continuità del servizio informatico limitando i danni al patrimonio informativo a fronte di una emergenza.
26. Il personale autorizzato all'accesso ad informazioni personali sensibili è stato opportunamente addestrato a rispettare le regole di riservatezza minime: rispetto della dignità dell'interessato; attenzione, nei colloqui o nella raccolta di informazioni per l'anamnesi, evitando di far conoscere a terzi informazioni sullo stato di salute del paziente; far rispettare le distanze di cortesia nel rispetto dei canoni di riservatezza; modalità specifiche di comunicazione a terzi di informazioni riservate; eliminazione dove possibile di tutte le informazioni che possano mettere in correlazione il paziente e l'indicazione della struttura, reparto o esame eseguito; comunicare all'interessato informazioni sul suo stato di salute solo per il tramite di un medico.
27. Nell'attività di video sorveglianza solo le persone nominate per iscritto sono autorizzate alla visione dei contenuti video e le registrazioni vanno conservate esclusivamente per il periodo di tempo necessario al massimo entro le ventiquattro ore successive la registrazione.

Tabella 1: Criteri di valutazione

Criteri di valutazione delle minacce

Livello	Linee guida per la verosimiglianza
1 - Bassa	È applicabile ad almeno uno dei seguenti: - la minaccia si può verificare con frequenza inferiore rispetto a quanto riportato dalle ricerche più note; - in caso di attacco deliberato, i dati sono poco appetibili e l'immagine aziendale non è compromessa e pertanto i tentativi di attacco o non sono iniziati o sono condotti da malintenzionati scarsamente preparati da un punto di vista tecnico e con scarse risorse a disposizione. - in caso di attacco non deliberato, l'ambito è poco complesso e quindi è difficile commettere errori; - in caso di eventi naturali, gli studi dimostrano che la minaccia può verificarsi molto raramente.
2 - Media	È applicabile ad almeno uno dei seguenti: - la minaccia si può verificare secondo quanto riportato dalle ricerche più note; - in caso di attacco deliberato, i dati sono poco appetibili e l'immagine aziendale non è compromessa e quindi può essere condotto da malintenzionati non particolarmente motivati, mediamente preparati da un punto di vista tecnico e con scarse risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque rari; - in caso di attacco non deliberato, l'ambito è mediamente complesso e quindi possono essere commessi errori; - in caso di eventi naturali, gli studi dimostrano che la minaccia può verificarsi nella media dei casi studiati.
3 - Alta	È applicabile ad almeno uno dei seguenti: - la minaccia si può verificare più frequentemente rispetto a quanto riportato dalle ricerche più note; - in caso di attacco deliberato, i dati sono appetibili o l'immagine aziendale è compromessa, e quindi può essere condotto da malintenzionati molto motivati, tecnicamente preparati e con ingenti risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque portati molto di frequente; - in caso di attacco non deliberato, l'ambito è di elevata complessità (per esempio per molteplicità di sedi, tipologie di sistemi informatici, utenti interni e/o esterni) e quindi è facile siano commessi errori; - in caso di eventi naturali, gli studi dimostrano che la minaccia si verifica quasi certamente.

Criteri di valutazione delle informazioni

Liv.	R- Riservatezza	I - Integrità	D- Disponibilità
1 - Basso	Organizzazione I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici. Interessati La mancanza di riservatezza ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	Organizzazione I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. Interessati La mancanza di intergrità ha impatti lievi (p.e. fastidio e tempo necessario per correggere le informazioni).	Organizzazione L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti. Interessati La mancanza di disponibilità ha impatti lievi (p.e. fastidio e tempo necessario per correggere le informazioni).
2 - Medio	Organizzazione I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. Interessati La mancanza di riservatezza ha impatti, non critici e che creano piccole difficoltà (p.e. costi, paura, incomprensioni, stress, malanni minori) a causa degli effetti sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	Organizzazione I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. Interessati La mancanza di integrità ha impatti, non critici e che creano piccole difficoltà (p.e. costi, mancato accesso a servizi, incomprensioni, stress, malanni minori), a causa degli effetti vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	Organizzazione L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti. Interessati La mancanza di disponibilità ha impatti, non critici e che creano piccole difficoltà (p.e. costi, mancato accesso a servizi, incomprensioni, stress, malanni minori), a causa degli effetti vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

3 - Alto	Organizzazione I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine) e un'eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. Interessati La mancanza di riservatezza ha elevato impatto (esempi: fondi non disponibili, blocco da parte di enti economici, danni alla proprietà, perdita del posto di lavoro, denunce, peggioramento della salute) che può essere superato con difficioltà sulla vita sociale o personale degli interessati.	Organizzazione I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. Interessati La mancanza di integrità ha elevato impatto (esempi: fondi non disponibili, blocco da parte di enti economici, danni alla proprietà, perdita del posto di lavoro, denunce, peggioramento della salute) sulla vita sociale o personale degli interessati.	Organizzazione L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti. Interessati La mancanza di disponibilità ha elevato impatto (esempi: fondi non disponibili, blocco da parte di enti economici, danni alla proprietà, perdita del posto di lavoro, denunce, peggioramento della salute) sulla vita sociale o personale degli interessati.

4 - Critico	Organizzazione La diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione. Interessati La mancanza di riservatezza ha impatti non reversibili sulla vita degli interessati in termini di: - perdita di autonomia; - esclusione (p.e. inabilità a lavorare); - perdita di libertà; - danni fisici (p.e. danni fisici o mentali a lungo termine o morte); - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	Organizzazione La mancanza di integrità delle informazioni ha elevati impatti sul business aziendale o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. Interessati La mancanza di integrità ha impatti non reversibili sulla vita degli interessati in termini di: - perdita di autonomia; - esclusione (p.e. inabilità a lavorare); - perdita di libertà; - danni fisici (p.e. danni fisici o mentali a lungo termine o morte); - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	Organizzazione L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche. Interessati La mancanza di disponibilità ha impatti non reversibili sulla vita degli interessati in termini di: - perdita di autonomia; - esclusione (p.e. inabilità a lavorare); - perdita di libertà; - danni fisici (p.e. danni fisici o mentali a lungo termine o morte); - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

Criteri di valutazione dei controlli di sicurezza

Livello	Linee guida per la valutazione
1- Inadeguato	Il controllo non è previsto o è assente nella pratica.
2- Parzialmente adeguato	Il controllo è applicato sporadicamente o in modo completamente inadeguato, non garantendone quindi l'efficacia.
3- Quasi adeguato	Sono state rilevate mancanze al controllo, soprattutto di tipo formale (per esempio, inesattezze nelle procedure relative).
4- Adeguato	Il controllo è sistematicamente applicato e non sono state rilevate inadeguatezze al controllo.

Figura 1 – Organigramma sicurezza dati sensibili