VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO

SU DATI RETROSPETTIVI

(ART. 110 D. LGS. 196/2003, Provvedimento Garante n. 146/2009)

La valutazione di impatto (DPIA) consente di identificare in modo puntuale i rischi per la protezione dei dati personali quando vengono pianificati nuovi progetti di ricerca o aggiornati progetti di ricerca in corso e di individuare le azioni necessarie per mitigare tali rischi.

Una valutazione di impatto, secondo l'Autorità Garante per la protezione dei dati personali, deve sempre essere effettuata negli studi retrospettivi quando:

- il trattamento dei dati personali è su larga scala;
- vengono trattate categorie particolari di dati, ad esempio dati genetici;
- l'attività comporta il data linkage di molteplici e diversi archivi di dati;
- l'attività prevede la rilevazione di dati per individui vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.);
- la base giuridica per il trattamento dei dati non è riferibile al consenso al trattamento, a ricerche condotte sulla base di disposizioni di legge o regolamento o al diritto, o ad altre specifiche fattispecie previste dal GDPR e dal Codice Privacy.

A CURA DEL RICERCATORE

Titolo dello studio: Valutazione della perfomance della chirurgia cardiaca congenita utilizzando dati amministrativi: un confronto retrospettivo multicentrico di un modello basato su ICD-9 con il punteggio di complessità di Aristotele

Codice di Protocollo: ALMA

Titolare del trattamento: Policlinico San Donato S.p.A.

Principal Investigator: Prof. Alessandro Giamberti

Unità: Cardiochirurgia Pediatrica e Cardiochirurgia dei Congeniti Adulti

Data compilazione: 20/11/2025

<table>
<tr><td colspan="2">TRATTAMENTO DEI DATI</td></tr>
<tr><td colspan="2">Descrizione del trattamento</td></tr>
<tr><td>Sinossi dello Studio</td><td>
<table>
<tr><td>Obiettivi e Finalità</td><td>Lo studio si propone di sviluppare e validare un nuovo modello di aggiustamento del rischio basato su dati amministrativi (ICD9-PM) per la cardiochirurgia congenita, confrontandolo con il modello clinico fondato sull’Aristotle Basic Complexity Score. L’obiettivo principale è verificare se i dati amministrativi, se opportunamente modellati, possano costituire uno strumento valido, equo e trasferibile per la valutazione e il confronto delle performance ospedaliere in questo ambito complesso.</td></tr>
<tr><td>Popolazione</td><td><u>Criteri di inclusione</u>
- Pazienti adulti e pediatrici che abbiano eseguito un intervento di cardiochirurgia congenita nel periodo luglio 2023 - agosto 2025

<u>Criteri di esclusione</u>
- Saranno esclusi i pazienti sottoposti a procedure non cardiache, a impianto isolato di pacemaker o defibrillatore, a trapianto cardiaco e quelli con dati mancanti riguardo all’outcome primario, ovvero la mortalità intraospedaliera</td></tr>
<tr><td>Disegno dello Studio</td><td>Studio osservazionale retrospettivo di coorte multicentrico, basato sulla raccolta parallela di dati clinici e amministrativi per la stessa popolazione di pazienti, con un approccio comparativo tra due centri di riferimento con caratteristiche differenti: un centro ad alto volume e complessità (IRCCS Policlinico San Donato) e un centro regionale con casistica più tipica (Arnas - Civico di Palermo).</td></tr>
<tr><td>Numero di Soggetti</td><td>1.500</td></tr>
<tr><td>Durata dello Studio</td><td>12 mesi</td></tr>
</table>
</td></tr>
<tr><td colspan="2">Tipologia di dati raccolti</td></tr>
<tr><td>Modalità di raccolta (fonte dei dati) (barrare anche più caselle)</td><td>☒ da cartelle cliniche/documentazione sanitaria
☐ da archivi di dati clinici (esempio Dossier Sanitario Elettronico, RIS-PACS)
☐ da archivi di test diagnostici
☐ da dati di laboratorio
☒ da database amministrativi
☐ altro (specificare)
_____</td></tr>
<tr><td>Trattamento dei dati (indicare il supporto utilizzato per la rilevazione e conservazione dei dati)</td><td>☐ In formato cartaceo
☒ In formato digitale
☐ In formato cartaceo / digitale</td></tr>
</table>

	☐ altro (specificare) _____
Categorie di persone interessate	☒ pazienti ☐ volontari sani ☐ operatori sanitari ☐ *altro (specificare)* _____
Categorie di dati trattati	☒ dati sulla salute fisica o psichica ☐ dati genetici ☐ informazioni sulla vita sessuale ☐ informazioni sull'orientamento sessuale ☐ informazioni sugli stili di vita e/o le condizioni socioeconomiche ☐ informazioni su istruzione e formazione professionale ☐ anamnesi lavorativa ☐ informazioni su religione o altre credenze ☐ *altro (specificare)* _____
I dati personali (anche pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono comunicati/condivisi con altri?	☒ No ☐ Sì In caso positivo, selezionare uno o più ambiti di comunicazione: ☐ Promotore ☐ Altri centri partecipanti ☐ CRO
I dati personali (anche pseudonimizzati e che non siano pertanto anonimi o aggregati) vengono trasferiti all'estero?	☒ No ☐ Sì Se sì ☐ Paesi area UE ☐ Paesi extra UE In quale/i Paese/i all'interno dell'area o extra UE _____

Misure di protezione dei dati	
Verranno conservati i dati identificativi dei partecipanti?	☒ No ☐ Sì Se sì, specificare le ragioni sottese a tale esigenza: _____ _____ _____
Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca	Per non identificare direttamente l'interessato sono adottate le seguenti misure: ☐ Adozione di tecniche crittografiche ☒ Utilizzo di codici univoci per ciascun partecipante. Solo il responsabile della ricerca o altri soggetti autorizzati, possono (con l'uso di mezzi ragionevoli) collegare i codici all'identità dei partecipanti ☐ Altro, specificare in dettaglio _____ _____ Per anonimizzare o aggregare i dati, anche in un momento successivo alla raccolta, sono adottate le seguenti misure: ☐ I dati personali, a seguito della raccolta sono eliminati definitivamente senza la possibilità di risalire ai dati originali ☒ I dati personali sono sostituti da uno o più identificatori, che possono essere utilizzati per un set di dati o per ogni singolo dato con distruzione del dato personale originario ☐ Sono distrutti i dati che possono essere idonei a identificare gli interessati e sono conservati i soli dati aggregati ☐ Altro (specificare) _____

PRINCIPI, FINALITA' E BASI GIURIDICHE	
Necessità e proporzionalità	
Gli scopi del trattamento sono specifici, espliciti e legittimi?	X Sì ☐ No Motivare la risposta: 1. Specificità degli scopi: Gli scopi del trattamento sono chiaramente e analiticamente definiti all'interno del protocollo. In relazione agli obiettivi dello studio il trattamento è legato esclusivamente alla ricerca così come dettagliatamente descritta e non a ulteriori scopi; pertanto, le finalità risultano circoscritte al contesto descritto. L'uso dei dati è confinato a uno scopo ben definito e non a fini generici o non correlati. 2. Esplicitazione degli scopi: Gli scopi del trattamento sono comunicati chiaramente negli endpoints del protocollo. Gli stessi sono funzionali a raccogliere evidenze scientifiche, migliorare la comprensione delle patologie/trattamenti descritti, e i relativi dati saranno trattati in modo proporzionale all'obiettivo. 3. Legittimità degli scopi: Per quanto riguarda la legittimità, lo studio osservazionale deve rispettare i requisiti legali per la ricerca scientifica previsti dal GDPR e dalle normative nazionali applicabili. Poiché il trattamento è finalizzato alla ricerca, e non a scopi commerciali, rientra nelle finalità legittime ai sensi dell'art. 9 del GDPR, che consente il trattamento di dati sanitari per motivi di ricerca scientifica, soggetto all'adozione di adeguate misure di sicurezza e minimizzazione dei dati. 4. Proporzionalità e necessità: Riguardo a proporzionalità e necessità, i dati trattati sono strettamente necessari a raggiungere gli obiettivi dello studio. Nel contesto di uno studio retrospettivo, ciò implica l'uso di dati già raccolti in precedenza, riducendo al minimo il rischio di interferenze non necessarie con la protezione dei dati degli interessati. L'utilizzo di dati anonimi o pseudonimizzati, ove applicabile, sarà sempre impiegato quale misura di mitigazione per limitare il rischio.
I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	X Sì ☐ No Motivare la risposta: La valutazione circa la pertinenza, limitazione e necessità in relazione alle finalità dello studio in oggetto è basata sul principio di minimizzazione dei dati (art. 5(1)(c) del GDPR): 1. Adeguatezza dei dati: I dati raccolti sono appropriati per raggiungere le finalità dello studio. Nello studio osservazionale retrospettivo descritto, significa che i dati selezionati oggetto di trattamento sono strettamente necessari per rispondere ai quesiti oggetto della ricerca e alle ipotesi formulate nel protocollo.

	I dati trattati sono scelti in base alla loro rilevanza scientifica e clinica rispetto agli obiettivi dello studio. 2. Pertinenza dei dati: I dati sono pertinenti ovvero hanno un legame diretto con gli scopi dello studio. Gli stessi sono rilevanti per rispondere agli specifici quesiti scientifici che lo studio intende esplorare. Non vengono trattati dati che non hanno una connessione chiara con le finalità dichiarate, riducendo il trattamento a informazioni essenziali per la validità scientifica dello studio. 3. Limitazione dei dati (minimizzazione): Il protocollo prevede la raccolta dei soli dati strettamente necessari per conseguire le finalità dello studio. I dati sono limitati per ridurre l'impatto sulla privacy degli interessati, evitando la raccolta di informazioni sovrabbondanti o ridondanti. Poiché lo studio è retrospettivo, verranno trattati dati già raccolti per altri scopi (quali la cura dei pazienti), relativamente ai quali si sono accuratamente selezionate solo le informazioni essenziali per l'analisi. Si farà ricorso a tecniche di anonimizzazione o pseudonimizzazione, ove applicabile, per limitare l'identificabilità degli individui. 4. Necessità dei dati: Relativamente al principio di necessità lo studio non potrebbe essere condotto correttamente senza il trattamento dei dati previsti dal protocollo. Ogni categoria di dato trattato è necessaria per fornire risultati significativi e validi scientificamente. La raccolta di ulteriori dati fuori protocollo non essenziali non sarebbe in alcun modo giustificata. Pertanto, è possibile considerare i dati adeguati perché appropriati allo scopo dello studio, pertinenti perché direttamente legati alle finalità dichiarate e limitati in quanto raccolti solo nella misura strettamente necessaria per la ricerca, nel rispetto del principio di minimizzazione dei dati previsto dal GDPR.
Integrità ed esattezza	
I dati sono esatti e aggiornati?	X Sì ☐ No Motivare la risposta: La valutazione rispetto alla correttezza dei dati e all'aggiornamento è stata fatta in linea con il principio di esattezza previsto dall'art. 5(1)(d) del GDPR: 1. Esattezza dei dati: Lo studio osservazionale retrospettivo si basa su dati già esistenti, raccolti in precedenza per finalità cliniche. Poiché originariamente utilizzati per diagnosi e trattamenti medici, i dati sono stati raccolti e registrati con un alto livello di accuratezza e precisione, in quanto necessari per garantire la cura dei pazienti. Le fonti dei dati, quali ad esempio cartelle cliniche, referti o database ospedalieri, sono dunque affidabili in quanto strumentali al corretto trattamento del paziente, il che assicura una raccolta attenta e precisa delle informazioni. 2. Validazione delle fonti dei dati:

	Tutte le fonti dei dati sono istituzionalmente validate e soggette a rigorosi controlli di qualità. Vengono applicate procedure per la revisione e la verifica dei dati clinici, riducendo così il rischio di errori. I dati utilizzati sono stati raccolti in conformità a questi protocolli di qualità, assicurando la loro precisione. 3. Controlli e verifiche incrociate: All'interno dello studio, sono attuati meccanismi di controllo per garantire l'esattezza dei dati utilizzati. Processi di revisione e pulizia dei dati sono posti in essere per assicurare che non vi siano errori evidenti o duplicazioni [selezionare se del caso tra 4-Eyes Check, Double Data Entry, Source Data Verification (SDV), Query Management, Edit Checks, Audit Trail, Risk-Based Monitoring, Statistical Data Cleaning, Validation and Cross-Validation] 4. Aggiornamento dei dati: Lo studio retrospettivo utilizza dati storici, pertanto i dati utilizzati sono pertinenti per il periodo temporale di riferimento dello studio. L'aggiornamento dei dati si riferisce alla loro coerenza rispetto al momento storico e al contesto clinico in cui sono stati raccolti. In quest'ottica, i dati non devono pertanto essere "aggiornati" nel senso tradizionale, ma devono riflettere fedelmente lo stato di salute o il trattamento del paziente in quel determinato periodo. 5. Misure di mitigazione del rischio: Esclusivamente i dati accurati e affidabili vengano inclusi nelle analisi finali: lo studio adotta misure di mitigazione come l'esclusione di record non completi o poco chiari. Pertanto i dati trattati nello studio sono esatti perché raccolti da fonti affidabili e soggette a controlli di qualità, accurati nel contesto clinico originario e aggiornati rispetto al periodo storico di interesse. Inoltre, lo studio prevede misure per verificare la correttezza dei dati e garantire che qualsiasi eventuale errore venga identificato e corretto.
Limitazione della conservazione	
Per quanto tempo verranno conservati i dati raccolti?	Indicare il numero di mesi/anni: 3 anni Decorso tale termine i dati verranno: ☒ Anonimizzati completamente ☐ Distrutti ☐ altro (*specificare*) _____

Basi giuridiche	
Quali sono le basi giuridiche del trattamento?	☒ art. 9, par. 2, lett. j) GDPR[1] ☐ art. 110, co. 1 primo periodo Codice Privacy[2] ☐ art. 110, co. 1, secondo periodo Codice Privacy[3]
MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO	
Informativa e consenso	
SOLO SE LA BASE GIURIDICA È L'ART. 110, CO. 1, SECONDO PERIODO ***Indicare i motivi per i quali non è possibile fornire l'informativa ai partecipanti allo Studio (soggetti interessati) e acquisirne il consenso***	☐ motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione ☐ sebbene sia stato svolto ogni ragionevole sforzo organizzativo, non è possibile contattare gli interessati in ragione del numero molto alto di interessati non contattabili/non raggiungibili ☐ deceduti o non contattabili
Come sono informati del trattamento gli interessati?	☒ E' stata pubblicata una informativa per pubblici proclami sul sito del promotore ☐ E' stata pubblicata una informativa per pubblici proclami sul sito di tutti i centri partecipanti
E' stata predisposta una valutazione di impatto ai sensi dell'art. 35 del GDPR?	☒ si ☐ no
E' stata pubblicata la valutazione di impatto?	☒ sul sito del promotore ☐ sul sito di tutti i centri partecipanti

[1] il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

[2] Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità' all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.

[3] Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, se del caso documentando altresì i ragionevoli sforzi profusi per tentare di contattarli.
Nei predetti casi, i titolari del trattamento di dati sulla salute per finalità di ricerca medica, biomedica e epidemiologica riferiti a soggetti deceduti o non contattabili devono altresì svolgere e pubblicare la valutazione di impatto, ai sensi dell'art. 35 del Regolamento, dandone comunicazione al Garante.

E' stata comunicato l'avvenuto svolgimento e pubblicazione della valutazione di impatto al Garante Privacy?[4]	☐ si ☐ no ☒ non necessario
Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR	
E' stata predisposta una procedura ad hoc da parte del Titolare?	☒ Sì ☐ No
Come fanno gli interessati a esercitare i loro diritti	Rivolgendosi direttamente ai titolari del trattamento o ai rispettivi dpo così come indicato nell'informativa

[4] Solo nel caso in cui la base giuridica sia art. 110, co. 1, secondo periodo Codice Privacy[4]

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esistenti	Note
Organigramma interno	X	○ Ruoli e Responsabilità
Controllo accessi	X	○ L'accesso avviene tramite account personali. ○ Sono applicate politiche di minimizzazione e restrizione dell'accesso ai dati personali. ○ L'autenticazione è effettuata tramite password e, in alcuni casi, tramite autenticazione a due fattori. ○ Sono adottate delle politiche di complessità delle password in coerenza con le buone pratiche di settore
Gestione dei cambiamenti	X	○ Ogni modifica ai sistemi IT è valutata, registrata e monitorata. ○ E' stata definita una procedura generale per la protezione dei dati personali, comprensiva di valutazioni in ottica by design e by default, volta a individuare i requisiti di protezione dei trattamenti e a implementare e mantenere i sistemi e le applicazioni garantendo livelli di sicurezza adeguati. ○ L'acquisizione di componenti del sistema informativo tiene conto dei requisiti di sicurezza dei trattamenti che dovranno essere supportati e delle garanzie offerte dal fornitore.
Strumenti di sicurezza e protezione	X	○ Firewall, anti-malware centralizzati e strumenti di protezione per le postazioni di lavoro. ○ Monitoraggio continuo del sistema IT per rilevare incidenti di sicurezza.
Gestione degli incidenti	X	○ Le violazioni dei dati personali vengono gestite tramite procedure di escalation, coinvolgendo il DPO. ○ È attivo un sistema di monitoraggio continuo (SIEM e SOC) per raccogliere e analizzare i log. ○ Il titolare mantiene un registro delle violazioni dei dati personali.
Rapporti con i Responsabili	X	○ Il titolare gestisce i rapporti con i propri Responsabili del trattamento attraverso accordi formalizzati che comprendono specifiche clausole per assicurare la riservatezza dei dati trattati e l'obbligo per i Responsabili di operare in conformità alla normativa sul trattamento dei dati personali, in particolare, per quanto riguarda le misure di sicurezza, in riferimento agli art. 28 e 32.

Pseudonimizzazione e cifratura	X	○ Pseudonimizzazione e cifratura sono utilizzate per limitare l'identificabilità dei dati. ○ Viene applicata la cifratura nelle connessioni VPN, nei servizi HTTPS e nelle comunicazioni machine-to-machine.
Continuità operativa	X	○ L'infrastruttura IT è progettata per garantire la continuità operativa tramite due datacenter distanti almeno 20 km. ○ I dati di backup sono conservati in un sito di recupero dati a oltre 100 km.
Formazione e gestione del personale	X	○ Il personale riceve formazione istituzionale con corsi FAD sulla protezione dei dati e sicurezza informatica, con incontri di aggiornamento periodici awareness e sensibilizzazione. ○ Il personale con ruoli specifici nell'ambito della data protection (Local Privacy Executive e Local Privacy Contact) riceve una formazione specifica ulteriore.
Sicurezza delle postazioni di lavoro e delle reti	X	○ Le postazioni di lavoro sono aggiornate regolarmente e protette da sistemi anti-malware. ○ Le reti sono protette da firewall e strumenti di monitoraggio delle intrusioni.
Backup e Vulnerability Assessment	X	○ Backup giornalieri dei dati e test periodici del sistema di ripristino. ○ Valutazioni periodiche della vulnerabilità per identificare possibili rischi di sicurezza.
Sicurezza fisica	X	○ I datacenter sono protetti da misure fisiche e ambientali (protezione da incendi, allagamenti, controllo accessi fisici). ○ I datacenter sono certificati TIER3 e TIER4.

APPENDICE

MINACCE

ACCESSO ILLEGITTIMO AI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti Potenziali
Perdita di controllo dei propri dati
Utilizzo da parte di terzi di dati dell'interessato

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia
Comportamenti sleali/fraudolenti
Attacco informatico (es. social engineering, man in the middle, denial of service, brute force, etc.)
Furto e/o perdita di dispositivi, supporti di memorizzazione, documenti

Quali sono le fonti di rischio?

Fonte
Fonti umane esterne (es. criminali informatici, fornitori, utenti)
Fonti umane interne accidentali (es. collaboratori negligenti)

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Politiche di trasmissione dei dati; Crittografia; Pseudonimizzazione

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	Importante
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Limitato

MODIFICHE INDESIDERATE DEI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti Potenziali
Dati non esatti e/o non aggiornati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia
Errore operativo

Fonte
Fonti umane interne accidentali (es. collaboratori negligenti)

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); antivirus/firewall; Back – up dei dati

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?	Limitato
Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?	Trascurabile

PERDITA DI DATI

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Una perdita dei dati potrebbe causare l'alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio; tuttavia non si tratta di dati originali

Impatti Potenziali
Costi aggiuntivi

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Minaccia
Errore operativo

Quali sono le fonti di rischio?

Fonte
Eventi tecnologici (es. guasti, malfunzionamenti, etc.)
Fonti umane interne accidentali (es. collaboratori negligenti)

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; antivirus/firewall; Tracciabilità, Gestione postazioni; Politiche di tutela della privacy¸ Politiche di sicurezza informatica

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	Trascurabile
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Trascurabile

VALUTAZIONE DEL RISCHIO

PROBABILITA' (P)	*IMPATTO (I)*	*RISCHIO (R=P*I)*
Probabilità trascurabile: 1 Probabilità limitato: 2 Probabilità importane: 3 Probabilità massima: 4	Impatto trascurabile: 1 Impatto limitato: 2 Impatto importante: 3 Impatto massimo: 4	Rischio basso: R< 6 Rischio medio: 7<R<11 Rischio alto: R>11

MATRICE DI VALUTAZIONE DEL RISCHIO

		IMPATTO§§			
PROBABILITA' §	**MASSIMO**	4	8	12	16
	IMPORTANTE	3	6	9	12
	LIMITATO	2	4	6	8
	TRASCURABILE	1	2	3	4
		TRASCURABILE	**LIMITATO**	**IMPORTANTE**	**MASSIMO**

§ Frequenza con la quale si possono verificare criticità nel trattamento dei dati: **Rischio molto basso**: è probabile che non si verifichi mai; **Basso**: non è probabile che si verifichi, ma può accadere; **Medio**: si può verificare occasionalmente; **Alto**: è probabile che si verifichi, ma non in modo persistente/stabile;

§§ Impatto atteso: **Molto basso**: è improbabile che possa avere un qualsiasi impatto; **Basso**: può avere un impatto; **Medio**: è probabile che abbia un impatto; **Alto**: molto probabile che abbia un impatto significativo;

MINACCIA	**VALORE DEL RISCHIO (P*I)**	**LIVELLO DI RISCHIO**	**VALUTAZIONE COMPLESSIVA** (SOMMA COLONNA LIVELLO RISCHIO)
ACCESSO ILLEGITTIMO	3*2	6	**6**
MODIFICHE INDESIDERATE DEI DATI	1*2	2	
PERDITA DI DATI	1*1	1	

Classificazione	**Intervallo del rischio**
Assenza di Rischio	Valore finale tra 0 e 2 compresi
Rischio Limitato	Valore finale tra 3 e 6 compresi
Rischio Importanto	Valore finale tra 7 e 11 compresi
Rischio Massimo	Valore finale tra 12 e 16 compresi