DPIA
ex art. 35 GDPR

INDICE

Il contesto normativo del *Data Protection Impact Assessment*	3
Data Protection Impact Assessment (DPIA)	7
A) Contesto	7
B) Misure di sicurezza	10
B.1) Misure di sicurezza organizzative	10
B.2) Misure di sicurezza tecniche	12
C) DPIA	14
C.1) Accesso illegittimo	15
C.2) Modifica indesiderata	17
C.3) Perdita accidentale	18
Grafico DPIA	19

IL CONTESTO NORMATIVO DEL DATA PROTECTION IMPACT ASSESSMENT

Il *Data Protection Impact Assessment* (per brevità anche DPIA) è uno strumento importante in termini di responsabilizzazione *(principio di accountability),* in quanto soccorre e sostiene il Titolare del trattamento non soltanto nel rispettare e far rispettare le prescrizioni del GDPR, ma anche nel dimostrare di aver adottato le misure idonee a mitigare il rischio durante tutte le fasi trattamentali. In altri termini, la Valutazione d'Impatto sulla Protezione dei Dati è una procedura di *risk management* che permette di dimostrare la conformità con le norme in materia di protezione dei dati personali europee e domestiche. Muovendo i passi dal dettato normativo, segue il testo dell'art. 35 GDPR:

"ART. 35

Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi."

La disciplina sulla *DPIA*, contenuta nel GDPR, deve essere integrata anche da quanto specificato dal *WP29* (oggi *European Data Protection Board* - EDPB) nelle linee guida concernenti la valutazione di impatto sulla protezione dei dati, nonché i criteri per stabilire se un trattamento possa o meno presentare un rischio privacy più o meno elevato.

In particolare, le linee guida citate ampliano l'obbligatorietà della valutazione di impatto, oltre ai casi espressamente indicati dal regolamento all´art. 35, par. 3, GDPR, anche in quelli che comportano la comunicazione di dati su larga scala tra diversi titolari e/o trattamenti

sistematici di dati genetici o sanitari, tenendo conto del volume dei dati, della durata e dell'attività di trattamento.

Il presente documento è, inoltre, uno strumento dedicato alla valutazione del rischio ed ha lo scopo di fornire informazioni basate sia su evidenze che su metodi di analisi, al fine di rendere agevole l'adozione di decisioni informate circa il trattamento di particolari rischi.
Le informazioni ottenute consentono, quindi, di identificare i fattori determinanti, gli eventi potenzialmente dannosi e suggerire le azioni correttive possibili da mettere in atto per prevenire la ripetizione degli eventi stessi.
Nella prospettiva della gestione del rischio privacy, tale documento risponde al principio fondamentale dell'*accountability*, intesa quale dimostrazione di come il titolare del trattamento abbia posto in essere tutte le misure di sicurezza volte a tutelare i diritti e le libertà degli interessati.

La responsabilizzazione, quale obbligo di rendere conto di ciò che si fa e ciò che si fa fare, rappresenta il fulcro della nuova frontiera della privacy in quanto aspetto essenziale per l'esercizio di una corretta ed efficace *governance*.

Il Regolamento UE 2016/679 pone, altresì, la necessità di rendere conto anche dell'adozione di comportamenti proattivi, tali da "*dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR*" (artt. 23-25, in particolare, e l'intero Capo IV del GDPR).

Ne consegue, dunque, che è affidato al Titolare del trattamento dei dati il compito di decidere autonomamente le modalità, le misure di sicurezza e i limiti del trattamento stesso, nel rispetto delle disposizioni normative ed alla luce dei criteri indicati nel Regolamento UE, oltre che a quelli indicati dall'ordinamento interno (Codice Privacy - D.lgs. 196/2003, come novellato dal D.lgs. 101/2018) e rispetto alle Linee Guida e Regole Deontologiche previste dal Garante per la Protezione dei Dati Personali.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by design and by default*" (art. 25 GDPR), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio e per impostazione predefinita le garanzie indispensabili al fine di soddisfare i

requisiti del Regolamento stesso e tutelare i diritti e le libertà degli interessati, tenendo conto del contesto complessivo ove il trattamento viene svolto e dei rischi connessi.

Fondamentali fra tali attività sono quelle relative al successivo criterio del rischio inerente al trattamento; quest'ultimo è da ritenersi, infatti, come il rischio capace di impattare negativamente sulle libertà e sui diritti degli interessati (considerando 75-77).

Tali criticità dovranno essere analizzate attraverso un apposito processo di valutazione (artt. 35 e 36 GDPR) tenendo conto dei rischi noti o ipotizzabili e delle misure tecniche, fisiche e organizzative che il Titolare ritiene di dover adottare per mitigare tali rischi.

In ossequio a tali criteri, il presente documento viene redatto in base alle tecniche ed alle modalità della norma ISO/IEC 31000:2018, "*Risk Management – Principles and guidelines*", che descrive in dettaglio il processo logico e sistematico che porta alla mitigazione e controllo dei rischi.

La *ratio* della scelta risiede nella necessità di conferire connotati positivi alla gestione del rischio, anche attraverso la percezione dello stesso come opportunità, mediante una lettura del pericolo quale possibilità di innovazione.

Ulteriore ed importante elemento di valutazione è il contenuto dello standard ISO/IEC 31010:2009 (*Risk Management e Risk Assessment Techniques*) ove vengono riportati i concetti della gestione dei rischi e le diverse tecniche atte alla loro valutazione nei diversi ambiti.

È, infine, doveroso adeguarsi alle disposizioni contenute nelle norme:

- ISO/IEC 29134:2017 ("*Information technology – Security techniques – Guidelines for privacy impact assessment*") che indica linee guida applicabili a tutte le tipologie di strutture, pubbliche e private, al fine di creare, organizzare ed implementare progetti GDPR *compliant*;

- ISO/IEC 27002:2017 ("*Information Technology - Security techniques - Code of practice for information security controls*") che indica le linee guida per gli standard di sicurezza delle informazioni organizzative e pratiche di gestione della sicurezza delle informazioni, compresa la selezione, l'implementazione e la gestione dei controlli;

- ISO/IEC 27005:2018 ("*Information security risk management*") che, è in parte applicabile anche alla valutazione del rischio connesso al trattamento dei dati

personali; assumono importanza determinante le appendici dedicate all'approfondimento di alcuni aspetti della gestione dei rischi e, in particolare, quella relativa al catalogo delle minacce;

- ISO/IEC 27701:2019 ("*Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines*") che fornisce requisiti e linee guida per costruire, implementare, mantenere e migliorare costantemente un PIMS (*Privacy Information Management System* o sistema di gestione delle informazioni sulla privacy), sia qualora l'organizzazione operi come titolare del Trattamento (*Data Controller*), che come Responsabile (*Data Processor*).

- ISO 31000:2018 ("Risk management -- Principles and guidelines") fornisce principi e linee guida generali per la gestione del rischio ed è applicabile a tutte le tipologie di organizzazioni. La ISO 31000 può essere applicata a qualsiasi tipo di rischio e nel corso dell'intero ciclo di vita di un'organizzazione, in merito a molteplici attività come la definizione di strategie e decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e beni.

In conclusione, il rischio può essere definito come la combinazione delle probabilità di un evento e della gravità delle sue conseguenze. Qualunque tipo di iniziativa implica potenzialmente eventi e conseguenze che rappresentano possibili benefici (elementi positivi) o minacce alla sicurezza dell'attività trattamentale posta in essere (elementi negativi).

Data Protection Impact Assessment (DPIA)

Titolare del trattamento:

Istituto Superiore di Sanità

Nome Attività:

Valutazione d'Impatto sui Registri relativi alle malattie rare

Data di creazione:

11 maggio 2023

A) CONTESTO

Raccolta dei dati direttamente dall'interessato, relativi alle malattie rare all'interno dei seguenti Registri:

- *Registro Nazionale Malattie Rare (RNMR);*
- *Registro per la Ricerca Scientifica e Clinica sulla sindrome di Lennox Gastaut;*
- *Registro per la Ricerca Scientifica e Clinica sulla sindrome di Lesch- Nyhan;*
- *Registro per la Ricerca Scientifica e Clinica sulla sindrome di Prader Willi;*
- *Registro per la Ricerca Scientifica e Clinica sulla Narcolessia e le Ipersonnie del sistema nervoso centrale (ReN&IS);*
- *Registro per la Ricerca Scientifica e Clinica sulla sindrome di Angelman (RANG);*
- *Registro per la Ricerca Scientifica e Clinica sulla spina bifida;*

- *Registro per la Ricerca Scientifica e Clinica sull'Emoglobinuria Parossistica Notturna;*
- *Registro per la Ricerca Scientifica e Clinica sulla sclerosi tuberosa;*
- *Registro per la Ricerca Scientifica e Clinica sulla sindrome di Pitt- Hopkins;*
- *Registro per la Ricerca Scientifica e Clinica sulla sindrome di Mowat Wilson;*
- *Registro per la Ricerca Scientifica e Clinica sulla sindrome di Struge Weber;*
- *Registro per la Ricerca Scientifica e Clinica sulla fibrosi polmonare idiopatica;*
- *Registro per la Ricerca Scientifica e Clinica sulla malattia di Lafora.*

1) Finalità del trattamento:

- ✓ Studio e ricerca scientifica

2) Categorie di interessati:

- ✓ Pazienti
- ✓ Persone particolarmente vulnerabili

3) Numero di interessati:

- ✓ Da 1 a 100

4) Sono somministrate le informazioni privacy all'interessato?

- ✓ Si

5) Come sono rese all'interessato le informazioni privacy?

- ✓ Consegna diretta all'interessato
- ✓ Pubblicazione sul sito web dell'ISS - CNMR

6) Sono previste modalità per l'esercizio dei diritti dell'interessato? (quali, il diritto di accesso, di rettifica, di cancellazione, di limitazione, di portabilità dei dati, di opposizione)

- ✓ Si

7) Quali sono le modalità per l'esercizio dei diritti dell'interessato?

- ✓ A mezzo mail/PEC

8) Categorie di dati personali:

- ✓ Dati anagrafici pseudonimizzati
- ✓ Dati relativi alla salute/sanitari
- ✓ Dati antropometrici
- ✓ Dati genetici

9) Elencare le attività di trattamento effettuate:

- ✓ Raccolta direttamente dall'interessato
- ✓ Registrazione
- ✓ Conservazione
- ✓ Organizzazione
- ✓ Consultazione
- ✓ Elaborazione
- ✓ Selezione
- ✓ Estrazione
- ✓ Raffronto
- ✓ Utilizzo
- ✓ Blocco/Limitazione
- ✓ Comunicazione
- ✓ Cancellazione
- ✓ Distruzione

10) Modalità di conservazione:

- ✓ Digitale

11) Cancellazione:

- ✓ Sino al raggiungimento delle finalità del trattamento

12) Categorie di destinatari:

- ✓ Responsabile del trattamento *ex* art. 28 GDPR
- ✓ Titolari autonomi del trattamento ex art. 24 GDPR

13) Piattaforme, dispositivi e/o applicativi utilizzati nell'ambito dell'attività di trattamento in esame:

- Piattaforma RegistRare

14) Avviene un trasferimento di dati personali al di fuori dei confini nazionali?

- ✓ Si

15) Trasferimento verso Paesi UE/SEE:

- ✓ Non applicabile

16) È previsto un trasferimento verso Organizzazioni Internazionali (es. OMS; CDC; FAO; ONU)?

- ✓ Si (*European Reference Networks* (ERN); *International Rare Diseases Research Consortium* (IRDiRC); *International Conference on Rare Diseases & Orphan Drugs* (ICORD)

17) Base Giuridica del Trattamento *ex* art. 6 GDPR:

- ✓ Consenso interessato (art. 6, par. 1, lett. A)

18) Base Giuridica del Trattamento *ex* art. 9 GDPR:

- ✓ Consenso rafforzato dell'interessato (art. 9, par. 2, lett. A)

19) Ove applicabile, come si ottiene il consenso degli interessati?

- ✓ Tramite modulo cartaceo

20) Tipologia di trattamento:

- ✓ Trattamenti non occasionali di dati relativi a soggetti vulnerabili quali minori, disabili, anziani, infermi di mente, pazienti e richiedenti asilo.

B) MISURE DI SICUREZZA

B.1) MISURE DI SICUREZZA ORGANIZZATIVE

21) Sicurezza dell'archiviazione della documentazione cartacea:

- ✓ Non applicabile

22) Nomina delle Persone autorizzate per designazione

- ✓ Si

23) Nomina dei delegati al trattamento:

- ✓ Si

24) Nomina dei Responsabili del trattamento:

- ✓ Si

25) Elaborazione ed adozione di policy privacy aziendali:

- ✓ No

26) Controllo degli accessi fisici:

- ✓ Si

27) Quali?

- ➢ L'infrastruttura fisica che ospita gli impianti informatici dell'ISS per l'erogazione sia di servizi interni, sia di servizi esterni a sostegno delle attività di ricerca, sviluppo e trasferimento tecnologico è suddivisa su due *Data Center.* Il *Data Center* principale è ubicato attualmente nell'Area A al piano B dell'edificio 52, mentre il secondario nell'Area C presso Giano della Bella (GB). La sicurezza fisica dei *Data Center* ISS è il complesso di soluzioni tecnico- pratiche atte a impedire che utenti non autorizzati possano accedere a risorse, sistemi, dispositivi, apparati, informazioni e dati di natura riservata, essa prevede: l'utilizzo di porte di accesso blindate all'area del *Data Center* e l'impiego di sistemi di identificazione personale per il controllo dell'accesso e la videosorveglianza con registrazione

28) Formazione del personale:

- ✓ Si (Il personale dell'Istituto coinvolto sia in attività di ricerca sia in attività amministrativa periodicamente viene coinvolto in corsi di formazione e aggiornamento sulla sicurezza informatica)

29) Altra misura di sicurezza fisica e/o organizzativa implementata:

- ➢ Gli edifici ed i locali in cui risiedono i *server* sono dotati di un sistema di allarme antincendio; l'impianto elettrico è dotato di un gruppo elettrogeno per garantire la continuità dei sistemi informatici ospitati e di un sistema di allarme; presso i locali

del *Data Center* situato in Via Giano della Bella è stata predisposta una cassaforte ignifuga per la conservazione delle copie di *backup;* sono in corso lavori di adeguamento dei locali in cui sarà ospitato il *Data Center* principale dell'Istituto

B.2) MISURE DI SICUREZZA TECNICHE

30) Crittografia *Database*:

- ✓ Simmetrica (vengono applicati alla piattaforma RegistRare algoritmi di crittografia a chiave simmetrica e la crittografia a chiave simmetrica è usata per proteggere i dati in una VPN; viene attualmente utilizzato il 3DES, ma è in corso la sostituzione con l'AES a 256 bit)

Algoritmi di criptografia a chiave simmetrica	Lunghezza chiave (in bit)	Descrizione
DES	56	Anche se piuttosto vecchio, il DES è ancora usato. Il DES fu progettato per essere realizzato in hardware, quindi è molto lento se usato da un software.
3DES	112 and 168	Cripta i dati tre volte con il DES, quindi si ritiene che sia molto più resistente agli attacchi rispetto al DES. É molto lento in confronto a cifrari a blocchi, quale ad esempio AES.
AES	128, 192, and 256	AES è molto veloce sia nella versione software sia nella versione hardware, è facile da realizzare e richiede poca memoria.

31) Sistema operativo *workstation*:

- ✓ Windows

32) Aggiornamento sistema operativo:

- ✓ Windows Si

33) Configurazione *workstation*:

- ✓ Utente con restrizioni
- ✓ Crittografia dei dati
- ✓ Cambio password temporizzato

34) Tecniche di anonimizzazione:

- ✓ Non applicabile

35) Tecniche di pseudonimizzazione:

- ✓ Funzione crittografica di Hash (viene applicato al codice fiscale un algoritmo di hashing; tramite la funzione di Hash, i dati vengono portati ad una lunghezza uniforme, indipendentemente dalla dimensione del valore di partenza; il codice hash generato non è reversibile ed è, pertanto, impossibile tornare al codice fiscale di partenza)

36) Partizionamento:

Fisso (la piattaforma RegistRare è suddivisa in moduli che rappresentano sottosistemi, come ad esempio un modulo per la gestione dei dati di diagnosi e un altro per la gestione dei dati di arruolamento; tutti i moduli rappresentano parti funzionali)

37) Controllo degli accessi logici:

- ✓ Si

38) Quali strumenti vengono utilizzati?

- ➢ *login* con nome utente e *password*
- ➢ gestione autorizzazioni in base alla funzione/ruolo

(la piattaforma RegistRare è in grado di autenticare gli utenti, verificare che essi siano autorizzati a eseguire determinate azioni e monitorare l'accesso e l'utilizzo delle informazioni.

Le funzionalità implementate sono:

Autenticazione degli utenti: la piattaforma richiede agli utenti inserimento delle credenziali corrette, come nome utente e password, per accedere alle sue funzionalità e dati. La password ha regole di creazione ben definite con scadenza semestrale.

Autorizzazione degli utenti: la piattaforma attribuisce ruoli e funzionalità specifiche a seconda del tipo di utente che viene autorizzato.

Monitoraggio degli accessi: la piattaforma registra tutte le attività degli utenti, come l'accesso ai dati, le modifiche apportate e le operazioni eseguite)

39) Tracciabilità:

- ✓ Si

40) Quali strumenti vengono utilizzati?

- La piattaforma RegistRare fa riferimento a documenti di analisi che tracciano lo sviluppo della piattaforma. Per quanto riguarda i requisiti, le specifiche, la progettazione, il codice sorgente, i test e la manutenzione del software si fa riferimento alle procedure di gestione che vengono utilizzate in Istituto Superiore di Sanità

41) Misure anti-malware:

- ✓ *Antivirus*
- ✓ *Anti-malware*

(L'ISS applica *software antivirus, anti-malware e anti-spam*)

42) Backup:

- ✓ Continuo (il Servizio di Informatica esegue backup periodici e i file di backup sono conservati su storage centralizzato dell'ISS)

43) Sicurezza dei canali informatici:

- ✓ *Firewall* (la sicurezza perimetrale è protetta da un cluster di next- generation firewall (NGFW) Check Point con banda passante a 10 Gbps)
- ✓ presso i *Data Center* dell'ISS esiste un sistema *Disaster Recovery* che permette di archiviare i dati critici dell'Istituto

C) DPIA

44) Vengono applicate e/o osservate linee guida, *best practice* di settore, norme UNI/ISO/IEC, codice di condotta, regolamenti aziendali, etc.?

- ✓ No

45) La finalità di trattamento è specifica, esplicita e legittima?

- ✓ **Specifica**: è ben delineata ed individuata nella necessità del titolare di raccogliere, mediante piattaforma RegistRare, i dati relativi alle malattie rare all'interno dei rispettivi Registri

- ✓ **Esplicita**: in quanto rappresentata chiaramente agli interessati per il tramite delle informazioni privacy *ex* art. 13 GDPR consegnate in forma cartacea personalmente ai medesimi interessati, in calce alle quali è presente apposito modulo di consenso al trattamento dei dati personali, nonché pubblicate sul sito web dell'ISS - CNMR
- ✓ **Legittima:** in quanto sorretta da idonea base giuridica del trattamento rinvenibile, in relazione all'attività trattamentale svolta in favore dei pazienti, nell'art. 6, par. 1, lett. a) GDPR ossia "*l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità*", nonché nella deroga di cui all'art. 9, par. 2, lett. a) GDPR, in quanto "*l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche*".

46) Come viene rispettato il principio di minimizzazione dei dati?

- ➢ Sono raccolti esclusivamente dati necessari al conseguimento della specifica finalità del trattamento.

C.1) ACCESSO ILLEGITTIMO

47) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di accesso illegittimo dovesse concretizzarsi?

- ✓ Perdita del controllo dei dati personali
- ✓ Decifratura non autorizzata della pseudonimizzazione
- ✓ Pregiudizio alla reputazione
- ✓ Perdita di riservatezza dei dati personali protetti da segreto professionale
- ✓ Conoscenza da parte di terzi non autorizzati

48) Quali sono le principali minacce che potrebbero concretizzare il rischio?

- ✓ Compromissione di informazioni
- ✓ Azioni non autorizzate
- ✓ Attacchi di ingegneria sociale

49) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne

✓ Fonti umane esterne

ALTAMENTE PROBABILE (4)	**4**	**8**	**12**	**16**
PROBABILE (3)	**3**	**6**	**9**	**12**
POCO PROBABILE (2)	**2**	**4**	**6**	**8**
IMPROBABILE (1)	**1**	**2**	**3**	**4**
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	**LIEVE (1)**	**MEDIO (2)**	**GRAVE (3)**	**GRAVISSIMO (4)**

C.2) MODIFICA INDESIDERATA

50) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di modifica indesiderata dei dati dovesse concretizzarsi?

- ✓ Limitazione dei diritti

51) Quali sono le principali minacce che potrebbero concretizzare il rischio?

- ✓ Danni fisici
- ✓ Azioni non autorizzate

52) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

C.3) PERDITA ACCIDENTALE

53) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di perdita di dati dovesse concretizzarsi?

- ✓ Limitazione dei diritti

54) Quali sono le principali minacce che potrebbero concretizzare il rischio?

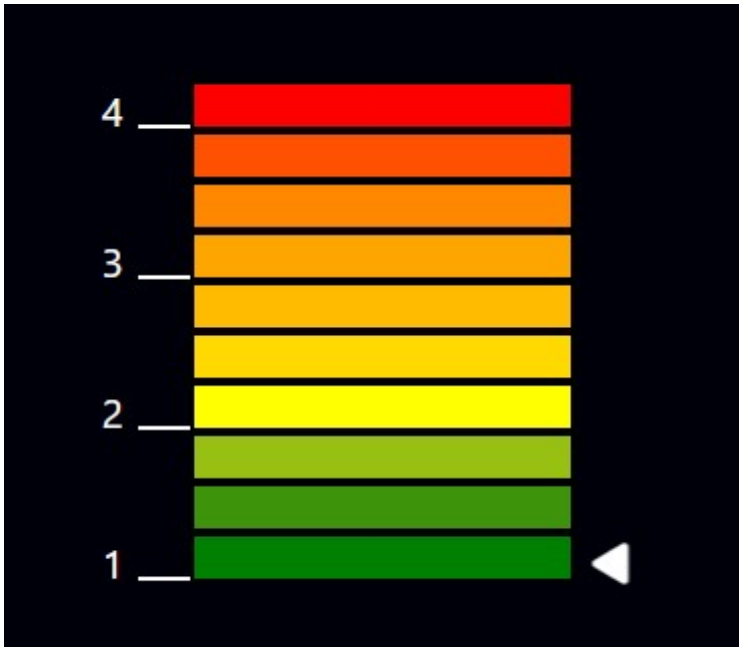
- ✓ Danni fisici
- ✓ Eventi naturali
- ✓ Perdita di servizi essenziali
- ✓ Azioni non autorizzate
- ✓ Compromissione di funzioni

55) Quali sono le principali fonti di rischio?

- ✓ Fonti umane interne
- ✓ Fonti umane esterne
- ✓ Fonti non umane

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
1, 2, 3 TRASCURABILE 4, 6, 8 LIMITATO 9, 12, 16 MASSIMO	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

GRAFICO DPIA



TRASCURABILE
LIMITATO
SIGNIFICATIVO
MASSIMO