Privacy by design e misure di sicurezza

Prof. Avv. Stefano Aterno

Pensare alla tutela dei dati fin dalla progettazione del modello di trattamento

……..e adempiere agli obblighi prima dell’inizio effettivo del trattamento stesso

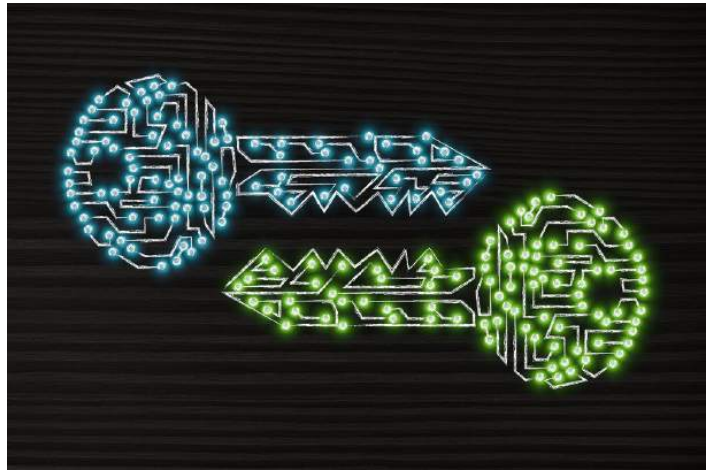
Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25)

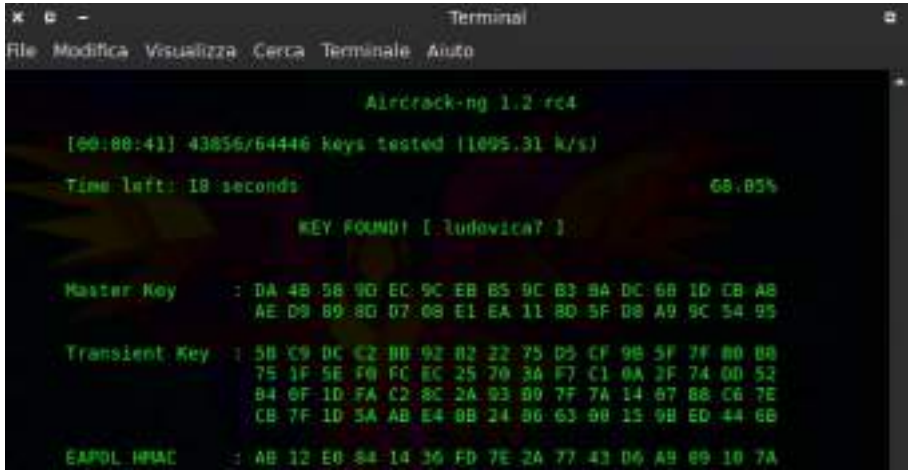
Principio della «***Privacy by design***» fin dall'atto della progettazione e prima dell'esecuzione del trattamento prevedere adeguate misure tecniche ed organizzative

Principio della «**P*rivacy by default***» che ricalca il **principio di necessità**; trattamento solamente per le finalità previste e per il periodo strettamente necessario a tali fini

Principio di responsabilizzazione (cd. principio di accountability) (art. 5, co. 2)

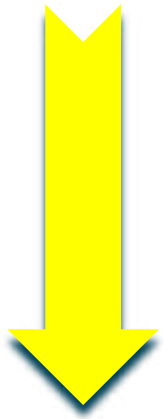
Le misure di sicurezza





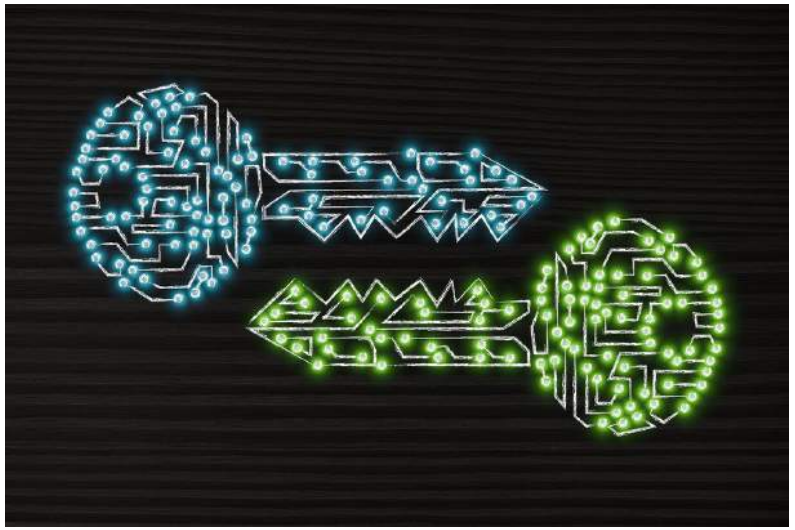
Sicurezza del trattamento e misure di sicurezza (art. 32)

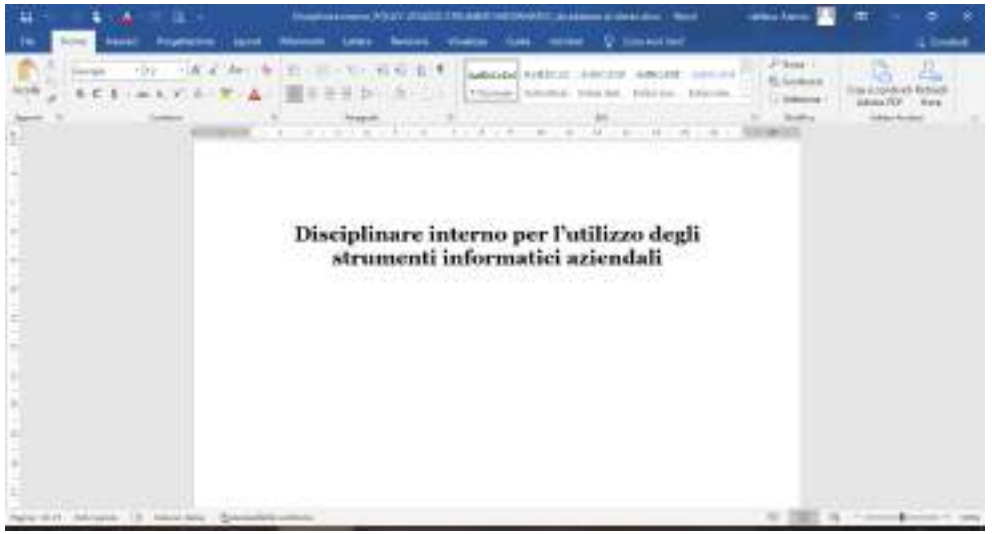
Il Titolare del trattamento deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.



Analisi dei rischi

Tecniche e Organizzative





Sicurezza del trattamento e misure di sicurezza (art. 32)

Misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la **pseudonimizzazione** e la **cifratura** dei dati personali

b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi** di trattamento

c) la capacità di **ripristinare tempestivamente la disponibilità e l'accesso dei dati** personali in caso di incidente fisico o tecnico

d) una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento**

Pseudonimizzazione dei dati personali

Nome	Giulia Bianchi
Genere	F
Diagnosi	Febbre emorragica

Schermata con dati in chiaro

Nome	Silvia Rossi
Genere	F
Diagnosi	Febbre emorragica

Schermata schermata con dati pseudonimizzati

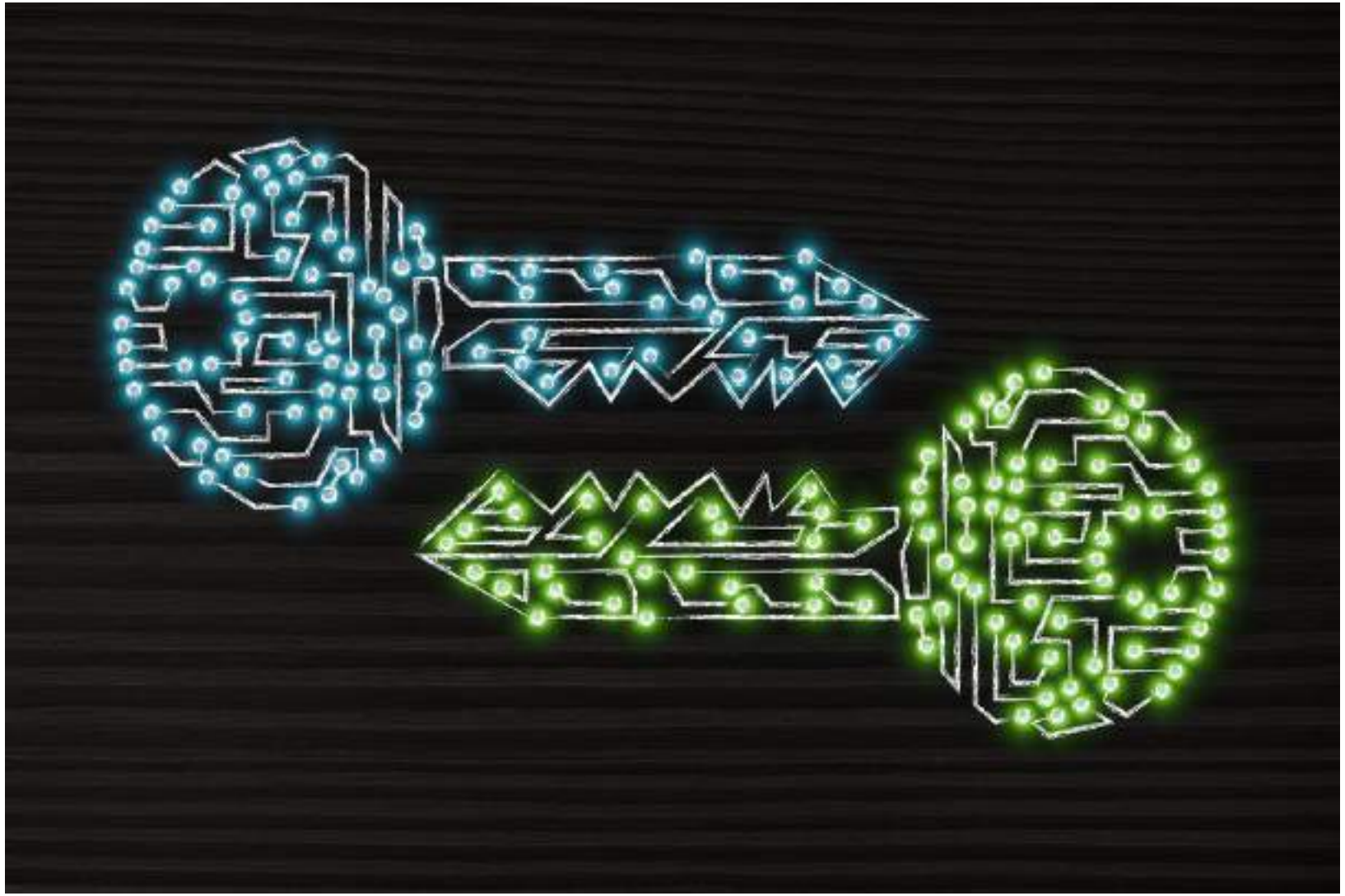
Nome	No Access
Genere	F
Diagnosi	Febbre emorragica

Schermata dati non accessibili

Nome	XXX
Genere	F
Diagnosi	Febbre emorragica

Schermata con dati anonimi

Cifratura




Don't
Forget
To Backup

la resilienza dei sistemi e dei servizi di trattamento

L'accountability e l'approccio basato sul rischio
Considerando 74 (art. 5, par. 2 e art. 24)

Tenuto conto

della natura | dell'ambito di applicazione | del contesto | delle finalità del trattamento | dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

il titolare del trattamento mette in atto misure

tecniche | organizzative

adeguate per

garantire | ed essere in grado di dimostrare

che il trattamento è effettuato conformemente al regolamento

Sicurezza del trattamento - considerando 77 (art. 32)

Gli orientamenti per la messa in atto di opportune misure e per DIMOSTRARE la conformità da parte del titolare o del responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti mediante:

CODICI DI CONDOTTA

CERTIFICAZIONI

LINEE GUIDA DEL COMITATO

INDICAZIONI DEL RPD

CHE COSA SI INTENDE PER *RISCHIO*?

Il RISCHIO

Per “rischio” si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà.

D’altro canto, la “gestione del rischio” è definibile come l’insieme coordinato delle attività finalizzate a guidare e monitorare un Titolare nei riguardi di tale rischio.

ANALI DEI RISCHI

È il processo di comprensione della natura del rischio e di determinazione del livello di rischio

Fonte : Cesare Gallotti, Sicurezza delle informazioni- versione gennaio 2019

ELEMENTI DA CONSIDERARE NELLA INDIVIDUAZIONE DEL RISCHIO

ERRORI DA EVITARE:

Non bisogna confondere la gestione dei rischi con il tema delle misure di sicurezza

Il rischio non si riferisce al titolare ma al soggetto interessato

ATTENZIONE!


Non solo la sicurezza del trattamento
La valutazione del rischio deve riguardare
Ma anche gli effetti complessivi del trattamento

Aspetti riguardanti la sicurezza del trattamento

- **DISPONIBILITÀ**
  -distruzione
  -indisponibilità
  -perdita
- **INTEGRITÀ**
  -alterazione
- **RISERVATEZZA**
  -divulgazione
  -accesso

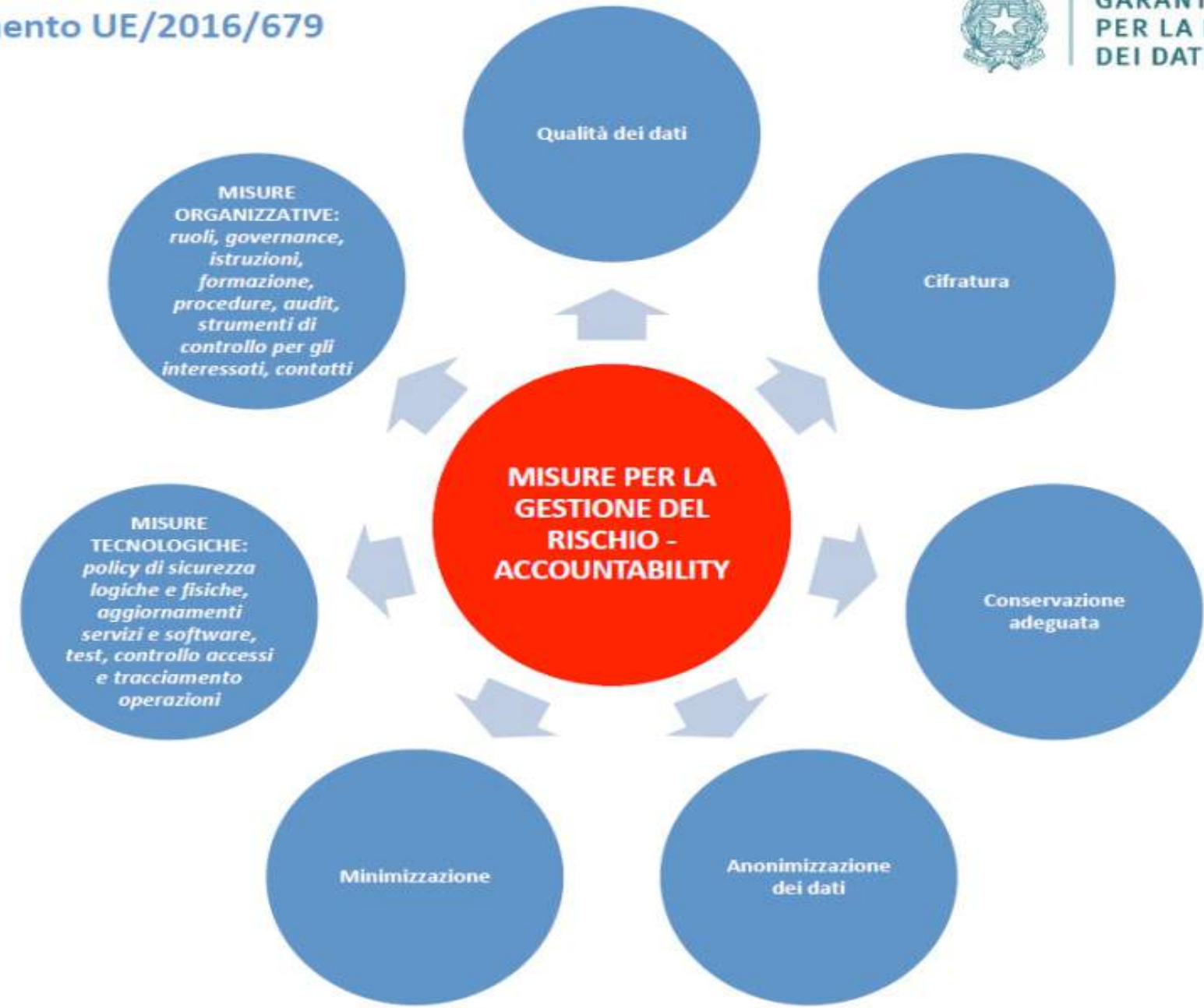
Regolamento UE/2016/679

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

QUALI SONO LE MISURE PER LA GESTIONE DEL *RISCHIO*?

Regolamento UE/2016/679

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI



Sicurezza informatica: Associare **le minacce** agli asset

Sicurezza dei dati: Associare **le minacce alla tutela dei dati personali** e quindi ai rischi per gli stessi

GRAVITA' DEL RISCHIO

- Classificazione della **gravità** del rischio:

a) BASSO: gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente, superabile senza difficoltà. A titolo esemplificativo e non esaustivo, costituiscono impatti trascurabili: (i) impatti fisici come mal di testa passeggero; (ii) impatti materiali come la perdita di tempo dovuta a ripetizione delle procedure o all'attesa della loro effettuazione, riutilizzo dei dati a scopo di pubblicità mirata per beni di consumo corrente; (iii) impatti psicologici: semplice fastidio, impressione di violazione della privacy senza danno reale (intrusione commerciale);

b) MEDIO BASSOi: (i) impatti fisici come una lieve affezione fisica (es: malattia lieve a seguito del mancato rispetto di controindicazioni), diffamazione che dia luogo a rappresaglie fisiche; (ii) impatti materiali come pagamenti non pianificati (ad esempio multe non dovute), negazione dell'accesso a servizi amministrativi o commerciali, pubblicità online mirata su un aspetto di vita privata che la persona voleva mantenere riservata; (iii) impatti psicologici come disturbo psicologico lieve ma oggettivo, senso di violazione della privacy senza danni irreparabili, intimidazione sui social network;

c) MEDIO ALTO: gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative. A titolo esemplificativo e non esaustivo, costituiscono impatti significativi: (i) impatti fisici come una grave affezione fisica che provochi danni a lungo termine (aggravamento dello stato di salute a seguito di una errata assunzione di responsabilità o del mancato rispetto di controindicazioni), alterazione dell'integrità fisica; (ii) impatti materiali come perdite monetarie non indennizzate, perdita di opportunità uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), perdita dell'abitazione, del posto di lavoro; (iii) impatti psicologici come grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche;

d) ALTO: gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare. A titolo esemplificativo e non esaustivo, costituiscono impatti massimi: (i) impatti fisici come affezione fisica a lungo termine o permanente, alterazione permanente dell'integrità fisica, decesso; (ii) impatti materiali come rischio finanziario, indebitamento ingente, impossibilità di lavorare, incapacità di ricollocazione, smarrimento di elementi di prova nell'ambito di un contenzioso, perdita di accesso a infrastrutture vitali (acqua, elettricità, ecc.); (iii) impatti psicologici come disturbo psicologico a lungo termine o permanente, sanzione penale, allontanamento, perdita di legami familiari, perdita della capacità di agire, cambio di stato amministrativo e/o perdita dell'autonomia legale (tutela) ecc.

probabilità del RISCHIO

- Classificazione della probabilità del rischio:

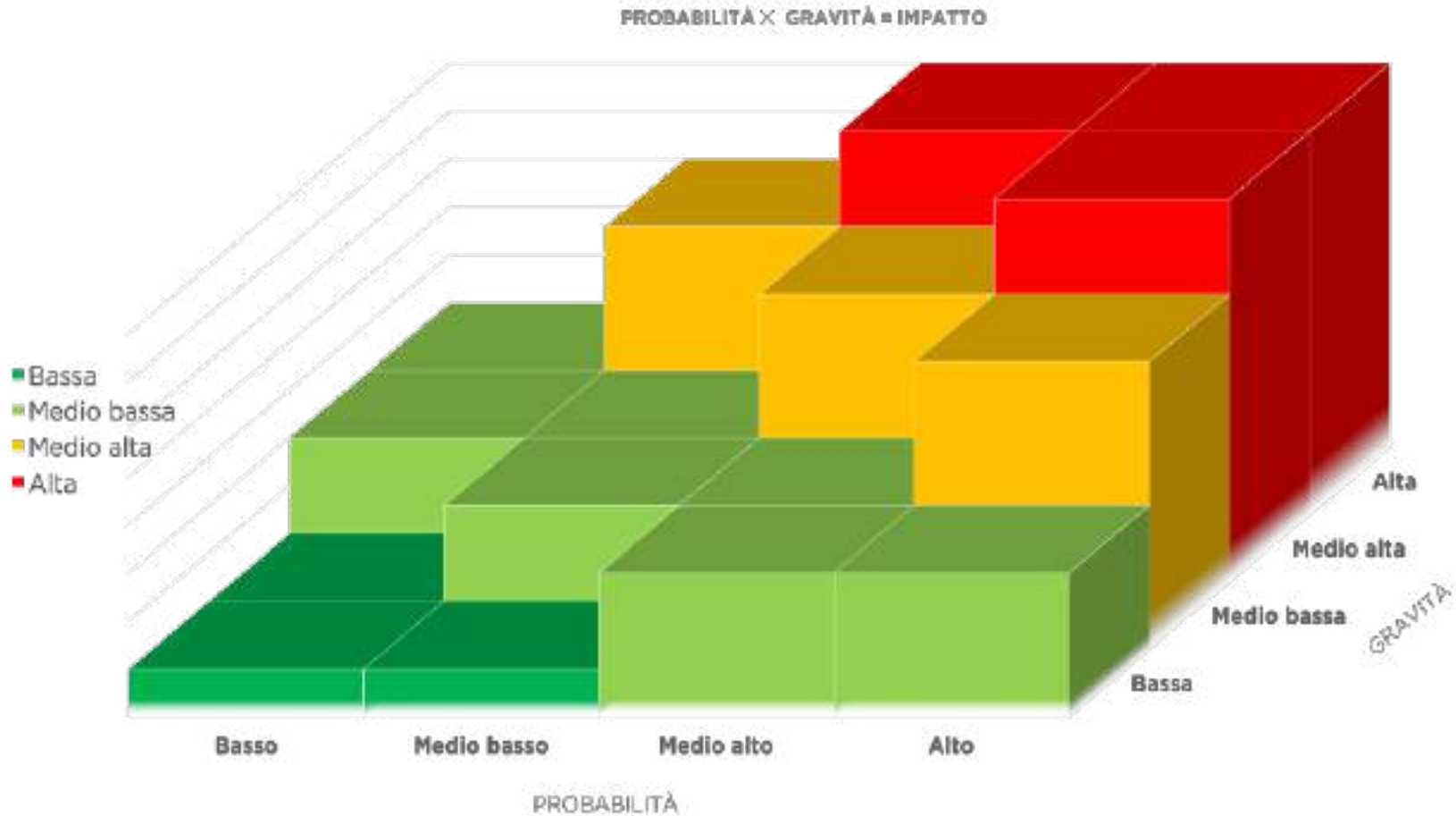
a) BASSO: appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge e codice d'ingresso);

b) MEDIO BASSO: appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge);

c) MEDIO ALTO: appare possibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in uffici dell'organizzazione ove l'accesso è controllato da un incaricato all'ingresso);

d) ALTO: appare estremamente facile per le fonti di rischio considerate concretizzare una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione pubblicamente accessibile).

Fonte : Cesare Gallotti, Sicurezza delle informazioni- versione gennaio 2019


PROBABILITÀ X GRAVITÀ = IMPATTO
Bassa
Medio bassa
Medio alta
Alta
Alta
Medio alta
Medio bassa
Bassa
GRAVITÀ
Basso
Medio basso
Medio alto
Alto
PROBABILITÀ

Grazie per l’attenzione

resto a vostra disposizione per eventuali domande

Prof. Avv. Stefano Aterno

saterno@e-lex.it

www.stefanoaterno.eu

e-lex STUDIO LEGALE