

### valutazione del rischio e individuazione criteri

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla probabilità di accadimento (P) ed alle conseguenze di tale evento (C). Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

LR = livello di rischio

P = probabilità di accadimento

C = conseguenze

Alla probabilità di accadimento dell'evento P è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle conseguenze (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

## MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di probabilità e conseguenze è rappresentata in figura seguente:

Probabilità	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	$(1 \leq LR \leq 3)$
Medio - basso	$(4 \leq LR \leq 6)$
Rilevante	$(8 \leq LR \leq 12)$
Alto	$(15 \leq LR \leq 25)$

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

### valutazione del rischio normalizzato

Nel caso in cui, quindi, l'indice di rischio si colloca nel range  $15 \div 25$ , l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.

In questo caso si procede ad un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

$$RN = f(P, C, Vu)$$

Dove:

P = probabilità

C = conseguenze generate dall'evento

V = vulnerabilità rispetto al grado di adeguatezza delle misure

$$RN = f (P, C, Vu)$$



In prima battuta viene ricavato il rischio intrinseco  $R_i$  come prodotto della probabilità  $P$  e delle conseguenze  $C$ , in base agli indici numerici assegnati ad entrambi i fattori.

Alla probabilità  $P$  è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle conseguenze ( $C$ ) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

PROBABILITÀ	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	(1 ≤ Ri ≤ 2)
Basso	(3 ≤ Ri ≤ 4)
Rilevante	(6 ≤ Ri ≤ 9)
Alto	(12 ≤ Ri ≤ 16)

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.

Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> </ul>
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> </ul>
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> <li>Modifica non autorizzata</li> <li>Divulgazione non autorizzata</li> <li>Accesso dati non autorizzato</li> </ul>
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> <li>Modifica non autorizzata</li> <li>Divulgazione non autorizzata</li> <li>Accesso dati non autorizzato</li> </ul>
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> <li>Modifica non autorizzata</li> <li>Divulgazione non autorizzata</li> <li>Accesso dati non autorizzato</li> </ul>

Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>
---	--

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla Vulnerabilità (Vu) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
Vu	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	Valori di riferimento
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$