



Metodologia di analisi dei rischi adottata

La presente sezione riporta la metodologia utilizzata dall'organizzazione per analizzare i rischi relativi al trattamento dei dati personali, al fine di tutelare i dati personali, con particolare riferimento a disponibilità, riservatezza e integrità dei dati.

Sommario

1. Introduzione
2. Processo di valutazione dei rischi
3. Elementi del processo di analisi del rischio
4. Metodologia applicata
5. Algoritmo del fattore di rischio
6. Parametri di calcolo del fattore di rischio
 - Peso VULNERABILITA' (P_V)
 - Peso CONTROMISURE (P_{CM}):
 - Coefficienti di ponderazione contromisure dirette e indirette
 - Peso ASSET (P_A)
 - PROBABILITÀ (P)
 - DANNO (D)
7. Scala dell'indice di rischio



1. Introduzione

Lo schema utilizzato per l'analisi dei rischi si basa sui principi e sulle linee guida dello **standard ISO 31000 Risk Management – Principles and guidelines** e dello **standard ISO 27001** per il trattamento del rischio relativo alla sicurezza delle informazioni, applicati in funzione dell'obiettivo specifico dell'organizzazione di **tutelare i dati personali, con particolare riferimento a disponibilità, riservatezza e integrità dei dati**.

Conseguentemente **i rischi valutati sono focalizzati sulla tutela dei diritti e delle libertà delle persone fisiche** e non sui rischi per l'organizzazione stessa, come avviene in altri ambiti (a titolo esemplificativo, per la sicurezza delle informazioni).

Il sistema di gestione del rischio adottato mira ad essere:

- un approccio alla gestione del rischio sistematico, strutturato e tempestivo;
- adattabile ai trattamenti di dati specifici di ogni organizzazione;
- dinamico, iterativo e reattivo al cambiamento;
- parte integrante di tutti i processi di trattamento dei dati;
- di supporto al titolare ed ai responsabili nell'assunzione di scelte consapevoli e ponderate.

2. Processo di valutazione dei rischi

Il processo adottato può essere così semplificato:

Definizione del Contesto: definizione della natura, ambito di applicazione, contesto e finalità del trattamento

Identificazione del rischio: identificazione delle minacce, ossia degli eventi indesiderati che incidono su disponibilità, riservatezza e integrità dei dati personali oggetto di trattamento

Analisi del rischio: identificazione delle vulnerabilità che gravano sull'organizzazione, tenuto conto dello stato di attuazione delle contromisure, della verosimiglianza di accadimento dei rischi e delle relative conseguenze

Ponderazione del rischio: predisposizione di una griglia di valutazione dell'esposizione al rischio per ogni trattamento

Trattamento del rischio: predisposizione di un piano di trattamento del rischio

Attività trasversali al processo di gestione del rischio

Monitoraggio e riesame: metodologia sistematica di verifica e sorveglianza con registrazioni documentate e conseguente aggiornamento

Comunicazione e consultazione: metodologia sistematica di partecipazione di tutti i soggetti coinvolti nel processo di gestione del rischio



3. Elementi del processo di analisi del rischio

Di seguito sono elencati gli elementi coinvolti nel processo di analisi dei rischi.

RISCHIO

Per rischio ci si riferisce al grado di probabilità di attuazione di un evento indesiderato (minaccia) tenuto conto della gravità della sua concretizzazione.

I rischi definiti consistono in 36 minacce, che incombono sulla disponibilità, integrità e riservatezza dei dati personali.

ASSET

Per asset, ai fini dell'analisi dei rischi, ci si riferisce ai beni, intesi come luoghi fisici, risorse umane, risorse strumentali, soggetti esterni, che sono, direttamente o indirettamente, collegati al trattamento dei dati.

VULNERABILITA'

Per vulnerabilità si intendono le suscettibilità intrinseche dell'organizzazione, nel suo insieme o per specifici asset, ad essere danneggiate da un attacco, con conseguente concretizzazione delle relative minacce.

Il sistema prende in considerazione circa 160 vulnerabilità intrinseche degli asset, sulla base di:

- obiettivi di controllo di cui allo standard **UNI CEI ISO IEC 27001** per il trattamento del rischio relativo alla sicurezza delle informazioni;
- **Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni** emanate dall'**AgID** (Agenzia per l'Italia Digitale) di cui alla *Circolare 2/2017 del 18 aprile 2017*.

CONTROMISURE

Le contromisure sono le misure da applicare o applicate dall'organizzazione per contrastare l'attuazione dell'evento indesiderato.

Il sistema analizza lo stato di attuazione di circa 160 contromisure atte a contrastare le vulnerabilità dell'organizzazione. L'attuazione di talune contromisure può influenzare il peso (livello di criticità) di molteplici vulnerabilità correlate indirettamente, tramite un sistema di *coefficienti di ponderazione*.

QUESITI

Il sistema si fonda su un complesso sistema di quesiti, tra loro interconnessi, che consentono di:

- semplificare e standardizzare la rilevazione delle informazioni necessarie al processo di gestione del rischio;
- favorire la partecipazione di soggetti diversi al processo.

Le risposte fornite dall'utente ai quesiti hanno una duplice finalità:

- popolare il sistema con le informazioni relative all'organizzazione;
- raccogliere i dati necessari al calcolo dell'indice di rischio.

TRATTAMENTO

Trattandosi di una valutazione del rischio finalizzata alla protezione dei dati personali per i diritti e le libertà delle persone fisiche, tale valutazione non può prescindere dal Trattamento dei dati personali, che può essere considerato il **Contesto del processo di gestione del rischio**.

PROBABILITA'

La probabilità di concretizzazione della minaccia è l'elemento dell'analisi che il sistema chiede di valorizzare all'utente in base alla **frequenza storica di accadimento**. Tale coefficiente viene assegnato ai singoli rischi (minacce) correlati ad ogni specifico trattamento. Tale correlazione consente di elaborare l'analisi dei rischi tenendo conto della **Definizione del contesto**, che in ambito di tutela dei dati personali, si sostanzia in natura, ambito, contesto e finalità del trattamento (cfr. *Considerando 90 Regolamento 2016/679 e UNI ISO 31000 Risk Management - Principles and guidelines*).

DANNO

Il danno è la **gravità** delle conseguenze in caso di attuazione della minaccia. Il sistema consente di valorizzare il danno derivante dall'attuazione di uno specifico rischio (minaccia) per ogni singolo trattamento. Tale valorizzazione si basa, in larga parte, sui criteri proposti nel **WP 248** Rev. 01 "*Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento 'possa presentare* Ex Ordinanza 25/2020 - Soggetto Attuatore del Commissario Delegato—Coordinatore della Struttura Tecnica di Supporto—Assessorato Regionale alla Salute Piazza Ottavio Ziino 24—90145 Palermo—0917075610—soggettoattuatore.prosicilia@pec.it—soggettoattuatore.o25cs.covid@regione.sicilia.it www.potenziamentoreteospedaliera.sicilia.it—Codice Fiscale e Partita Iva 97356510822



un rischio elevato' ai sensi del Regolamento 2016/679" per individuare i trattamenti che possono presentare un rischio elevato e che quindi sono soggetti a DPIA (Data Protection Impact Assessment).

Il sistema così sviluppato consente all'Organizzazione di:

- valutare in modo continuativo i rischi che gravano sui propri trattamenti, così da individuare quelle situazioni in cui una determinata tipologia di trattamenti "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche";
- completare tale analisi valutando anche i criteri relativi alla realizzazione di una **Valutazione di impatto** (DPIA) di cui al *Regolamento 2016/679 art. 35 commi 1 e 3 integrati, ai sensi del comma 4, dai criteri di cui al WP248 Rev. 01.*

4. Metodologia applicata

A livello di singolo trattamento il sistema individua gli asset direttamente o indirettamente ad esso collegati. Per ognuno di essi, il processo di analisi dei rischi analizza le vulnerabilità, ossia le suscettibilità intrinseche ad essere danneggiati da un attacco, con conseguente concretizzazione delle relative minacce, e le contromisure, dirette o indirette, attuate, fornendo il livello di rischio. Tale livello tiene anche conto della probabilità e dell'impatto che l'attuazione della minaccia avrebbe sui dati personali trattati, per mezzo degli specifici asset.

Tale metodologia può essere riassunta nella seguente funzione:

$$R_T = f (V_T , P_T , D_T)$$

dove:

R_T è l'indice di rischio che insiste sul Trattamento, espresso in valori percentuali,

V_T è l'indice di vulnerabilità degli asset coinvolti nel trattamento, tenuto conto delle contromisure, dirette o indirette, attuate e del livello di criticità espresso sul singolo asset,

P_T è la probabilità di accadimento dell'evento indesiderato sul trattamento,

D_T è la gravità delle conseguenze della concretizzazione dell'evento indesiderato sul trattamento.

Il sistema può essere così rappresentato:



5. Algoritmo del fattore di rischio

L'algoritmo utilizzato per calcolare il fattore di rischio di concretizzazione di determinate minacce che incombono sulla sicurezza dei dati personali è rappresentato dalla funzione che segue.



$$R_T = \max \left[V_A = \left[\frac{P_A P_V \left(1 - \frac{\sum_{i=0}^{N_{ca}} P_n(i)}{\sum_{j=0}^{N_{ct}} P_n(j)} \right)}{P_{Amax} P_{Vmax}} I_c + (1 - I_c) \frac{P}{P_{max}} \right] I_V + (1 - I_V) \left(\frac{1 - D_m}{\ln N_{cd}} \ln N_{cdp} + D_m \right) \right]$$

Dove:

P_A = Peso Asset

P_V = Peso Vulnerabilità

P_{Amax} = Peso massimo asset

P_{Vmax} = Peso massimo vulnerabilità

N_{ca} = Numero contromisure attuate

N_{ct} = Numero totale di contromisure che sono valutate sull'asset

$$P_n(i) = \text{peso normalizzato della contromisura} = \frac{P_c}{\sqrt{\sum P_c^2}}$$

P_c = peso contromisura

I_c = Influenza dell'attuazione delle contromisure sul fattore di rischio complessivo

P = probabilità di accadimento della minaccia

P_{max} = valore massimo della probabilità

I_V = Influenza delle vulnerabilità sul fattore di rischio complessivo

D_m = valore minimo normalizzato del danno

N_{cd} = numero totale di criteri aggravanti al danno considerati

N_{cdp} = numero di criteri aggravanti presenti sul trattamento

6. Parametri di calcolo del fattore di rischio

Semplificando l'algoritmo, il sistema di calcolo del fattore di rischio di concretizzazione di una minaccia utilizzato può essere espresso con la seguente funzione:

$$R_T = \max \{ V_A = f(P_A, P_V - P_{CM}, P, D) \} \forall A \in \mathbb{T}$$

dove:

R_T = Livello di rischio a cui è esposto il trattamento

V_A = Grado di vulnerabilità di ogni asset

P_A = Peso attribuito all'asset su cui grava la vulnerabilità

P_V = Peso attribuito alla vulnerabilità

P_{CM} = Peso ponderato delle contromisure dirette e indirette

P = Probabilità di accadimento dell'evento indesiderato

D = Gravità del danno derivante dalla concretizzazione dell'evento indesiderato



$\forall A \in \mathbb{T}$ Per qualunque Asset appartenente al Trattamento

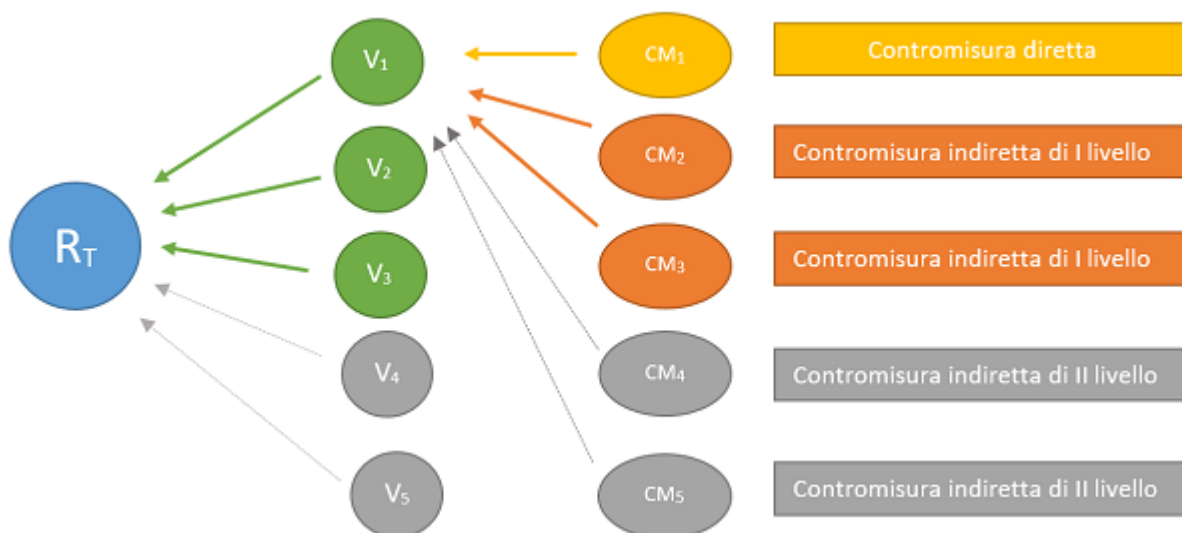
Nel dettaglio:

Peso **VULNERABILITA'** (P_V)

Peso attribuito alle suscettibilità intrinseche dell'organizzazione, nel suo insieme o per specifici asset, ad essere danneggiate da un attacco, con conseguente concretizzazione delle relative minacce.

Peso **CONTROMISURE** (PC_M)

Le contromisure sono le misure da applicare o applicate dall'organizzazione per contrastare l'attuazione dell'evento indesiderato o per influenzare le conseguenze dello stesso. Nel sistema utilizzato le contromisure si dividono in tre categorie:



- **Contromisure dirette:** misure per contrastare l'attuazione dell'evento indesiderato che influenzano **direttamente le vulnerabilità** degli asset.
- **Contromisure indirette di primo livello:** misure per contrastare l'attuazione dell'evento indesiderato che influenzano **indirettamente le vulnerabilità** degli asset.
- **Contromisure indirette di secondo livello:** misure che influenzano indirettamente il rischio associato alla concretizzazione di un evento indesiderato e che, conseguentemente, influenzano **indirettamente le vulnerabilità** degli asset.

ESEMPIO ESPLICATIVO:

RISCHIO (R) di "Accesso ai dati non autorizzato"

La **Vulnerabilità (V)** "Mancato utilizzo di credenziali di autenticazione" che incide sul Rischio su indicato è influenzata da:

- **Contromisura diretta di primo livello (CM):** implementazione di un sistema di accesso tramite credenziali di autenticazione.
- **Contromisura indiretta di primo livello (CM):** utilizzo di credenziali di autenticazione che rispettino i requisiti minimi di complessità.
- **Contromisura indiretta di secondo livello (CM):** adozione da parte dell'organizzazione di regole di sicurezza dei dati personali.

Ad ogni contromisura è associato un peso, che corrisponde alla capacità della contromisura di abbattere le vulnerabilità e, quindi, i rischi derivanti da tali vulnerabilità.



La vulnerabilità residua e, conseguentemente, il grado di esposizione al rischio dell'organizzazione tiene conto, in modalità ponderale, di tutte le tipologie di contromisure.

Il modello matematico, inoltre, è adattato affinché il livello di rischio residuo possa essere tendente a zero ma non pari a zero, secondo la logica dell'inesistenza del rischio zero.

Coefficienti di ponderazione contromisure dirette e indirette

Il sistema utilizza due livelli di ponderazione dell'influenza delle contromisure sui rischi:

- **ponderazione in base al peso degli elementi Contromisure (CM) e Vulnerabilità (V):** il sistema utilizza come coefficienti di ponderazione i pesi delle contromisure (P_{CM}) ed i pesi delle vulnerabilità ad esse direttamente collegate (P_V);
- **ponderazione in base al tipo di Contromisura (CM), diretta o indiretta:** il sistema assegna un ulteriore coefficiente di ponderazione in base al tipo di influenza esercitata dalle contromisure sulle vulnerabilità e, quindi, sul rischio.

Peso ASSET (P_A)

Per peso Asset si intende il peso attribuito ai singoli beni, intesi come luoghi fisici, risorse umane, risorse strumentali, soggetti esterni, che sono, direttamente o indirettamente, collegati al trattamento dei dati.

Gli asset a cui viene associato un peso possono essere sintetizzati nelle seguenti categorie:

- Organizzazione
- Risorse umane
- Trattamento
- Soggetti esterni
- Luoghi
- Postazioni di lavoro
- Dispositivi portatili
- Dispositivi di telelavoro
- Server
- Storage
- Rete interna
- Rete wireless
- Firewall
- Switch
- Router
- Software
- Sistemi di comunicazioni elettronica
- Motore database

PROBABILITÀ (P)

La probabilità di accadimento della minaccia (evento indesiderato) è un parametro valorizzato dall'utente in base alla **frequenza storica di accadimento** di specifici eventi sui trattamenti dei dati analizzati.

DANNO (D)

Il danno è inteso come la gravità delle conseguenze in caso di attuazione della minaccia (evento indesiderato). Il sistema consente di valorizzare la gravità del danno derivante dall'attuazione di uno specifico rischio (minaccia) per ogni singolo trattamento.

I criteri di valutazione del danno sono indicativamente i criteri proposti dalle "Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento 'possa presentare un rischio elevato' ai sensi del Regolamento 2016/679" (**WP 248**).




Nel calcolo viene dato per assunto che il solo fatto che il trattamento abbia come oggetto dati personali comuni comporti un danno, in caso di concretizzazione dell'evento, sotto al quale non è logico scendere. Partendo da ciò,



il livello effettivo di danno in base al numero dei succitati criteri attuati sul trattamento viene calcolato seguendo l'andamento di una curva logaritmica.

7. Scala dell'indice di rischio

La scala del livello di rischio utilizzata si configura come segue:

-  Rischio molto basso
-  Rischio basso
-  Rischio medio
-  Rischio alto
-  Rischio molto alto

In base al livello di rischio ottenuto il sistema fornisce indicazioni sulle azioni di contrasto e miglioramento da attuare. Nel sistema sono inoltre disponibili i report necessari ai titolari ed ai responsabili per ponderare il rischio e predisporre i piani di trattamento dello stesso.