Estratto 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

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 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:

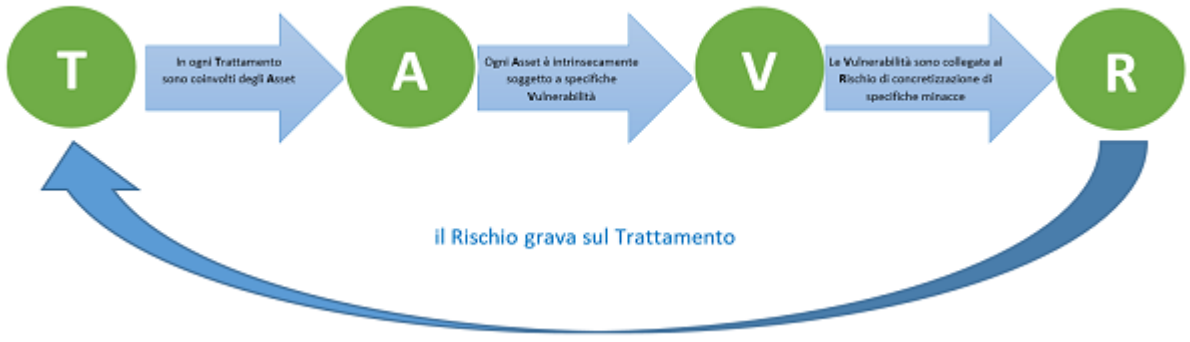
R_T è l'indice di rischio che insiste sul Trattamento, espresso in valori percentuali,

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. 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.

Privacy – Livello di rischio generale per trattamenti

Il presente documento, "Privacy – Livello di rischio generale sul trattamento", fornisce un elenco dei trattamenti di dati personali svolti dal titolare del trattamento con l'indicazione di un valore di rischio generale incombente sul trattamento.

Tale valore va inquadrato come il livello massimo di rischio a cui è esposto il singolo trattamento e viene assegnato al trattamento stesso selezionando, tra tutti i rischi che incombono sul medesimo, quello che ha raggiunto il livello più alto.

Trattamento	Rischio
Studio osservazionale retrospettivo prospettico monocentrico e prospettico MFVR2024-11	36%

Privacy - Livello di rischio specifico per trattamento

Il presente documento, "Privacy - Livello di rischio specifico per trattamento", fornisce, per ogni specifico trattamento di dati personali svolti dal titolare del trattamento, l'elenco delle minacce incombenti, con indicazione degli asset coinvolti e del grado di rischio.

Nel dettaglio, il report che segue mostra, per ogni trattamento:

- l'elenco dei rischi (minacce) che incombono sul trattamento;
- l'elenco delle tipologie di asset collegate al trattamento;
- il livello massimo di ogni rischio per ogni tipologia di asset.

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

Per ogni tipologia di asset collegata, il processo di analisi dei rischi analizza le vulnerabilità, ossia le suscettibilità intrinseche ad essere danneggiate da un attacco, con conseguente concretizzazione delle relative minacce, e le contromisure, dirette e indirette, attuate per ridurre l'attuazione delle minacce, fornendo conseguentemente il livello di rischio (%) visualizzato. 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.

Le ultime tre colonne rappresentano l'ambito di impatto del rischio(minaccia).

Rischio	Applicativi web e portale internet	Backup	Firewall	Luoghi	Motori database	Organizzazione generale	Rete interna	Server	Storage	Switch	Disponibilità	Riservatezza	Integrità
Trattamento: Studio osservazionale retrospettivo prospettico monocentrico e													
R0001 - Malfunzionamento o degrado apparecchiature	10%		9%	6%		9%		20%	12%	20%	X		X
R0005 - Ingressi non autorizzati a locali e/o aree ad accesso ristretto	10%		9%	7%	11%	10%		11%	12%	9%		X	
R0008 - Esposizione a condizioni metereologiche estreme				6%		9%							X
R0009 - Incendio				6%		9%					X		X
R0010 - Terremoto				6%		9%					X		X
R0011 - Allagamento				6%		9%					X		X
R0012 - Altri eventi calamitosi e/o sociopolitici						9%					X		X
R0013 - Copia abusiva di dati	10%	8%	9%	7%	11%	36%		11%	12%	9%		X	
R0014 - Furto di dati	10%	9%	9%	7%	11%	36%	7%	11%	12%	9%	X	X	
R0015 - Modifica non autorizzata di dati	10%	9%	9%		11%	36%		11%	12%	9%			X
R0016 - Presa visione abusiva di dati	10%	8%	9%	7%	11%	36%		11%	12%	9%		X	
R0017 - Corruzione e/o inaccessiblità dei dati	10%	9%	9%		11%	9%	7%	11%	12%	9%	X		X
R0018 - Trattamento illecito dei dati	9%		8%	7%		10%				8%		X	
R0019 - Uso non autorizzato dei dati	10%		9%		11%	9%		11%	12%	9%		X	
R0020 - Comunicazione illegale dei dati	9%		8%			10%				8%		X	
R0021 - Diffusione illegale dei dati						12%						X	
R0022 - Mancata conservazione di dati	10%	9%	9%	7%		9%		11%	12%	9%	X		X
R0023 - Mancata restituzione di dati						9%					X	X	
R0024 - Mancata eliminazione dei dati raggiunta la finalità						10%		6%		6%		X	
R0031 - Accessi non autorizzati	10%		8%	7%	11%	9%	7%	11%	12%	9%		X	
R0032 - Carenza di consapevolezza, disattenzione o incuria	11%	11%	9%			12%		13%	13%	10%	X	X	X
R0033 - Errore nello svolgimento di mansioni	11%	11%	10%		12%	11%		13%	13%	10%	X	X	X
R0034 - Ignoranza procedure di gestione						11%					X	X	X

	R0036 - Guasto ai sistemi complementari			10%	8%		11%		12%	13%	10%	X		X