Roma, 09/03/2018

Corso di alta formazione sulla protezione dei dati personali

Responsabile della protezione dei dati (DPO)

La valutazione d'impatto sulla protezione dei dati personali

Relatore Ing. Andrea Cenni

Auditor ISDP 10003 - Protezione Dati Personali
Valutatore Privacy Uni 11697
andrea.cenni@studioingcenni.it | 328 72 30 906 | Linkedin

Il contesto (D. Lgs. 196/2003)

- Sia la direttiva 95/46/CE che il D.Lgs. 196/2003 appaiono essere disposizioni prescrittive, quasi "*paternalistiche*", l'autorità garante stabilisce quali sono i trattamenti potenzialmente effettuabili da un titolare (autorizzazioni generali – art. 40), in caso di introduzione, ad es., di nuove tecnologie o criticità in genere, il titolare ricorre all'autorità garante per avere disposizioni e istruzioni su come trattare i dati personali ricorrendo a quelle tecnologie (art. 41);
- il legislatore scende così in dettaglio rispetto a come i trattamenti dei dati personali devono essere implementati tanto da descrivere un mansionario tecnico puntuale (allegato B), in cui si stabiliscono delle misure minime da implementare da parte del titolare per una corretta gestione delle rischiosità legate ai dati personali in sua custodia;
- Il titolare è accompagnato per mano nell'implementare un trattamento, appare quasi un esecutore di disposizioni che il contesto esterno, l'autorità oppure il legislatore, gli ha fornito (art. 17).

Il contesto (Reg. UE 679/2016)

- La vera novità introdotta dal regolamento riguarda gli obblighi in capo al titolare. L'approccio del legislatore non è più quello della direttiva, ovvero una normativa prescrittiva che scendeva nel merito di quali trattamenti erano effettuabili, autorità garante, e di come implementarli, allegato B;
- Si rovescia questo assunto, il legislatore dà al titolare piena facoltà di effettuare un qualsivoglia trattamento secondo il principio dell'*accountability* (responsabilità + credibilità + consapevolezza + affidabilità);
- Il legislatore parte dal presupposto che il titolare del trattamento – o il responsabile del trattamento - sia consapevole di cosa significhi trattare dati personali, si aspetta dunque che il titolare descriva proceduralmente come i dati personali sono trattati/organizzati, quali sono le rischiosità a cui sono soggetti tali dati e in virtù di questa misurazione di rischio metta in atto misure tecniche ed organizzative adeguate volte a rendere tali rischiosità accettabili, tollerabili, tali cioè da non rappresentare, quei rischi, una minaccia per i diritti e le libertà fondamentali delle persone fisiche.

Il contesto (Reg. UE 679/2016)

- Il titolare è così responsabilizzato a gestire una materia complessa come il trattamento e di conseguenza la protezione dei dati personali in sua custodia che sotto particolati condizioni è affiancato da una figura nuova, il DPO o il Data Protection Officer, responsabile della protezione dei dati, un organo di controllo e di indirizzo ad uso e consumo del titolare, di fatto una sorta di "*autorità garante in piccolo*";
- Il principio della accountability del titolare del trattamento è sancito dall'art. 5 – principi applicabili al trattamento di dati personali, paragrafo 2: *Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)*.
- L'altro grande onere in capo al titolare è la gestione del rischio collegato al trattamento di dati personali. La parola rischio è forse la più citata e richiamata all'interno del regolamento.

La Rivoluzione Copernicana

Art. 32, par. 1: Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio …

Misure Minime

Gestione del rischio (*risk management*)

D.lgs. 196/2003: tre obblighi per i titolari del trattamento:

- prevedere misure di sicurezza idonee a ridurre i rischi (art. 31);
- adottare in ogni caso le "misure minime" previste dal Codice, e quindi di assicurare comunque un livello minimo di protezione dei dati personali (art. 33);
- adottare le misure "necessarie" prescritte dal Garante ai sensi dell'art. 154, comma 1, lett. c (Provvedimenti generali o specifici nei confronti di singoli titolari del trattamento).

Rischio vs GDPR

- Il concetto di rischio permea l'intero Regolamento:

Articolo	Descrizione
art. 5 par. 1 lett. f), par 2	Principi applicabili al trattamento di dati personali e competenza del titolare
art. 24	Responsabilità del titolare del trattamento
Art. 25	Privacy by design e privacy by default
Art. 28 par. 3 lett. e)	Responsabile del trattamento
Art. 32	Sicurezza del trattamento
Art. 33 par. 3 lett. c)	Notifica di una violazione dei dati personali all'autorità di controllo
Art. 35 par. 1, 7 lett. c) e d)	Valutazione d'impatto sulla protezione dei dati
Art. 39 par 2	Compiti del responsabile della protezione dei dati
Art. 47 par. 2 lett. d)	Norme vincolanti d'impresa
Art. 49 par. 6	Deroghe in specifiche situazioni

Concetto di rischio

Per Pericolo si intende la proprietà o la qualità intrinseca di un determinato fattore avente la potenzialità di causare un danno;

Il Rischio di un evento accidentale è la combinazione tra la Probabilità (o frequenza) del verificarsi di un dato evento dannoso e la Gravità (detta magnitudo) delle sue conseguenze:

- frequenza: probabilità che l'evento si verifichi in un determinato intervallo di tempo;
- magnitudo: entità delle possibili perdite e dei danni conseguenti al verificarsi dell'evento.

Rischio = Frequenza x Magnitudo

Rischio: Effetto dell'incertezza sugli obiettivi

[Guida ISO 73:2009, definizione 1.1]

Tipologie di rischio

Eliminabile o eludibile

- Eliminazione alla fonte. Intervento sul processo produttivo e sulla pianificazione del lavoro. Importante nella fase di progettazione ex novo o di revisione. Laddove tecnicamente possibile costituisce l'intervento prioritario. Rientrano in questa fase tecniche di workaround oppure di trasferimento del rischio

Riducibile

- Se il rischio non è eliminabile deve essere mitigato. La riduzione di basa sull'adozione di opportune misure di prevenzione (agiscono sulla frequenza) e protezione (agiscono sulla magnitudo)

Tollerabile

- (accettabile): il rischio è ridotto ad un livello che può essere sopportato dall'organizzazione, tenuto conto dei propri obblighi legislativi. L'Azienda o l'Ente si assumono l'onere delle conseguenze del verificarsi di un evento dannoso eventualmente coprendo il rischio residuo con una polizza assicurativa di tipo "*bonus malus*". Casi ALARP ("*As Low As Reasonably Practicable*") dovrebbero essere oggetto di revisione. Se il rischio non è tollerabile va comunicato al Garante per ottenere istruzioni (consultazione preventiva, art. 36)

Protezione dei dati: cosa contrastare(art. 4, p.to 12)

- Si deve contrastare la: art. 4, p.to 12: «*violazione dei dati personali*»: *la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;* (C85)
- Dunque occorre tutelare i dati personali in termini di:
  - Riservatezza → art. 5, par. 1, lettera f);
  - Autenticità → art. 5, par. 1, lettera d): i dati personali sono *esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);*
  - Integrità → art. 5, par. 1, lettera f): i dati personali *sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»);*
  - Disponibilità → art. 5, par. 1, lettera e) i dati sono *conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati […].*

RAID: ISO 27001 + GDPR (autenticità = esatti + aggiornati)

Protezione dei dati. Cos'è previsto dal GDPR (art. 32 e C83)

- Art. 32, par. 1. *Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto 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;* (ISO 27001 + business continuity)

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

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

Protezione dei dati. Cos'è previsto dal GDPR (art. 32 e C83)

- Art. 32, par. 2. *Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.*

- C83. *Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.*

Protezione dei dati. Cos'è previsto dal GDPR (art. 35 e C75-C76)

- Art. 35, par. 1. *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.*
- Art. 35, par. 7. *La valutazione contiene almeno:*

a) *una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*

b) *una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*

c) *una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e*

d) *le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*

Protezione dei dati. Cos'è previsto dal GDPR (art. 35 e C84, C89-C93, C95)

- Art. 35, par. 11. *Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.*

- La Valutazione d'impatto (PIA) è obbligatoria in caso di trattamenti che possano comportare rischi elevati per la libertà ed i diritti del cittadino come, ad es.:

Trattamento su larga scala di dati sensibili

Attività di profilazione

Sistematica sorveglianza su larga scala di zona accessibile al pubblico

Altri trattamenti previsti dalle autorità di controllo

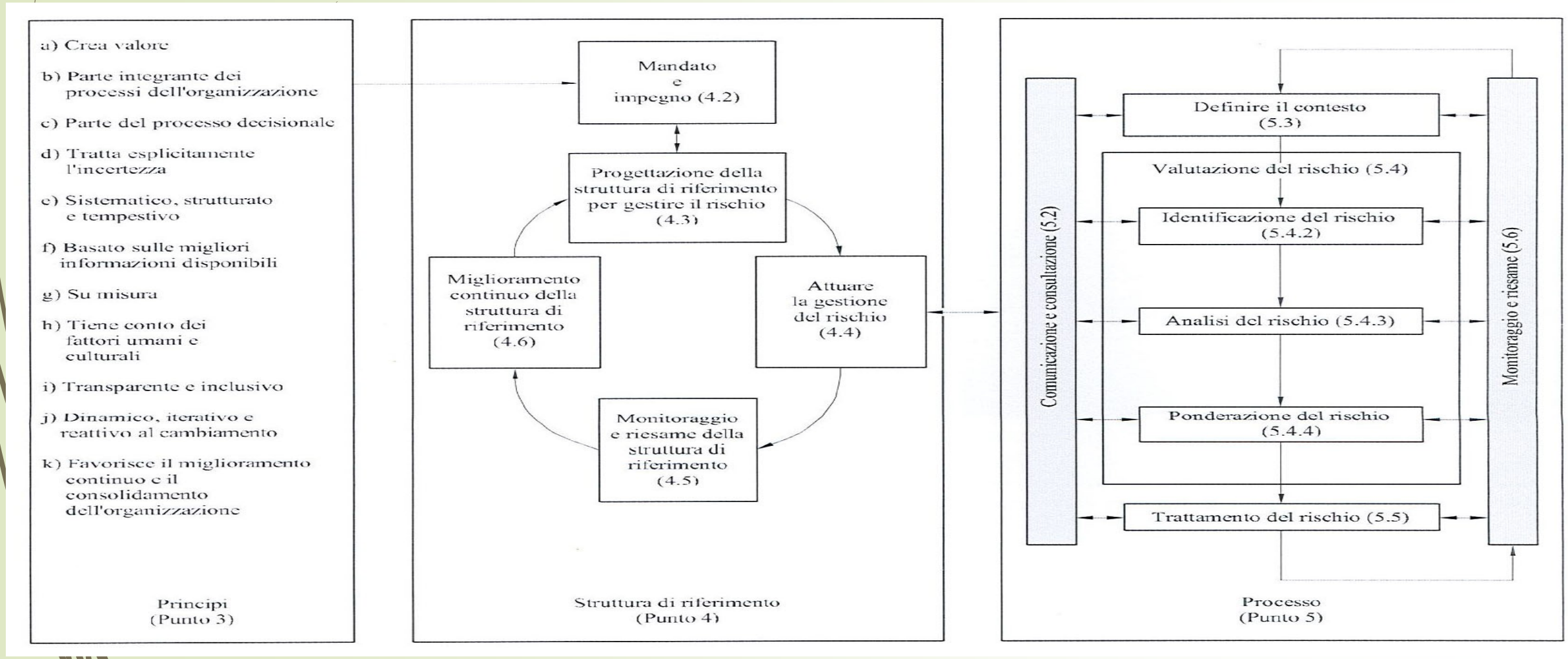
Protezione dei dati. Cos'è previsto dal GDPR (art. 35 e C75-C76)

- C75. I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Protezione dei dati. Cos'è previsto dal GDPR (art. 35 e C75-C76)

- C76. La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

ISO 31000:2010



Risk-Based Thinking: cosa devo fare?

Pianificare le azioni per annullare i rischi: come posso evitare o eliminare il rischio come posso mitiga rischio?

Attuare un piano: intraprendere azioni

Analizzare e dare priorità ai rischi e alle opportunità dell'organizzazione: cosa è accettabile? cosa non è accettabile?

Controllare l'efficacia delle azioni: funziona?

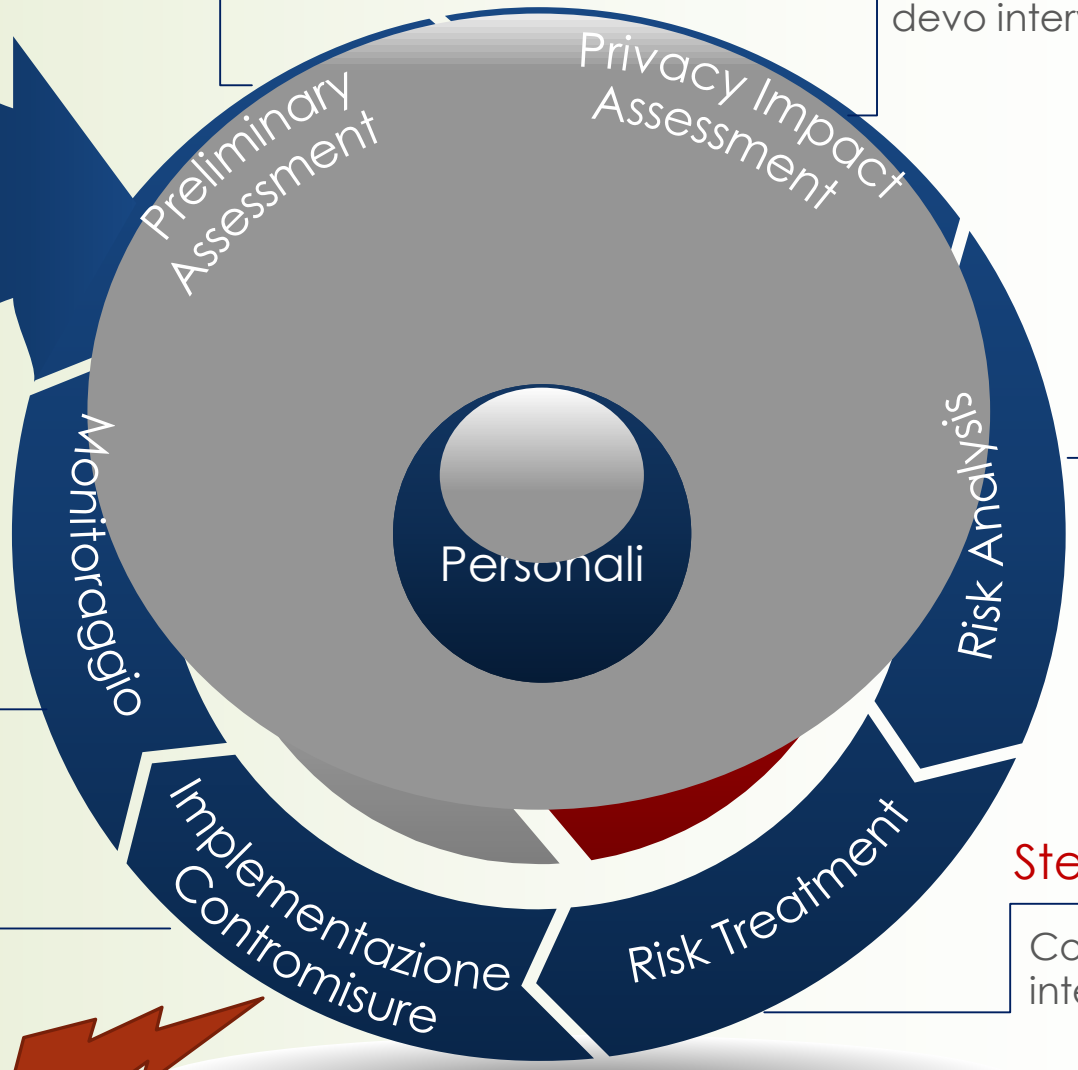
Imparare dall'esperienza: miglioramento continuo

Un approccio sistemico

Esiti visite ispettive/Contestazioni

Nuovi processi/Nuove tecnologie

Nuove normative di Legge



Step 1

Cosa debbo proteggere?

Step 2

Con quale priorità devo intervenire?

Step 3

Dove devo intervenire?

Step 4

Come devo intervenire?

Step 5

Ho delle metriche di efficienza ed efficacia?

Step 6

L'intervento è efficace?

Evento dannoso

Cosa devo proteggere?

- La definizione del perimetro di intervento (dominio della tutela dei dati) è la fase critica di tutto lo schema:

  perimetro errato = dati personali non protetti = non conformità.

- Per una corretta definizione del dominio della tutela dei dati occorre effettuare un Preliminary Assessment, ovvero:
  - Censire i processi aziendali che trattano dati personali;
  - Censire i trattamenti effettuati sui dati personali;
  - Censire i sistemi, applicazioni e database a supporto dei processi rientranti nel dominio della tutela dei dati.

Con quale priorità devo intervenire ?

- La definizione della priorità di intervento dipende dalla criticità, da un punto di vista Privacy, del processo, ovvero dal valore dei dati da esso trattati:

  maggiore criticità → maggiore priorità di intervento.

- Per definire la criticità di un processo occorre effettuare un Privacy Impact Assessment.
- La PIA consente di definire la criticità di un processo attraverso l'identificazione della natura del dato personale e la valutazione dell'impatto che la compromissione della R/A/I/D dei dati trattati causerebbe ai diritti e alle libertà degli interessati in termini di (esempio non esaustivo):
  - Discriminazione
  - Danni alla reputazione
  - Furto d'identità
  - Frodi
  - Perdite finanziarie

Dove devo intervenire ?

- Individuare puntualmente dove intervenire per tutelare la RAID dei dati personali è fondamentale per evitare sprechi di risorse:

  maggiore focalizzazione → minore spreco di risorse.

- Per identificare i punti su cui focalizzare gli interventi occorre utilizzare un approccio risk-based (c.d. «RA»).
- La Risk Analysis consente di individuare il livello di esposizione al rischio di Riservatezza, Autenticità, Integrità e Disponibilità dei dati personali trattati dal processo in esame.
- Gli interventi, siano essi di natura tecnica, organizzativa o procedurale, dovranno focalizzarsi sui processi e/o relative tecnologie a supporto, che al termine della RA risulteranno esposti ad alto rischio RAID.

Come devo intervenire ?

- Definire un piano di intervento «equilibrato» è fondamentale per mitigare i rischi rilevati con un impegno sostenibile per l'azienda ed un rischio residuo accettabile:

  maggiore equilibrio → maggiore sostenibilità.

- Un piano di intervento «equilibrato» richiede un'attività di Risk Treatment, ovvero l'esecuzione di un processo che, sulla base dei risultati della PIA e della RA, consente di:
  - Definire la strategia di gestione del rischio (Evitare, Mitigare, Accettare, Trasferire)
  - Individuare, tramite una valutazione costi / benefici delle varie alternative, gli interventi, organizzativi, tecnologici e/o procedurali da porre in essere
  - Accettare consapevolmente il rischio residuo
  - Attribuire la giusta priorità ai vari interventi

L'intervento è efficace ?

- Conoscere lo stato dell'arte degli interventi effettuati, ovvero delle misure di sicurezza implementate, è fondamentale per avere la certezza che gli investimenti fatti abbiano prodotto o stiano producendo gli effetti attesi:

  Monitoraggio → Controllo della situazione

- L'attività di monitoraggio deve essere finalizzata a rilevare, attraverso obiettivi di controllo e indicatori di performance chiari e misurabili :
  - L'effettivo stato di implementazione delle misure di sicurezza
  - L'efficacia delle misure implementate
  - L'effettiva e corretta applicazione del framework
  - La conformità ai requisiti del Regolamento

Punti di attenzione

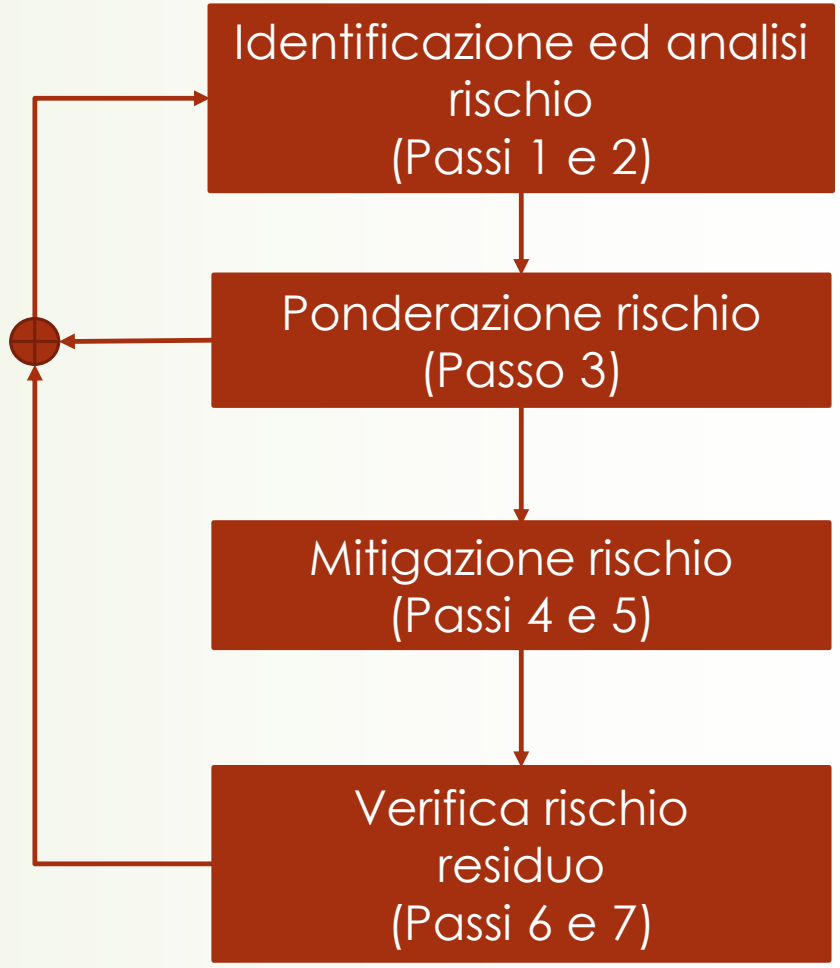
- Lo schema illustrato deve essere:
  - Reiterato periodicamente
  - Attuato a fronte di specifici eventi, quali:
    - Definizione di un nuovo processo/trattamento, modifica/eliminazione di un processo/trattamento esistente
    - Adozione di nuove tecnologie a supporto dei processi/trattamenti in essere
    - Cambi normativi
    - Risultanze di attività di Internal Auditing, Verifiche Ispettive, Monitoraggio
- Lo schema deve essere documentato e devono essere debitamente conservate le evidenze della sua applicazione.
- Si deve prevedere il coinvolgimento di un mix di competenze in grado di rilevare, analizzare e valutare ambiti che vanno dai business process alle reti passando dalle tecnologie e soluzioni di security.
- L'applicazione del framework non deve essere limitata ai soli processi che trattano dati personali in formato digitale.

Gestione del dei rischio

Da un punto di vista pratico, la società deve analizzare e successivamente mitigare i rischi connessi al trattamento dei dati personali, come preliminarmente individuati e redigere un documento di gestione del rischio

Valutazione rischio

Trattamento rischio



Gestione del rischio – step1

Individuazione di tutti i pericoli potenziali derivanti dal trattamento e correlate gravità. Questa fase deve essere sviluppata ignorando tutte le soluzioni tecniche ed organizzative che sono state adottate nell'effettuare il trattamento per ridurne la pericolosità. Questo percorso risulta difficoltoso quando l'analisi dei rischi viene redatta quando il processo è già attivo. E' invece un valido strumento progettuale, quando viene affrontato nella fase preliminare di definizione delle specifiche di funzionamento, in quanto consente di individuare tutti i pericoli connessi con il trattamento e di indirizzare quindi le soluzioni tecnico/organizzative verso la loro eliminazione (rif. GDPR art. 25 "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita").

Per la PIA	Per l'analisi dei rischi
Art. 35 + C.75 – C.76	Art. 32 + C.83

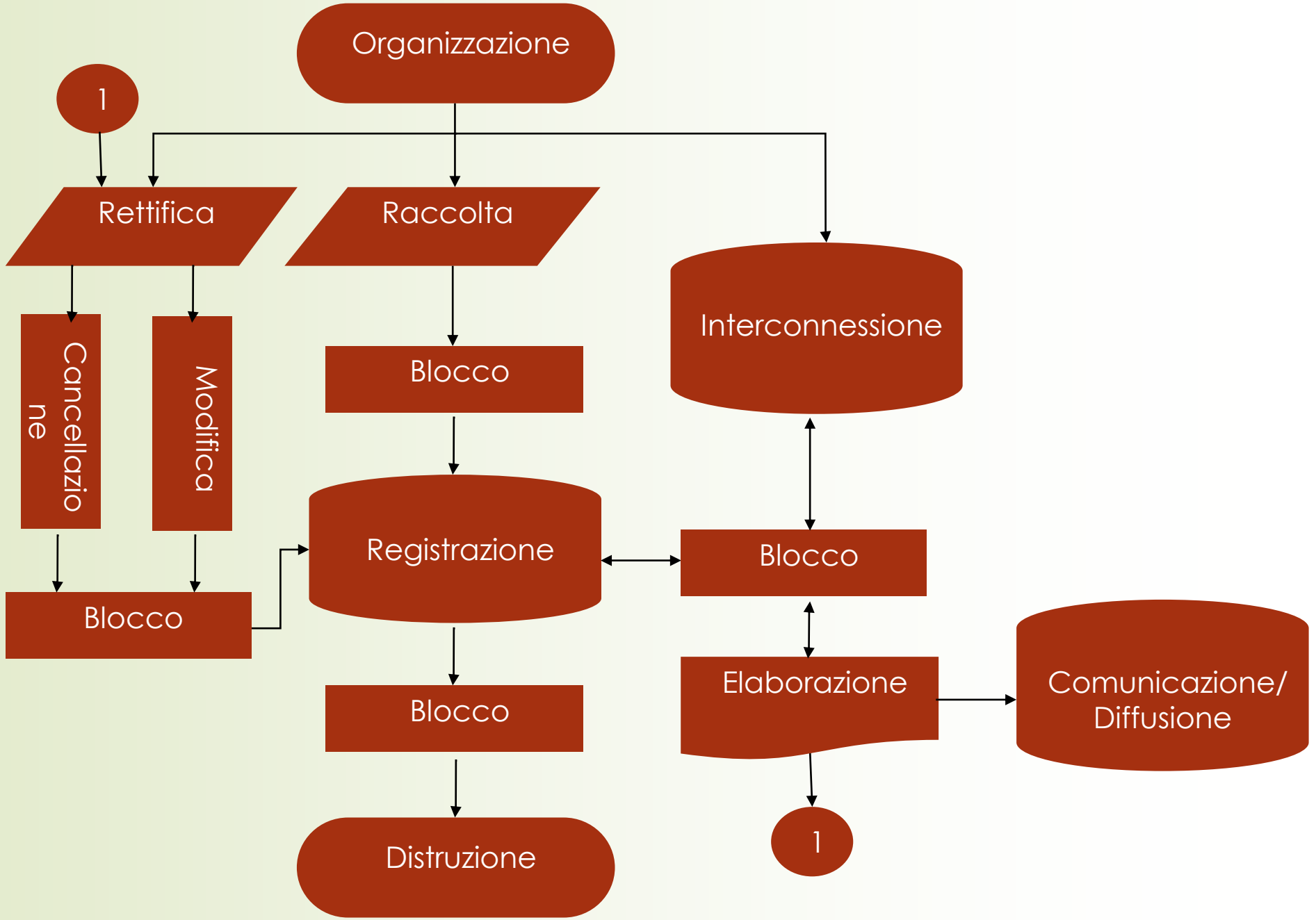
Gestione del rischio – step 2

Individuazione delle cause e relative probabilità associabili ad ogni pericolo potenziale. Questa analisi è utile per valutare la probabilità con cui il relativo pericolo si può manifestare. Fra le cause probabili di pericolo occorre prendere in considerazione sia il dato a sé stante che il relativo trattamento, anche in funzione del grado di preparazione e di adeguatezza degli operatori (c.d. "Responsabili" ed "Incaricati"), degli strumenti di lavoro loro affidati nonché della reciproca interazione fra questi ultimi.

Fondamentale è riuscire a modellare il trattamento secondo i canoni caratteristici della protezione dei dati personali, ad es., facendo uso della definizione di cui all'art. 4, c. 1, lettera a) del D. Lgs. 196/2003:

"trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Analisi del trattamento (step 2)



Gestione del rischio – step 2

Alla stessa maniera può essere conveniente individuare le classi di eventi tra quelle già consolidate in letteratura.

Ad. Es, per continuità con il previgente D.Lgs. 196/2003, è possibile assumere quali eventi rischiosi (ovvero che possono generare danni) quanto indicato nella tabella 3 "analisi dei rischi" del "Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)" pubblicato dal Garante della Privacy in data 11/06/2004.
http://www.privacy.it/archivio/garanteprovv20040611.html

Eventi (step. 2)

- Comportamenti degli operatori:
  - Sottrazione di credenziali di autenticazione;
  - Carenza di consapevolezza, disattenzione o incuria;
  - Comportamenti sleali o fraudolenti;
  - Errore materiale;
  - Altro evento;
- Eventi relativi agli strumenti:
  - Azione di virus informatici o di programmi suscettibili di recare danno;
  - Spamming o tecniche di sabotaggio;
  - Malfunzionamento, indisponibilità o degrado degli strumenti;
  - Accessi esterni non autorizzati;
  - Intercettazione di informazioni in rete;
  - Altro evento;
- Eventi relativi al contesto:
  - Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria;
  - Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.);
  - Errori umani nella gestione della sicurezza fisica;
  - Altro evento.

Gestione del rischio – step 3

Definizione del rischio potenziale che ne deriva. E' in sintesi il prodotto della gravità del pericolo per la probabilità che l'evento pericoloso si manifesti come analizzato al punto 2).

Rischio	Effetto 1	Effetto 2
Causa 1	P1xG1	P1xG2
Causa 2	P2xG1	P2xG2

Gestione del rischio – step 4

Valutazione dell'efficacia delle misure protettive adottate per ridurre il rischio. Quando il rischio potenziale rilevato al punto 3) assume livelli significativi ovvero non è "tollerabile", è necessario adottare delle soluzioni (c.d. "misure di mitigazione") che ne riducano la gravità del potenziale danno. Occorre comunque non trascurare l'eventuale aggiunta di un ulteriore rischio che la soluzione adottata può aver introdotto. Nella valutazione della riduzione del rischio occorre considerare sia l'attenuazione del rischio primario che l'introduzione del nuovo rischio.

Rischio	Macro Misura Sicurezza	Tipologia Misura Sicurezza
Furto di credenziali di autenticazione	Sistema di Autenticazione	Protettiva
	Formazione	Preventiva
Carenza di consapevolezza, disattenzione o incuria	Sistema di Autenticazione	Protettiva
	Formazione	Preventiva

Gestione del rischio – step 5

Valutazione dell'efficacia delle misure preventive adottate per ridurre il rischio. Di non minore importanza rispetto a quelle protettive, le misure preventive, tanto di tipo tecnico che organizzativo, agiscono riducendo la probabilità di accadimento del danno. Tra gli elementi di riduzione del rischio facenti parte di questa categoria è possibile annoverare:

- Soluzioni tecniche predittive;
- Formazione/mansionari;
- Polizze assicurative/fondi rischi a bilancio.

Formazione	Formazione ad incaricati e responsabili sul ruolo e i compiti
	Formazione agli incaricati specifica sulle misure informatiche
	Formazione periodica agli incaricati sulla gestione della sicurezza fisica

Gestione del rischio – step 6

Valutazione del rischio residuo. E' la valutazione del livello di rischio che rimane dopo l'adozione di tutte le soluzioni adottate. E' necessario verificare se il rischio "residuo" è an-cora inaccettabile o meno per stabilire se la causa definita al punto 2) ha soddisfatto i requisiti di sicurezza espressi dal GDPR.

Rischio Residuo = Frequenza x Magnitudo / Σ (Misure Mitigazione)

Gestione del rischio – step 7

Limite di accettabilità del rischio residuo. Come indicato all'articolo 24, paragrafo 1 del GDPR "Responsabilità del titolare del trattamento", il rischio residuo finale deve assumere dei livelli considerati accettabili: "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché 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 e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*".

Pertanto il livello di rischio residuo accettabile non è un valore assoluto che può essere stabilito a priori, ma dipende dallo specifico trattamento in esame.

Gestione del rischio – step 7

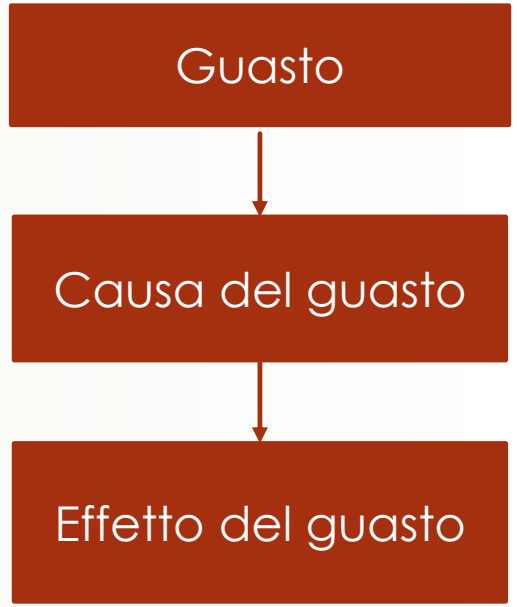
Un buon criterio per definire il limite massimo di accettabilità del livello di rischio è quello di riferirsi al pericolo potenziale più grave presente nel trattamento e calcolare il rischio residuo che ne risulta dopo aver adottato sia le soluzioni in conformità all'art. 32 del GDPR, che le ulteriori soluzioni che si sono ritenute necessarie in base, anche, a specifiche Norme di Legge e/o Tecniche.

Questo "livello massimo di rischio residuo", laddove ritenuto accettabile, non deve essere superato, da alcun altro pericolo potenziale una volta opportunamente mitigato.

Qualora, invece, il livello massimo di rischio residuo non fosse accettabile e trovandosi l'Azienda nell'impossibilità di non effettuare il relativo trattamento, sarà necessario attivare la procedura di consultazione preventiva (rif. GDPR, art. 36 "Consultazione preventiva") nei confronti del Garante.

FMEA

Il problema più rilevante che insorge nell'affrontare un'analisi dei rischi, è quello di renderla facilmente "leggibile" sia all'Organismo Notificato, sia al Garante ed agli Interessati che possono richiedere in qualsiasi momento di analizzare il trattamento a fronte di possibili incidenti (rif. GDPR, art. 33 "notifica di una violazione dei dati personali all'autorità di controllo" ed art. 34 "comunicazione di una violazione dei dati personali all'interessato") o di richieste di dimostrazione della conformità al GDPR (rif. GDPR, art. 58 "poteri" dell'autorità di controllo ed art. 15 "diritto di accesso dell'interessato"). Una stesura dell'analisi dei rischi puramente "descrittiva" è da evitare in quanto i contenuti sono prettamente soggettivi, di difficile interpretazione e soprattutto facilmente discutibili.



Per ovviare al problema della "soggettività" dell'analisi dei rischi, è possibile applicare una delle tecniche riconosciute dalla ISO 31010 "gestione del rischio" quali, ad esempio, le metodologie FMEA (c.d. "Failure Modes and Effects Analysis" ovvero "analisi sui modi di guasto e sui potenziali effetti) riferite alla sicurezza.

FMEA step 1

Individuazione di tutti i pericoli potenziali derivanti dal trattamento e correlate gravità. Questa valutazione deve astenersi dal prendere in considerazione le soluzioni tecnico/organizzative adottate per risolvere il pericolo potenziale. Deve considerare la gravità del danno che può essere arrecato all'interessato i cui dati personali sono soggetti a trattamento, ipotizzando che il danno avvenga sicuramente, e assegnando in conclusione un "indice di gravità" (IG). A livello numerico è possibile adottare una valutazione del pericolo agganciata alla valutazione economica del danno espresso in unità monetarie generiche facendo riferimento a esempi di tabelle assicurative di risarcimento dei danni:

Effetto dell'evento pericoloso		IG
Estremamente pericoloso	Morte	10^10
Pericoloso	Lesione o menomazione grave/ permanente	10^9
Alto	Lesione o menomazione lieve/temporanea	10^7
Basso	Danno lieve ed oggettivo alle persone o alle cose	10^5
Minore	Danno lieve e soggettivo alle persone o alle cose	10^3

FMEA step 2

Individuazione delle cause e relative probabilità associabili ad ogni pericolo potenziale. Per ogni pericolo potenziale possono individuarsi diverse possibili cause, ognuna delle quali ha una sua propria probabilità di manifestarsi. Pertanto nella quantificazione dell'analisi dei rischi occorre prendere in considerazione ogni causa potenziale, applicando ad ognuna di esse il suo "indice di probabilità" (IP) in virtù dell'esperienza e della conoscenza acquisita in merito allo specifico dato personale, del suo trattamento e dell'adeguatezza degli ambienti, degli strumenti e del personale preposti al medesimo. La probabilità deve essere calcolata sull'intera durata del trattamento come riportata nei registri delle attività di trattamento. Prendendo a riferimento le esperienze presenti in letteratura (si vedano, ad es. le metodologie HFMEA della Joint Commission on Accreditation of Healthcare Organizations) si assume la scala d'incidenza che segue:

Causa e sua incidenza sull'evento pericoloso		IP
Frequente	Una volta ogni 100 o meno Interessati oppure un evento ogni giorno o meno	10^0
Probabile	Una volta ogni 1.000 Interessati oppure un evento ogni mese	10^-1
Occasionale	Una volta ogni 100.000 Interessati oppure un evento ogni anno	10^-2
Remota	Una volta ogni 500.000 di Interessati oppure un evento ogni 10 anni	10^-4
Molto poco probabile	Una volta ogni 1.000.000 di Interessati oppure un evento ogni 100 anni	10^-6

FMEA step 3

Definizione del rischio potenziale che ne deriva. Quando è definito l'indice di probabilità (IP) per ogni causa di pericolo potenziale, la cui gravità è espressa con il suo indice (IG), si ricava il rischio potenziale ovvero l'" indice di priorità del rischio" (IPR) dalla formula:

$$IPR = IG \times IP$$

FMEA step 4

Valutazione dell'efficacia delle misure protettive adottate per ridurre il rischio. Come accennato precedentemente, affinché il processo di analisi dei rischi sia il più efficace possibile, la soluzione tecnico/organizzativa deve essere presa in considerazione solamente in questa fase dell'analisi dei rischi. Ogni soluzione adottata può essere più o meno efficace a ridurre il rischio potenziale, per cui si propone di indicare tale efficacia come da tabella seguente attraverso un "indice di efficacia protettiva" (IEprot):

Efficacia della misura protettiva adottata per abbattere il rischio	Indice di efficacia protettiva (IEprot)
Inesistente	10^0
Limitata	10^-1
Discreta	10^-2
Buona o Efficace	10^-4
Sicura o conforme alle Norme Legislative e/o Tecniche	10^-6

FMEA step 5

Valutazione dell'efficacia delle misure preventive adottate per ridurre il rischio. Come visto al paragrafo precedente può essere considerato utile adottare ulteriori elementi di riduzione del rischio potenziale. La quantificazione numerica dell'" Indice di Efficacia Preventiva" (IEprev) può essere conforme all'esempio della tabella seguente:

Efficacia della misura preventiva adottata per abbattere il rischio	Indice di efficacia preventiva (IEprev)
Inesistente	10^0
Limitata	10^-1
Discreta	10^-2
Buona o efficace	10^-4

FMEA step 6

Valutazione del rischio residuo. A questo punto, avendo quantificato ogni singolo contributo degli elementi che concorrono a valutare il rischio residuo, la quantificazione del suo "indice di rischio residuo" (IRR) può essere ottenuta dall'applicazione di una formula come da esempio seguente:

$$IRR = IG \times IP \times IEprot \times IEprev$$

A titolo esemplificativo, un pericolo potenziale di morte (IG=10^10) la cui probabilità di manifestarsi nel tempo è occasionale (IP=10^-2) genera un rischio potenziale di IPR=10^8. Applicando una soluzione a "regola d'arte" (IEprot=10^-4, IEprev=10^-2) il rischio residuo è:

$$Exp(IRR) = 10 - 2 - 4 - 2 = 2$$

Da cui:

$$IRR = 10^2$$

FMEA step 7

Accettabilità del rischio residuo. I rischi che cadono nella zona verde sono tollerabili e non richiedono particolare attenzione né ulteriori analisi; quelli nella zona gialla (detti, nella terminologia ISO 14971, "ALARP" ovvero "As Low As Reasonably Practicable") sono tollerabili ma è opportuno farne oggetto di revisione, in ordine crescente di indice di rischiosità residua, in ottica ISO 9001 di miglioramento continuo delle prestazioni dell'organizzazione; infine quelli della zona rossa non sono tollerabili e devono essere resi tali con ulteriori azioni correttive previa, eventuale, consultazione del Garante.

Exp(IRR)		Molto poco probabile	Remota	Occasionale	Probabile	Frequente
		-6	-4	-2	-1	0
Estremamente pericoloso	10	4	6	8	9	10
Pericoloso	9	3	5	7	8	9
Alto	7	1	3	5	6	7
Basso	5	-1	1	3	4	5
Minore	3	-3	-1	1	2	3

Riscontri oggettivi a sostegno dell'analisi dei rischi

Qualsiasi trattazione, sia pure "numerica", non può avere alcun valore se non poggia su indiscutibili elementi che argomentino e dimostrino in maniera oggettiva le soluzioni che l'Azienda ha adottato per limitare i rischi. Questo aspetto è indispensabile per dimostrare che quanto riportato nell'analisi dei rischi sia concretamente riferito alla realtà del trattamento:

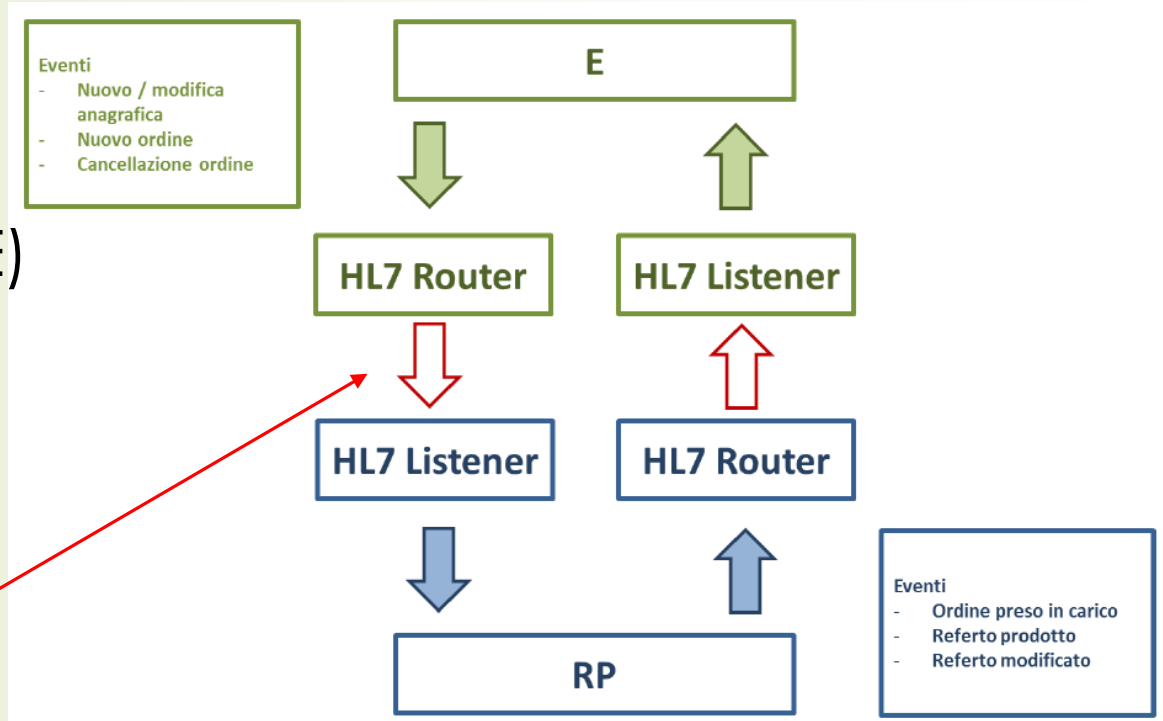
- Schemi e disegni tecnici;
- Calcoli o simulazioni;
- Schede o specifiche tecniche degli strumenti in uso;
- Documentazione del software;
- Specifiche di collaudo;
- Report di test e prove eseguite;
- Procedure gestionali;
- Mansionari;
- Registri della formazione erogata;
- Verifiche ispettive interne;
- Report indicatori performance;
- Analisi statistiche;
- Riferimenti bibliografici;
- Altri documenti.

Caso pratico: Sistema Informativo Sanitario

SIS della struttura S:

SID amministrativo (E)
SID diagnostico (RP)

E ed RP sono sulla stessa LAN



Che cosa succede dal punto di vista della rischiosità del dato trasmesso?

Eventi HL7

Evento / *Trigger*	Codifica HL7
Invio Nuovo/Modifica anagrafica paziente a RP	ADT^A31
Invio nuovo ordine a RP	ORM^O01 - ORC NW
Invio cancellazione ordine a RP	ORM^O01 - ORC CA
Ricezione da RP presa in carico ordine	ORM^O01 - ORC SC
Ricezione da RP url referto	MDM^T02
Ricezione da RP url referto modificato	MDM^T10

- comunicazione basata su HL7
- condivisione delle anagrafiche dei pazienti
- ordini/prestazioni da erogare e fatturare su E
- ordini/prestazioni erogare e refertare su RP
- accesso condivisione dei referti prodotti

Monetizzare il rischio

Un'organizzazione investe in sicurezza se si esprime in termini di denaro il danno potenziale a cui è soggetta

Equazione del rischio (da ISO 27001:2013)
Rischio = Minaccia x Vulnerabilità X Danno

Causa e sua incidenza sull'evento pericoloso		IP
Frequente	Una volta ogni 100 o meno Interessati oppure un evento ogni giorno o meno	10^{0}
Probabile	Una volta ogni 1.000 Interessati oppure un evento ogni mese	10^{-1}
Occasionale	Una volta ogni 100.000 Interessati oppure un evento ogni anno	10^{-2}
Remota	Una volta ogni 500.000 di Interessati oppure un evento ogni 10 anni	10^{-4}
Molto poco probabile	Una volta ogni 1.000.000 di Interessati oppure un evento ogni 100 anni	10^{-6}

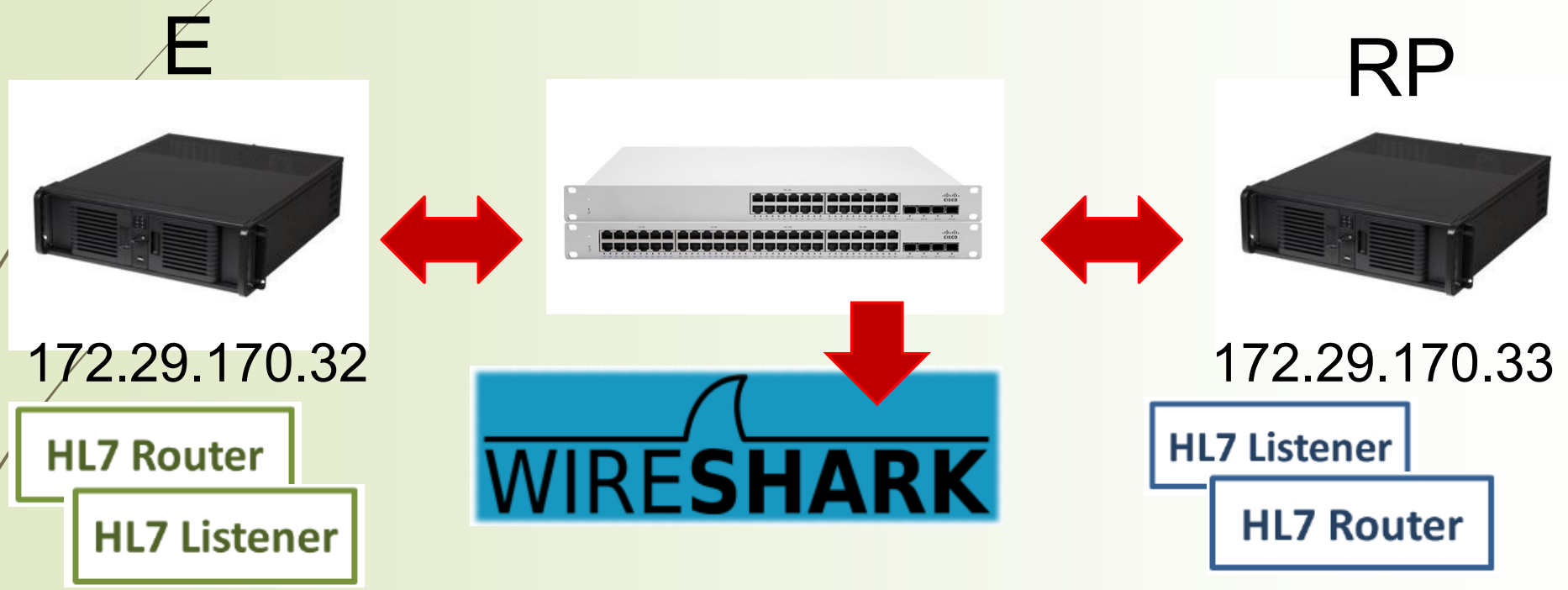
~ 29 € a paziente fatturato annuo / n. pazienti

~ 1 attacco anno (rapporto Clusit 2017)

Rapporto Clusit 2017

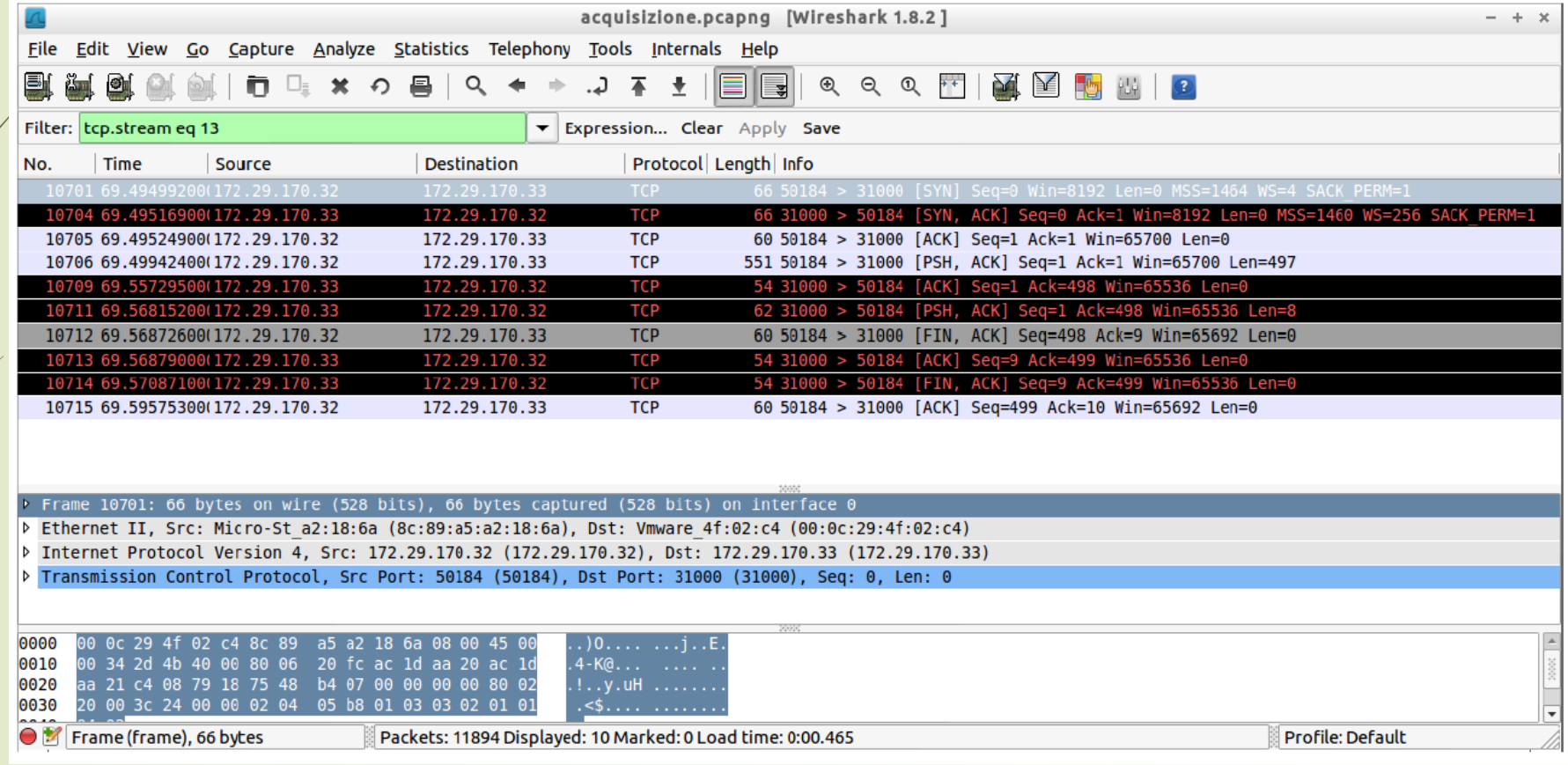
- Dal punto di vista statistico, oggi qualsiasi organizzazione, indipendentemente dalla dimensione o dal settore di attività, ha la ragionevole certezza che subirà un attacco informatico di entità significativa entro i prossimi 12 mesi, mentre oltre la metà ne hanno subito almeno uno nell'ultimo anno.
- Sottostimare i rischi, procrastinare l'adozione di contromisure adeguate, ed affidarsi alla "buona sorte", non sono più opzioni percorribili.

Analisi della vulnerabilità (sniffer)



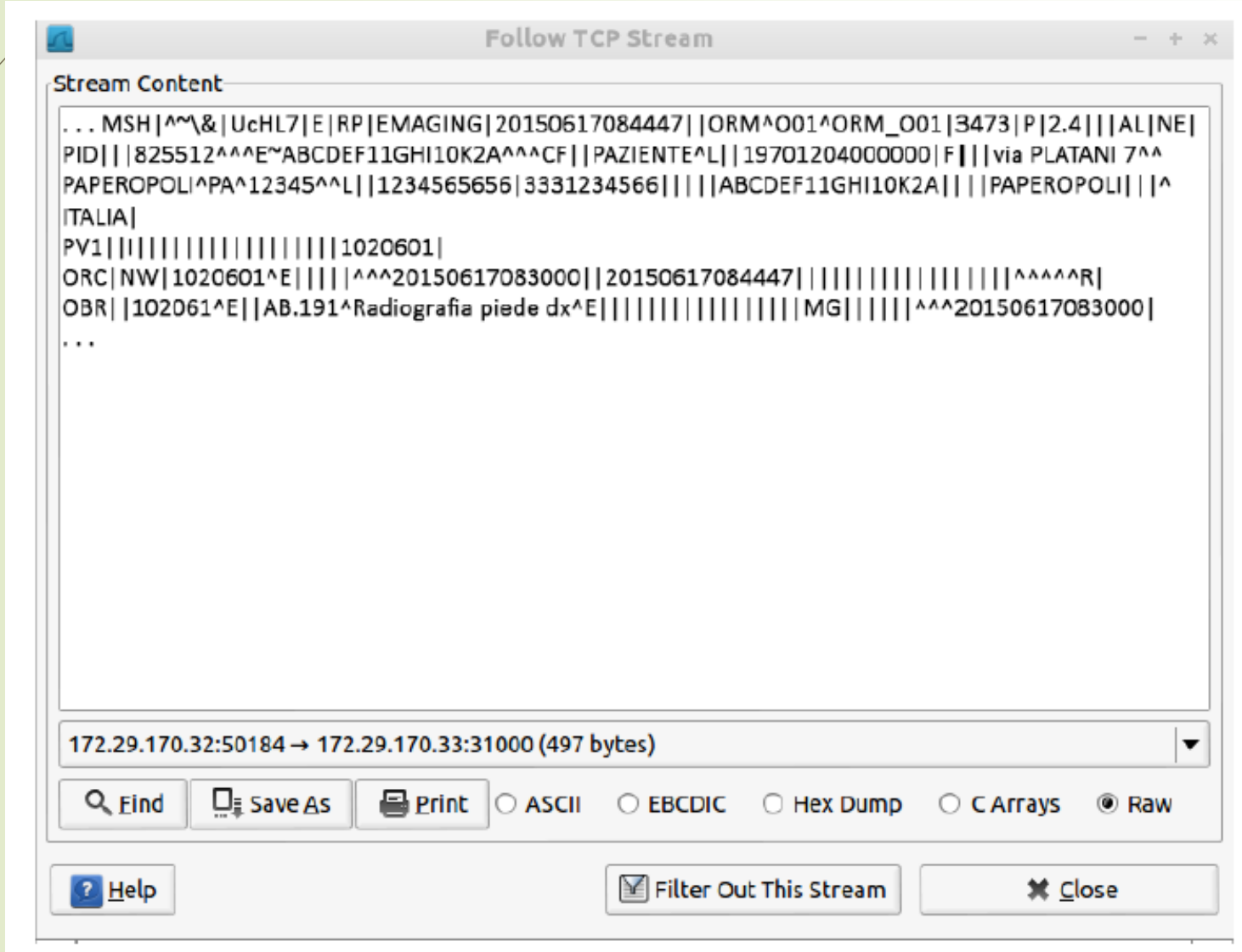
- strumento in grado di intercettare le informazioni scambiate da due entità
- si memorizzano tutti gli header e i payload incapsulati secondo lo standard definito dallo stack TCP/IP

Evidenze raccolte



Pacchetti in transito in transito da HL7 Router (E) a HL7 Listner (RP)

Messaggio HL7



Esempio di messaggi intercettabili

```
MSH|^~\&|UcHL7|E|RP|EMAGING|20150617084447||ORM^O01^ORM_O01|3473|P|2.4
|||AL|NE|
PID|||825512^^^E~ABCDEF11GHI10K2A^^^CF||PAZIENTE^L||19701204000000|F|||via
PLATANI
7^^PAPEROPOLI^PA^12345^^L||1234565656|3331234566|||||ABCDEF11GHI10K2A||||P
APEROPOLI|||^ITALIA|
PV1|||I|||||||||||||||||1020601|
ORC|NW|1020601^E||||^^^20150617083000||20150617084447|||||||||||||||||^^
^^^R|
OBR||1020601^E||AB.191^Radiografia piede
dx^E|||||||||||||||||MG||||||^^^20150617083000|
```

```
MSH|^~\&|UcHL7|E|RP|EMAGING|20150617083306||ADT^A31|3469|P|2.4||
|AL|NE|
PID|||825512^^^E~ABCDEF11GHI10K2A^^^CF||PAZIENTE^L||19701204000000
|F|||via PLATANI
7^^PAPEROPOLI^PA^12345^^L||1234565656|3331234566|||||ABCDEF11GHI10
K2A||||PAPEROPOLI|||^ITALIA|
```

variazione anagrafica

sessione operativa: inserimento, in carico, refertata

```
MSH|^~\&|UcHL7|RP|E|EMAGING|20150617084447||ORM^O01^ORM_O01|3473|P|
2.4|||AL|NE|
PID|||825512^^^E~ABCDEF11GHI10K2A^^^CF||PAZIENTE^L||19701204000000|F|||via
PLATANI
7^^PAPEROPOLI^PA^12345^^L||1234565656|3331234566|||||ABCDEF11GHI10K2A|||
|PAPEROPOLI|||^ITALIA|
PV1|||I|||||||||||||||||1020601|
ORC|SC|1020601^E||||^^^20150617083000||20150617084447|||||||||||||||||^^
^^^R|
OBR||1020601^E||AB.191^Radiografia piede
dx^E|||||||||||||||||20150617085416106915|MG|||||||||||ABCDEF11GHI10K2B&
OPERATORE&1
```

```
MSH|^~\&|UcHL7|RP|E|EMAGING|20150617084447||MDM^T02^MDM_T02|3473|P
|2.4|||AL|NE|
PID|||825512^^^E~ABCDEF11GHI10K2A^^^CF||PAZIENTE^L||19701204000000|F|||v
ia PLATANI
7^^PAPEROPOLI^PA^12345^^L||1234565656|3331234566|||||ABCDEF11GHI10K2A||
||PAPEROPOLI|||^ITALIA|
PV1|||I|||||||||||||||||1020601|
TXA||REFERTORP|PDF||20150617092006|||^DOTTOTRE.1^^^CF^^^|||21735100371
099100277|||||||||ABCDEF11GHI10K2E^DOTTORE^1^^^^^^^^^^
OBX||ED|DOCUMENTO||^URL^application^p
||||F
OBX||ED|
OBX||TX|AB.191^Radiografia piede dx^RP^20150617085416106915^Radiografia piede
dx^RP||
```

Conseguenze

- si ricostruisce la comunicazione tra E ed RP: nessuna confidenzialità.
- solo controlli formali e logici nella comunicazione, no hash crittografiche: integrità non garantita in senso forte.
- no cifratura asimmetrica per firmare messaggi: non è garantita l'autenticazione dell'origine dei dati.
- no terza parte fidata per la firma (con timestamp) di eventi: monitoraggio debole e non repudiation non garantita in senso forte.

Criticità maggiore

- Vulnerabilità esistente, attaccante può:

- ricostruire l'anagrafica dei pazienti;
- ricostruire le prestazioni radiologiche fruite;
- no accesso referti.

- Si rammenti la definizione di dato sensibile "… *IDONEO A* …".

Quantificazione del Rischio

Probabilità	Pazienti	Vulnerabilità	Danno	Rischio
0,01	1	1	€ 29,00	€ 0,29
0,01	10	1	€ 290,00	€ 2,90
0,01	100	1	€ 2.900,00	€ 29,00
0,01	1.000	1	€ 29.000,00	€ 290,00
0,01	10.000	1	€ 290.000,00	€ 2.900,00
0,01	100.000	1	€ 2.900.000,00	€ 29.000,00
0,01	1.000.000	1	€ 29.000.000,00	€ 290.000,00

- Tabella della rischiosità in funzione della dimensione dell'organizzazione
- NON tiene conto di sanzioni da parte dell'Autorità Garante
- Attuazione di un piano in relazione al valore da difendere

Contromisure: canale dedicato

- Possibilità di mitigazione:

- Doppia scheda di rete su E ed RP;
- erogazione normale servizio;
- Comunicazione fisica dedicata per traffico HL7.

- Effetto sulla probabilità, non sulla vulnerabilità.

Contromisure: SSL/TLS

- HL7 agnostico rispetto alla comunicazione.

- Abilitazione protocollo SSL/TLS sopra TCP/IP;
- certificati per garantire oltre alla confidenzialità;
- autenticazione e non rifiuto.

- Se i sistemi E ed RP sono sicuri: vulnerabilità = 0

Grazie dell'attenzione