Massimiliano Bonsignori
(Ingegnere in Torino - Gruppo di Studio Privacy OPEN Dot Com)

Le misure di “adeguatezza” per la protezione dei dati personali

Garanzia e dimostrazione di conformità

Reg. (UE) 2016/679
art. 24 co. 1

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per

1. garantire ed
2. essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento.

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

Riesame ed aggiornamento

Reg. (UE) 2016/679
art. 24 co. 1

- Le misure tecniche e organizzative sono riesaminate e aggiornate
- qualora necessario
- Ad es. art.29 D.Lgs.81/2008 *mutatis mutandis* →

- La valutazione dei rischi deve essere immediatamente rielaborata
  - in occasione di modifiche del processo produttivo o della organizzazione del lavoro significative ai fini della Protezione dei dati personali, o
  - in relazione al grado di evoluzione della tecnica, della prevenzione o della protezione o
  - a seguito di incidenti (data breach) significativi o
  - quando i risultati della sorveglianza del DPO ne evidenzino la necessità.
- *A seguito di tale rielaborazione, le misure debbono essere aggiornate*

Politiche di protezione dei dati

Reg. (UE) 2016/679
art. 24 co. 2

- Se ciò è proporzionato rispetto alle attività di trattamento, il titolare del trattamento attua **politiche adeguate** in materia di protezione dei dati
  - (Tra le misure tecniche ed organizzative adeguate)

Privacy by design

Reg. (UE) 2016/679
art. 25

- **sia al momento di determinare i mezzi del trattamento**
- **sia all'atto del trattamento stesso**

il titolare del trattamento mette in atto misure tecniche e organizzative adeguate volte a

1. attuare in modo efficace i principi di protezione dei dati (es. Minimizzazione)
2. a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati
   - Tenendo conto
   - dello stato dell'arte e dei costi di attuazione
   - nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento,
   - come anche dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

Privacy by default

Reg. (UE) 2016/679
art. 25

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire

1. che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento
   Tale obbligo vale per
   - la quantità dei dati personali raccolti,
   - la portata del trattamento,
   - il periodo di conservazione e
   - l'accessibilità
2. che non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica

E i responsabili?

Reg. (UE) 2016/679
art. 28 co. 1, 3

- Il titolare del trattamento ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti **per mettere in atto misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato

- Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
- …
- c) adotti tutte le misure richieste ai sensi dell'articolo 32

Misure di sicurezza

“Vecchio” D.Lgs. 196/2003 art. 31

- I dati personali oggetto di trattamento sono custoditi e controllati mediante l'adozione di **idonee e preventive misure di sicurezza**
  - anche in relazione alle conoscenze acquisite, in base al progresso tecnico,
  - alla natura dei dati e alle specifiche caratteristiche del trattamento,
  - in modo da ridurre al minimo i **rischi** di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Reg. (UE) 2016/679 art. 32

- il titolare e i responsabili del trattamento mettono in atto **misure tecniche e organizzative adeguate per** garantire un livello di **sicurezza** adeguato al **rischio**
  - 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

Approccio basato sul rischio

- Le misure tecniche e organizzative per la protezione dei dati personali dovrebbero, secondo GDPR, essere adeguate al rischio presentato.
- Il GDPR attribuisce particolare importanza alla nozione di rischio, stabilendo parametri specifici di protezione dei dati che devono essere considerati per la sua valutazione, in particolare la natura, la portata, il contesto e le finalità del trattamento.
- Inoltre, mette chiaramente in relazione il rischio con le misure adottate per preservare i diritti e le libertà delle persone.

Sicurezza e GDPR

- È importante notare che la sicurezza (nel senso di integrità e riservatezza) è stabilita come uno dei principi relativi al trattamento dei dati personali (articolo 5 del GDPR)
- Ciò pone la sicurezza al centro della protezione dei dati unitamente al resto dei principi di protezione dei dati, ad esempio liceità, correttezza e trasparenza, limitazione delle finalità, accuratezza e limitazione dello spazio di archiviazione
- La sicurezza del trattamento dei dati personali è principalmente dettata dagli articoli 24 e 32
- La valutazione dei rischi è principalmente dettata dagli articoli 32, 33, 34, 35, 36 del GDPR

Impatto potenziale

- Questo approccio, infatti, introduce l'impatto di una potenziale violazione dei dati personali alle persone interessate come un aspetto importante della valutazione del rischio
- È anche importante notare che la nozione di rischio è in generale centrale nel GDPR come soglia per attuare diversi obblighi, ad esempio per quanto riguarda
  1. la notifica di violazioni dei dati personali (articoli 33 e 34 del GDPR).
  2. la conduzione della valutazione dell'impatto sulla protezione dei dati (articolo 35 GDPR).
  3. la consultazione preliminare con le autorità competenti (articolo 36 del GDPR).

Rischi di cui tenere conto

"Vecchio" D.Lgs. 196/2003 art. 31

1. di distruzione o perdita, anche accidentale, dei dati stessi,
2. di accesso non autorizzato
3. di trattamento non consentito o non conforme alle finalità della raccolta.

- in modo da **ridurli al minimo**

Reg. (UE) 2016/679 art. 24 co. 1

- per i diritti e le libertà delle persone
- che derivano, in particolare:

1. dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata
2. dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati

- per **valutare l'adeguato livello di sicurezza**

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!

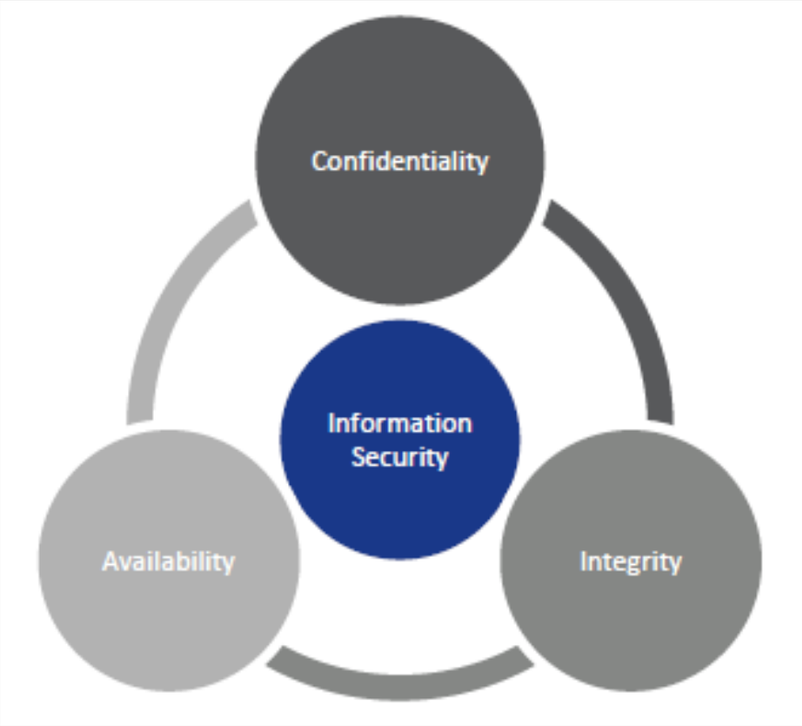
Non solo la sicurezza del trattamento

La valutazione del rischio deve riguardare

Ma anche gli effetti complessivi del trattamento

Confidentiality - Integrity - Availability

- Il modello più utilizzato per guidare lo sviluppo e l'implementazione di un framework per la gestione della sicurezza delle informazioni all'interno di un'organizzazione è rappresentato dalla cosiddetta triade della CIA:
  - Confidentiality - riservatezza
  - Integrity - integrità
  - Availability - disponibilità
- delle informazioni.



Aspetti riguardanti la sicurezza

Disponibilità

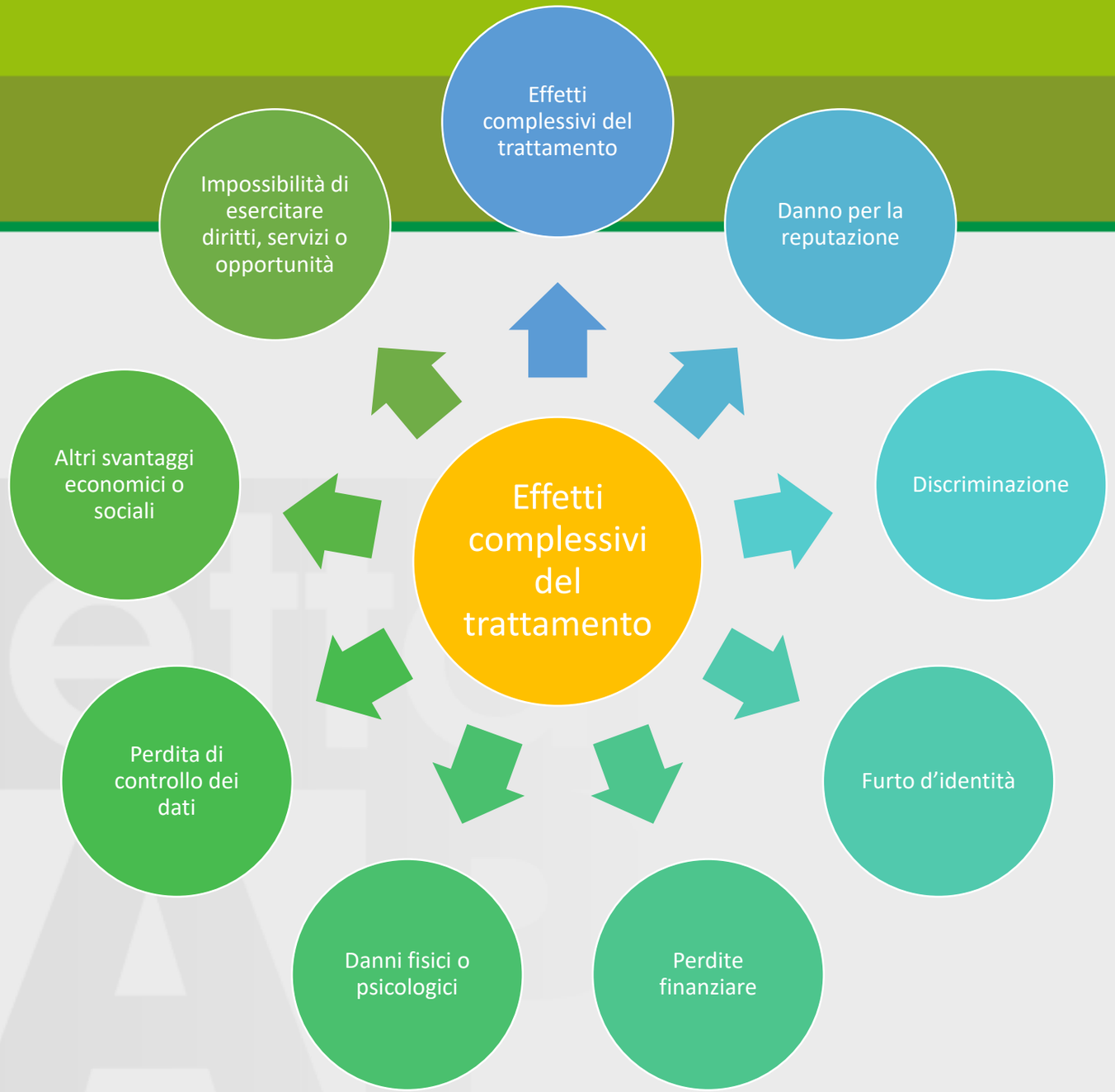
- distruzione
- indisponibilità
- perdita

Riservatezza

- divulgazione
- accesso

Integrità

- alterazione


Effetti complessivi del trattamento
Effetti complessivi del trattamento
Danno per la reputazione
Discriminazione
Furto d’identità
Perdite finanziare
Danni fisici o psicologici
Perdita di controllo dei dati
Altri svantaggi economici o sociali
Impossibilità di esercitare diritti, servizi o opportunità

Linee guida del Gruppo di lavoro Articolo 29 (WP248rev.1)

- 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
- Il rischio viene definito come combinazione dei fattori “probabilità di accadimento” e “dimensioni del danno” conseguenti alla esposizione ai pericoli o fattori di rischio.
- R=f(P,D) in genere R=PxD

Scenari di esempio

1) comportamenti degli operatori:

- sottrazione di credenziali di autenticazione
- carenza di consapevolezza, disattenzione o incuria
- comportamenti sleali o fraudolenti
- errore materiale

2) eventi relativi agli strumenti:

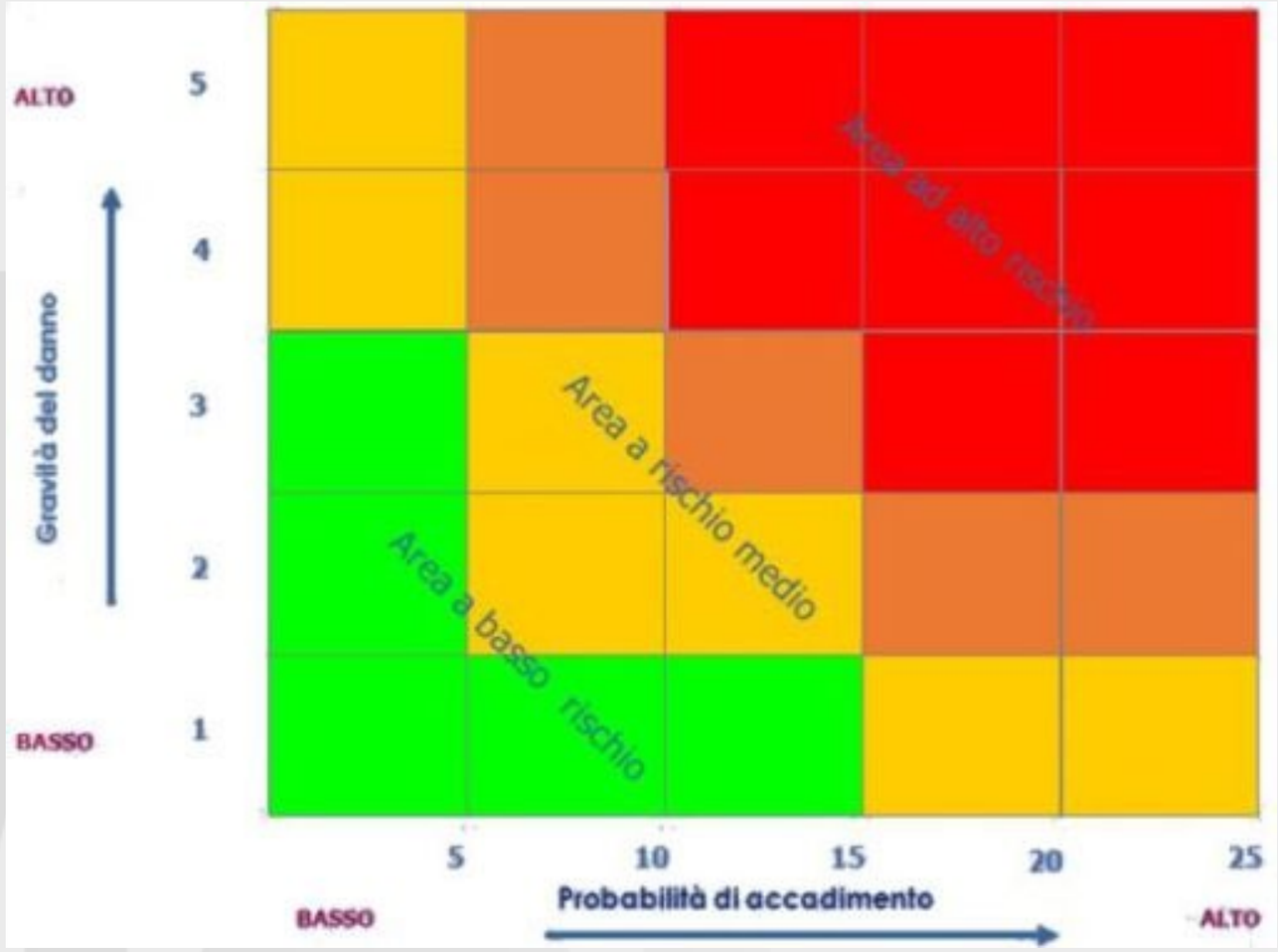
- azione di virus informatici o di programmi suscettibili di recare danno
- spamming o tecniche di sabotaggio
- malfunzionamento, indisponibilità o degrado degli strumenti
- accessi esterni non autorizzati
- intercettazione di informazioni in rete

3) eventi relativi al contesto fisico-ambientale:

- ingressi non autorizzati a locali/aree ad accesso ristretto
- sottrazione di strumenti contenenti dati
- eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria
- guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
- errori umani nella gestione della sicurezza fisica

Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)

Matrice di rischio 4x4



Probabilità di accadimento

- Uno stesso scenario incidentale può evolversi in modi diversi e presentare differenti esiti in termini di danno (es. varie conseguenze di una divulgazione di dati non autorizzata o accidentale),
- La probabilità può essere stimata sulla base di
  - valutazioni statistiche (come nel caso degli infortuni) o
  - presunzioni (più o meno fondate)
    - anche attraverso procedure e checklist validate

Impatto: gravità del danno

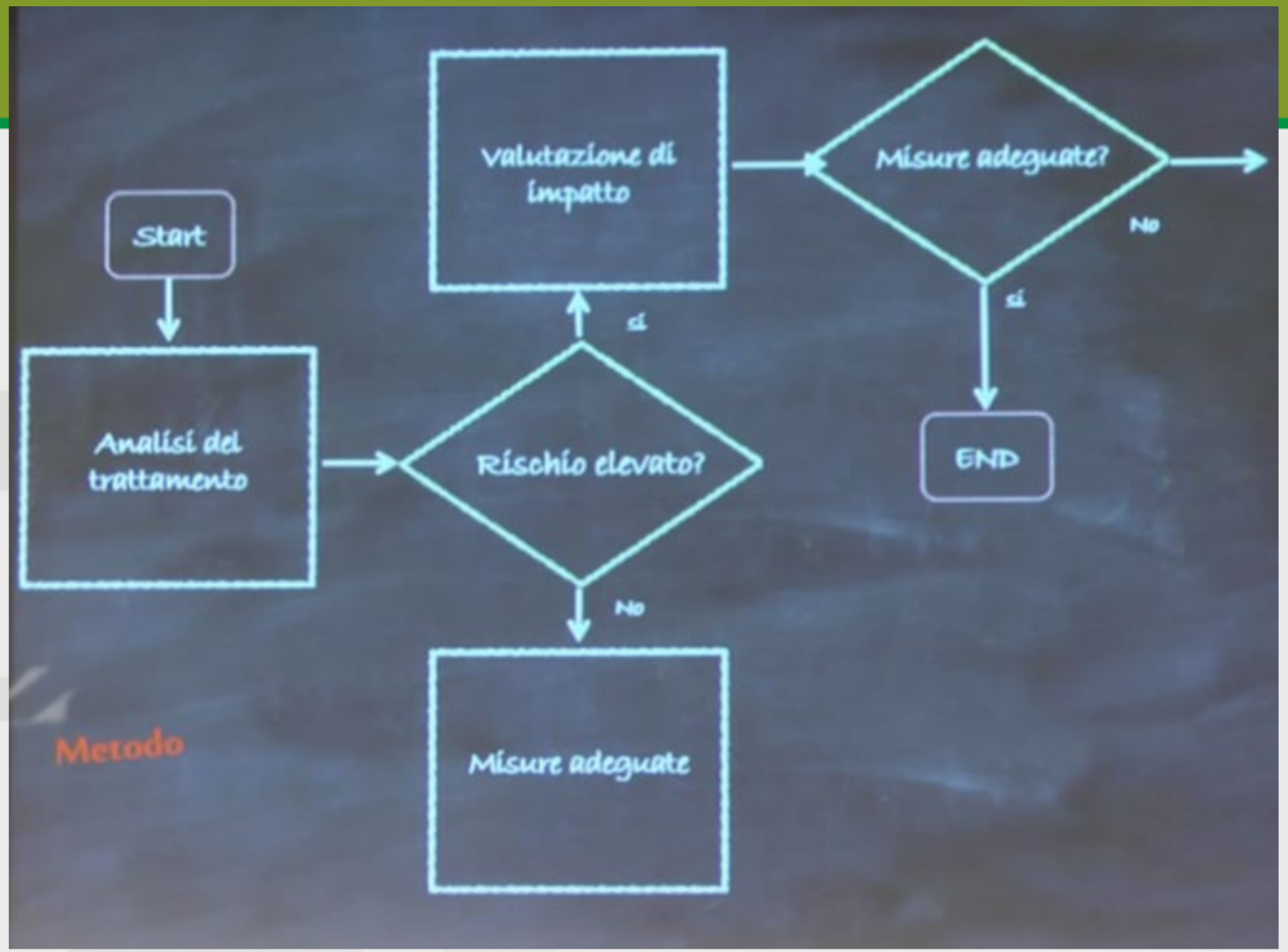
- Nel processo di valutazione del rischio "tipico", i rischi sono stimati in base al loro potenziale impatto per l'organizzazione.
- **Nel caso del trattamento dei dati personali, tuttavia, gli impatti sono considerati in relazione alle libertà e ai diritti delle persone.**
- Questa è una differenza significativa poiché modifica l'analisi degli impatti nei confronti dei possibili effetti negativi che un individuo può subire, tra cui ad esempio il furto di identità o la frode, la perdita finanziaria, danni fisici o psicologici, umiliazione, danni alla reputazione o addirittura minacce alla vita.
- Durante l'esecuzione di tale analisi, la scala (ad esempio il numero di individui affetti) potrebbe non essere rilevante: l'impatto è elevato anche se può portare gravi effetti avversi solo a una singola persona.
- Un'ulteriore sfida è che, per calcolare l'impatto, è necessario considerare anche eventuali effetti collaterali secondari per i diritti e le libertà delle persone.

Descrizione dei livelli dell’impatto

- Si deve valutare l'impatto sui diritti e sulle libertà fondamentali delle persone, derivanti dalla possibile perdita di sicurezza dei dati personali. Vengono considerati quattro livelli di impatto
- **Basso-Low**: gli individui possono incontrare alcuni piccoli inconvenienti, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidio, seccature, ecc.).
- **Medio-Medium**: gli individui possono incontrare disagi significativi che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, mancato accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
- **Elevato-High**: le persone possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
- **Molto Elevato-Very High**: le persone possono avere conseguenze significative, o addirittura irreversibili, che non possono superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)

Sicurezza

- Prevenzione, eliminazione parziale o totale di danni, pericoli, rischi
- Condizione di essere al sicuro
- Condizione di essere protetti contro le conseguenze di guasti, danni, errori, incidenti, disastri o di qualsiasi altro evento che potrebbe essere considerato non desiderabile, di tipo fisico, sociale, emotivo, professionale, psicologico o di altro tipo
  - Controllo dei pericoli riconosciuti per raggiungere un livello accettabile di rischio


Start
Analisi del trattamento
Rischio elevato?
si
No
Valutazione di impatto
Misure adeguate?
No
si
END
Misure adeguate
Metodo

Misure adeguate

Reg. (UE) 2016/679
art. 24-28

- Politiche di protezione
- Riesame ed aggiornamento
- P. by design
- P. by default
- Accordi, contratti, designazioni
  - (Contitolari, Responsabili, Rappresentanti)

Formazione e istruzioni obbligatorie

Reg. (UE) 2016/679
art. 29, art. 32 co. 4

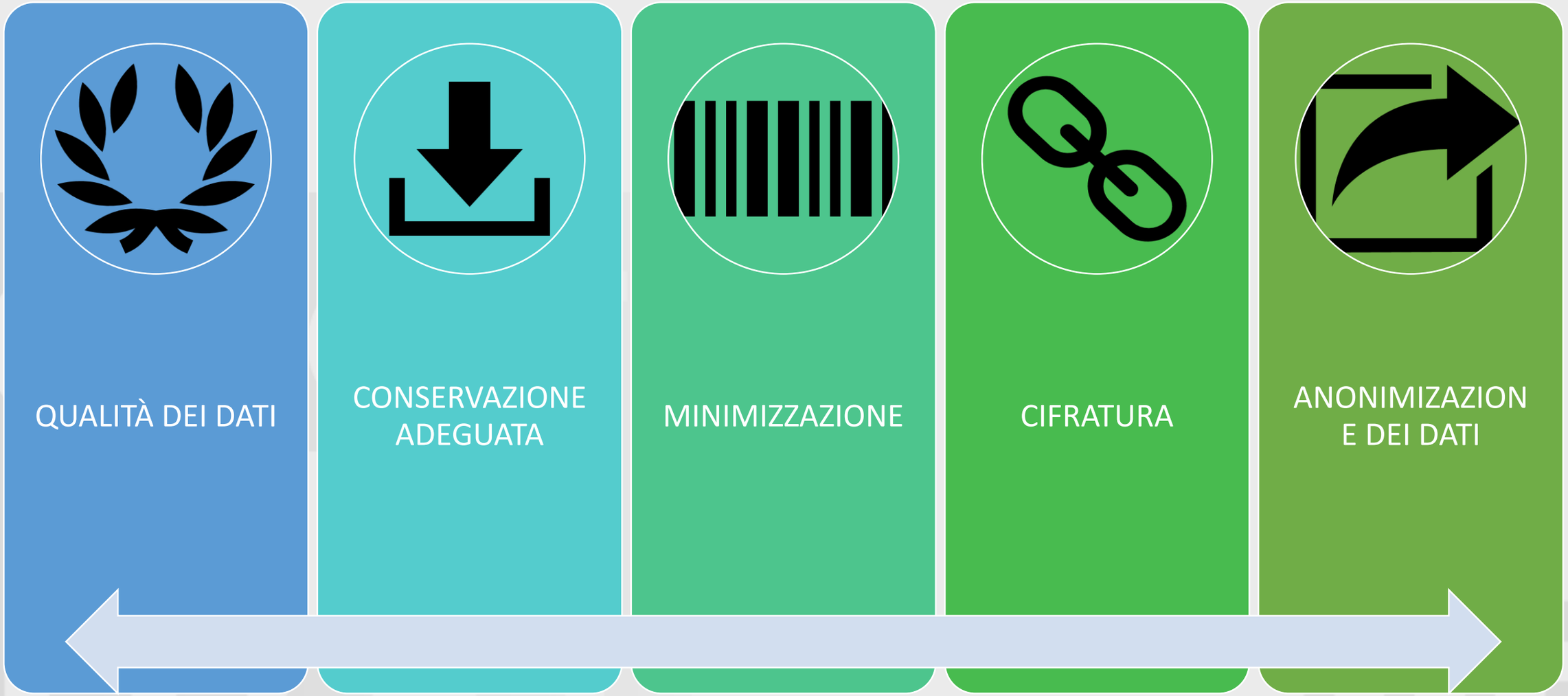
- Chiunque (incaricato o responsabile) abbia accesso ai dati deve essere istruito al riguardo da parte del titolare del trattamento

Misure di sicurezza, tra cui…

Reg. (UE) 2016/679
art. 32

- Pseudonimizzazione
- Cifratura dei dati personali
- Capacità di assicurare su base permanente **la riservatezza, l'integrità, la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento
- Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Quali sono le misure per la gestione del rischio? ACCOUNTABILITY



Quali sono le misure per la gestione del rischio? ACCOUNTABILITY

MISURE TECNOLOGICHE

- policy di sicurezza logiche e fisiche,
- aggiornamenti servizi e software,
- test,
- controllo accessi
- tracciamento operazioni

MISURE ORGANIZZATIVE

- ruoli,
- governance,
- istruzioni,
- formazione,
- procedure,
- audit,
- strumenti di controllo per gli interessati,
- contatti

Esempi: le «vecchie» misure minime

“Vecchio” D.Lgs. 196/2003
artt. 33-36 Allegato B

Nel caso di utilizzo di strumentazione elettronica:

- Utilizzazione di un sistema autenticazione informatica;
- Adozione di procedure di gestione delle credenziali di autenticazione
- Utilizzazione di un sistema di autorizzazione
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- Adozione di procedure per la custodia di copie di sicurezza (back-up), il ripristino della disponibilità dei dati e dei sistemi
- Aggiornamento periodico di sistemi operativi, software di protezione e di trattamento

Esempi: le «vecchie» misure minime

"Vecchio" D.Lgs. 196/2003
artt. 33-36 Allegato B

- **Definizione dei compiti e dell'ambito del trattamento consentito**
- Previsione di **procedure per un'idonea custodia** di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- Previsione di **procedure per la conservazione** di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati

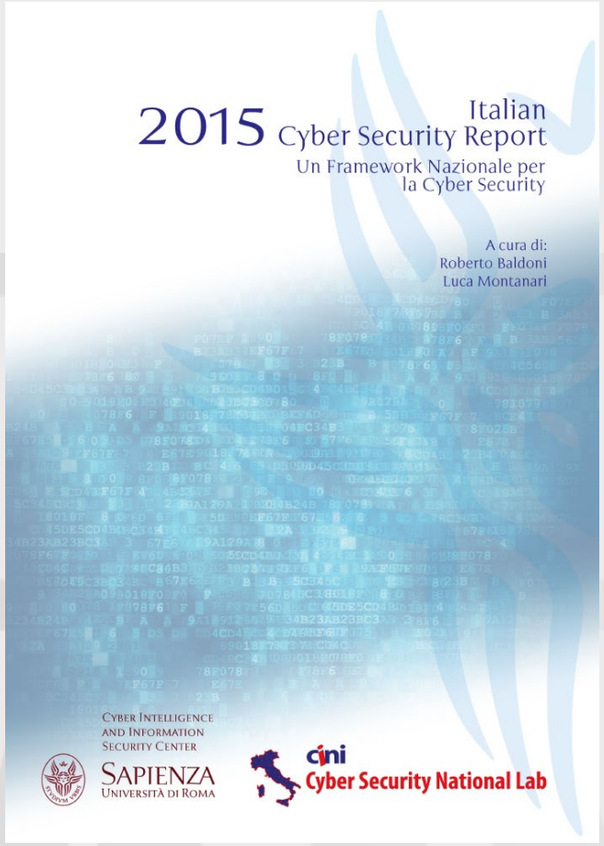
Almeno una volta all'anno:

- Effettuazione dell'**analisi dei rischi** di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta
- **Aggiornamento dell'individuazione dell'ambito del trattamento consentito** ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- **Formazione ed informazione** degli incaricati/responsabili

Information Management System for Personal Data

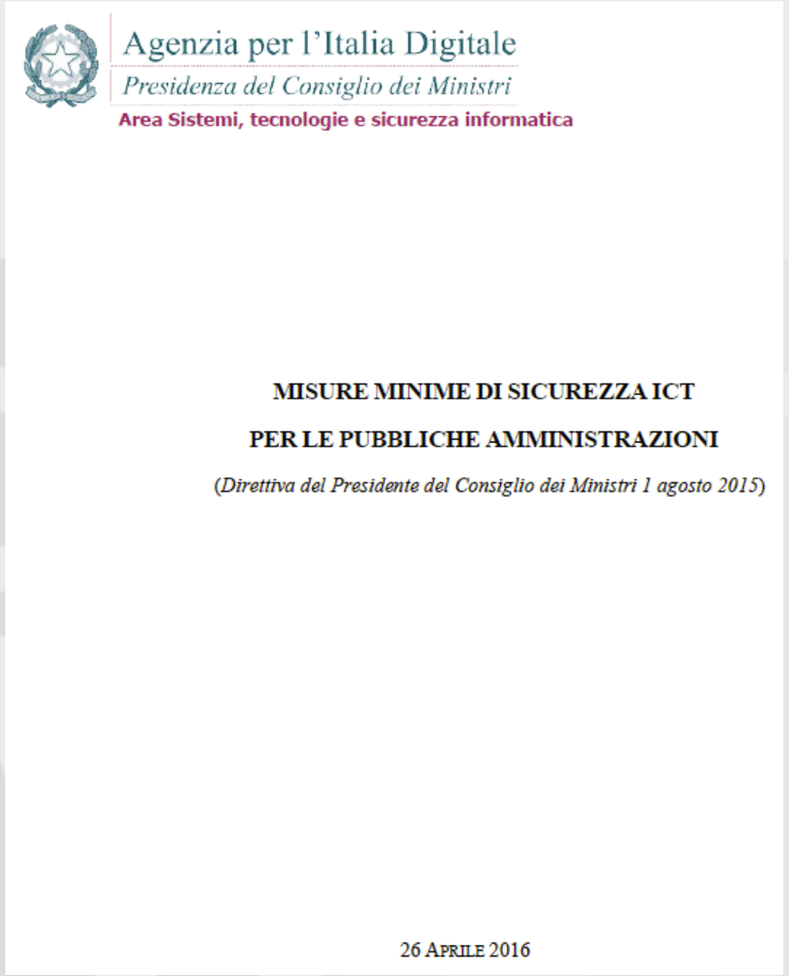
- la disposizione del GDPR va oltre la semplice adozione di specifiche misure di sicurezza, supportando la creazione di un sistema completo di gestione delle informazioni per la protezione della riservatezza, dell'integrità, della disponibilità e della resilienza dei dati personali.
- Vanno tenute sotto controllo tutte le dimensioni della sicurezza delle informazioni (riservatezza, integrità e disponibilità), richiedendo esplicitamente un processo per testare, valutare e valutare l'efficacia delle misure adottate.

Framework nazionale per cybersecurity



- Per offrire alle organizzazioni un approccio omogeneo per affrontare la cyber security, al fine di ridurre il rischio legato alla minaccia cyber
- L'approccio è legato a una analisi del rischio e non a standard tecnologici
- Si fornisce una contestualizzazione per Piccole-Medie Imprese, ovvero una contestualizzazione per tipologia di azienda quindi indipendente dal settore di business
- Ci sono suggerimenti su come utilizzare il Framework per una grande impresa

AgID Basic Security Controls (ABSC)


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Sistemi, tecnologie e sicurezza informatica

MISURE MINIME DI SICUREZZA ICT

PER LE PUBBLICHE AMMINISTRAZIONI

(Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)

26 APRILE 2016

- prende le mosse dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC "CIS Critical Security Controls for Effective Cyber Defense" nella versione 6.0 di ottobre 2015
- viene indicato l'identificatore della Subcategory del Framework Core del Framework Nazionale per la Cyber Security

Inventario degli asset come misura di sicurezza

- **ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI**
- *Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso*

- **ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI**
- *Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione*

Cloud and Big Data

ENISA has written a number of papers on Cloud Computing Security and recently focused on Big Data security.

Sub-topics:

- Cloud Security
- Big data

Cyber Security Education

ENISA is active in the area of education and awareness, using its knowledge to promote NIS skills.

Sub-topics:

- European Cyber Security Month
- EU Cyber Challenge
- NIS in Education

Data Protection

Privacy and data protection constitute core values of individuals and of democratic societies.

Sub-topics:

- Privacy by Design
- Privacy enhancing technologies
- Security of personal data
- Personal data breaches
- Online and mobile data protection

enisa *European Union Agency for Network and Information Security*

Incident Reporting

ENISA's work with Incident reporting and security regulation (Article 13a and Article 19).

Sub-topics:

- For Telcos
- For Trust Providers
- For Digital Service Providers (NIS Directive)

Step 1. Definizione del trattamento e del suo contesto

- Qual è l'operazione di elaborazione dei dati personali?
- Quali sono i tipi di dati personali trattati?
- Qual è lo scopo del trattamento?
- Quali sono i mezzi utilizzati per il trattamento dei dati personali?
- Dove avviene il trattamento dei dati personali?
- Quali sono le categorie di soggetti dei dati?
- Quali sono i destinatari dei dati?
- Rispondendo a queste domande, si deve prendere in considerazione le varie fasi dell'elaborazione dei dati (raccolta, archiviazione, utilizzo, trasferimento, eliminazione, ecc.) ed i loro parametri successivi.

Step 2. Comprensione e valutazione dell'impatto

- In questa fase l'organizzazione deve valutare il potenziale impatto sui diritti e le libertà delle persone che un incidente di sicurezza (correlato al sistema di elaborazione dei dati) potrebbe comportare.
- L'incidente di sicurezza può essere associato a qualsiasi tipo di violazione della riservatezza, integrità o disponibilità dei dati personali.
- Va notato che, a causa della natura ad hoc e della varietà dell'elaborazione dei dati personali, può essere utilizzato solo un **approccio qualitativo**, basato sulla comprensione generale (da parte dell'organizzazione) della sua specifica operazione di elaborazione dei dati.

Step 3. Definizione di possibili minacce e valutazione della loro probabilità

- Lo scopo è comprendere le minacce relative all'ambiente generale dell'elaborazione dei dati personali (esterni o interni) e valutarne la loro probabilità (probabilità di minaccia).
- Esempi di possibili minacce (ai dati personali):
  - Un utente malintenzionato inserisce codice nel form di un sito Web, con l'obiettivo di ottenere l'accesso ai dati personali memorizzati nel sistema
  - Un dipendente ruba i file di dati personali dal sistema interno.
  - Un attaccante esegue un attacco man-in-the-middle per intercettare le comunicazioni elettroniche.
  - Il dipendente di un ospedale (intenzionalmente o accidentalmente) modifica un parametro critico nella cartella clinica di un paziente.
  - A causa di un'interruzione di corrente, il sistema IT del database dei clienti non funziona.
  - Un'unità flash USB con file di dati personali viene persa in transito da un appaltatore

Step 3. Definizione di possibili minacce e valutazione della loro probabilità

- Per semplificare questo processo, sono state definite una serie di domande di valutazione che mirano a sensibilizzare sull'ambiente di elaborazione dei dati (che è chiaramente rilevante per le minacce).
- Si riferiscono a quattro dimensioni principali di questo ambiente (aree di valutazione), vale a dire:
  1. Risorse di rete e tecniche (hardware e software)
  2. Processi / procedure relativi all'operazione di elaborazione dei dati
  3. Diverse parti e persone coinvolte nell'operazione di elaborazione
  4. Settore aziendale e scala del trattamento
- Sulla base di questa comprensione, può essere eseguita la valutazione della probabilità di occorrenza della minaccia per ciascuna delle aree di valutazione
- Tuttavia potrebbero essere necessari dei fattori aggiuntivi, e quindi aree di valutazione, da prendere in considerazione dall'organizzazione, seguendo le specificità del suo ambiente di elaborazione dei dati personali

Step 4. Valutazione del rischio

- Dopo aver valutato l’impatto dell’operazione di trattamento dei dati personali e la relativa probabilità di minaccia, è possibile effettuare una valutazione finale del rischio

- Indipendentemente dal risultato finale di questo esercizio, l’organizzazione dovrebbe sentirsi libera di adeguare il livello di rischio ottenuto, tenendo conto delle caratteristiche specifiche dell'operazione di trattamento dei dati (che sono mancate durante il processo di valutazione) e fornendo un'adeguata giustificazione per tale adeguamento

Step 5. Misure di sicurezza

- A seguito della valutazione del livello di rischio, si può procedere alla selezione di adeguate misure di sicurezza per la protezione dei dati personali.
- Le linee guida ENISA considerano due ampie categorie di misure (organizzative e tecniche), ulteriormente suddivise in sottocategorie specifiche.
- Sotto ogni sottocategoria vengono presentate le misure per livello di rischio
  - Per raggiungere la scalabilità, si presume che tutte le misure descritte sotto il livello basso (verde) siano applicabili a tutti i livelli.
  - Allo stesso modo, le misure presentate sotto il livello medio (giallo) sono applicabili anche ad alto livello di rischio.
  - Le misure presentate sotto il livello alto (rosso) non sono applicabili a nessun altro livello di rischio.
- Va notato che l'abbinamento di misure a specifici livelli di rischio non dovrebbe essere percepito come assoluto. A seconda del contesto del trattamento dei dati personali, l'organizzazione può considerare l'adozione di misure aggiuntive, anche se sono assegnate a un livello di rischio più elevato.

GRUPPO DI MISURE ORGANIZZATIVE	CONTROLLI RILEVANTI rif. ISO/IEC 27001: 2013	
Politica di sicurezza e procedure per la protezione dei dati personali	A.5 Security policy	Poltica di sicurezza
Ruoli e responsabilità	A.6.1.1 Information security roles and responsibilities	Ruoli e responsabilità per la sicurezza delle informazioni
Politica di controllo degli accessi	A.9.1.1 Access control policy	Politica di controllo degli accessi
Gestione di risorse / asset	A.8 Asset management	Gestione degli asset
Gestione del cambiamento	A.12.1 Operational procedures and responsibilities	Procedure operative e responsabilità
Responsabili del trattamento	A.15 Supplier relationships	Relazioni con i fornitori
Gestione degli incidenti / Violazioni dei dati personali	A.16 Information security incident management	Gestione degli incidenti relativi alla sicurezza delle informazioni
Business continuity (Continuità operativa)	A.17 Information security aspects of business continuity management	Aspetti della gestione della continuità operativa relativi alla sicurezza delle informazioni
Riservatezza da parte del personale	A.7 Human resource security	Sicurezza delle risorse umane
Formazione	A.7.2.2 Information security awareness, education and training	Consapevolezza, formazione e addestramento per la sicurezza delle informazioni

GRUPPO DI MISURE TECNICHE	CONTROLLI RILEVANTI rif. ISO/IEC 27001: 2013	
Controllo degli accessi e autenticazione	A.9 Access control	Controllo deli accessi
Registrazione dei log e monitoraggio	A.12.4 Logging and monitoring	Registrazione dei log e monitoraggio
Sicurezza di server / database	A.12 Operations security	Sicurezza operativa
Sicurezza delle postazioni di lavoro	A.14.1 Security requirements of information systems	Requisiti di sicurezza dei sistemi informativi
Sicurezza di rete e delle comunicazioni	A.13 Communications Security	Sicurezza delle comunicazioni
Back-up (Salvataggi di sicurezza)	A.12.3 Back-Up	Back-up
Dispositivi mobili / portatili	A.6.2 Mobile devices and teleworking	Dispositivi mobili e telelavoro
Sicurezza nell'intero ciclo di vita dell'applicazione	A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes	Gestione delle vulnerabilità tecniche & Sicurezza nei processi di sviluppo ed assistenza
Cancellazione/distruzione dei dati	A.8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment	Smaltimento dei supporti & Smaltimento sicuro o riutilizzo delle attrezzature
Sicurezza fisica	A.11 – Physical and environmental security	Sicurezza fisica ed ambientale