Le analisi dei rischi nel GDPR

Giancarlo Butti

Giancarlo Butti

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni.

Oltre 150 corsi e seminari tenuti presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, AIIA, UNIVERSITA DI MILANO, CEFRIEL, ABI…; già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei.

Ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate.

Ha pubblicato 25 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 23 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT.

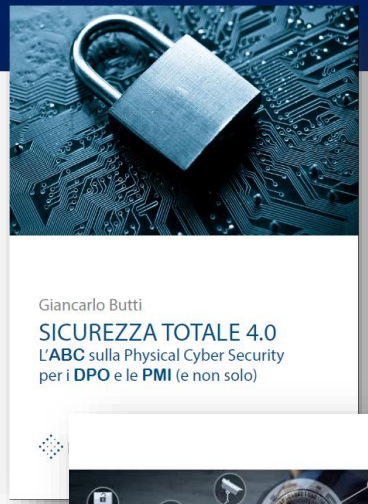
Socio e già proboviro di AIEA è socio del CLUSIT e del BCI.

Partecipa a numerosi gruppi di lavoro.

Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

Note sul copyright

Alcuni testi derivano da queste mie pubblicazioni



Indice

L’analisi dei rischi ai sensi del GDPR

- Aspetti particolari:
  - Non è la DPIA
  - È obbligatoria
  - Non riguarda gli interessati, ma le persone fisiche
  - Non riguarda i rischi del Titolare e quindi le tradizionali tecniche di analisi del rischio (ad esempio ai sensi della 27001) non sono conformi
  - Non comprende solo la sicurezza:
    - aspetti di sicurezza (art. 32)
    - aspetti di conformità (art. 24)
    - rispetto dei principi (art. 25)

Aspetti di sicurezza

	Ejemplos de posibles daños físico, material o moral
Despreciable: *Los interesados no se verán prácticamente afectados o encontrarán alguna pequeña inconveniencia*	▪ Molestias o irritación. ▪ Se incumplen obligaciones materiales sin perjuicios relevantes. ▪ No se priva de los derechos y libertades.
Limitado: *Los interesados podrán encontrar inconveniencias no significativas*	▪ Estrés o padecimientos físico menores. ▪ Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos. ▪ Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
Significativo: *Los interesados encontrarán consecuencias significativas, que deberían poder superar sin dificultades serias.*	▪ Empeoramiento del estado de salud o agresiones físicas. ▪ Apropiación indebida de fondos, pérdida del empleo o incumplimiento de obligaciones materiales con perjuicios económicos relevantes. ▪ Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.
Máximo: *Los interesados encontrarán consecuencias significativas o incluso irreversibles, que podrán no llegar a superarse.*	▪ Agresiones físicas con consecuencias irreparables. ▪ Asunción de una deuda inafrontable, imposibilidad de volver a trabajar o incumplimiento de obligaciones materiales con perjuicios económicos irreparables. ▪ Se agrede significativamente contra los derechos y libertades de los interesados, por ejemplo, padecimiento psicológico con consecuencias a largo plazo o irreparables por la divulgación de datos sensibles.

Analisi dei rischi

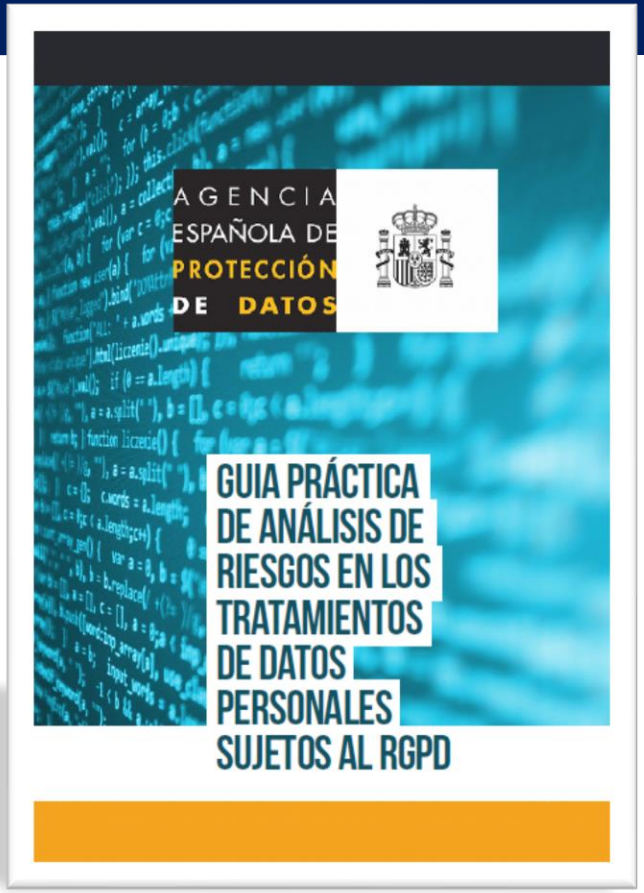
Principales riesgos potenciales identificados

Protección de de la información:

- Integridad de los datos personales:
- Modificación o alteración de datos personales no intencionada
- Disponibilidad de los datos personales:
- Pérdida o borrado no intencionado de datos personales
- Confidencialidad de los datos personales:
- Acceso no autorizado a los datos personales

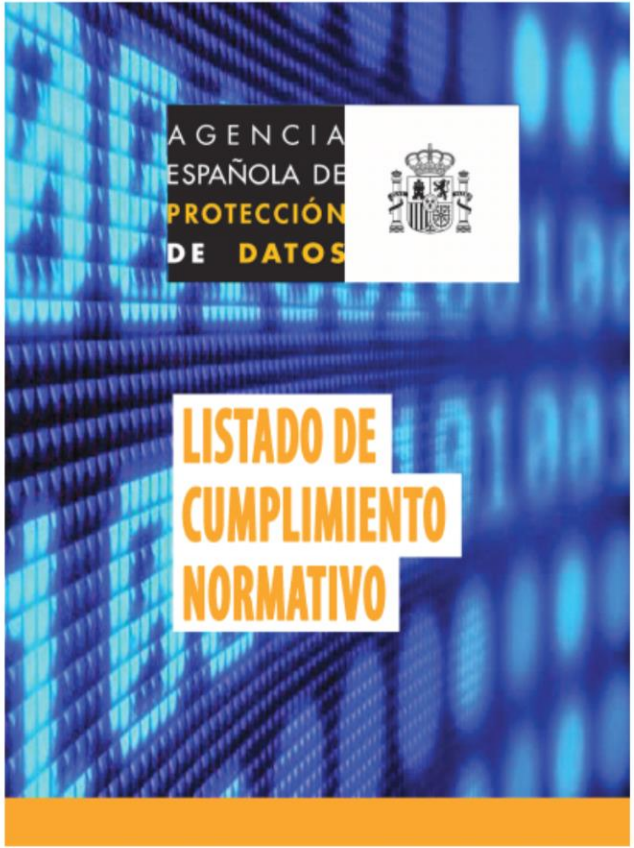
Riesgos asociados al cumplimiento:

- Garantizar el ejercicio de los derechos de los interesados:
- Ausencia de procedimientos para el ejercicio de derechos
- Garantizar los principios relativos al tratamiento:
- Ausencia de legitimidad para el tratamiento de los datos personales
- Tratamiento ilícito de datos personales



Aspetti di conformità

PRINCIPIOS RELATIVOS AL TRATAMIENTO	
Se recogen los datos personales con fines determinados	
Se recogen los datos personales con fines explícitos	
Se recogen los datos personales con fines legítimos	
Se tratan ulteriormente de manera incompatible con otros fines	
Los datos personales se mantienen exactos	
Se mantienen actualizados	
Se rectifican los datos personales inexactos respecto de la finalidad	
Se suprimen los datos personales inexactos respecto de la finalidad	
Se mantienen durante más tiempo del necesario respecto de la finalidad	
Se tratan con fines de archivo en interés público	
Se tratan con fines de investigación científica	
Se tratan con fines históricos	
Los datos personales se tratan con fines estadísticos	
Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos	
Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos	
Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental	
Se mantiene la trazabilidad de los fines del tratamiento	



Aspetti legati ai principi

Articolo 5

Principi applicabili al trattamento di dati personali

1. I dati personali sono: (C39)

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ***(«liceità, correttezza e trasparenza»)***;

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ***(«limitazione della finalità»)***;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ***(«minimizzazione dei dati»)***;

Aspetti legati ai principi

Articolo 5 - Principi applicabili al trattamento di dati personali

d) 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»)***;

e) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ***(«limitazione della conservazione»)***;

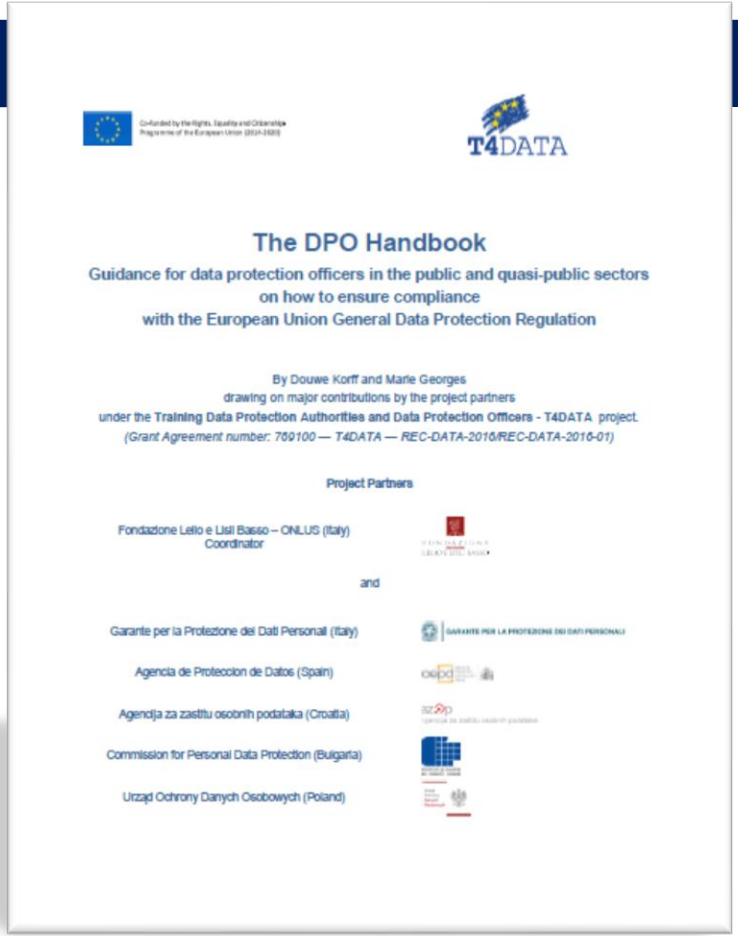
Aspetti legati ai principi

Articolo 5 - Principi applicabili al trattamento di dati personali

f) 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»)***.

DPO Handbook

However, it should be noted that **“risks to the rights and freedoms of natural persons” do not flow only from data breaches**. The



T4DATA

The DPO Handbook

Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation

By Douwe Korff and Marie Georges
drawing on major contributions by the project partners
under the Training Data Protection Authorities and Data Protection Officers - T4DATA project.
(Grant Agreement number: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

Project Partners

Fondazione Lelio e Lisli Basso – ONLUS (Italy)
Coordinator

and

Garante per la Protezione dei Dati Personali (Italy)

Agencia de Proteccion de Datos (Spain)

Agencija za zastitu osobnih podataka (Croatia)

Commission for Personal Data Protection (Bulgaria)

Urząd Ochrony Danych Osobowych (Poland)

Indice

Non solo sicurezza

In questo corso ci occupiamo principalmente di sicurezza, ma l'analisi dei rischi è richiesta anche dagli artt. 24 e 25 che non si occupano solo di sicurezza.

Processo di valutazione della sicurezza

Il processo di valutazione della sicurezza comprende:

- la verifica dell'attività di valutazione effettuata dal Titolare al fine di determinare il livello di rischio per una o più finalità di trattamento
- la verifica delle misure di sicurezza implementate
- la verifica nel dettaglio, della implementazione e gestione della singola misura di sicurezza
- la verifica di coerenza fra il livello di rischio individuato e le misure di sicurezza adottate

Processo di valutazione della sicurezza

Il requisito normativo:

- È stato implementato?
- È conforme?
- È attuato?

Indice

La sicurezza nel GDPR

Articolo *25* ***Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita***

1.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*** *costituiti dal trattamento, 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, quali la pseudonimizzazione, volte ad attuare in modo efficace i* ***principi di protezione dei dati****, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

La sicurezza nel GDPR

Articolo *5* ***Principi applicabili al trattamento di dati personali****:*

1.I ***dati personali*** *sono:*

…

f) 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”).*

La sicurezza nel GDPR

Articolo *32* ***Sicurezza del trattamento***

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;

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

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

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.

Indice

Oggetto di tutela

Articolo *5* ***Principi applicabili al trattamento di dati personali****:*

1.I ***dati personali*** *sono:*

…

f) 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”).***

La sicurezza nel D.lgs 196/03 old

Art. 31. Obblighi di sicurezza

1. I ***dati personali oggetto di trattamento sono custoditi e controllati****, 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, mediante l'adozione di idonee e preventive misure di sicurezza,* ***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***

Oggetto di tutela

Art. 5 GDPR	Art. 31 D.Lgs.
Trattamenti non autorizzati Trattamenti illeciti Perdita accidentale Distruzione accidentale Danno accidentali	Accesso non autorizzato Trattamento non consentito Trattamento non conforme alle finalità della raccolta Distruzione anche accidentale Perdita anche accidentale

Oggetto di tutela i **DATI PERSONALI**

Oggetto di tutela

Articolo 24 - ***Responsabilità del titolare del trattamento (C74-C78)***

1. 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.*

Oggetto di tutela

Articolo *25* ***Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita***

1.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*** *costituiti dal trattamento, 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, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

Oggetto di tutela

Articolo *32* ***Sicurezza del trattamento***

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:*

…

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.***

Oggetto di tutela

Gli articoli 24, 25 e 32 hanno invece come oggetto di tutela

I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE.

Non i **DATI I PERSONALI ma I DIRITTI E LE LIBERTÀ**

Non degli **INTERESSATI** (data subject), ma delle **PERSONE FISICHE** (natural person)

Oggetto di tutela

Articolo 35 Valutazione d'impatto sulla protezione dei dati

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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*

Articolo 33 Notifica di una violazione dei dati personali all'autorità di controllo

1.In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un ***rischio per i diritti e le libertà delle persone fisiche.*** *Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*

Oggetto di tutela

Una banca tratta i dati non solo dei propri clienti, sia persone fisiche, sia persone giuridiche (quest'ultime non tutelate dal GDPR), ma anche di tutti i soggetti, fra cui persone fisiche, che ricevono o dispongono bonifici nei confronti dei clienti.

In caso di accesso illegale ai dati di un conto corrente, ad esempio di una clinica che tratta malattie particolari, i dati dei clienti della clinica potrebbero essere diffusi con conseguenze anche gravi (ad esempio discriminazioni).

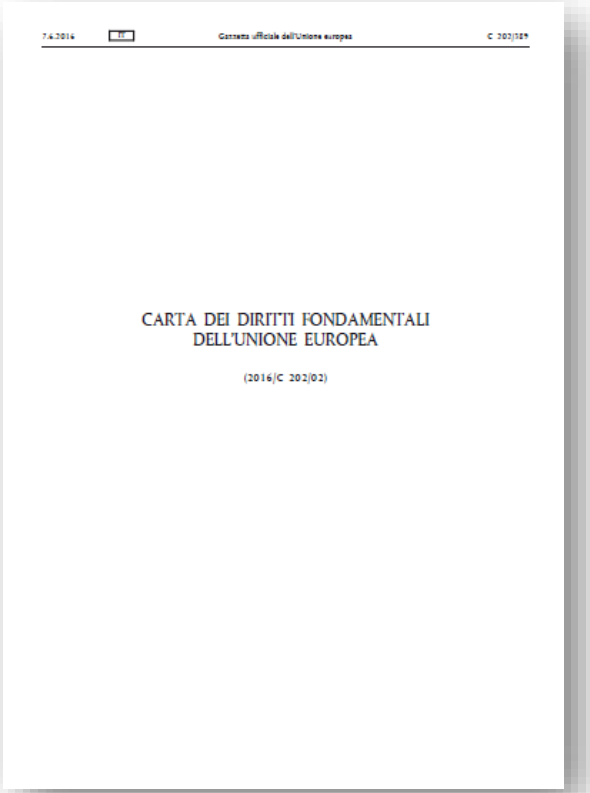
Tali soggetti, non necessariamente sono degli interessati, in quanto non è detto che siano soggetti identificabili da parte della banca, ma potrebbero esserlo da parte di altri soggetti.

Oggetto di tutela

Ancor più significativo è il caso, realmente accaduto, di violazione di un sito di incontri fra persone sposate.

Nel caso specifico la diffusione dei dati degli iscritti al sito ha portato a molti divorzi ed anche suicidi. È evidente che chi ha subito una violazione dei propri diritti non sono soltati i soggetti i cui dati sono stati violati, ma anche i rispettivi coniugi e familiari.

Oggetto di tutela


7.6.2016 IT Gazzetta ufficiale dell'Unione europea C 202/389

CARTA DEI DIRITTI FONDAMENTALI
DELL'UNIONE EUROPEA

(2016/C 202/02)

*2.1.2 Volte ad attuare i principi di protezione dei dati in modo efficace e tutelare **i diritti e le libertà degli interessati***

- diritti e le libertà fondamentali **delle persone fisiche** → Carta dei diritti fondamentali dell'UE
  - TITOLO I DIGNITÀ
  - TITOLO II LIBERTÀ
  - TITOLO III UGUAGLIANZA
  - TITOLO IV SOLIDARIETÀ
  - TITOLO V CITTADINANZA
  - TITOLO VI GIUSTIZIA

Oggetto di tutela

I diritti e le libertà delle persone fisiche

Parere 218/14 del WP29:

- *…Risks, which are related to potential negative impact on the data subject's rights, freedoms and interests, should be determined taking into consideration specific objective criteria (…).*
- *In the context referred to above, the scope of "the rights and freedoms" of the data subjects primarily concerns the right to privacy* ***but may also involve other fundamental rights*** *such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.*

Oggetto di tutela

I diritti e le libertà delle persone fisiche

(75) 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…***

Indice

Analisi del rischio e GDPR

FUORI PERIMETRO

Rischio del Titolare
Rischio derivante da violazione di dati di persone non fisiche (art. 130)

- Interruzione, alterazione o limitazione nella produzione o erogazione dei servizi
- Perdite economiche (dirette, indirette, consequenziali)
- Perdita della clientela
- Rischi reputazionali (danni di immagine)
- Rischi legali, contrattuali
- Rischio sanzionatorio

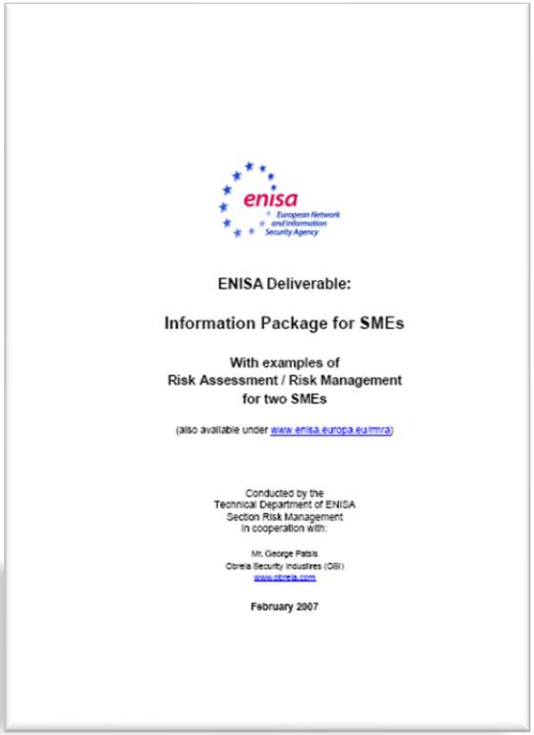
OBBLIGATORIA

Rischio derivante da violazione di dati di persone fisiche

Diritti e libertà fondamentali

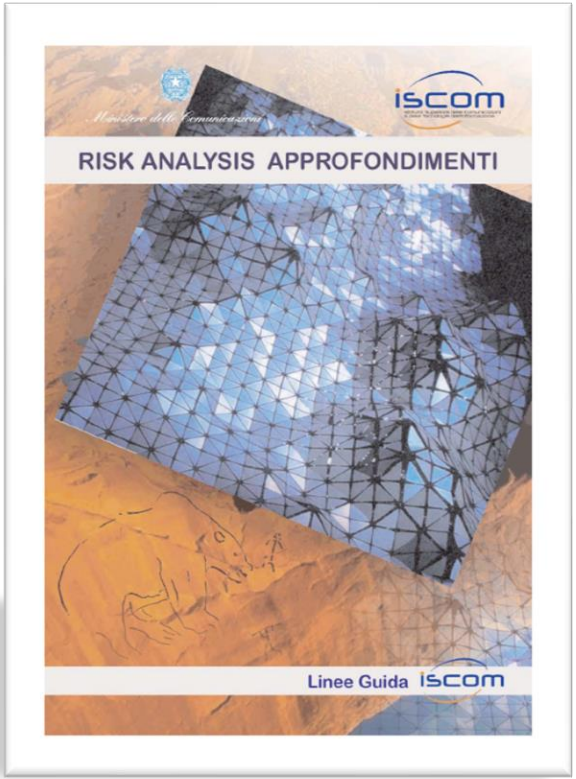
DATI PERSONALI

Analisi del rischio



Austrian IT Security Handbook
Cramm
Dutch A&K analysis
Ebios
ISF methods
ISO/IEC IS 13335-2
(ISO/IEC IS 27005)
ISO/IEC IS 17799
ISO/IEC IS 27001
ISO 31010
IT-Grundschutz
Marion (replaced by Mehari)
Mehari
Octave
SP800-30 (NIST)

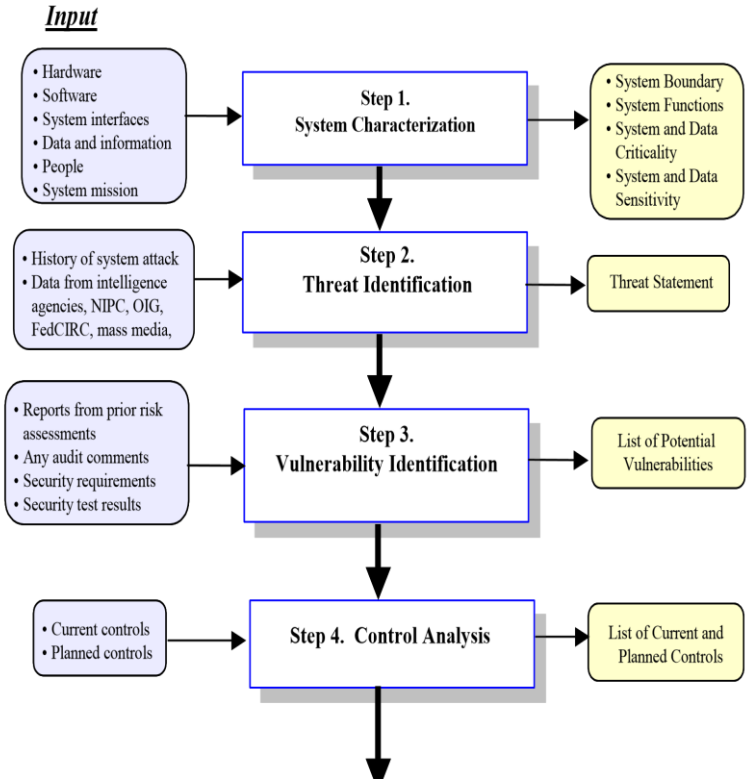
Analisi del rischio



AS/NZS 4360:2004 RISK MANAGEMENT
BSA – Baseline Security Assessment
Ce.TRA - Continuous e.Business Threat and Risk Analysis
CRAMM
Defender Manager
EBIOS
ERAM - Enterprise Risk Assessment and Management
FIRM (Fundamental Information Risk Management)
ISA – Information Security Assessment
ISO/IEC 21827 - System Security Engineering, Capability Maturity Model
NET.RISK
NORA - Network Oriented Risk Analysis methodology
OCTAVE® - Operationally Critical Threat, Asset, and Vulnerability EvaluationSM
OSSTMM – Open Source Security Testing Methodology Manual
PRA – Psychological Risk Assessment
RAF - Risk Analyis Facility
RISKWATCH (versione per l'Italia)
SARA - Simple to Apply Risk Analysis
SPRINT – Simplified Process for Risk Identification
SSM - Scalable Security Model

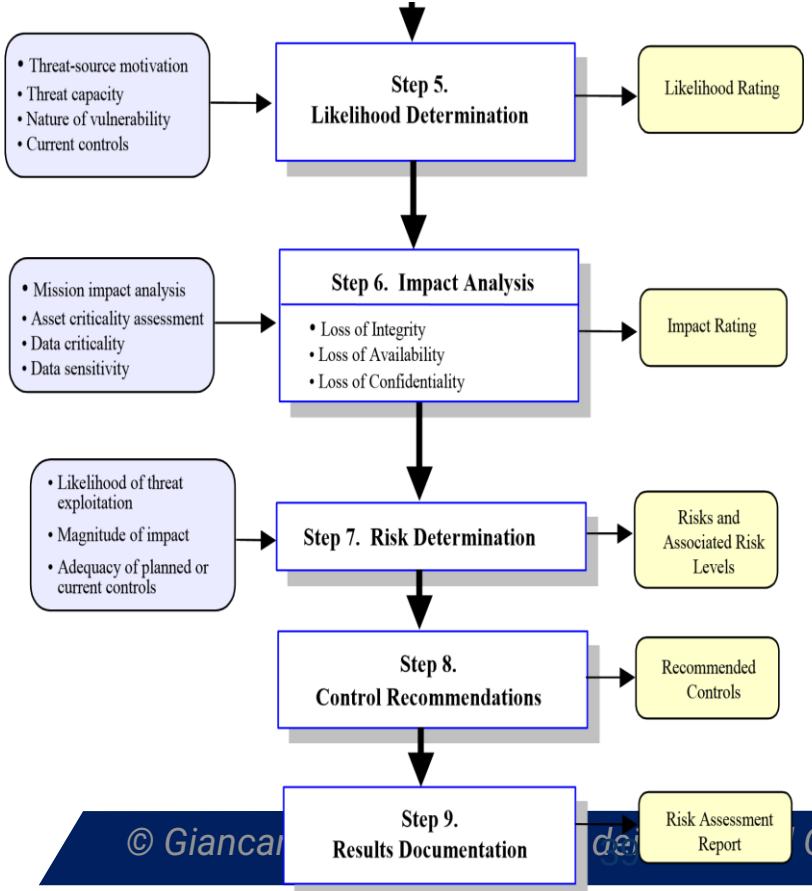
Analisi del rischio

Risk Management Guide for Information Technology Systems (NIST)

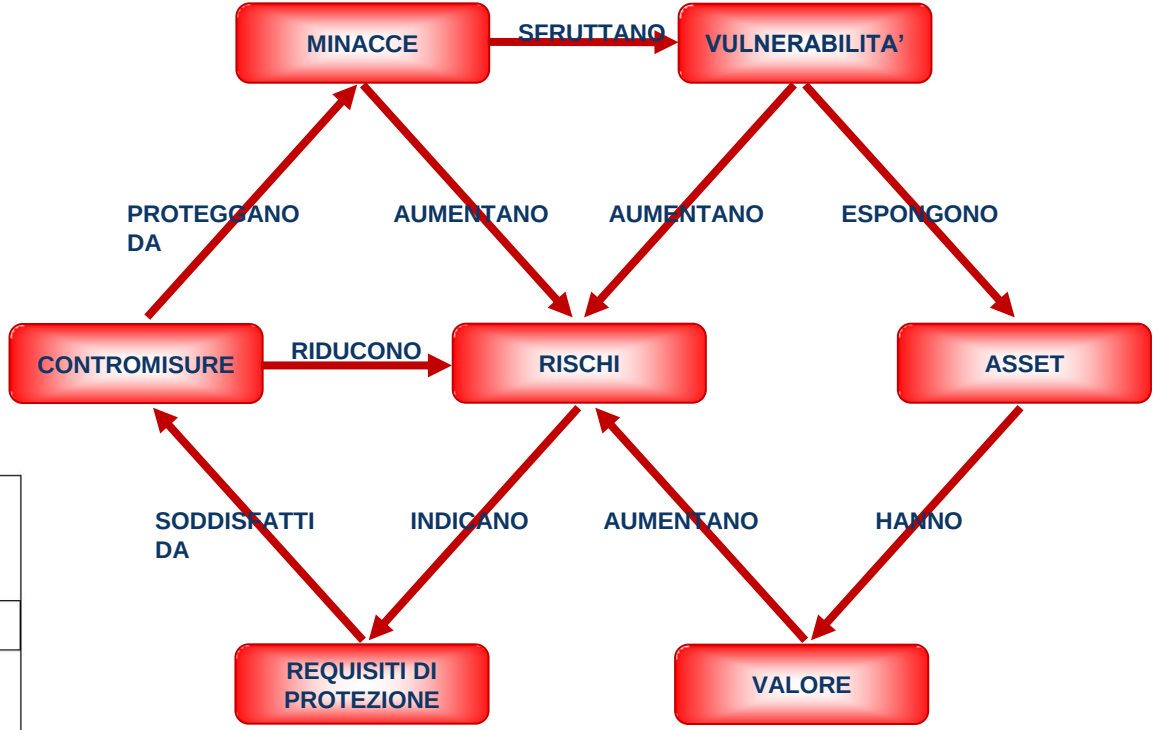


Analisi del rischio

Risk Management Guide for Information Technology Systems (NIST)



Analisi del rischio



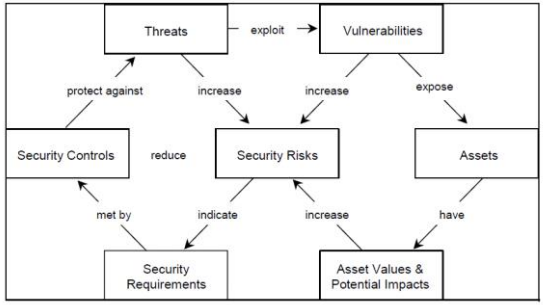


Figure 3: Risk concept relationship
(Source: Australian Standard Handbook of Information Security Risk Management – HB231:2000)

Analisi del rischio

La Linea Guida ISCOM – RISK ANALYSIS APPROFONDIMENTI descrive i seguenti elementi come caratteristici delle varie metodologie di analisi dei rischi, qui sintetizzati:

Rischio

Il rischio è l'eventualità che una ***minaccia*** possa trasformarsi realmente in ***danno***, comportando così un determinato ***impatto***.
Il "rischio potenziale" o "intrinseco" è il livello di rischio a prescindere dalle contromisure, mentre quello "effettivo" o "residuo" tiene conto di quelle implementate.

Minaccia

La minaccia viene definita come un evento di natura dolosa o accidentale che, sfruttando una ***vulnerabilità*** del sistema, potrebbe provocare un ***danno***.

Analisi del rischio

Vulnerabilità

Rappresenta una debolezza intrinseca o dovuta a condizioni di esercizio o assenza di controlli, che può essere sfruttata da una ***minaccia*** per arrecare ***danno***.

Danno

Il danno è la conseguenza (spesso identificata da una perdita di riservatezza, integrità e/o disponibilità dell'informazione) del verificarsi di un ***rischio*** o dell'attuarsi di una ***minaccia***.
A volte viene distinto il danno in "tangibile" (danno monetario) e "intangibile" (danno immateriale).

Impatto *(*sinonimo spesso di danno)
Le possibili definizioni sono:
misura o entità del ***danno***
effetto sull'azienda del verificarsi di una **minaccia** (effetto reale del ***danno*** sul sistema).

Analisi del rischio

- L’approccio **QUALITATIVO** prevede una valutazione del rischio su una scala qualitativa (ad esempio alto, medio, basso).
- L’approccio **QUANTITATIVO**, invece, riconduce le valutazioni ad un valore numerico puntuale, spesso inteso come la perdita economica derivante dal verificarsi del rischio. Si tratta di un approccio più difficile ed oneroso del primo perché costringe ad un censimento ed una valorizzazione degli asset e ad una valorizzazione delle perdite che si avrebbero in caso di incidente.
- L’approccio **SEMI QUANTITATIVO** è un compromesso fra i primi due, nel quale le valutazioni sono effettuate in termini qualitativi e, successivamente, trasformate in numeri per poterle elaborare attraverso algoritmi di calcolo, come se si trattasse di valutazioni quantitative.

Analisi del rischio

Analisi	Fase	Possibile errore / limitazione	Possibile rimedio
Qualitativa	Raccolta dati	Errori di valutazione Stime soggettive	**Introduzione di scale di riferimento per probabilità ed impatti**
	Elaborazione	Tabelle empiriche basate sull'associazione Impatto-Probabilità, possibili errori grossolani.	**Passare ad un metodo quantitativo**
	Utilizzo	I rischi sono visti uno per uno. La reportistica abbastanza limitata.	**Passare ad un metodo quantitativo**
Quantitativa	Raccolta dati	Errore di valutazione Valutazioni soggettive (medesima precisione del metodo qualitativo)	**Introduzione di scale di riferimento per probabilità ed impatti**
	Elaborazione	Calcolo matematicamente corretto del prodotto: probabilità-impatto. Non vengono introdotte "distorsioni" rispetto ai dati in input.	-.
	Utilizzo	Sono disponibili dati che, pur approssimati, rappresentano il rischio in termini anche quantitativi e quindi utilizzabili per ulteriori analisi / sintesi ed elaborazioni in ottica di governo dei rischi.	-

Tipi di scala

Indice	Probabilità annuale		Impatto evento singolo	
4	**Molto frequente**	*100 volte / anno*	**Estremo**	1.000.000€
3	**Frequente**	*10 volte / anno*	**Molto alto**	100.000€
2	**Poco frequente**	*1 volta / anno*	**Alto**	10.000€
1	**Raro**	*ogni 10 anni*	**Basso**	1.000€

x 10
x 10
x 10

Relazione fra misure

Rischio è una funzione di PROBABILITA’ e IMPATTO

La relazione cambia in funzione del **tipo di scala** utilizzata

Nel caso di scala lineare la relazione è un prodotto :

RISCHIO = PROBABILITA’ x IMPATTO

Nel caso di scala logaritmica la relazione è la somma :

RISCHIO = PROBABILITA’ + IMPATTO

Trattamento del rischio convenzionale

- Ridurre il rischio (contromisure)
  - Ridurre l'impatto
  - Ridurre la probabilità
- Eliminare il rischio
- Trasferire il rischio
  - Assicurativo
  - Non assicurativo
- Accettare il rischio

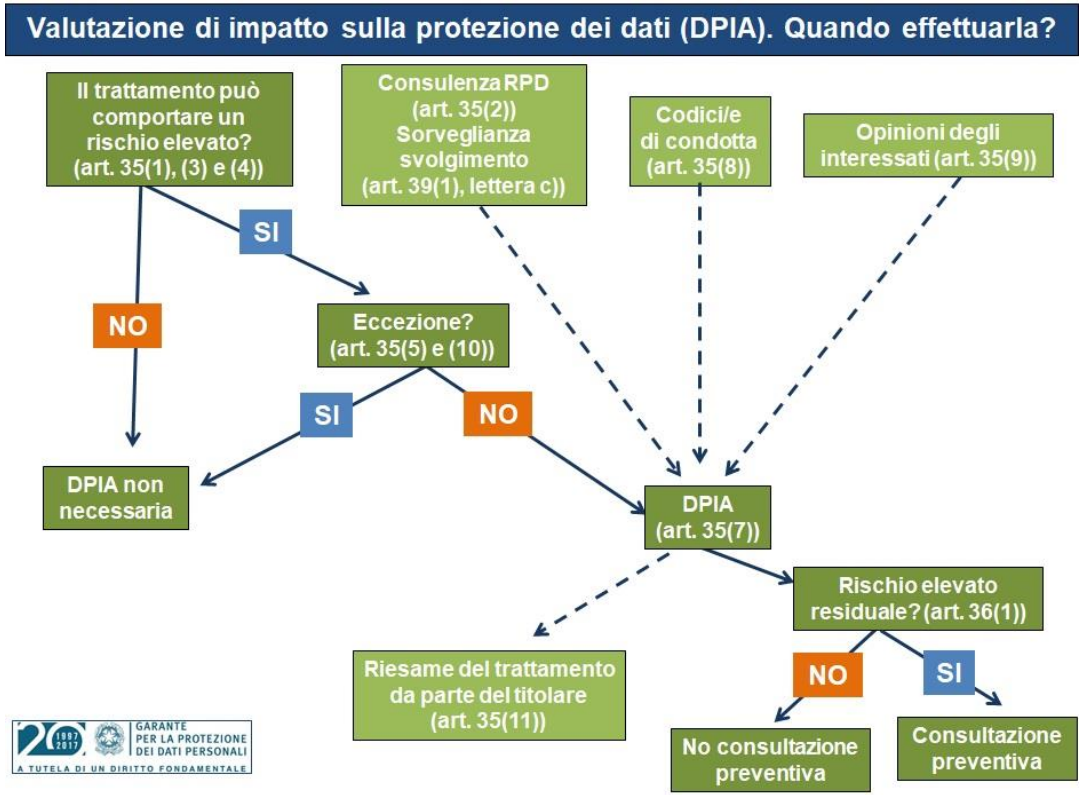
Da Sicurezza Totale, Giancarlo Butti, ITER

Trattamento del rischio GDPR

- Non è un rischio del Titolare ma delle persone fisiche che possono subire danni dal trattamento
    - Non può essere accettato
    - Non può essere trasferito
- Nel caso in cui il rischio sia elevato è necessario effettuare una DPIA
    - La valutazione in merito al fatto che il rischio sia elevato deriva:
        - Da un'analisi del rischio (artt. 24, 25, 32)
        - In quanto definito dalla normativa

Da Sicurezza Totale, Giancarlo Butti, ITER

Trattamento del rischio nel GDPR



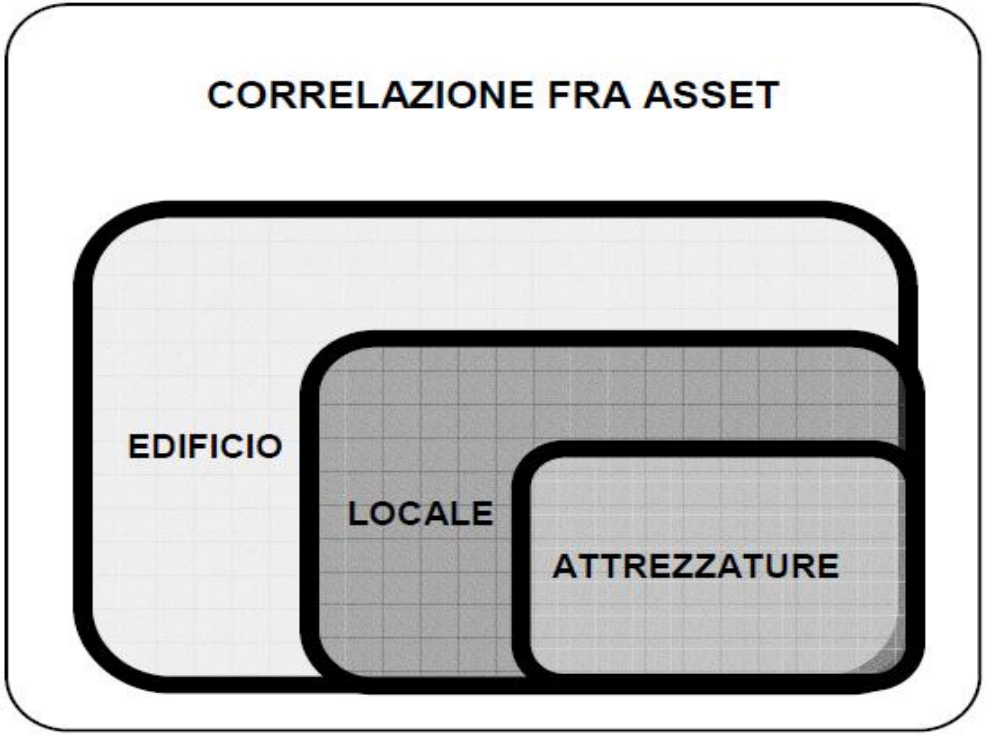
Il ciclo dell’analisi del rischio

L’analisi del rischio non è un’attività che viene svolta solo una volta, ma necessita di revisione continua. Infatti possono variare tutti gli elementi che entrano nella valutazione; in particolare:

- gli asset
- la correlazione fra asset
- le minacce/vulnerabilità
- la probabilità che la minaccia si manifesti
- la valorizzazione dei rischi
- le misure di sicurezza in atto
- il rapporto costo/benefici

Da Sicurezza Totale, Giancarlo Butti, ITER

Limiti dei modelli di analisi del rischio



La maggior parte dei modelli di analisi dei rischi non effettua una correlazione fra gli asset

Da Sicurezza Totale, Giancarlo Butti, ITER

Particolarità del GDPR

- L’oggetto su cui si effettua la valutazione di impatto sono i diritti e le libertà delle persone fisiche
- L’oggetto su cui si effettua la valutazione della probabilità sono i dati personali

Particolarità del GDPR

- La **PROBABILITÀ** è di norma valutata secondo i seguenti criteri:
  - azione volontaria
    - appetibilità del bene
    - vulnerabilità rispetto alle varie minacce
    - determinazione dell'attaccante
  - azione involontaria, evento naturale

    vulnerabilità rispetto alle varie minacce

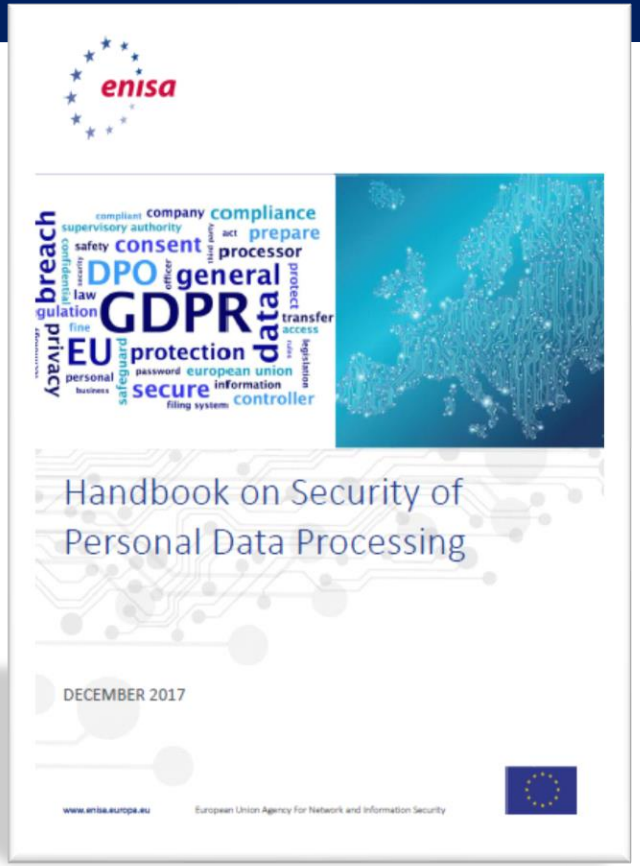
Particolarità del GDPR

- Tuttavia:
  - i dati personali potrebbero non essere l'oggetto di un attacco, ma essere coinvolti sono incidentalmente. Diventa quindi ulteriormente difficile valutare la probabilità di accadimento di un evento
  - Il Titolare non ha visibilità del numero delle persone fisiche che possono essere coinvolte (può conoscere al limite solo gli interessati)

Particolarità del GDPR

- Nella valutazione dell'**IMPATTO** il Titolare non ha reale visibilità di tutti i soggetti coinvolti (le persone fisiche) in quanto di norma ha solo visibilità sugli interessati.

Metodologia ENISA



Metodologia ENISA

La metodologia di ENISA presenta numerosi vantaggi:

- È relativamente semplice
- È pensata per il GDPR; l'oggetto di tutela sono i diritti e le libertà delle persone fisiche
- Non necessità di mappature ulteriori rispetto a quanto il titolare ha già fatto per la compilazione dei Registri delle attività di trattamento
- La probabilità di accadimento di un evento avverso è intrinseco nell'applicazione
- Propone delle contromisure organizzate per livello di rischio

Metodologia di analisi del rischio

- **Definition of the processing operation and its context**.
- Understanding and evaluation of **impact**.
- Definition of possible threats and evaluation of their **likelihood** (threat occurrence probability).
- Evaluation of **risk** (combining threat occurrence probability and impact).

Livello di granularità

L’articolo 32.1 richiede che la valutazione delle misure di sicurezza siano valutate in base ad una serie di parametri:

- stato dell'arte e costi di attuazione delle misure di sicurezza
- **natura, oggetto, contesto e finalità del trattamento**
- rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

Livello di granularità

*(76) La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguard**o 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.*

Elementi di cui tenere conto

Stato dell’arte

→ di tenere conto degli attuali progressi compiuti dalla tecnologia disponibile sul mercato.

→ rimanere sempre aggiornati sulle opportunità e i rischi

- 20. Lo «stato dell’arte» è un concetto dinamico che non può essere definito staticamente con riguardo a un determinato momento, bensì dovrebbe essere oggetto di una valutazione continuativa nel contesto dei progressi tecnologici. Di fronte a tali progressi, un titolare può riscontrare che una misura in precedenza atta a conferire un livello di protezione adeguato ora non lo è più. Trascurare l’aggiornamento sui progressi tecnologici potrebbe, quindi, comportare una mancata osservanza dell’articolo 25.
- 21. Il criterio dello «stato dell’arte» non si applica esclusivamente alle misure tecnologiche, ma anche a quelle organizzative. La mancanza di misure organizzative adeguate può ridurre o compromettere del tutto l’efficacia di una tecnologia scelta. Possono costituire esempi di misure organizzative l’adozione di politiche interne, la formazione aggiornata in materia di tecnologia, sicurezza e protezione dei dati nonché politiche di gestione e di governance della sicurezza informatica.

Elementi di cui tenere conto

Costi di attuazione

- Il costo si riferisce alle risorse in generale, compresi il tempo e le risorse umane.

- 25. Le misure individuate devono pertanto garantire che l'attività di trattamento prevista dal titolare non comporti trattamenti di dati personali in violazione dei principi, indipendentemente dal costo di tali misure.

Elementi di cui tenere conto

Natura, ambito di applicazione, contesto e finalità del trattamento

- 28. In breve, il concetto di natura può essere inteso come le caratteristiche intrinseche del trattamento. L'ambito di applicazione fa riferimento alla dimensione e all'ampiezza del trattamento. Il contesto riguarda le circostanze nel trattamento che possono influenzare le aspettative degli interessati, mentre la finalità si riferisce agli obiettivi del trattamento.

Livello di granularità

- 1. What is the personal data processing operation?
- 2. What are the types of personal data processed?
- 3. What is the purpose of the processing?
- 4. What are the means used for the processing of personal data?
- 5. Where does the processing of personal data take place?
- 6. Which are the categories of data subjects?
- 7. Which are the recipients of the data?

Livello di granularità

Registro delle attività di trattamento

- le finalità del trattamento
- una descrizione delle categorie di interessati e delle categorie di dati personali
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1

Mappatura

- sistemi informativi e degli archivi
- collocazione

Livello di granularità

PROCESSING OPERATION DESCRIPTION	EVALUATION OF STAFF	
Personal Data Processed	First and last name, position within the SME, date of employment, employment history, technical skills, knowledge and behaviours (work performance evaluation reports)	
Processing Purpose	Assessment of the performance and professional characteristics that arise in the execution of the work	
Data Subject	Employees	
Processing Means	Human Resources IT System	
Recipients of the Data	Internal	Line Managers
Data Processor Used	In-house (no data processor)	

Livello di granularità

PROCESSING OPERATION DESCRIPTION	ORDER AND DELIVERY OF GOODS	
Personal Data Processed	Contact information (last and first name, address, telephone number) payment data (credit card, bank account information)	
Processing Purpose	Order and delivery of goods	
Data Subject	Customers	
Processing Means	Order Management system	
Recipients of the Data	External	Payment services provider
	External	Delivery services provider
	Internal	Customer Relation Management (CRM) system
	Internal	Enterprise Resource Planning (ERP) system
Data Processor Used	In-house and external parties	

Valutazione di impatto sui diritti e le libertà

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Valutazione di impatto

- Type of personal data
- Criticality of the processing operation
- Volume of the personal data processed
- Special characteristics of the data controller/processor
- Special characteristics of the data subject

Valutazione di impatto

NO	QUESTION	EVALUATION
I.1.	Please reflect on the impact that an unauthorized disclosure (loss of confidentiality) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.	☐ Low ☐ Medium ☐ High ☐ Very high
I.2.	Please reflect on the impact that an unauthorized alteration (loss of integrity) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.	☐ Low ☐ Medium ☐ High ☐ Very high
I.3.	Please reflect on the impact that an unauthorized destruction or loss (loss of availability) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.	☐ Low ☐ Medium ☐ High ☐ Very high

Valutazione di impatto

ENISA propone una valutazione dell'impatto delle violazioni di dati personali basata sulla seguente formula:

$$SE = DPC \times EI + CB$$

Valutazione di impatto

Data Processing Context (DPC): Addresses the type of the breached data, together with a number of factors linked to the overall context of processing.

Ease of Identification (EI): Determines how easily the identity of the individuals can be deduced from the data involved in the breach.

Circumstances of breach (CB): Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security of the breached data, as well as any involved malicious intent.

Valutazione di impatto

Data processing context can be adjusted according to the importance of data (simple, behavioural, financial etc.) assigned by the specific DPA

Ease of identification can take into account the reality in a given country and its legal system (public availability of personal numbers, names, addresses etc.)

Circumstances of a breach offer the highest flexibility to adjust the final result to the needs of a DPA

Valutazione di impatto

Table 1: Data Processing Context (DPC)		Score
Simple data	Eg. biographical data, contact details, full name, data on education, family life, professional experience, etc.	
	Preliminary basic score: when the breach involves ''simple data'' and the controller is not aware of any aggravating factors.	1
	The DPC score could be increased by 1, e.g. when the volume of "simple data" and/or the characteristics of the controller are such that certain profiling of the individual can be enabled or assumptions about the individual's social/financial status can be made.	2
	The DPC score could be by 2, e.g. when the "simple data" and/or the characteristics of the controller can lead to assumptions about the individual's health status, sexual preferences, political or religious beliefs.	3
	The DPC score could be increased by 3, e.g. when due to certain characteristics of the individual (e.g. vulnerable groups, minors), the information can be critical for their personal safety or physical/psychological conditions.	4
Behavioural data	Eg. location, traffic data, data on personal preferences and habits, etc.	
	Preliminary basic score: when the breach involves ''behavioural data'' and the controller is not aware of any aggravating or lessening factors.	2
	The DPC score could be decreased by 1, e.g. when the nature of the data set does not provide any substantial insight to the individual's behavioural information or the data can be collected easily (independently from the breach) through publicly available sources (e.g. combination of information from web searches).	1
	The DPC score can be increased by 1, e.g. when the volume of "behavioural data" and/or the characteristics of the controller are such that a profile of the individual can be created, exposing detailed information about his/her everyday life and habits.	3
	The DPC score can be increased by 2, e.g. if a profile based on individual's sensitive data can be created.	4

Valutazione di impatto

Increasing factors

- The volume of the breached data (for the same individual)
- Special characteristics of the data controller
- Special characteristics of the individuals

Decreasing factors

- Invalidity/inaccuracy of the data
- Public availability
- Nature of data

Valutazione della probabilità

La metodologia di Analisi dei rischi ENISA, a differenza delle altre, ha predefinito il valore della probabilità, la cui valutazione è basata sull'esito della compilazione di 4 diverse tabelle che riassumono l'ambiente in cui sono trattati i dati personali:

- Network and technical resources (hardware and software)
- Processes/procedures related to the data processing operation
- Different parties and people involved in the processing operation
- Business sector and scale of the processing

Valutazione della probabilità

	A. NETWORK AND TECHNICAL RESOURCES	
1.	**Is any part of the processing of personal data performed through the internet?**	When the processing of personal data is performed fully or partially through the open Internet, possible threats from external online attackers increase (e.g. Denial of Service, SQL injection, Man-in-the-Middle attacks), especially when the service is available (and, thus, traceable/known) to all internet users.
2.	**Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)?**	When access to an internal data processing system is provided through the internet, the likelihood of external threats increases (e.g. due to external online attackers). At the same time the likelihood of (accidental or intentional) misuse of data by the users also increases (e.g. accidental disclosure of personal data when working in public spaces). Special attention should be given to cases where remote management/administration of the IT system is allowed.
3.	**Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service?**	Connection to external IT systems may introduce additional threats due to the threats (and potential security flaws) that are inherent to those systems. The same applies also to internal systems, taking into account that, if not appropriately configured, such connections may allow access (to the personal data) to more persons within the organization (which are not in principle authorized for such access).
4.	**Can unauthorized individuals easily access the data processing environment?**	Although focus has been put on electronic systems and services, the physical environment (relevant to these systems and services) is an important aspect that, if not adequately safeguarded, can seriously compromise security (e.g. by allowing unauthorized parties to gain physical access to the IT equipment and network components or failing to provide protection of the computer room in the event of a physical disaster).
5.	**Is the personal data processing system designed, implemented or maintained without following relevant best practices?**	Poorly designed, implemented and/or maintained hardware and software components can pose serious risks to information security. To this end, good or best practices accumulate the experience of prior events and can be regarded as practical guidelines of how to avoid exposure and achieve certain levels of resilience.

Valutazione della probabilità

	B. PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	
6.	**Are the roles and responsibilities with regard to personal data processing vague or not clearly defined?**	When roles and responsibilities are not clearly defined, access (and further processing) of personal data may be uncontrolled, resulting to unauthorized use of resources and compromising the overall security of the system.
7.	**Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined**	When acceptable use of resources is not clearly mandated, security threats might arise due to misunderstanding or intentional misuse of the system. The clear definition of policies for network, system and physical resources can reduce potential risks.
8.	**Are the employees allowed to bring and use their own devices to connect to the personal data processing system?**	Employees using their personal devices within the organization could increase the risk of data leakage or unauthorized access to the information system. Moreover, as devices are not centrally controlled, they may introduce additional bugs or viruses into the system.
9.	**Are employees allowed to transfer, store or otherwise process personal data outside the premises of the organization?**	Processing of personal data outside the premises of the organization can offer a lot of flexibility, but at the same time introduces additional risks, both related to the transmission of information through possibly insecure network channels (e.g. open Wi-Fi networks), as well as unauthorised use of this information.
10.	**Can personal data processing activities be carried out without log files being created?**	The lack of appropriate logging and monitoring mechanisms can increase intentional or accidental abuse of processes/procedures and resources, resulting to the subsequent abuse of personal data.

Valutazione della probabilità

	C. PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	
11.	**Is the processing of personal data performed by a non-defined number of employees?**	When access (and further processing) of personal data is open to a large number of employees, the possibilities of abuse due to human factor increase. Clearly defining who really needs to access the data and limiting access only to those persons can contribute to the security of personal data.
12.	**Is any part of the data processing operation performed by a contractor/third party (data processor)?**	When the processing is performed by external contractors, the organization may lose partially the control over these data. Moreover, additional security threats may be introduced due to the threats that are inherent to these contractors. It is important for the organization to select contractors that can offer a high level of security and to clearly define what part of the processing is assigned to them, maintaining as much as possible a high level of control.
13.	**Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated?**	When employees are not clearly informed about their obligations, threats from accidental misuse (e.g. disclosure or destruction) of data many significantly increase.
14.	**Is personnel involved in the processing of personal data unfamiliar with information security matters?**	When employees are not aware of the need of applying security measures, they can accidentally pose further threats to the system. Training can greatly contribute to making employees aware both of their data protection obligations, as well as the application of specific security measures.
15.	**Do persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data?**	Many personal data breaches occur due to the lack of physical protection measures, such as locks and secure destruction systems. Paper based files are usually part of the input or the output of an information system, can contain personal data and should also be protected from unauthorized disclosure and re-use.

Valutazione della probabilità

	D. BUSINESS SECTOR AND SCALE OF PROCESSING	
16.	**Do you consider your business sector as being prone to cyberattacks?**	When security attacks have already taken place in a specific business sector, there is an indication that the organization would probably need to take additional measures to avoid a similar event.
17.	**Has your organization suffered any cyberattack or other type of security breach over the last two years?**	If the organization has already been attacked or there are indications that this might have been the case, additional measures need to be taken to prevent similar events in the future.
18.	**Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?**	Security bugs/vulnerabilities can be exploited to perform attacks (cyber or physical) to systems and services. Security bulletins containing important information regarding security vulnerabilities that could affect the aforementioned systems and services should be considered.
19.	**Does a processing operation concern a large volume of individuals and/or personal data?**	The type and volume of personal data (scale) can make the processing operation attractive to attackers (due to the inherent value of these data).
20.	**Are there any security best practices specific to your business sector that have not been adequately followed?**	Sector specific security measures are usually adjusted to the needs (and risks) of the particular sector. Lack of compliance with relevant best practices might be an indicator of poor security management.

Valutazione della probabilità

Se in un'area di valutazione tutte le risposte sono positive, l'organizzazione deve considerare la probabilità di minaccia alta, mentre se tutte sono negative, la probabilità di minaccia dovrebbe essere considerata bassa. Per i casi con 2-3 risposte positive, l'organizzazione dovrebbe considerare la probabilità di minaccia media.

Rispetto alle altre metodologie di analisi dei rischi, la valutazione della probabilità non è quindi lasciata all’analista, ma alla metodologia stessa.

Valutazione della probabilità

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
NETWORK AND TECHNICAL RESOURCES	☐ Low	1
	☐ Medium	2
	☐ High	3
PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
BUSINESS SECTOR AND SCALE OF PROCESSING	☐ Low	1
	☐ Medium	2
	☐ High	3

Valutazione della probabilità

OVERALL SUM OF THREAT OCCURRENCE PROBABILITY	THREAT OCCURRENCE PROBABILITY LEVEL
4 - 5	Low
6 - 8	Medium
9 -12	High

Table 4: Evaluation of threat occurrence

Valutazione della rischio

IMPACT LEVEL

THREAT OCCURRENCE PROBABILITY	Low	Medium	High / Very High
Low		X	
Medium			
High			

Altre metodologie ufficiali

L'analisi del rischio è uno degli elementi della PIA

Indice

- Valutare la sicurezza
- La sicurezza nel GDPR
- L’oggetto di tutela
- Analisi del rischio
- **I rischi del titolare**
- Le misure di sicurezza

Rischio aziendale

IMPATTI

- economici (costi di ripristino, mancato guadagno ecc.);
- legali (contenziosi con clienti per mancata erogazione dei servizi ecc.);
- reputazionali;
- sanzionatori (sia dal punto di vista della normativa privacy, ma anche di altre normative, ad esempio quelle in ambito bancario);
- risarcitori (nei confronti delle PERSONE FISICHE, o meglio di CHIUNQUE, abbia subito un danno in seguito alla violazione della normativa privacy).

Valutazione del rischio

- La valutazione dei rischi del titolare può avvenire con metodologie tradizionali, in particolare per quanto attiene i rischi:
  - economici (costi di ripristino, mancato guadagno ecc.);
  - legali (contenziosi con clienti per mancata erogazione dei servizi ecc.);
  - reputazionali;

- Ci limitiamo a considerare in questa presentazione il rischio specifico derivante dal GDPR e quindi:
  - sanzionatori;
  - risarcitori.

Rischio aziendale: risarcitorio

Articolo 82

Diritto al risarcimento e responsabilità (C142, C146, C147)

*1. **Chiunque** subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.*

any person:

- *Interessati*
- *Persone fisiche*
- *Persone non fisiche*

Rischio aziendale: risarcitorio

IMPATTO

- Platea indefinita:
  - Ipotesi composizione:
    - Interessanti (numero noto)
    - Persone fisiche collegate agli interessati (ad esempio 2)
  - Ipotesi risarcimento a persona:
    - Trattamento dati normali> 1000 euro
    - Trattamento dati sanitari> 100.000 euro

- Un eventuale resistenza del Titolare rispetto alla richiesta di risarcimento poterà quasi sicuramente i soggetti che lo richiedono a rivolgersi all'autorità Garante, che verrà pertanto informata della presunta violazione della normativa da parte del Titolare (con tutte le conseguenze del caso per quanto riguarda una possibile visita ispettive ed a seguire le relative sanzioni).

Rischio aziendale: risarcitorio

PROBABILITÀ

- Legata principalmente alla violazioni dei dati personali, anche se non è il solo evento che potrebbe comportare danni (può esserlo ad esempio una informativa non completa)
- Proporzionale alle misure di contrasto a tale evento ed alla conformità del titolare

Rischio aziendale: sanzioni

IMPATTO

- Tipo di sanzione:
  - Pecuniaria (art. 83)
  - Penale
  - Inibitoria e di altra natura (art. 58)
- Valore della sanzione (se pecuniarie)
  - Tipo di violazione
  - Condizione della violazione
- Valore della sanzione (se non pecuniarie: ad esempio blocco dei trattamenti):
  - Mancato guadagno per blocco del servizio
  - Contenzioso legale con i clienti
  - Immagine

Rischio aziendale: sanzioni

PROBABILITÀ

- Visita ispettiva:
  - Programmata
  - In seguito a notifica di violazione
  - In seguito a segnalazione…
- Livello di conformità

Rischio aziendale: sanzioni

Si possono stimare?

- I parametri da considerare sono numerosi
  - criteri di calcolo della sanzione (art. 83)
  - è possibile violare uno specifico articolo in molti modi diversi in quanto la normativa è assolutamente generica nella sua formulazione (art. 83)

È molto difficile quindi desumere quali siano le sanzioni che le varie Autorità hanno attribuito ad una specifica violazione, e secondo quali criteri.

Difficile quindi utilizzare i dati disponibili per effettuare delle stime se non analizzando dettagliatamente i singoli verbali.

Rischio aziendale: sanzioni

Art. 83

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

Rischio aziendale: sanzioni

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Rischio aziendale: sanzioni

Art. 83

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del

fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

Rischio aziendale: sanzioni

Art. 83

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo

58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

Indice

La sicurezza nel GDPR – le misure obbligatore

Articolo *25* ***Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita***

…

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire 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****. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.*

La sicurezza nel GDPR – le misure obbligatore

Articolo *32* ***Sicurezza del trattamento***

---

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Le misure di sicurezza

- Per capire come valutare l'adeguatezza delle misure di sicurezza adottate dal Titolare è necessario rifarsi alla analisi dei rischi.
- Il risultato dell'analisi dei rischi porta solitamente a dare una scala di valutazione (ad esempio **ALTO, MEDIO, BASSO**) per ogni ambito di trattamento analizzato.
- L'adeguatezza delle misure di sicurezza implementate, dovrà quindi basarsi su una scala analoga.

Le misure di sicurezza – High

	MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
	Security policy and procedures for the protection of personal data	A.6	The security policy should be reviewed and revised, if necessary, on a semester basis.	A.5 Security policy
	Roles and responsibilities	B.4	The security officer should be formally appointed (documented). The tasks and responsibilities of the security officer should also be clearly set and documented.	A.6.1.1 Information security roles and responsibilities
	Roles and responsibilities	B.5	Conflicting duties and areas of responsibility, for examples the roles of security officer, security auditor, and DPO, should considered to be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of personal data.	A.6.1.1 Information security roles and responsibilities

Le misure di sicurezza – Medium risk

	MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
	Security policy and procedures for the protection of personal data	A.3	The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties	A.5 Security policy
	Security policy and procedures for the protection of personal data	A.4	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisation measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data.	A.5 Security policy
			An inventory of specific policies/procedures related to the	

Le misure di sicurezza – Low [illegible]k

	MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
	Security policy and procedures for the protection of personal data	A.1	The organization should document its policy with regards to personal data processing as part of its information security policy.	A.5 Security policy
	Security policy and procedures for the protection of personal data	A.2	The security policy should be reviewed and revised, if necessary, on an annual basis.	A.5 Security policy
	Roles and responsibilities	B.1	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.	A.6.1.1 Information security roles and responsibilities
	[illegible]	[illegible]	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures	A.6.1.1 Information security

Le misure di sicurezza: misure organizzative

- 4.1.1 Security management
  - 4.1.1.1 Security policy and procedures for the protection of personal data
  - 4.1.1.2 Roles and responsibilities
  - 4.1.1.3 Access control policy
  - 4.1.1.4 Resource/asset management
  - 4.1.1.5 Change management
  - 4.1.1.6 Data processors
- 4.1.2 Incident response and business continuity
  - 4.1.2.1 Incidents handling / Personal data breaches
  - 4.1.2.2 Business continuity
- 4.1.3 Human resources
  - 4.1.3.1 Confidentiality of personnel
  - 4.1.3.2 Training

Le misure di sicurezza: misure tecniche

- 4.2.1 Access control and authentication
- 4.2.2 Logging and monitoring
- 4.2.3 Security of data at rest
  - 4.2.3.1 Server/Database security
  - 4.2.3.2 Workstation security
- 4.2.4 Network/Communication security
- 4.2.5 Back-ups
- 4.2.6 Mobile/Portable devices
- 4.2.7 Application lifecycle security
- 4.2.8 Data deletion/disposal
- 4.2.9 Physical security

Le misure di sicurezza

NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

Low Impact Controls

Showing **115** controls:

No.	Control	Priority	Low	Moderate	High
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1	AC-1	AC-1	AC-1
AC-2	ACCOUNT MANAGEMENT	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	ACCESS ENFORCEMENT	P1	AC-3	AC-3	AC-3
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	P2	AC-7	AC-7	AC-7
AC-8	SYSTEM USE NOTIFICATION	P1	AC-8	AC-8	AC-8
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	P3	AC-14	AC-14	AC-14
AC-17	REMOTE ACCESS	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)

800-53

(Rev. 4)

Security Controls

Low-Impact

Moderate-Impact

High-Impact

Other Links

Families

Search

Le misure di sicurezza

NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

Moderate Impact Controls

Showing **159** controls:

No.	Control	Priority	Low	Moderate	High
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1	AC-1	AC-1	AC-1
AC-2	ACCOUNT MANAGEMENT	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	ACCESS ENFORCEMENT	P1	AC-3	AC-3	AC-3
AC-4	INFORMATION FLOW ENFORCEMENT	P1		AC-4	AC-4
AC-5	SEPARATION OF DUTIES	P1		AC-5	AC-5
AC-6	LEAST PRIVILEGE	P1		AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	P2	AC-7	AC-7	AC-7
AC-8	SYSTEM USE NOTIFICATION	P1	AC-8	AC-8	AC-8

800-53

(Rev. 4)

Security Controls

Low-Impact

Moderate-Impact

High-Impact

Other Links

Families

Search

Le misure di sicurezza

NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

High Impact Controls

Showing **170** controls:

No.	Control	Priority	Low	Moderate	High
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1	AC-1	AC-1	AC-1
AC-2	ACCOUNT MANAGEMENT	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	ACCESS ENFORCEMENT	P1	AC-3	AC-3	AC-3
AC-4	INFORMATION FLOW ENFORCEMENT	P1		AC-4	AC-4
AC-5	SEPARATION OF DUTIES	P1		AC-5	AC-5
AC-6	LEAST PRIVILEGE	P1		AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	P2	AC-7	AC-7	AC-7
AC-8	SYSTEM USE NOTIFICATION	P1	AC-8	AC-8	AC-8

800-53

(Rev. 4)

Security Controls

Low-Impact

Moderate-Impact

High-Impact

Other Links

Families

Search

Le misure di sicurezza

NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Family: AC - ACCESS CONTROL
Class:
Priority: P1 - Implement P1 security controls first.
Baseline Allocation:

Low	Moderate	High
AC-1	AC-1	AC-1

Jump To:

Revision 4 Statements
Control Description
Supplemental Guidance
References

All Controls > AC > **AC-1**

800-53 (Rev. 4)

Security Controls
Low-Impact
Moderate-Impact
High-Impact
Other Links
Families
Search

Control Description

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [Assignment: organization-defined frequency]; and

2. Access control procedures [Assignment: organization-defined frequency].

Le misure di sicurezza

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related to: PM-9

Control Enhancements

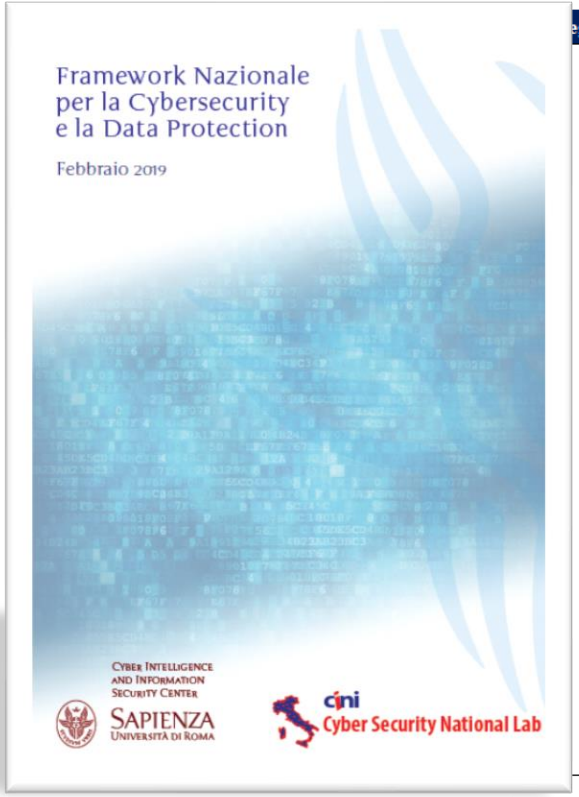
None.

References

NIST Special Publication 800-12	https://csrc.nist.gov/publications/search?keywords-lg=800-12
NIST Special Publication 800-100	https://csrc.nist.gov/publications/search?keywords-lg=800-100

NIST National Institute of Standards and Technology U.S. Department of Commerce

Framework nazionale



egory	Subcategory	Classe	Livello di Priorità
	PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato	Consigliata	ALTA
	PR.AC-3: L'accesso remoto alle risorse è amministrato	Consigliata	ALTA
	PR.AC-4: Gli accessi alle risorse e le autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	Consigliata	ALTA
	PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	Consigliata	ALTA
	PR.AC-6: Le identità sono comprovate, associate a credenziali e verificate durante le interazioni	Consigliata	ALTA
	PR.AC-7: Le modalità di autenticazione (es. autenticazione a singolo o multi fattore) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	Consigliata	ALTA

Documenti pubblici: controlli di sicurezza

Media Disposal

Objective

Media is declassified and approved for release before disposal into the public domain.

Scope

This section describes the disposal of media.

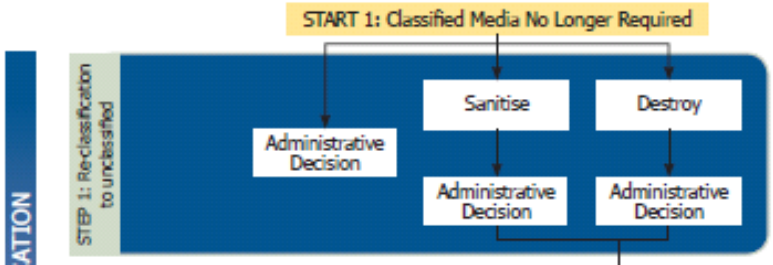
Context

Additional information relating to the disposal of ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Controls

Disposal procedures

The following diagram shows an overview of the typical disposal process. In the diagram there are two starting points, one for classified media and one for sensitive media. Also note that declassification is the entire process, including any reclassifications and administrative decisions, that must be completed before media and media waste can be released into the public domain.



Documenti pubblici: controlli di sicurezz

Managing cyber security incidents

Responsibilities and procedures

Documenting responsibilities and procedures for managing cyber security incidents in a system's System Security Plan (SSP), Standard Operating Procedures (SOPs) and Incident Response Plan (IRP) ensures that when a cyber security incident does occur, personnel can respond in an appropriate manner. In addition, ensuring that users are aware of reporting procedures assists in capturing any cyber security incidents that a system manager fails to notice.

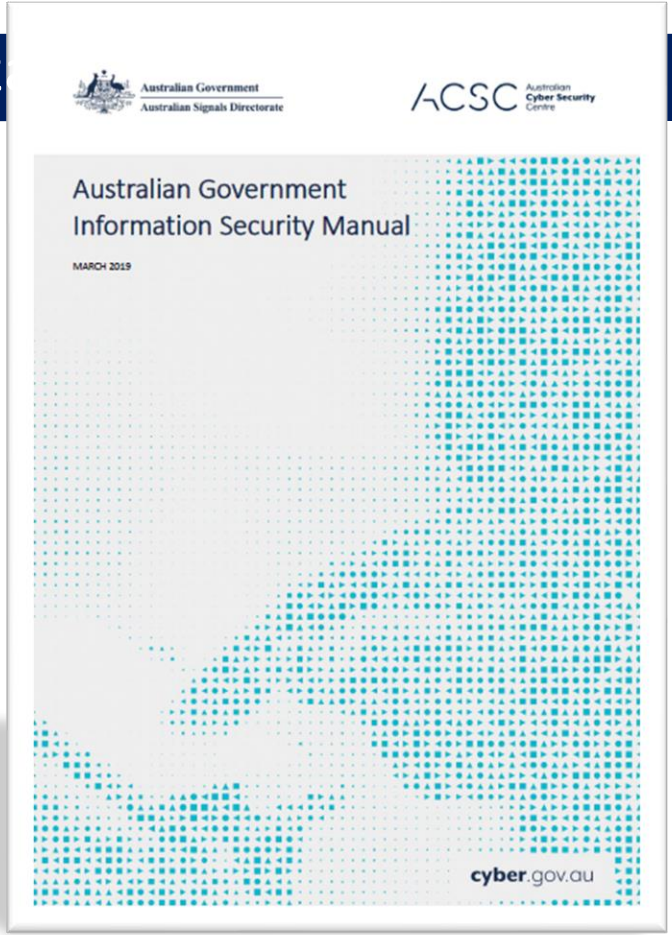
Security Control: 0122; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Cyber security incident responsibilities and procedures are detailed for each system in their security documentation.

Recording cyber security incidents

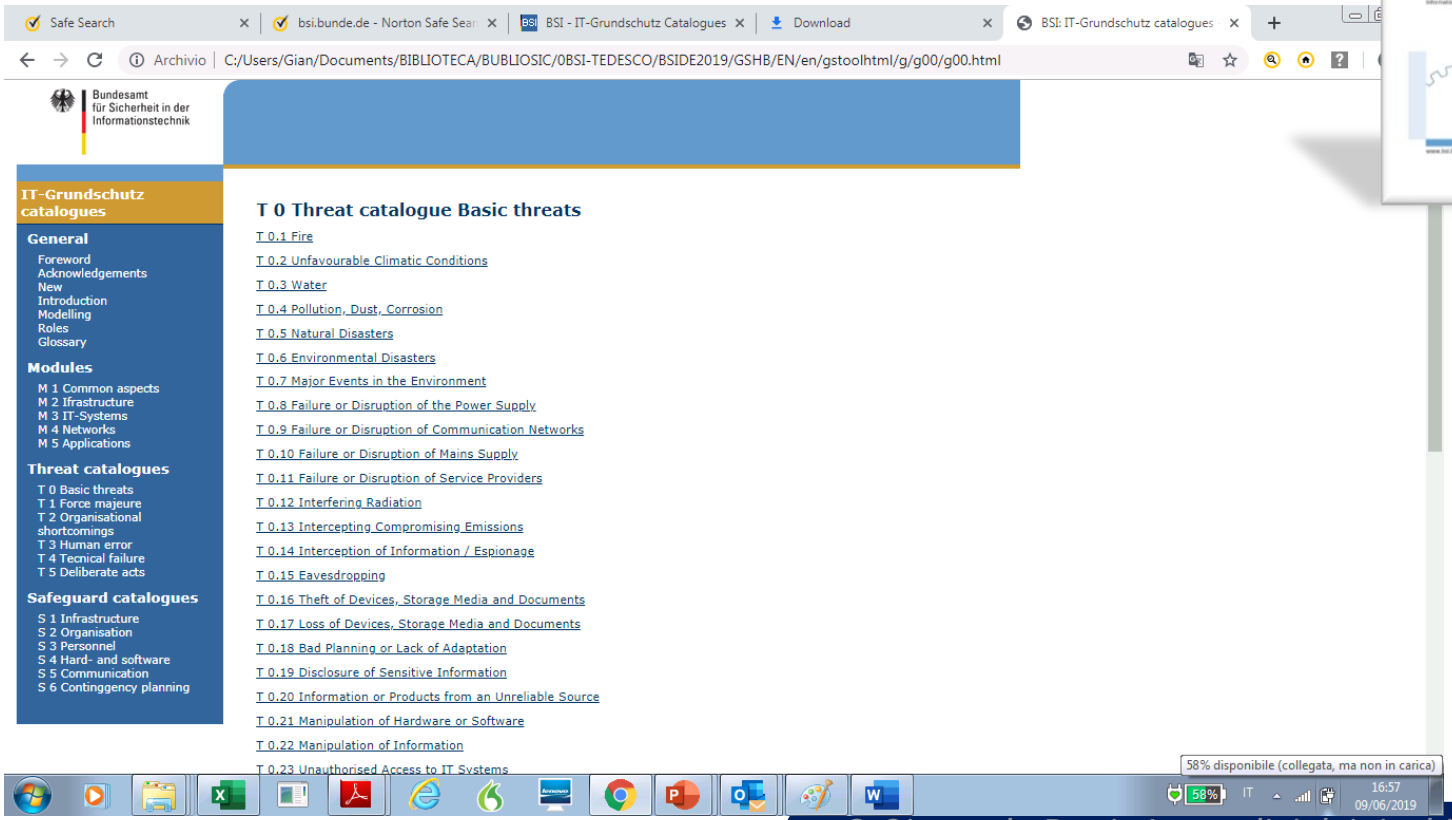
The purpose of recording cyber security incidents in a register is to highlight their type and frequency so that corrective action can be taken. This information, along with information on the costs of any remediation activities, can also be used as an input to future security risk assessments.

Security Control: 0125; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Cyber security incidents are recorded in a register with the following information:

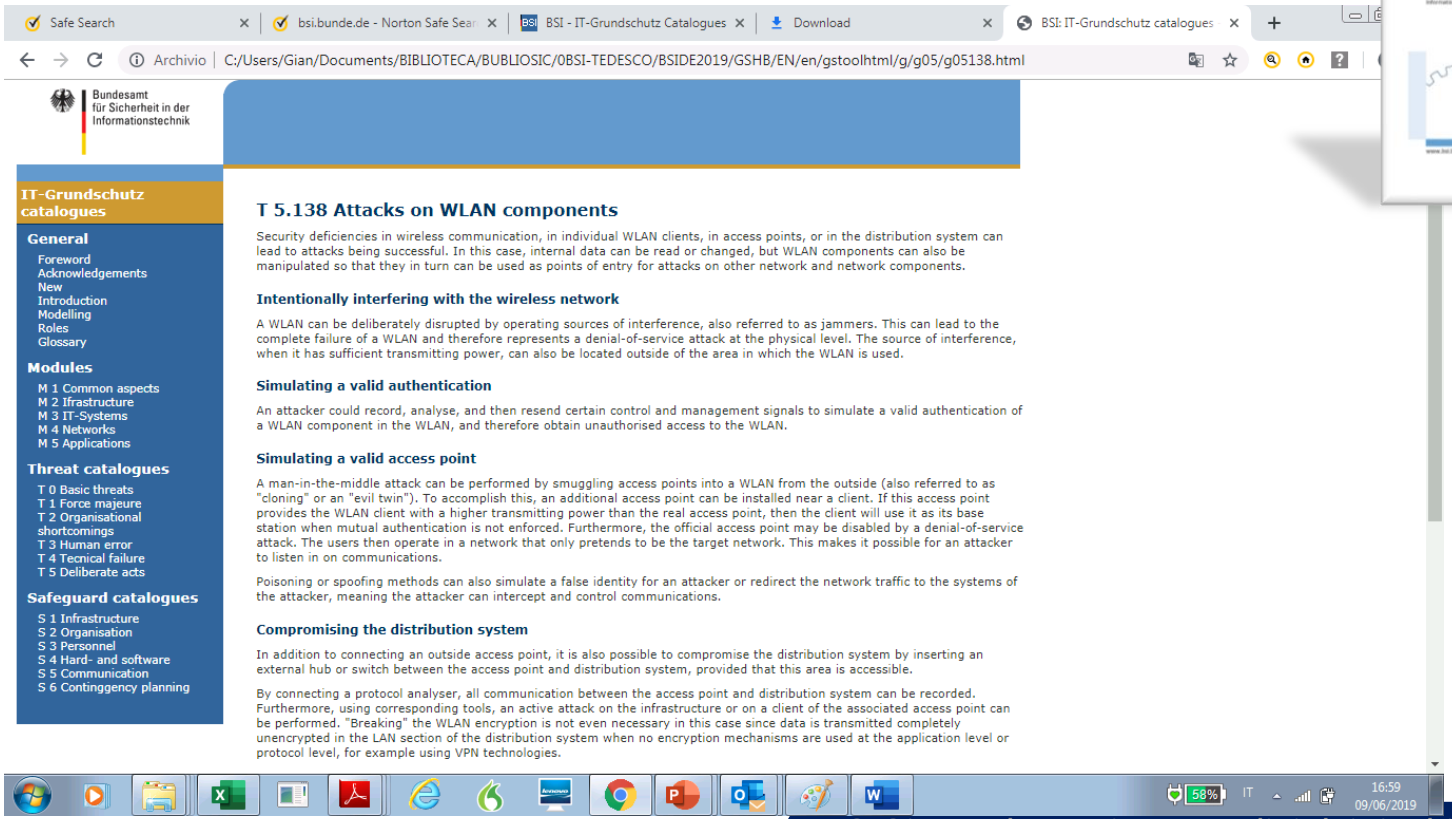
- *the date the cyber security incident occurred*
- *the date the cyber security incident was discovered*
- *a description of the cyber security incident*
- *any actions taken in response to the cyber security incident*
- *to whom the cyber security incident was reported.*

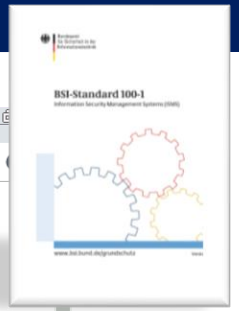


Documenti pubblici: controlli di sicurezza

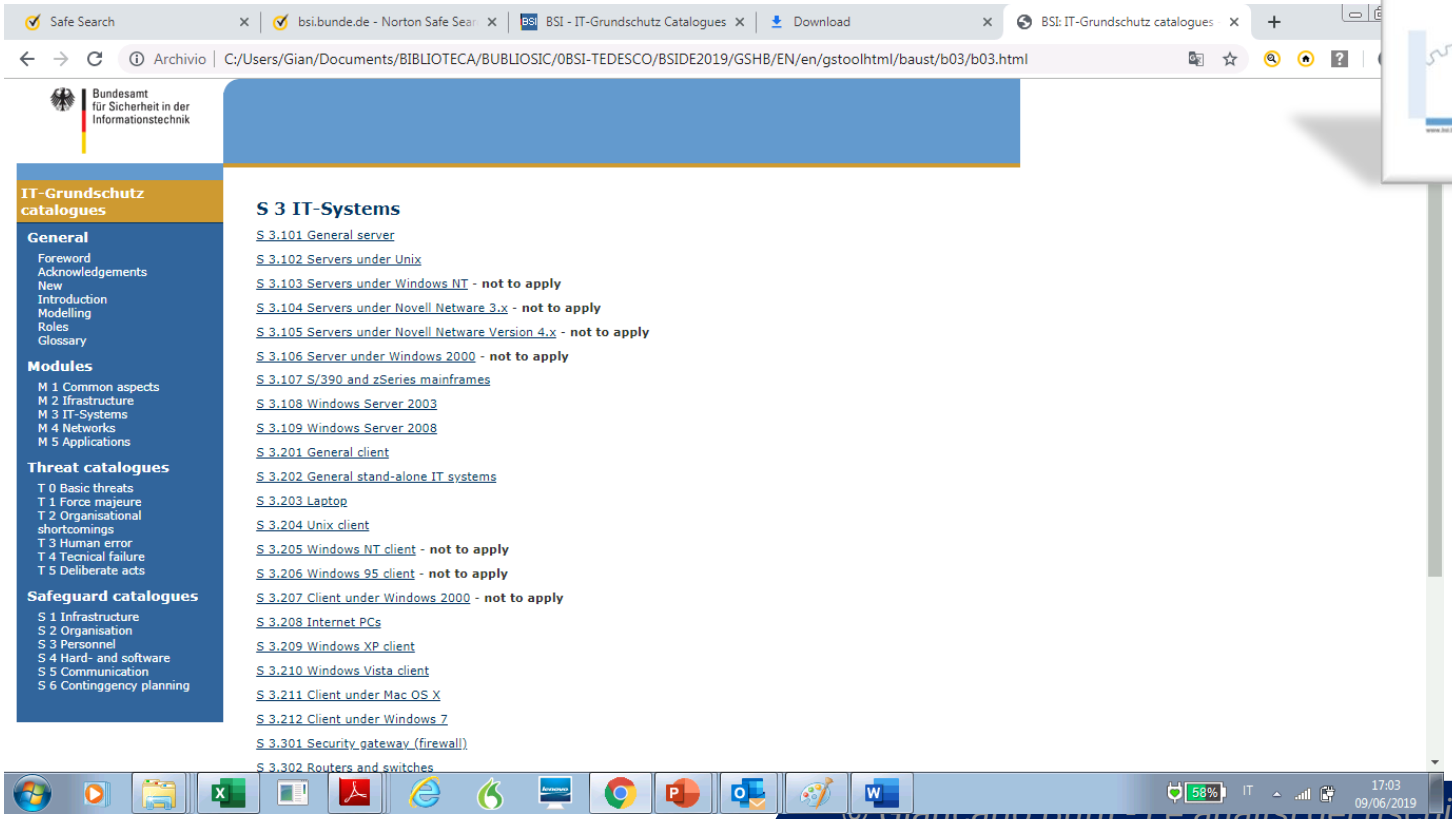


Documenti pubblici: controlli di sicurezza

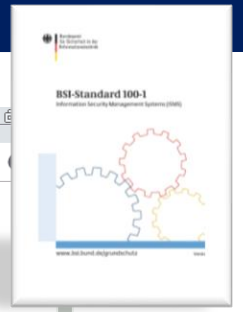




Documenti pubblici: controlli di sicurezza



Documenti pubblici: controlli di sicurezza



Safe Search | bsi.bunde.de - Norton Safe Sear | BSI - IT-Grundschutz Catalogues | Download | BSI: IT-Grundschutz catalogues

Archivio | C:/Users/Gian/Documents/BIBLIOTECA/BUBLIOSIC/0BSI-TEDESCO/BSIDE2019/GSHB/EN/en/gstoolhtml/baust/b03/b03102.html

Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz catalogues

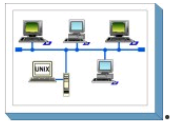
General
- Foreword
- Acknowledgements
- New
- Introduction
- Modelling
- Roles
- Glossary

Modules
- M 1 Common aspects
- M 2 Ifrastructure
- M 3 IT-Systems
- M 4 Networks
- M 5 Applications

Threat catalogues
- T 0 Basic threats
- T 1 Force majeure
- T 2 Organisational shortcomings
- T 3 Human error
- T 4 Tecnical failure
- T 5 Deliberate acts

Safeguard catalogues
- S 1 Infrastructure
- S 2 Organisation
- S 3 Personnel
- S 4 Hard- and software
- S 5 Communication
- S 6 Contingency planning

S 3.102 Servers under Unix



Description

Unix servers are computers that run the Unix operating system and offer services that can be requested by other IT systems in the network. The first Unix system was developed at the beginning of the 1970s. Meanwhile, there are numerous operating systems assigned to the Unix family. In this connection, the differentiation between

- classic Unix systems or Unix derivatives,
- certified UNIX systems (UNIX is a trademark of Open Group, only to be applied to certified systems meeting the corresponding specification), and
- functional Unix systems or Unix-style systems must be made.

Examples for classic Unix systems include the BSD series (FreeBSD, OpenBSD, and NetBSD), Solaris, and AIX. Linux is not a classic Unix system (the kernel is not based on the initial source code the development of the different Unix derivatives is based on), but a functional Unix system. This module considers all operating systems of the Unix family, i.e. also Linux as a functional Unix system.

This module only describes those threats and safeguards that apply specifically to Unix servers, which is why the threats and safeguards for general servers in module S 3.101 must be taken into account additionally.

Threat scenario

The following typical threats to the IT-Grundschutz of a Unix server are assumed to exist:

Organisational Shortcomings

T 2.15	Loss of confidentiality of sensitive data in the UNIX system

Human Error

T 3.10	Incorrect export of file systems under UNIX
T 3.11	Improper configuration of sendmail

Technical Failure

58% IT 17:05 09/06/2019

Documenti pubblici: controlli di sicurezza

Safe Search | bsi.bunde.de - Norton Safe Sear | BSI - IT-Grundschutz Catalogues | Download | BSI: IT-Grundschutz catalogues

Archivio | C:/Users/Gian/Documents/BIBLIOTECA/BUBLIOSIC/0BSI-TEDESCO/BSIDE2019/GSHB/EN/en/gstoolhtml/baust/b03/b03102.html

Planning and design

S 2.33	(Z)	Division of administrator roles under Unix
S 4.13	(A)	Careful allocation of identifiers
S 4.18	(A)	Administrative and technical means to control access to the system-monitor and single-user mode
S 5.16	(B)	Survey of network services
S 5.34	(Z)	Use of one-time passwords
S 5.64	(Z)	Secure Shell
S 5.83	(Z)	Secure connection of an external network with Linux FreeS/WAN

Implementation

S 4.9	(A)	Use of the security mechanisms of X Windows
S 4.14	(A)	Mandatory password protection under Unix
S 4.19	(A)	Restrictive allocation of attributes for Unix system files and directories
S 4.20	(B)	Restrictive allocation of attributes for Unix user files and directories
S 4.21	(A)	Preventing unauthorised acquisition of administrator rights
S 4.22	(Z)	Prevention of loss of confidentiality of sensitive data in the Unix system
S 4.23	(B)	Secure invocation of executable files
S 4.105	(A)	Initial measures after a Unix standard installation
S 4.106	(A)	Activation of system logging
S 5.17	(A)	Use of the NFS security mechanisms
S 5.18	(A)	Use of the NIS security mechanisms
S 5.19	(A)	Use of the sendmail security mechanisms
S 5.20	(A)	Use of the security mechanisms of rlogin, rsh, and rcp
S 5.21	(A)	Secure use of the telnet, ftp, tftp, and rexec
S 5.35	(A)	Use of the security mechanisms of UUCP
S 5.72	(A)	Deactivation of unnecessary network services

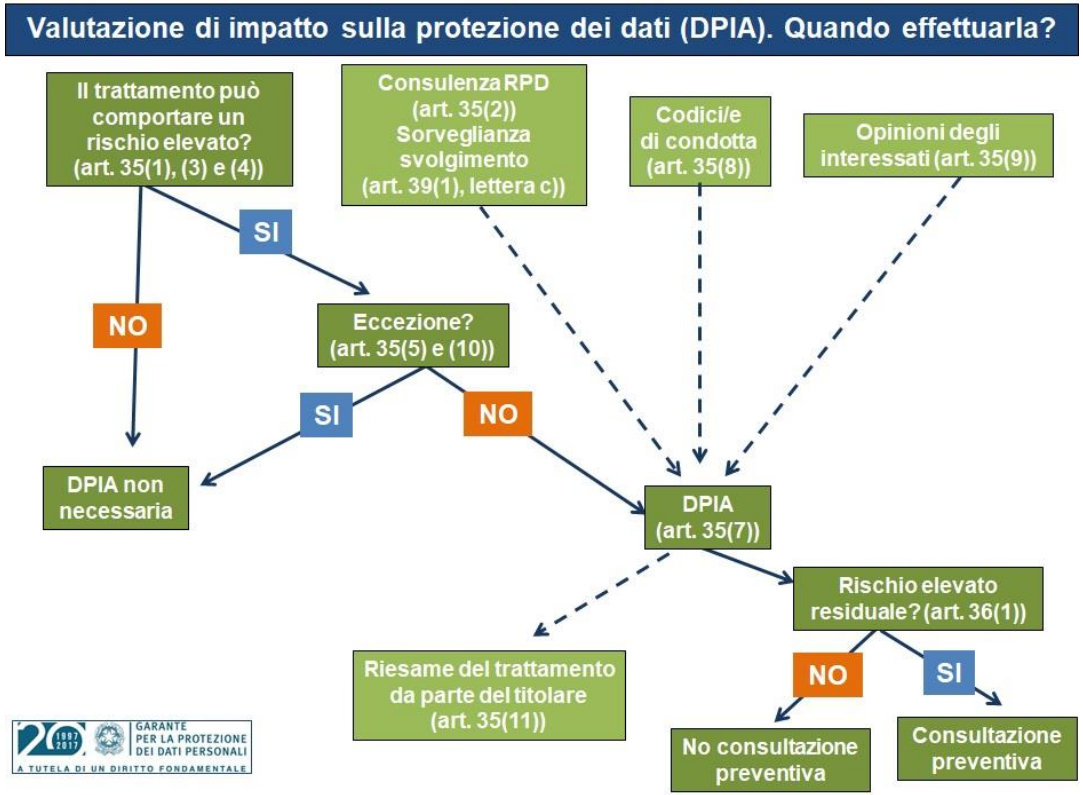
Operation

S 4.25	(A)	Use of logging in Unix systems
S 4.26	(C)	Regular security checks of Unix systems

Contingency Planning

58% IT 17:05 09/06/2019

Trattamento del rischio nel GDPR



Grazie per l'attenzione

Riferimenti:
338 9230742
giancarlo.butti@promo.it