UNIVERSITÀ POLITECNICA DELLE MARCHE

DII Dipartimento di Ingegneria dell'Informazione

unimc

Valutazione delle basi di dati

Paola Gasparini
Centro Servizi Informatici
Università Politecnica delle Marche
p.gasparini@staff.univpm.it

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Cosa aspettarsi da questo lavoro

Un prototipo di strumento per supportare il lavoro di creazione del registro dei trattamenti e/o delle DPIA

Valutazione del rischio

L'invincibilità dipende da noi.

La vulnerabilità del nemico dipende dai suoi sbagli.

(*E viceversa….)*

Come dice il saggio (Sun Tzu – L'arte della guerra)

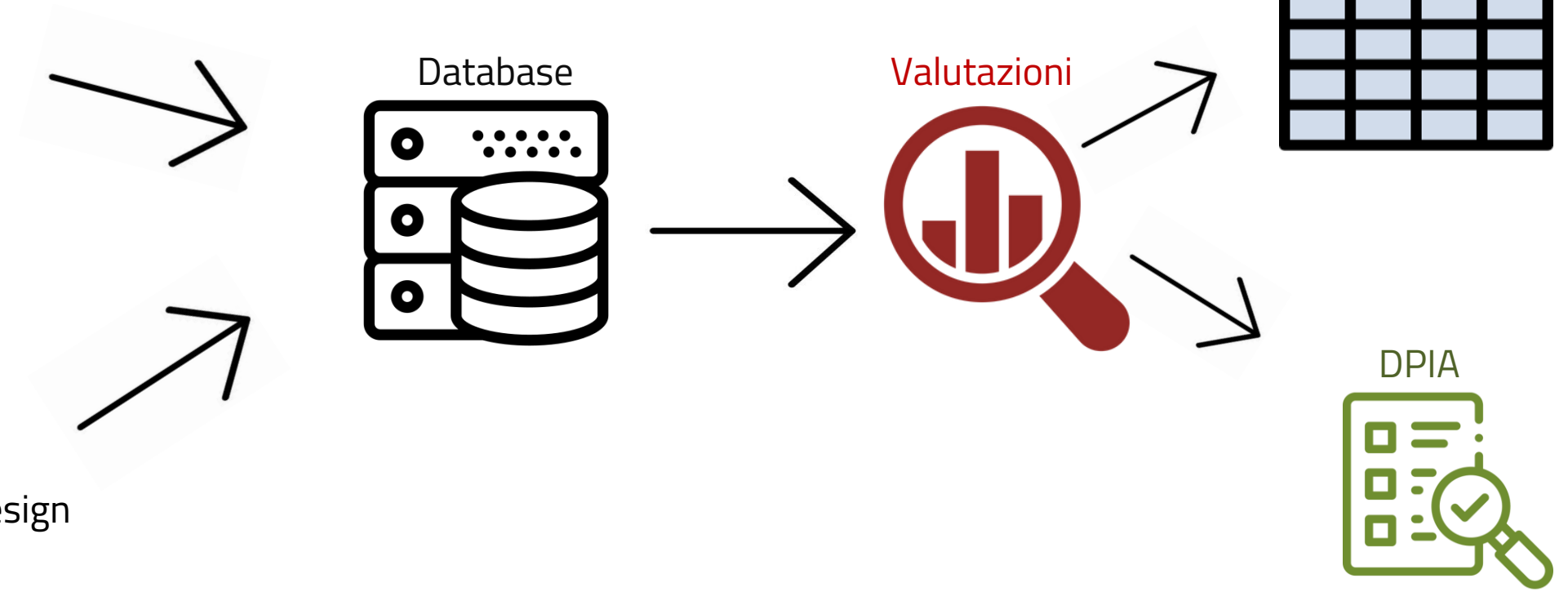
Le Basi di Dati al centro*

Risk Management

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

GDPR

1. Accountabilty
2. Protection by Design



(*) *a prescindere dai trattamenti*

Valutazione del rischio

$$R = G*P$$

Determinare la GRAVITA’

- quanto «pesano» le basi di dati nel definizione del rischio
- Le basi di dati sono uno degli assets da valutare in fase di risk assessment

Le basi di dati dalla prospettiva GDPR

Rischi: Riservatezza / Integrità / Disponibilità / Resilienza (*art. 32*)

Tipo di dati: dati personali (art. 4) , dati particolari (*art.9*)

L'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona).

Numerosità: DPIA (art.35) + Elenco delle tipologie di trattamenti soggetti al requisito di una... - Garante Privacy + WP248

Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento 'possa presentare un rischio elevato' ai fini del regolamento (UE) 2016/679) (possono comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di EUR oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore) .

Cosa le caratterizza dal punto di vista tecnologico

Hardware
server, server con ridondanza, cloud (varie tipologie)

Tipo di architettura
non strutturati, strutturati

Modalità di connessione

Le scelte tecnologiche possono avere impatto su:

diritti e le libertà delle persone fisiche

Cosa possiamo fare:

Riservatezza:

Art.25

- Protezione dati by design: pseudonimizzazione
- Protezione dati by default: minimizzazione

Necessaria collaborazione fra DBA (amministratori di sistema), programmatori, fornitori di soluzioni.

Cosa possiamo fare:

Integrità:

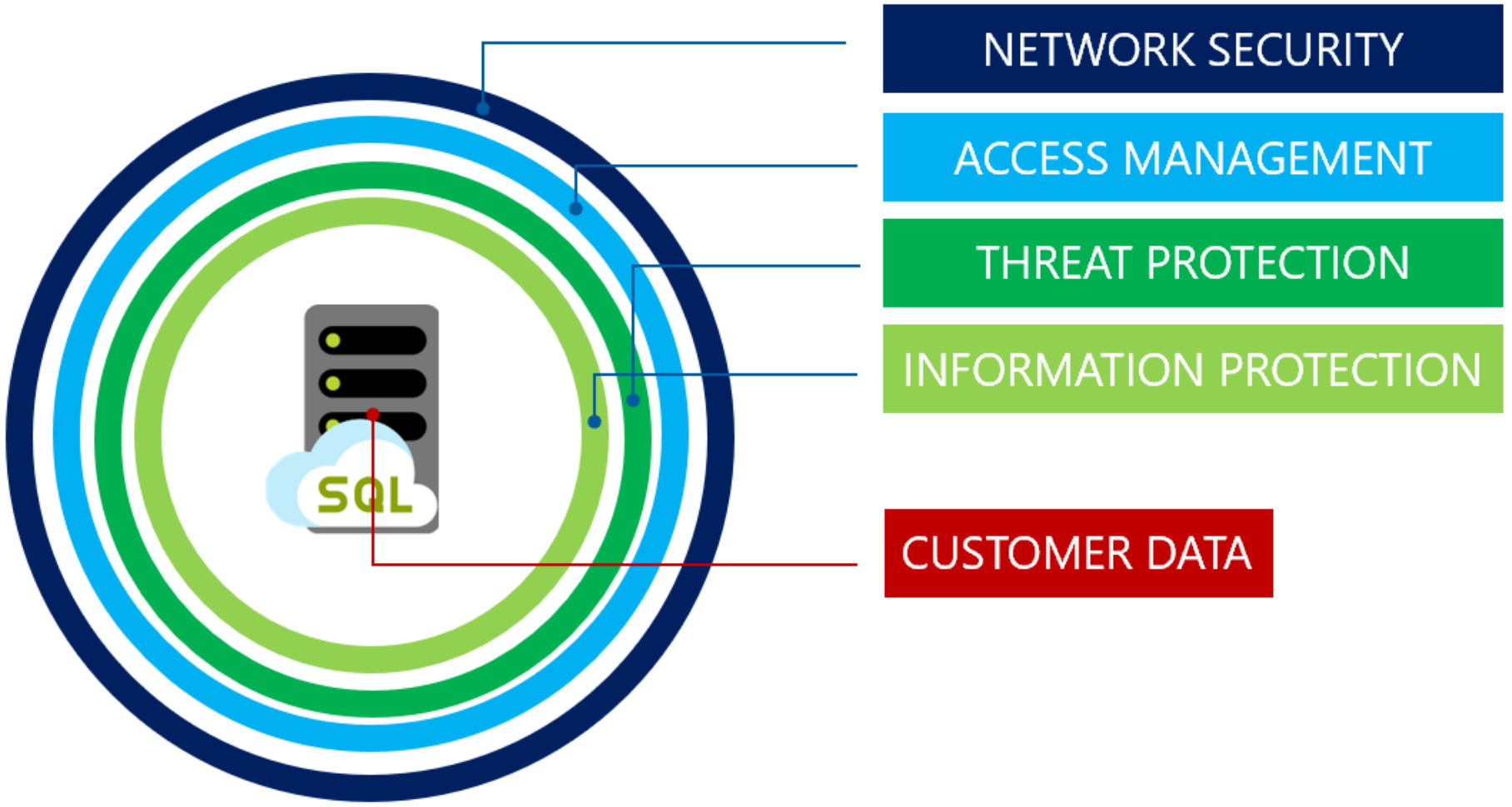
- Hardware
- Software
- Accessi con profili da amministratori
- Connessioni criptate

Cosa possiamo fare:

Disponibilità (e resilienza):

- Hardware
- Backup /Restore & Recover

Data Base Security



Utilizzo Framework per verifica maturità

Framework

Strumenti che ci aiutano a verificare la maturità dell'asset

- NIST
- CIS
- Mapping CIS/NIST
- FNCS
- MMS AGID + Circolare 628/2021

Fonte: ENISA

Prospettiva Data Protection

[Framework Nazionale per la Cybersecurity e la Data Protection + Metodologia di Assessment]

- Ci aiuta pubblicando una contestualizzazione per GDPR
- Attuare le azioni con priorità Alta

«La subcategory DP-ID.AM-8, riguarda l'individuazione e catalogazione dei trattamenti di dati personali. ….Dato l'impatto che una eventuale violazione o trattamento illecito di dati personali può avere sugli individui e sull'azienda stessa in seguito a eventuali sanzioni, appare evidente come i dati personali debbano essere considerati dati critici per l'azienda e in quanto tali vadano individuati e catalogati al pari delle altre tipologie di dato e dei sistemi critici per l'azienda»

FNCS – GDPR

Quali azioni?

Function	Category	Subcategory	Informative References
	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 1
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 2
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 · **Misure Minime AgID** ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6 · **Misure Minime AgID** ABSC 13.1.1, 13.2.1
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11 · **D.Lgs. 18/5/2018 n. 65** Art. 16(2)-(4) · **Misure Minime AgID** ABSC 5.2.1, 5.4, 5.10, 8.11.1
		DP-ID.AM-7: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	· **GDPR** - Artt. 24, 26-29, 37-39 · **D.Lgs. 30/6/2003 n. 196** Artt. 2-quaterdecies, 2-quinquiesdecies, 2-sexiesdecies · **ISO/IEC 29100:2011** 4.2, 4.3, 5.10
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati	· **GDPR** - Art. 30 · **ISO/IEC 29100:2011** 4.4
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	**ID.BE-1:** Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** Clause 4.1 · **NIST SP 800-53 Rev. 4** PM-8 · **D.Lgs. 18/5/2018 n. 65** Art. 4
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici per tutti gli stati di esercizio (es. sotto	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1

Proviamo a fare uno schema di valutazione

[Link al prototipo]

La minaccia più pericolosa

Grazie