Data Protection: la teoria e la pratica

23 giugno 2017

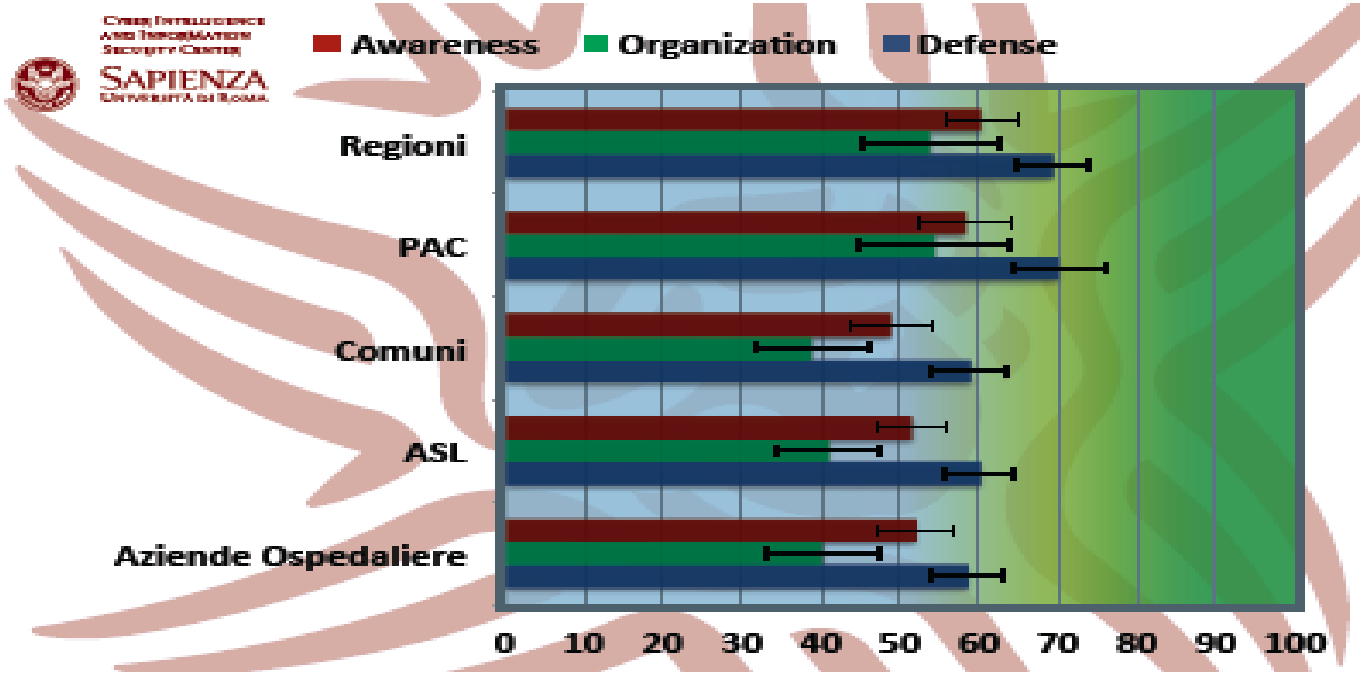
Hotel San Francesco - Alghero

Nuovo approccio metodologico alla privacy per le Aziende Sanitarie

Claudio Caccia - Presidente AISIS

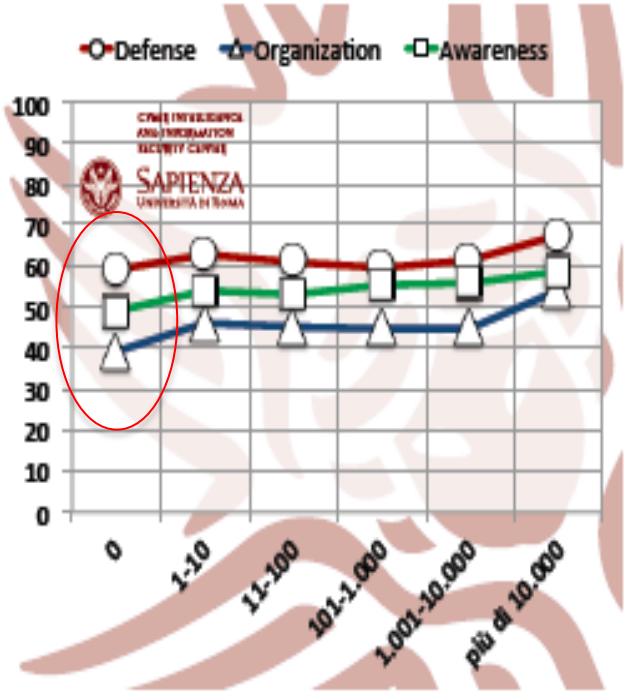
Nel Cyber Security Report dell'Università La Sapienza (2014) vengono definite delle KPI:

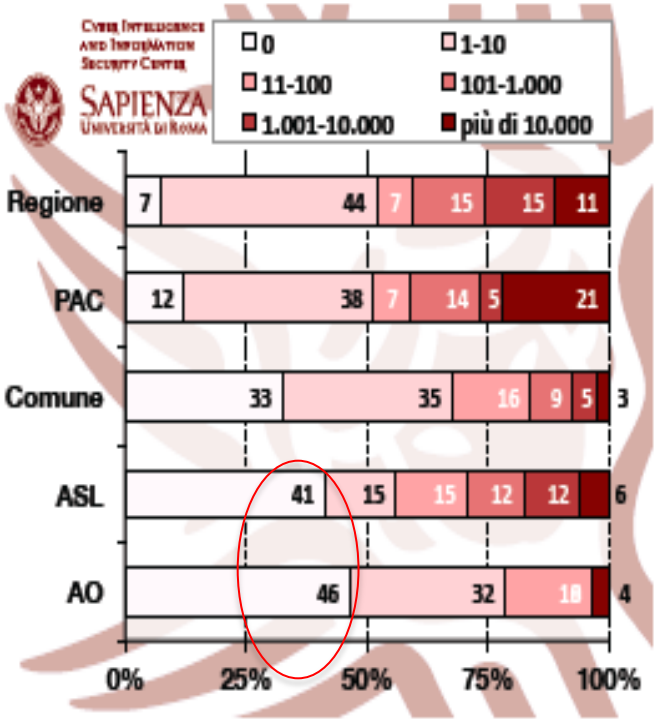
- Consapevolezza del problema
- Organizzazione: processi coinvolti/impattano sulla sicurezza
- Difesa: Aspetti tecnici che impattano sulla sicurezza



Asl e AO sono impreparate a monitorare e gestire la sicurezza

Dal Cyber Security Report dell'Università La Sapienza: gli attacchi….





Le Aziende che dichiarano di non avere ricevuto attacchi sono anche quelle che risultano avere tutte le kpi più basse (impreparate)

Tra questa tipologia di Aziende (quelle che sono impreparate) le Asl e AO sono le più numerose

Dal Cyber Security Report dell'Università La Sapienza: ICT risk management….

CYBER INTELLIGENCE AND INFORMATION SECURITY CENTER
SAPIENZA UNIVERSITÀ DI ROMA

	Sì	No	Non so
Comune	27	49	4
Azienda Sanitaria Locale (ASL)	10	21	3
Azienda Ospedaliera	10	17	2
Pubblica Amministrazione Centrale (PAC)	24	16	2
Regione	14	10	0

Domanda n.48: Viene eseguita periodicamente un'analisi di valutazione del rischio informatico (Risk Assessment)?

Due terzi di Asl e AO non effettuano valutazioni di ICT Risk Assessment

Innovazione digitale, Sicurezza e Privacy

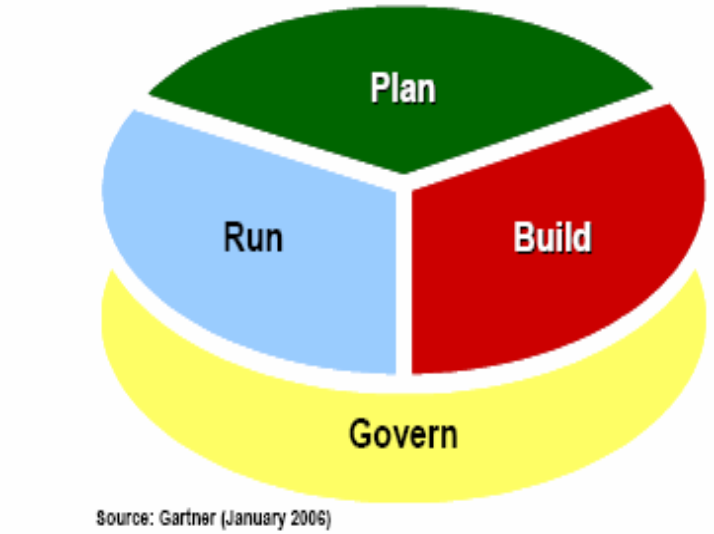
La complessità degli interventi da realizzare nell'area della **innovazione digitale** richiede la valutazione, in fase di pianificazione (**privacy by design**) del sistema informativo aziendale, di due considerazioni di fondo

- Non esiste il concetto di "sicurezza assoluta": qualsiasi sistema è **vulnerabile**. Mettere in sicurezza un sistema significa pianificare un insieme di procedure e strumenti che consentano di ridurre i rischi nella misura possibile o a livelli di accettabilità (Pfleeger, 2004, Cinotti, 2006)

- Gli interventi (**organizzativi, culturali, tecnologici, economici**) in materia di innovazione digitale, sicurezza e privacy **non costituiscono "limitazioni" a un utilizzo esteso e pervasivo di ICT** ma **rappresentano azioni di qualificazione e di miglioramento** del sistema informativo a fini di maggior tutela di tutti gli stakeholders coinvolti (azienda, professionisti che operano in essa, cittadini)

Innovazione digitale, Sicurezza e Privacy

La complessità degli interventi da realizzare suggerisce l'adozione di un approccio strutturato alla pianificazione delle attività in questa delicata area

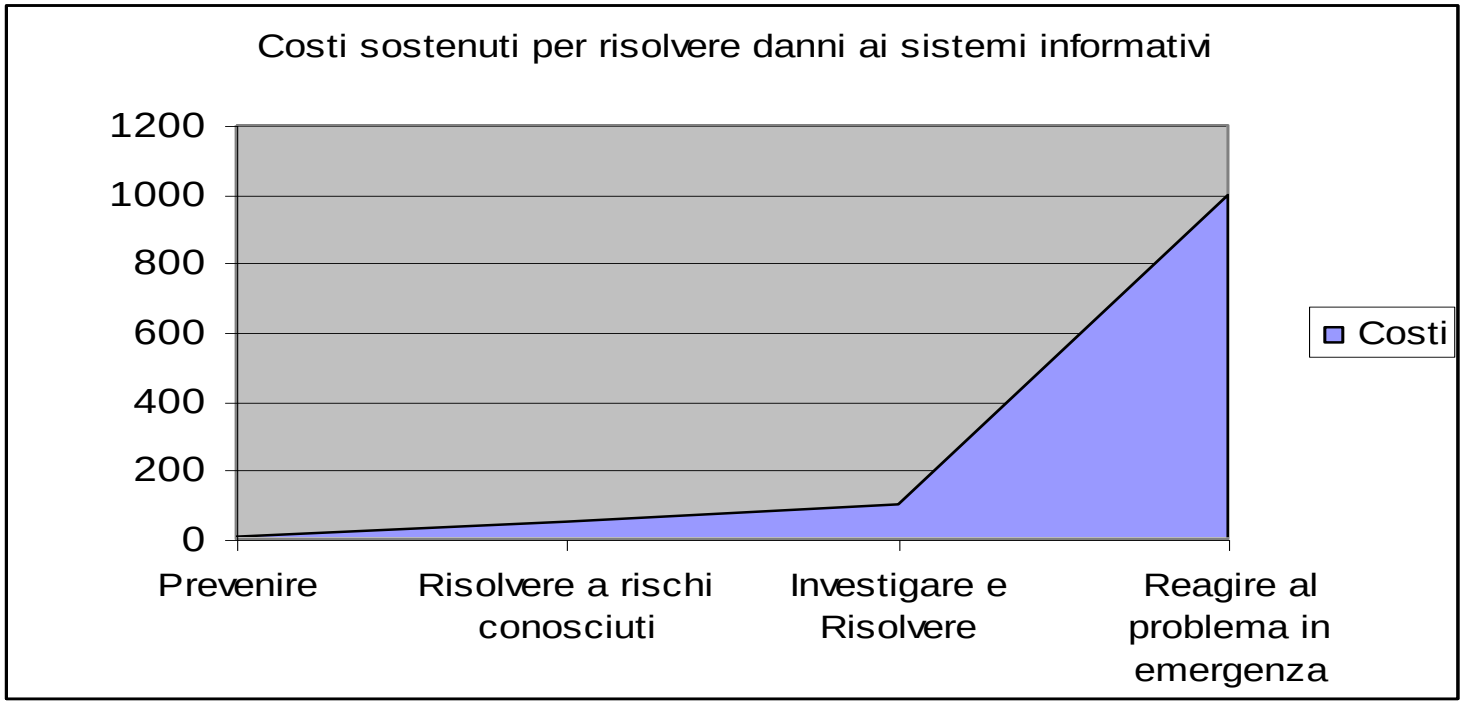


Risk and Security Activity Cicle

(Gartner)

Information Security Management System
(Standard BS7799)

Innovazione digitale, Sicurezza e Privacy



La spesa per la prevenzione dei rischi (pianificazione) rappresenta attualmente solo l'1% della spesa per Information Technology. Il differenziale dei costi da sostenere in caso di emergenza ha un rapporto di 1:1000

Novità contenute nel GDPR

Il GDPR è sostanzialmente basato sul concetto di "**accountability**" (responsabilizzazione)

Titolare agisce in modo "**proattivo**":

- dimostrare che i trattamenti sono coerenti con le linee guida del GDPR
- pianificare e mettere in atto misure tecniche e organizzative per poterne comprovare l'adeguatezza
- attivare un modello di monitoring delle misure tecnico-organizzative implementate

Privacy by design: disegnare le misure di Sicurezza e Privacy in fase di progettazione dei sistemi informativi

Privacy by default: disegnare le misure di Sicurezza e Privacy per default, come prerequisito di normale funzionamento dei sistemi infromativi

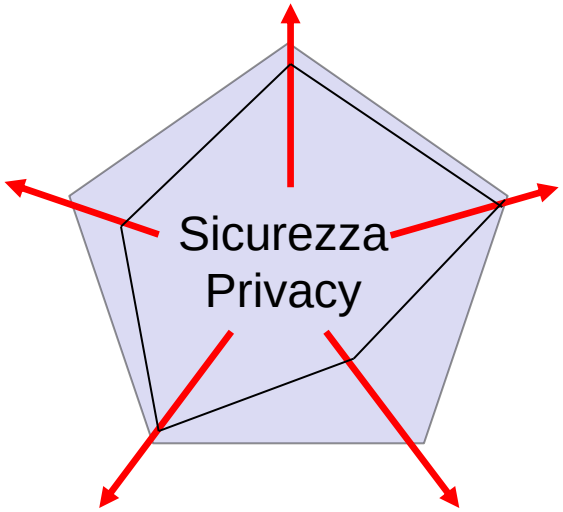
Un possibile nuovo approccio alla Sicurezza e Privacy

dove e quali sono i dati

DATA INVENTORY

MODIFICHE APPLICATIVI

misure tecniche sugli applicativi



VALUTAZIONE DEI RISCHI

quali rischi e impatti

MODIFICHE ARCHITETTURA

misure tecniche di sicurezza

MODIFICHE ORGANIZZATIVE

misure organizzative

Un possibile nuovo approccio alla Sicurezza e Privacy: DATA INVENTORY

Quali sono i dati che trattiamo e dove sono:

- Scopo del trattamento
- Descrizione dei dati d'uso
- Tipologia di dati trattati
- Dov'è il database
- Limiti per la cancellazione/perdita dei dati
- Descrizione delle misure di sicurezza
- Descrizione delle misure di backup e restore

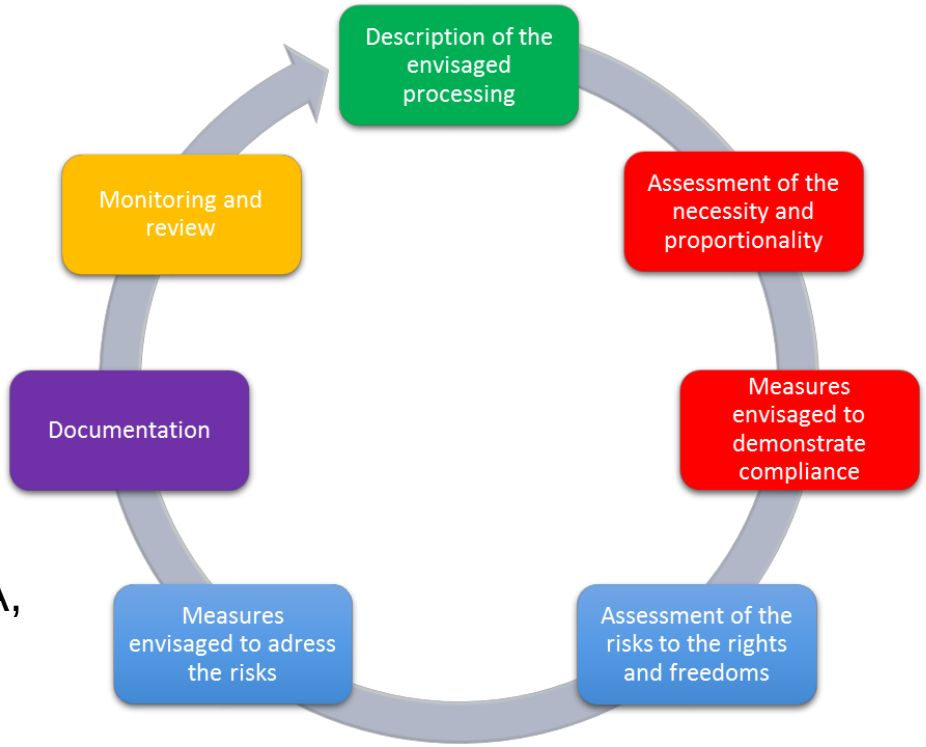
REGISTRO DEI TRATTAMENTI (art 30 GDPR)

	Scopo del trattamento	Descrizione dei dati d'uso	Tipologia di dati trattati	Descrizione database	Limiti per la cancellazione dei dati	Descrizione delle misure di sicurezza	Descrizione delle misure di backup
Trattamento 1							
Trattamento 2							
Trattamento 3							
Trattamento n							

Un possibile nuovo approccio alla Sicurezza e Privacy: Business Impact Analisys

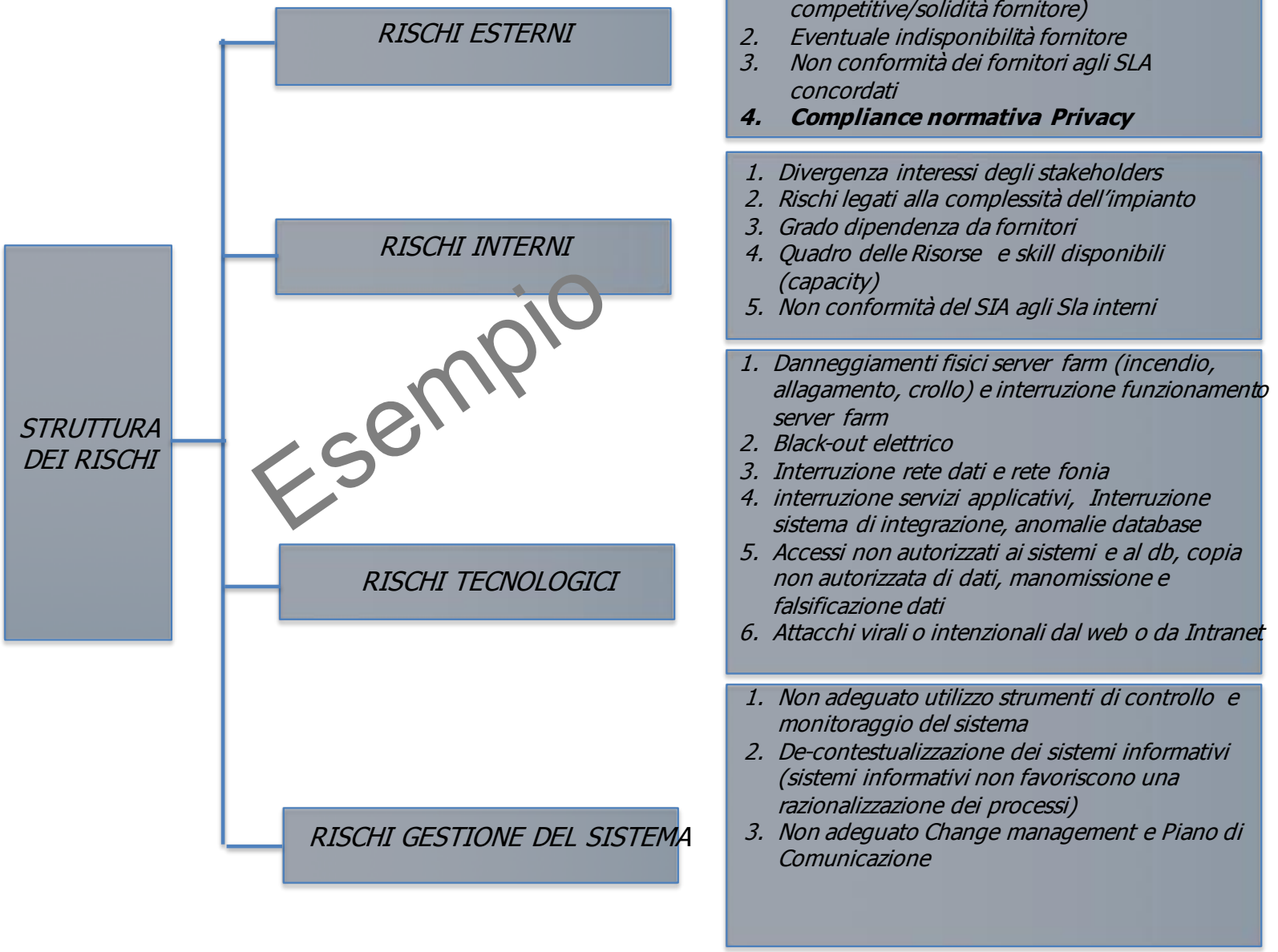
Valutazione d'impatto sulla protezione dei dati (art 35 GDPR):

- Analisi dei rischi
- Analisi degli impatti
- Monitoraggio sistematico nel tempo



Misure Minime di Sicurezza ICT per la PA, Linee guida Agid. GU n° 79, 4.4.2017

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.
ARTICLE 29 DATA PROTECTION WORKING PARTY, April 2017


STRUTTURA DEI RISCHI
RISCHI ESTERNI
1. Instabilità mercato (pressioni competitive/solidità fornitore)
2. Eventuale indisponibilità fornitore
3. Non conformità dei fornitori agli SLA concordati
4. Compliance normativa Privacy
RISCHI INTERNI
1. Divergenza interessi degli stakeholders
2. Rischi legati alla complessità dell'impianto
3. Grado dipendenza da fornitori
4. Quadro delle Risorse e skill disponibili (capacity)
5. Non conformità del SIA agli Sla interni
RISCHI TECNOLOGICI
1. Danneggiamenti fisici server farm (incendio, allagamento, crollo) e interruzione funzionamento server farm
2. Black-out elettrico
3. Interruzione rete dati e rete fonia
4. interruzione servizi applicativi, Interruzione sistema di integrazione, anomalie database
5. Accessi non autorizzati ai sistemi e al db, copia non autorizzata di dati, manomissione e falsificazione dati
6. Attacchi virali o intenzionali dal web o da Intranet
RISCHI GESTIONE DEL SISTEMA
1. Non adeguato utilizzo strumenti di controllo e monitoraggio del sistema
2. De-contestualizzazione dei sistemi informativi (sistemi informativi non favoriscono una razionalizzazione dei processi)
3. Non adeguato Change management e Piano di Comunicazione
Esempio

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

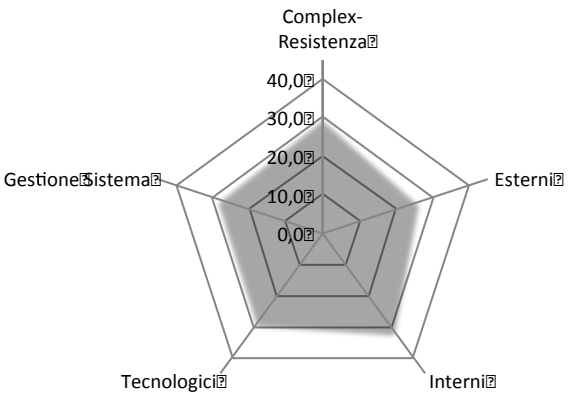
Associazione Italiana Sistemi Informativi in Sanità

Sicurezza Privacy

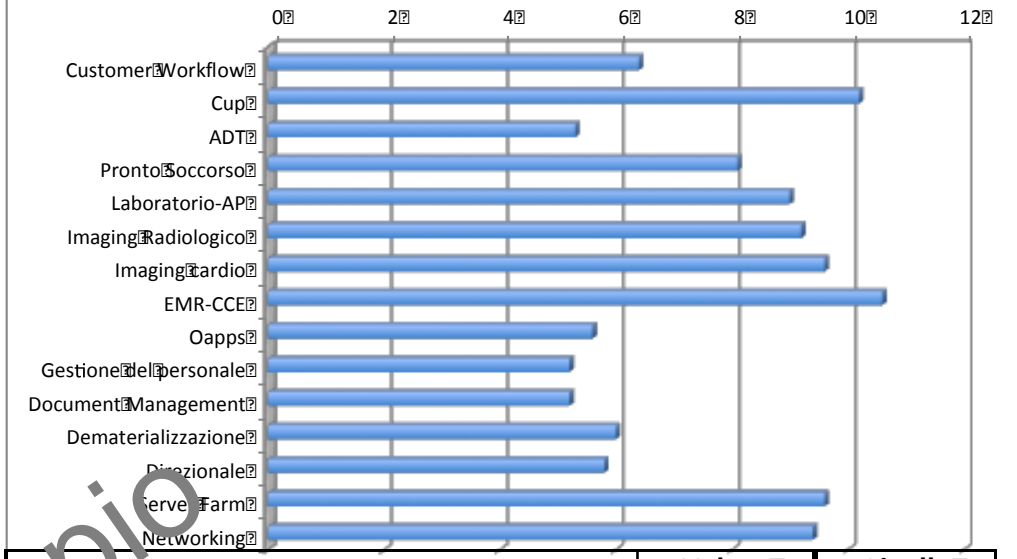
ANALISI RISCHI

Struttura dei rischi																
	Fornitore	Artexè	HiTech	Noemalife	Noemalife	Fuji	Medimatica	Noemalife	Noemalife	CS2	Infoline	Emc	Ifinmed	Oslo	Servizi Informatici	Fastweb
	Modulo applicativo	**Customer Workflow**	**CUP**	**PS**	**ADT**	**Imaging**	**Imaging Cardio** Altro Imaging	**LIS-AP**	**GALILEO**	**OAPPS**	**Personale**	**Document Management**	**Dematerializzazione**	**Direzionale**	**Server Farm**	**Networking**
Esterni (contesto)	Instabilità mercato (pressioni competitive/solidità fornitore)	2	2	1	1	1	1	1	2	1	1	1	2	1	2	2
	Eventuale indisponibilità fornitore	2	3	3	2	3	3	3	3	2	2	2	2	2	3	3
	Non conformità dei fornitori agli SLA concordati	3	3	3	2	3	3	3	3	1	1	1	2	2	3	3
	Variazioni normative di settore	1	2	1	1	1	1	1	3	1	1	1	2	2	1	1
Interni (organizzativi)	Divergenza interessi, Resistenza Stakeholder	1	3	1	1	1	3	1	3	2	2	2	3	3	2	1
	Rischi legati alla complessità dell'impianto	1	3	2	1	3	3	3	3	3	3	2	2	2	3	3
	Rischi legati al grado dipendenza dai fornitori	2	3	2	2	3	3	3	3	2	2	2	2	2	3	3
	Rischi legati al quadro delle Risorse e Skill disponibili (capacity)	2	3	2	1	3	3	3	3	2	2	2	2	2	3	3
	Non conformità del SIA agli SLA interni	2	3	2	1	3	3	3	3	1	1	1	1	1	3	3
Tecnologici	Danneggiamenti fisici Server farm (incendio, allagamento, crollo) e interruzione funzionamento Server farm	2	3	3	2	3	3	3	3	1	1	1	1	1	3	3
	Black-out elettrico	2	3	3	2	3	3	3	3	1	1	1	1	1	3	3
	Interruzione rete dati e rete telefonia	2	3	3	2	3	3	3	3	1	1	1	1	1	3	3
	Interruzione Servizi applicativi, interruzione sistema di integrazione, anomalie database	2	3	3	2	3	3	3	3	1	1	1	1	1	3	3
	Accessi non autorizzati ai sistemi e Db, copia non autorizzata di dati, manomissione e falsificazione dati	1	3	3	1	3	3	3	3	1	1	1	1	1	3	3
	Attacchi virali o intenzionali dal web o da Intranet	1	3	3	1	3	3	2	3	1	1	1	1	1	3	3
Gestione Sistema	Non adeguato utilizzo strumenti di controllo del sistema	1	2	2	1	3	3	3	3	2	2	2	2	2	3	3
	De-contestualizzazione dei Sistemi Informativi (sistemi informativi non favoriscono una razionalizzazione dei processi)	2	3	2	1	2	2	2	3	2	2	2	2	2	2	2
	Non adeguato Change Management e Piano comunicazione	1	3	1	1	2	2	2	3	2	2	2	2	2	2	2

Rischio complessivo Sistema Informativo



Indice di Rischio

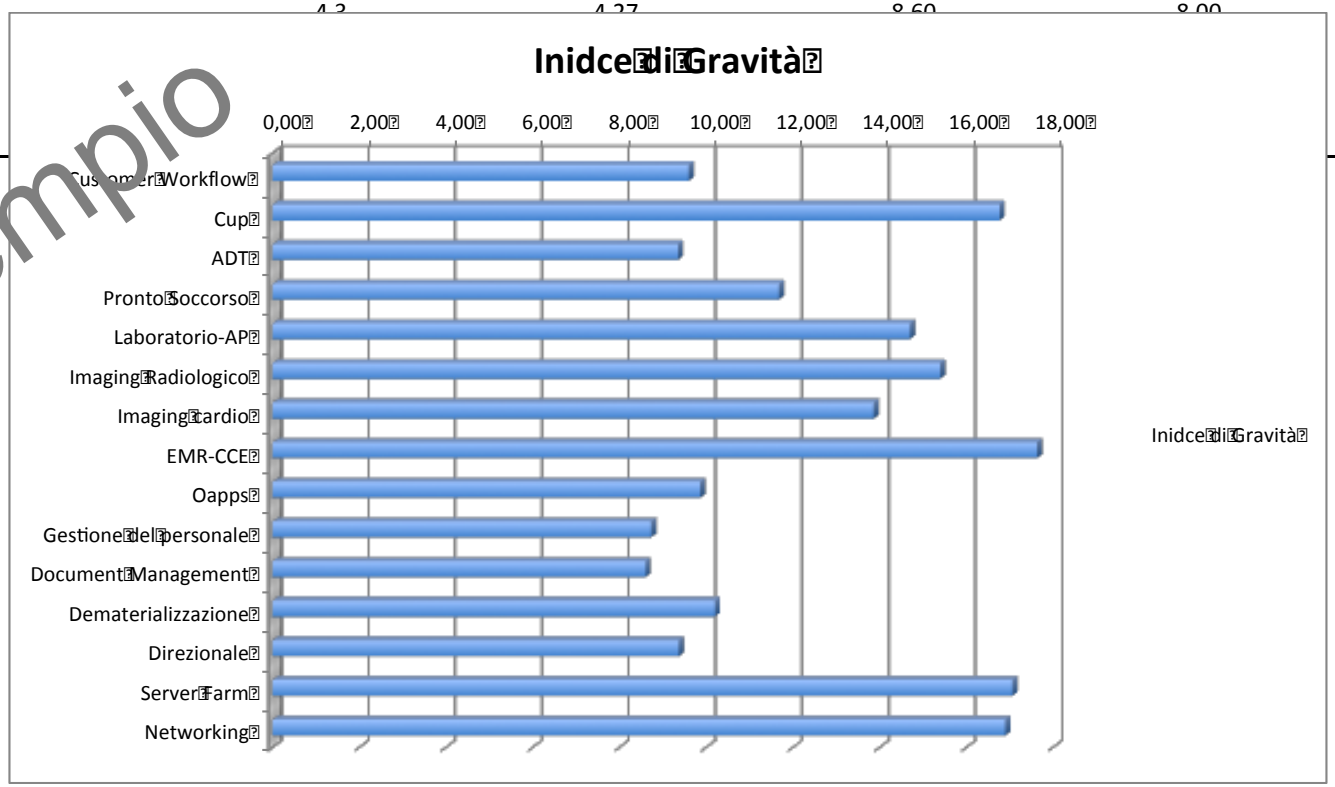


Matrice dei fornitori critici	Valore Criticità (1*)	Livello Criticità
Artexè	8	
HiTech	10	
Noemalife accoglienza	7	
Fuji	8	
Medimatica	8	
Noemalife diagnostica	8	
Noemalife EMR	11	
CS2	5	
Infoline	5	
Emc	5	
Ifinmed	8	
Servizi Informatici	9	
Fastweb	9	

Struttura Impatti																	
bassa 1, media 2, alta 3, critica 4	*Fornitore*	Artexè	HiTech	Noemalife	Noemalife	Noemalife	Noemalife	Fuji	Medimatica	Noemalife	CS2	Infoline	Emc	Ifinmed	Oslo	Servizi Informatici	Fastweb
	Macroprocesso	Customer workflow management	Prenotazione e Billing	Accettazione e dimissione	Pronto Soccorso	Laboratorio	Anatomia Patologica	Imaging Radiologico	Imaging cardio	EMR-CCE	Ciclo attivo, passivo e logistica	Gestione del personale	Document Management	Dematerializzazione	Direzionale	Server Farm	Networking
Tipologia Impatto																	
Impatti di Servizio	Importanza del Servizio all'interno dell'azienda	3	4	2	3	4	3	4	3	4	3	3	2	3	3	4	4
	l'interruzione determina un immediato impatto/disagio agli utenti	3	4	3	4	4	3	4	3	4	2	2	2	2	2	4	4
	Tipologia e volume utenza coinvolta	3	4	4	3	4	2	4	3	4	2	2	2	3	1	4	4
	è possibile recuperare ex post dati non acquisiti	1	4	1	2	3	2	3	3	4	1	1	1	2	1	4	4
	sono possibili procedure alternative	1	4	2	2	2	1	2	2	3	1	1	1	2	1	4	4
	livello di danno per l'Azienda	3	4	2	3	3	2	3	3	4	2	2	2	2	2	4	4
	Totale	***14***	***24***	***14***	***17***	***20***	***13***	***20***	***17***	***23***	***11***	***11***	***10***	***14***	***10***	***24***	***24***
Impatti Organizzativi	numero UU.OO. coinvolte	2	3	4	2	4	3	4	3	4	2	2	2	2	2	4	4
	numero sedi coinvolte	2	3	2	1	3	1	4	2	4	2	2	2	2	2	4	4
	numerosità addetti coinvolti	2	3	1	2	4	2	4	2	4	2	2	2	2	1	4	4
	interruzione determina blocco del processo	1	4	1	3	3	2	3	3	4	3	2	2	2	2	4	4
	interruzine determina impatti su altri processi/sistemi interdipendenti	2	4	3	3	3	3	3	3	4	2	2	2	2	2	4	4
	Totale	***7***	***14***	***9***	***9***	***14***	***9***	***14***	***10***	***16***	***9***	***8***	***8***	***8***	***7***	***16***	***16***
Impatti Tecnologici	numero pdl coinvolte	2	3	4	2	3	2	3	2	4	2	2	2	2	1	4	4
	complessità architettura server	1	3	2	1	3	2	3	2	4	3	2	2	3	3	4	4
	complessità architettura applicativa	1	3	1	1	3	2	4	2	3	3	2	2	3	3	4	4
	Interruzione servizi applicativi, interruzione sistema di integrazione, anomalie database	2	3	3	2	3	2	3	3	4	2	2	2	2	2	4	4
	Dimensione db	1	4	2	1	3	1	4	3	4	2	2	2	2	2	4	4
	Tempo ripristino/reinstallazione applicativo	2	4	2	2	3	2	4	3	4	4	2	2	3	3	4	4
	Tempo ripristino db	2	4	2	2	2	2	3	2	4	3	2	2	2	3	4	4
	Totale	***11***	***24***	***16***	***11***	***20***	***13***	***24***	***17***	***27***	***19***	***14***	***14***	***17***	***17***	***28***	***28***
Valutazione complessiva	**Indice di Impatto**	10,67	20,67	12,33	12,33	18,00	11,67	19,33	14,67	22,00	13,00	11,00	10,67	13,00	11,33	22,67	22,67
	RTO (tempo entro cui ripristinare in h)	2	2	2	2	2	4	2	4	2	4	8	8	8	4	1	1
	RPO (tempo messa in sicurezza dei dati in h)*	1	1	1	1	1	1	1	1	1	8	8	8	8	8	1	1

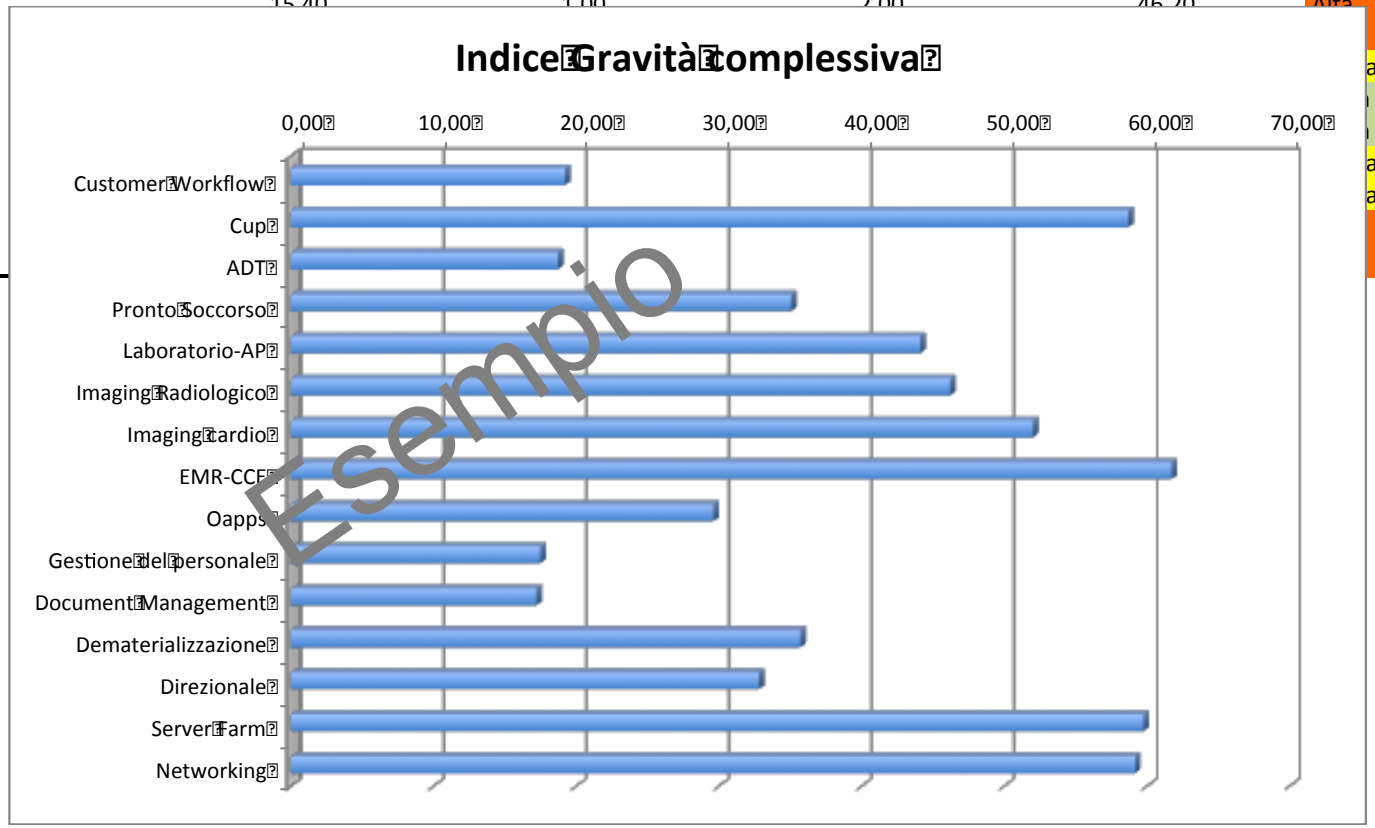
Fonte: Tipologie impatti riprese da Linee guida Agid

Impatto sui servizi	Indice di rischio	Indice di Impatto	Indice Gravità (rischio+Impatto)	RTO Recovered Time Objective	RPO Recovered Point Objecti
Customer Workflow	5,3	4,27	9,60	2,00	1,00
Cup	8,5	8,27	16,77	2,00	1,00
ADT	4,4	4,93	9,35	2,00	1,00
Pronto Soccorso	6,8	4,93	11,68	2,00	1,00
Laboratorio-AP	7,5	7,20	14,70	2,00	1,00
Imaging Radiologico	7,7	7,73	15,40	2,00	1,00
Imaging cardio	8,0	5,87	13,87	4,00	1,00
EMR-CCE	8,8	8,80	17,63	2,00	1,00
Oapps	4,7	5,20	9,87	4,00	8,00
Gestione del personale	4,3	4,40	8,73	8,00	8,00
Document Management	4,3	4,27	8,60	8,00	8,00
Dematerializzazione					8,00
Direzionale					8,00
Server Farm					1,00
Networking					1,00



Esempio

Matrice Gravità e probabilità di accadimento	Indice di Gravità	probabilità (1 bassa, 2 media, 3 alta)	vulnerabilità (1 bassa, 2 media, 3 alta)	Rischio complessivo in termini di gravità e probabilità	Priorità ripristino
Customer Workflow	9,60	1,00	1,00	19,20	Bassa
Cup	16,77	1,00	2,50	58,68	Alta
ADT	9,35	1,00	1,00	18,70	Bassa
Pronto Soccorso	11,68	1,00	2,00	35,05	Media
Laboratorio-AP	14,70	1,00	2,00	44,10	Alta
Imaging Radiologico	15,40	1,00	2,00	46,20	Alta
EMR-CCE					
Oapps					a
Gestione del personale					
Document Management					
Dematerializzazione					a
Direzionale					a
Server Farm					
Networking					

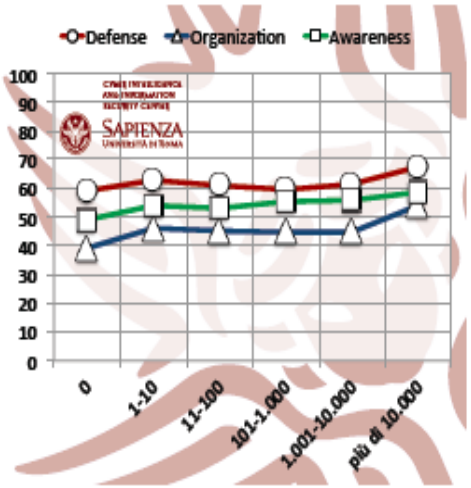


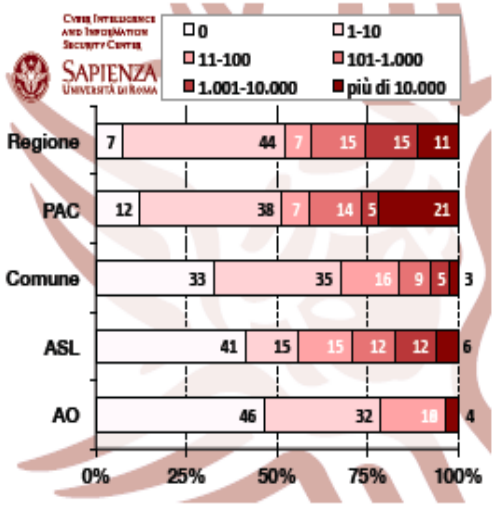
NB: Indice di Gravità Complessiva corrisponde all'indice di Rischio descritto in letteratura come R= Impatto*Probabilità*Vulnerabilità

Un possibile nuovo approccio alla Sicurezza e Privacy: MISURE ORGANIZZATIVE

Quali procedure organizzative porre in essere:

- Definizione Organigramma Privacy
- Definizione Titolarietà/Co-Titolarietà (Pdta)
- Nomina Responsabili dei trattamenti
- Nomina Data Protection Officer
- Gestione documentale degli interventi di Sicurezza e Privacy (documentazione Organizzativa e Tecnica)
- Notifica dei Data Breach

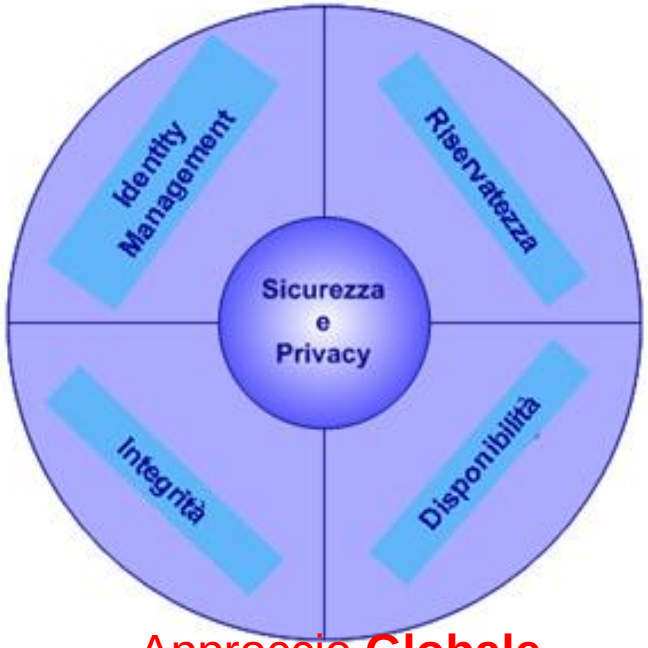




Un possibile nuovo approccio alla Sicurezza e Privacy: MISURE SICUREZZA TECNICHE

Quali misure di sicurezza tecnica adottare (art 32 GDPR):

- la pseudonimizzazione e la **cifratura dei dati** personali;
- la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali ir caso di incidente fisico o tecnico;
- una procedura **per testare, verificare e valutare regolarmente l'efficacia delle misure *tecniche e organizzative*** al fine di garantire la sicurezza del trattamento.



Approccio **Globale** (multidimensionale) e **Sistemico** (diverse variabili impattano sui processi di business e richiedono interventi Culturali, Organizzativi,Tecnologici, Economici)

Un possibile nuovo approccio alla Sicurezza e Privacy: MISURE sugli APPLICATIVI

Quali misure di sicurezza applicativa adottare (art dal 15 al 20 GDPR):

- Identity Management (e Single Sign on)

- Gestione unificata dell'informativa, consensi, rettifica e cancellazione (art da 7 a 10 e da 15 a 19);

- Diritto alla "**portabilità dei dati**" (art 20); "*L'interessato **ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico** i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti "*

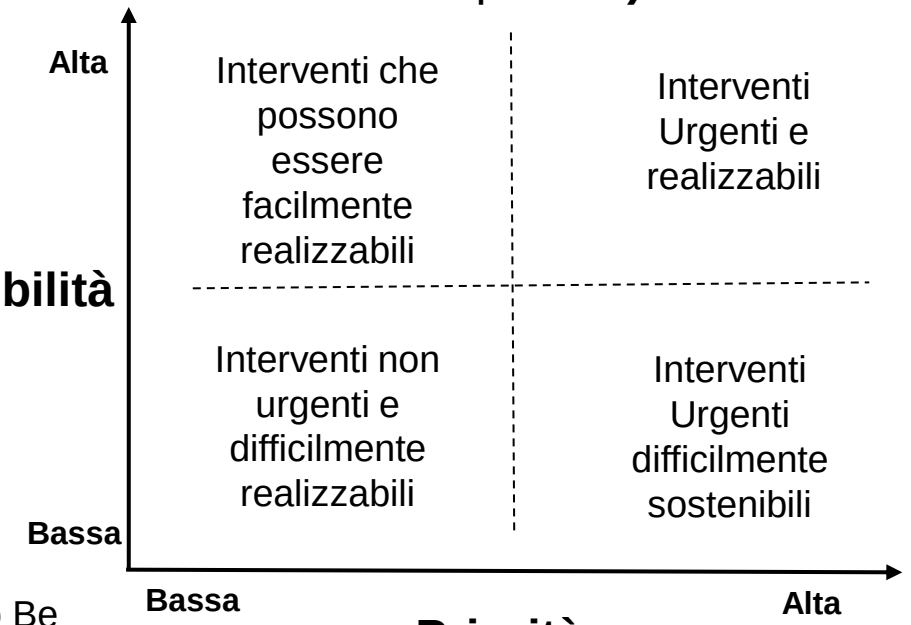
Un possibile nuovo approccio alla Sicurezza e Privacy: PIANO D'AZIONE

COME PROCEDERE ?

1. **Valutazione dell'As Is** (dove siamo, cosa c'è in Azienda, cosa possiamo consolidare e valorizzare, analisi trattamenti e rischi/impatti)
2. **Valutazione del To Be** (dove vogliamo andare, cosa fare in ragione all'analisi rischi/impatti, allo stato dell'arte, ai costi realmente Sostenibili)
3. **Definizione Piano di priorità**

(interventi progressivi, continuativi e documentati di compliance**)**

- Semplicità interventi
- Velocità implementazione
- Potenziali impatti generati
- Costi (Org.vi, Tecnol, Change)



- Gap tra As Is e To Be
- Livello di Risk Mitigation

Grazie dell'attenzione

presidenza@aisis.it
claudio.caccia@gmail.com
claudio.caccia@mail-bip.com